FORTINET

FortiNAC - Administration & Operation Guide

Version 8.5.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

FORTINET®

June 21, 2019
FortiNAC 8.5.0 Administration & Operation Guide
49-805-566662-20190621

TABLE OF CONTENTS

What's new in FortiNAC 8.5

Following are new features for FortiNAC 8.5. For information on features added between your current version and this, refer to prior versions of the Release Notes.

Feature	Description
Reporting: NCM reporting via scheduler Added Topology Container to Adapter	Ability to schedule a text based reports by reusing a Host View shared filter. The report output is a .csv file(s), columns can be configured along with the frequency. The feature can be used on a single FortiNAC system or in an NCM environment. In either case the shared filter on the local FortiNAC and in an NCM environment the filter will be used to read from all pods, the filter does not have to exist remotely. Running on an NCM will produce two .csv files. One file contains the combined results from all pods, allowing you to find every pod the host has connect to. The second file, which has "nodups" in the file name, contains only the last connection for a host.
FSSO - Fortinet Single Sign On	When FSSO is configured, FortiNAC sends a message to the FortiGate firewall each time a host connects to the network or the host IP changes, such as when a host is moved from the Registration VLAN to a Production VLAN. A message is also sent when one user logs off a host and a new user logs on to that same host while the host is still on-line. The message includes User ID, IP address, tags and group membership information which identifies the user to Fortinet and allows it to apply user specific policies.
AWS OVA/ AMI Support	Management for the FortiOS.
Logical Networks	Logical Networks allow you to create fewer Network Access Policies than before. For example, if All Guest users on your network should get to some kind of “Guest” network, you can create a “Guest” Logical Network, and create a policy for all Guest type users to be assigned to it. Then, you can define (or not define) what the “Guest” network means for each device as you add it to FortiNAC without having to create new policies. If the guest network on your new device is “Guest-10-10-2”, you can define Guest → Guest-10-10-2 in the device model configuration.
FortiAP support	Management for the FortiAP.

FortiNAC

FortiNAC integrates with your existing desktop security software, network directories and infrastructure, and security solutions. This gives your organization unlimited visibility to which users are on the network, which endpoint devices are on the network, and where and when users and devices are connecting. Additionally, Network Access Policies ensure that confidential resources are secure by tracking which users are allowed to have access, detailing which users may have already accessed those resources, and ensuring that private information remains private. FortiNAC simplifies IT operations by empowering administrators to create security policies that automate control over network access. Finally, our built-in tools and schema enable administrators to build reports for regulatory compliance.

FortiNAC is a flexible, modular security platform that allows solutions to be customized to fit your organization's needs. FortiNAC uses a unique out-of-band architecture that leverages your existing IT infrastructure to provide unparalleled visibility and to enable security policies to be applied automatically across the entire network.

The FortiNAC package installed on your appliance is referred to as FortiNAC throughout the documentation.

If you do not see a feature described in the documentation, it could be for one of the following reasons:

- You may not have purchased all of the features outlined in this documentation.
- You may not have permission to access the feature.

Introduction

This document provides comprehensive information on all of the features available in FortiNAC that are used to enforce network usage policies, monitor specific events, and automatically take actions. When FortiNAC recognizes an event, it takes the defined action, and logs both for tracking purposes. Configuration of individual FortiNAC components, such as groups and scheduled actions are included. Device integration information is provided through the Customer Portal.

The Requirements on page 1 section defines the host requirements for the FortiNAC Administrator User host. Refer to and Dashboard on page 37 topics to get started.

This documentation applies to the FortiNAC Server, FortiNAC Control Server, and FortiNAC Application Server appliances.

Requirements

The Administrator user interface requires a PC with a Pentium IV processor or above, 2 gigabytes of memory, and a browser.

Supported web browsers

Refer to the Release Notes for the most recent list of supported web browsers.

DNS configuration

The FortiNAC Server and FortiNAC Control Server appliances use CORBA to communicate between the web server and the browser. Within the FortiNAC Server and FortiNAC Control Server appliances, CORBA uses the sub-domain or host names (short names), not IP addresses, to communicate between the browser and server. The administrator's host and the FortiNAC Server and FortiNAC Control Server appliance host name must be in DNS.

If DNS is not available then each administrator's host must have a host entry for the FortiNAC Server and FortiNAC Control Server appliances.

If you are using Agent Version 3.0 or higher with security enabled, you cannot use the Fully Qualified Domain Name of the FortiNAC Server or Application Server. You must use the short name instead. If the FQDN is used and the Administrator's host is using the Persistent Agent, the agent cannot communicate with the FortiNAC appliances. This could prevent the Administrator from registering the host.

The 'nac' alias must not be included in DNS. For example, do not use an alias like "nac.abc.def.com" anywhere in DNS.

Windows

1. Edit the `hosts` file on the system. The hosts file is usually in the following directory: `C:\windows\system32\drivers\etc\hosts`.
2. Add this entry to the Hosts file:

   ```
   XXX.XXX.XXX.XXX Short_Name
   ```

   or

   ```
   XXX.XXX.XXX.XXX host_name
   ```

   Example:

   ```
   192.168.10.1 qa233
   ```
3. Reboot the computer after you change the `hosts` file.

Having multiple interfaces on the Administrator workstation can sometimes cause CORBA DNS problems, depending on the interface configuration settings.

Sample Windows Hosts File

```
# Copyright (c) 1993-1999 Microsoft Corp.

#

# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.

#

# This file contains the mappings of IP addresses to host names. Each entry

# should be kept on an individual line. The IP address should be placed in the first

# column followed by the corresponding host name followed by the short name.

# The IP address, the host name, and the short name should be separated by

# at least one space.
```

```
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the host name denoted by a '#' symbol.
#
# For example:
#
# XXX.XXX.XXX.XXX host.domain.com # source server
# XXX.XXX.XXX.XXX host_name # x client host

127.0.0.1 localhost
```

Linux

1. Edit the `hosts` file on the system. The hosts file is usually in the following directory: `/etc/hosts`
2. Add this entry to the Hosts file:

   `XXX.XXX.XXX.XXX Short_Name`

   Example:

   `192.168.10.10 qa233`

There is no need to reboot the system.

macOS

1. Locate the file named `hosts` in `/etc folder`.

   If the file does not exist, create one with a text editor. The hosts file contains information regarding the known hosts on the network.

   Separate the entries on each line with tabs. Do not use spaces. A # indicates the beginning of a comment; characters up to the end of the line are not interpreted by routines which search the file.

   Use a single line for each host file. Make sure each host line contains the Internet address of the host, the Qualified Host Name, and the Alias.

   Example:

   `xxx.xxx.xxx.xxx Qualified_Host_Name Alias`
2. Reboot the computer after you have edited and saved the hosts file.

IPv6 support

FortiNAC has the ability to support IPv6 addresses by allowing IPv6 endstations (hosts, devices) to communicate with FortiNAC's Portal and Agents.

Network device management and discovery in Topology requires networking equipment to have an IPv4 address.

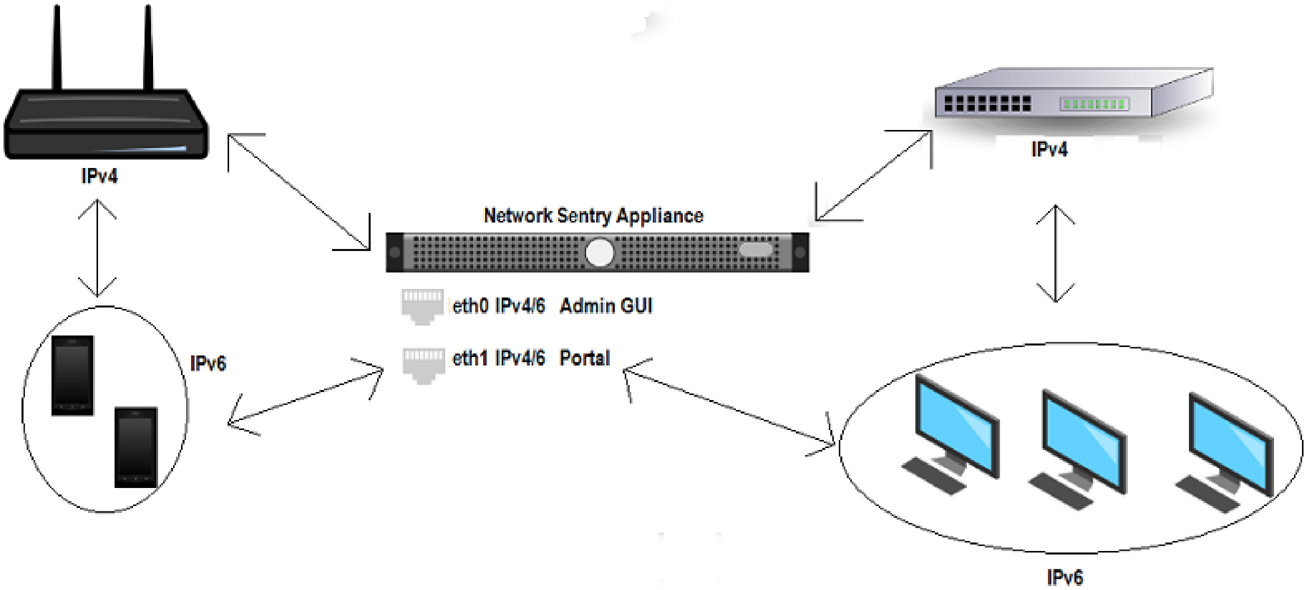
The FortiNAC GUI can support both IPv4 and IPv6.

Polling L3 (IP->MAC) data for devices is supported from the following vendors/switches:

- Cisco
- Juniper EX Switches
- HP ProCurve

Please contact Fortinet Support to request additional device support.

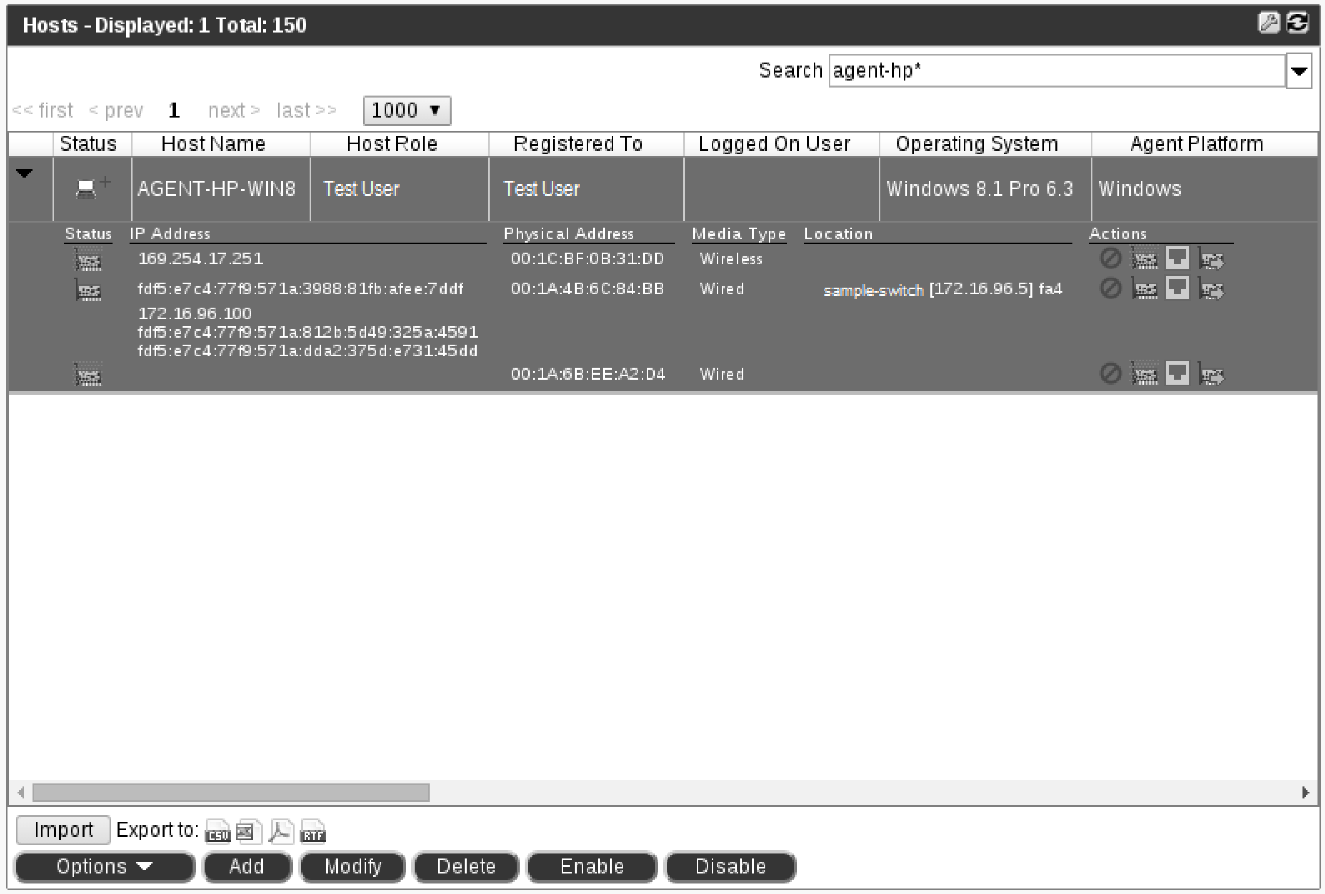
The following diagram illustrates how IPv6 hosts and devices communicate with FortiNAC using IPv4 routers and switches.



IPv6 hosts and devices can communicate with the FortiNAC via Portal and Agents. Both eth1 and eth0 support IPv4 and IPv6, enabling IPv6 hosts and devices to access the Portal. When a host or device uses IPv6, the IPv6 address is displayed in the Host view Figure 1) or Adapter view (Figure 2), in addition to any IPv4 addresses associated with the host or device. The FortiNAC Admin UI can be accessed using the IPv6 address assigned to eth0.

Supported for IPv6	Not Supported for IPv6
Portal Communication (eth1)	Device Management in Topology (Creation/Discovery of Network Devices)
Admin UI Access (eth0)	
Agent Communication	
L3 Polling IPv6 addresses displayed in the Host/Adapter views	

Hosts view displays IPv4 and IPv6 addresses for each adapter



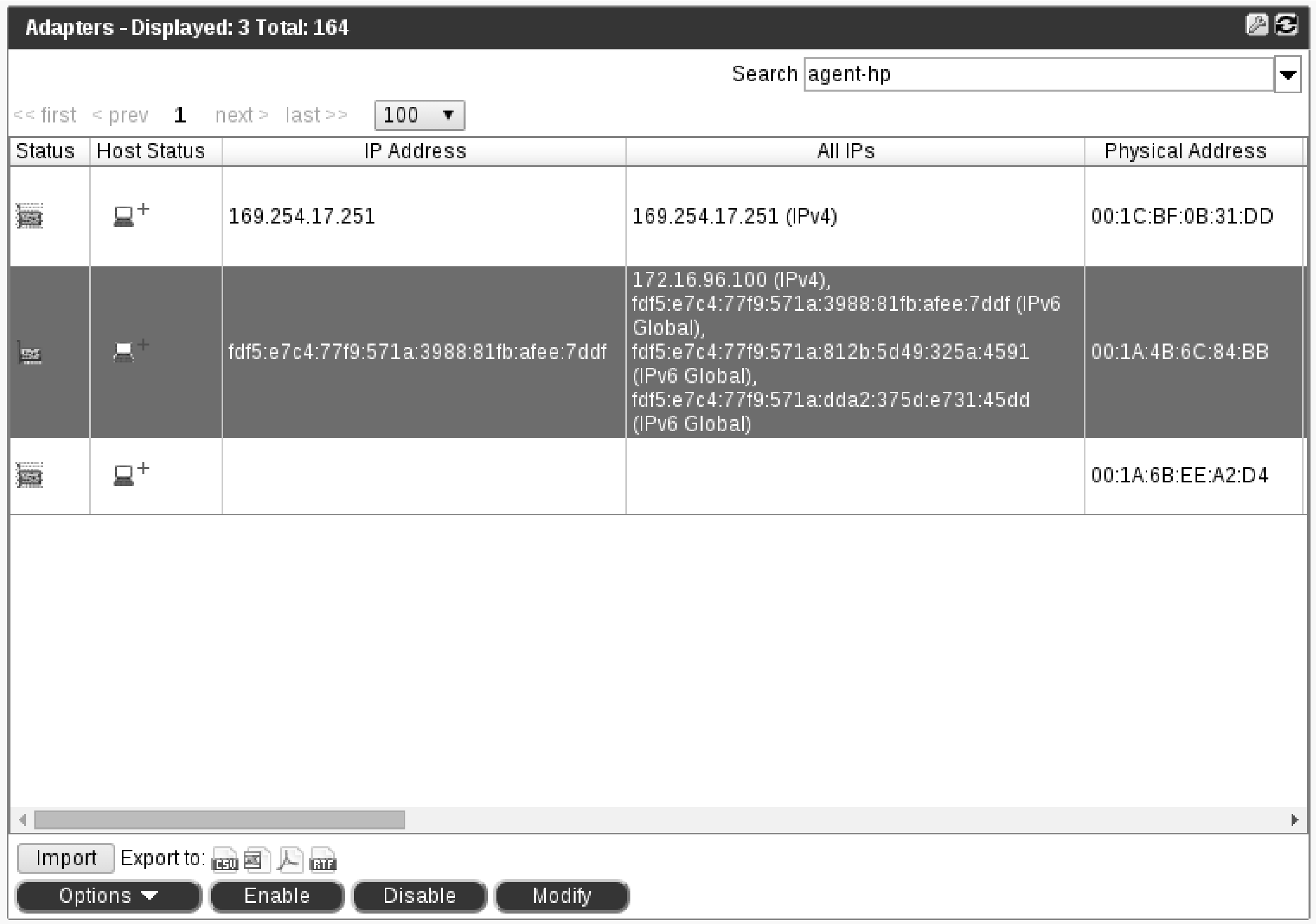
Hosts - Displayed: 1 Total: 150

Search agent-hp*

	Status	Host Name	Host Role	Registered To	Logged On User	Operating System	Agent Platform
▼		AGENT-HP-WIN8	Test User	Test User		Windows 8.1 Pro 6.3	Windows

Status	IP Address	Physical Address	Media Type	Location	Actions
	169.254.17.251	00:1C:BF:0B:31:DD	Wireless		
	fdf5:e7c4:77f9:571a:3988:81fb:afee:7ddf 172.16.96.100 fdf5:e7c4:77f9:571a:812b:5d49:325a:4591 fdf5:e7c4:77f9:571a:dda2:375d:e731:45dd	00:1A:4B:6C:84:BB	Wired	sample-switch [172.16.96.5] fa4	
		00:1A:6B:EE:A2:D4	Wired		

Adapters view displays IPv4 and IPv6 addresses in the IP address and all IPs fields



Adapters - Displayed: 3 Total: 164

Search agent-hp

Status	Host Status	IP Address	All IPs	Physical Address
		169.254.17.251	169.254.17.251 (IPv4)	00:1C:BF:0B:31:DD
		fdf5:e7c4:77f9:571a:3988:81fb:afee:7ddf	172.16.96.100 (IPv4), fdf5:e7c4:77f9:571a:3988:81fb:afee:7ddf (IPv6 Global), fdf5:e7c4:77f9:571a:812b:5d49:325a:4591 (IPv6 Global), fdf5:e7c4:77f9:571a:dda2:375d:e731:45dd (IPv6 Global)	00:1A:4B:6C:84:BB
				00:1A:6B:EE:A2:D4

Login procedure

The FortiNAC user interface is browser based. When you log in as an Administrator, you may create other Administrators and Administrative Users with an Admin Profile.

There are no spaces in the entry. `<Host Name>` is the name of the FortiNACappliance. You may substitute the IP address for the `<Host Name>` if you wish.

1. Enter one of the following URLs in the Address field of the browser window:

   `https://<Host Name>:8443/`

   or

   `http://<Host Name>:8080/`

2. Log in as an Administrator user. Enter the **User Name** and **Password**.

3. The End User License Agreement appears the first time any Administrative or Administrator user logs in. Click to Accept the terms. Clicking Disagree returns you to the Login dialog.
4. Add Administrator and Administrative accounts as needed. See Add an admin user on page 685 for instructions.
5. The FortiNAC user interface displays. The interface provides the appropriate privileges for whoever logs in. See Admin profiles and permissions on page 657 for more information on Admin User permissions.

Admin user interface connection errors

The table below contains a list of errors that could be displayed if you have problems connecting to the Admin User Interface.

Message	Code	Definition
Unable to connect to host <hostname>	1050	Indicates that FortiNAC was unable to open the port and contact the server. Possible reasons include: Access could be blocked by a firewall. Java cache may need to be cleared. Host name may be missing from the hosts file. See DNS configuration on page 2 for the location of the hosts file based on your operating system. Server may be down.

Licenses

The license key installed on your FortiNAC controls both the feature set that is enabled and the number of managed hosts, users and devices.

Types

The following licenses are available:

- **Base**: Network discovery, host profiling, and classification.
- **Plus**: Host registration, scanning, and access control, along with all base features.
- **Pro**: ATR (Automated Threat Response), along with all plus and base features.

All licenses include high availability.

License count

There are two types of license counts on FortiNAC: concurrent licenses and ATR licenses. License usage information is displayed on the Dashboard on page 37 and License management on page 215.

If you exceed your license count, a small time buffer is included to give you to purchase additional licenses. When this buffer is exceeded, FortiNAC does the following:

- No new registrations are allowed.
- Attempts at new registrations are presented with the message **Exceeded concurrent connection license limit**.
- Rogues, at-risk, and disabled hosts continue to be placed in isolation as they normally would be.
- Existing registered hosts and devices continue to have network access.

Concurrent licenses

The count of concurrent licenses is based on the total number of concurrent connections to your network that are managed by FortiNAC.There may be parts of your network that are not managed by FortiNAC.

This count includes hosts, servers or devices that are online on your network at any given time. When a host, server or device disconnects from the network, the license is released and can be used for another connection. For example, you may have 1000 hosts in your database but if only 100 are connected, then only 100 licenses are used.

A registered host will use a license if the host is seen by FortiNAC to be online, even if the host is not on an enforced port. When a registered host shows online, even if no one is logged on, a license is still used. When the licenses run out, no new devices can register and access the network.

The following devices use a concurrent license when connected:

- Online hosts in the host view (including registered hosts and IP phones)
- Online, non-infrastructure devices in topology view (servers, printers, IP phones)

The following devices don't use a concurrent license when connected:

- Rogue devices
- Switches, routers, wireless controllers and wireless access points in topology view

ATR licenses

These licenses are based on the total number of licenses configured for ATR that are currently in use by devices connected to your network.

Events and alarms

When the number of licenses used reaches 75%, 95% and 100% of total licenses an event is generated for each threshold and an alarm is triggered to warn you. These percentages are default values. Modify thresholds for these events under Event Management. See Event thresholds on page 858 for instructions.

Administrators must monitor the Alarm View, the Alarm panel on the dashboard or modify these alarms such that the alarms send a notification to administrators as they occur.

Event	Definition
Maximum Concurrent Connections Warning	Concurrent licenses in use has reached or exceeded 75% of total licenses. Threshold is configurable.

Event	Definition
Maximum Concurrent Connections Critical	Concurrent licenses in use has reached or exceeded 95% of total licenses. Threshold is configurable.
Maximum Concurrent Connections Exceeded	Concurrent licenses in use has reached 100% of total licenses.

Licenses are not released until users, hosts, devices or guests are disconnected from the network.

FortiNAC Control Manager

Licensed features

In a FortiNAC Control Manager environment, each appliance has its own license key that works in combination with the license on the FortiNAC Control Manager. Licensed features, such as Device Profiler, Integration Suite, Guest Manager and Endpoint Compliance, can be enabled for all managed appliances by including the feature in the license key for the FortiNAC Control Manager. To enable a licensed feature on a single appliance, the feature must be included in the license key for that appliance, but must not be included in the FortiNAC Control Manager license key.

License totals

License counts are shared across all managed FortiNAC appliances, but the maximum number of licenses is controlled by the FortiNAC Control Manager. For example, if the total number of Concurrent Connection licenses on the FortiNAC Control Manager is 1000, any of the managed appliances can use licenses from that pool, until all 1000 have been consumed. Appliance A may use 200 and appliance B may use 150, leaving 650 available. Dashboards for all appliances including the FortiNAC Control Manager would display the following: Total Licenses - 1000, Licenses In Use - 350, Licenses Available 650. Total licenses available and total licenses used are counted by the FortiNAC Control Manager and are displayed on the Dashboard of all appliances.

Any number of licenses can be used on any managed appliance as long as total for all combined does not exceed the 1000 licenses configured on the FortiNAC Control Manager. This affects Concurrent Connection licenses.

In a multi-FortiNAC Server environment, a host that is connected to both wired and wireless FortiNAC Servers will use two licenses.

If the NCM goes down, individual FortiNAC Servers will continue to use the NCM license counts.

License accounting for users and hosts

When users and their corresponding hosts move from one part of the network to another the FortiNAC appliance managing their network access may change. For example, if the switches on the first floor are managed by FortiNAC appliance A and the switches on the second floor are managed by FortiNAC appliance B, then network access control changes from Appliance A to Appliance B when a laptop is moved from the first floor to the second floor.

Hosts consume licenses when they are connected to the network. When a host is moved the license is released when the host disconnects. The same host consumes a license the next time it connects to the network regardless of where it connects.

License accounting for devices

When devices are moved from one part of the network to another the FortiNAC appliance managing their network access may change. If moving the device causes it to be managed by a different FortiNAC appliance, one license is released on the original appliance when the device disconnects from the network and then a new license is used when the device reconnects to the network. The device is included in the databases of both appliances but only consumes one license because it only has one connection.

Evaluation license keys

Evaluations license keys provide access to FortiNAC for a limited number of days allowing you to evaluate the system without purchasing a full license. Time is counted based on the amount of time the system has been running. When the system is shut down and restarted the time count continues from where it left off until the time limit is reached.

View time remaining

1. Select **System > Settings**.
2. In the tree and select **System Management**.
3. Select **License Management**.
4. Click **View**.
5. Verify the data in the **Evaluation Time** field. This field displays the number of days configured for the evaluation license. If you are not using an evaluation license, the **Evaluation Time** field does not display.

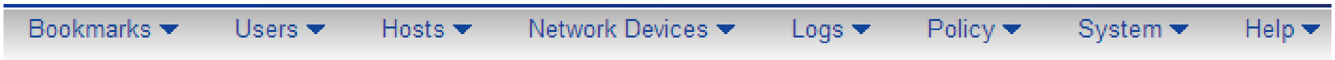
Installing a new key

1. If your Evaluation License Key has expired you are notified when you try to log into FortiNAC. The following message is displayed on the login window: **Your Evaluation License has expired.**
2. Request a new key from your sales representative.
3. Click **Enter New Key** to start the Configuration Wizard and apply the new key.
4. Click the **Enter New Key** link.
5. Enter the Configuration Wizard credentials.
6. The License Key Validation window is displayed.
7. Paste the text of the new License Key into the **License Key** field.
8. Click **OK** at the bottom of the License Key Validation window.
9. Close the Configuration Wizard and log into FortiNAC.

Navigation

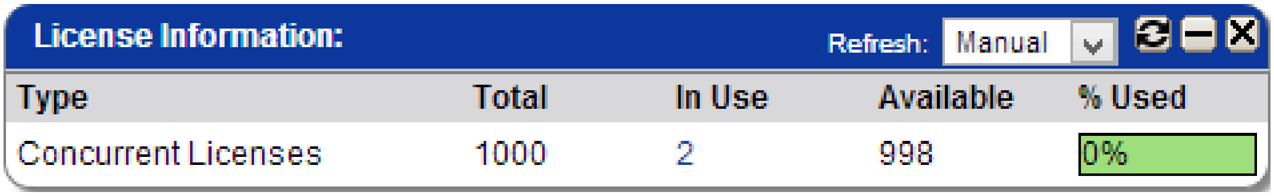
The first page displayed when you log into FortiNAC is the Dashboard. The window is divided into several sections that allow you to navigate the program. Individual windows have similar navigation mechanisms throughout the program.

Menu bar



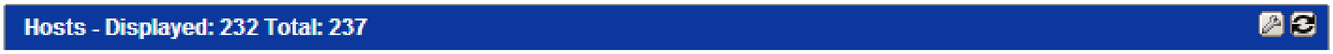
Use the drop-down menus to access program features and functions. The Dashboard can be accessed from the Bookmarks menu. See Menus on page 22 for a list of all menu options.

Title bars


License Information:

Refresh: Manual

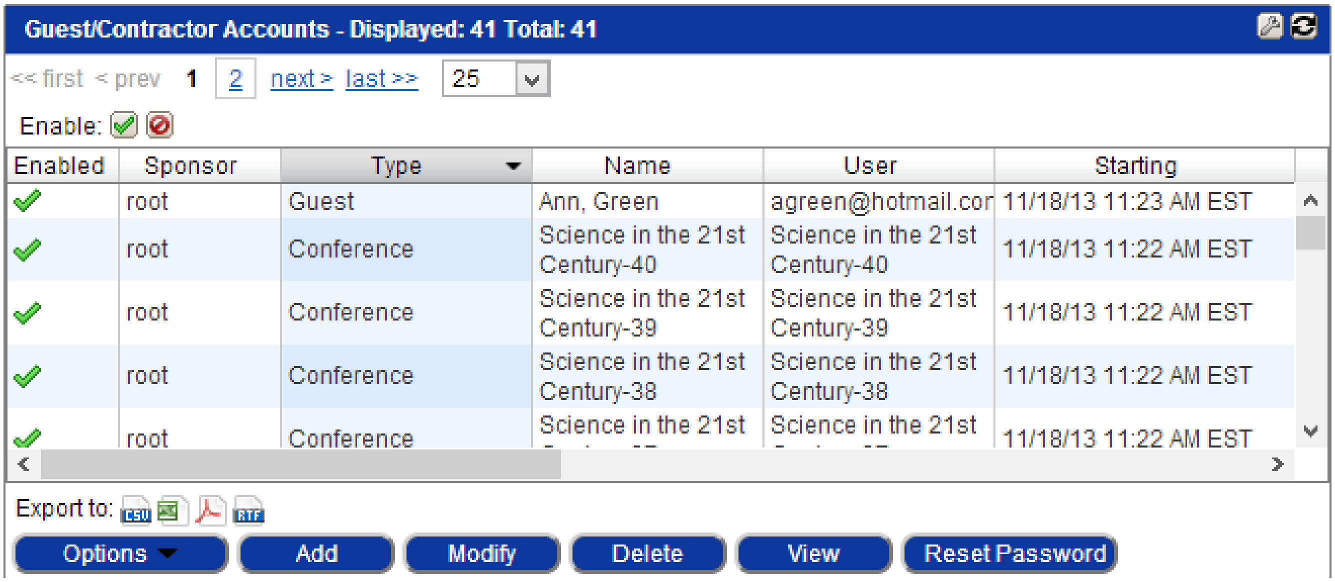
Type	Total	In Use	Available	% Used
Concurrent Licenses	1000	2	998	0%


Hosts - Displayed: 232 Total: 237

Views that contain tables provide record totals, navigation and configuration buttons within the title bar.

Field	Definition
Refresh	Drop-down list of options to set a refresh rate for the selected view.
⟳	Refresh the data in the view.
⊟	Minimize the view or close a section of the view.
☒	Close the view.
🔧	Opens the Settings dialog. Configure which columns display in the table view. In the case of the Host, Adapters or User View, tool tips can also be configured.
Displayed	Total number of records displayed. This number is shown on view that have a search or filter capacity to show the number of records displayed versus the total number of records in the database.
Total	Total number of records contained in the database.

Table views



Guest/Contractor Accounts - Displayed: 41 Total: 41

<< first < prev 1 2 next > last >> 25

Enable: ✓ ⊘

Enabled	Sponsor	Type	Name	User	Starting
✓	root	Guest	Ann, Green	agreen@hotmail.cor	11/18/13 11:23 AM EST
✓	root	Conference	Science in the 21st Century-40	Science in the 21st Century-40	11/18/13 11:22 AM EST
✓	root	Conference	Science in the 21st Century-39	Science in the 21st Century-39	11/18/13 11:22 AM EST
✓	root	Conference	Science in the 21st Century-38	Science in the 21st Century-38	11/18/13 11:22 AM EST
✓	root	Conference	Science in the 21st	Science in the 21st	11/18/13 11:22 AM EST

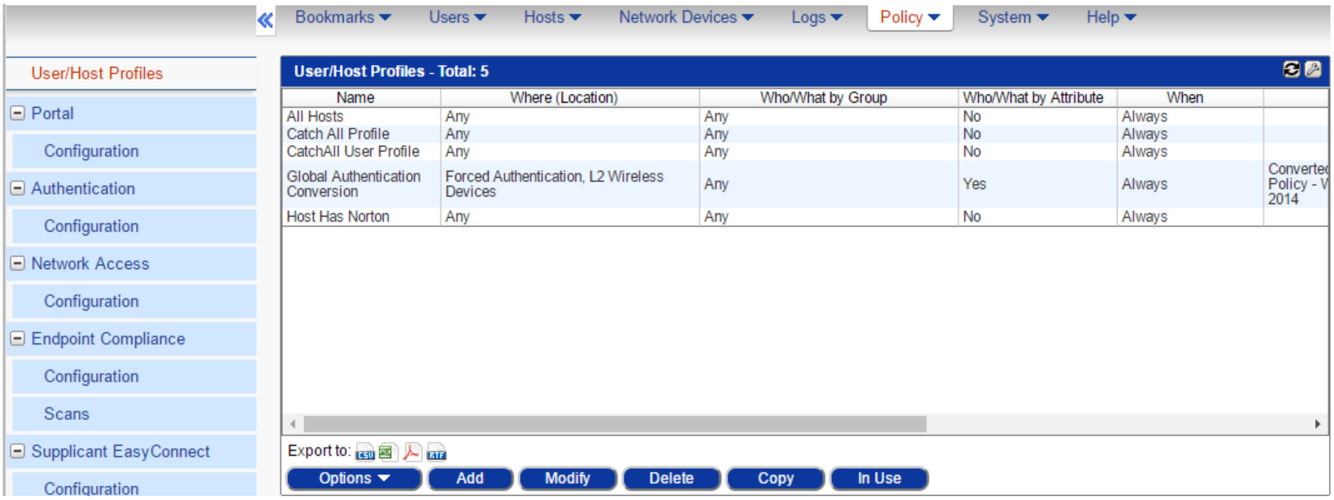
Export to: CSV ▨ ▨ RTF

Data is presented in tables throughout FortiNAC. Table Views have many common navigation options.

Field	Definition
Paging	Below the title bar there are navigation tools that allow you to quickly move through large numbers of records. These tools include the following: **<<first**—Takes you to the first page of records. **<prev**—Takes you back one page. **Page Number**—Current page number is displayed. **next>**—Takes you forward one page. **last>>**—Takes you to the last page. **Drop-down Box**—Allows you to select the number of records to be displayed on each page.
✓	Enables the selected record, such as a Device Profiling Rule.
⊘	Disables the selected record, such as a Device Profiling Rule.
↑ ↓	Moves the selected record up or down in the table, changing the records ranking in ranked tables, such as Device Profiling Rules or User/Host Profiles.
CSV ▨ ▨ RTF	Exports the selected records to CSV, Excel, PDF or RTF formats. See Export data on page 710.
Import	Imports records from a CSV file. See Import and export data on page 695.
Options Button	Displays a list of operations that can be done for the selected records. This button mimics the right-click menu options for operating systems that do not display a right-click menu, such as macOS.

Columns	
Sorting	Click a column head to sort by the data contained in that column. Click once to sort ascending. Click again to sort descending. Sort order is not saved once the view is closed.
Order	Change column order by selecting a column and dragging it to its new location. Column order is not saved once the view is closed.
Hide/Show	Right click on a column heading to display a list of all possible columns. Columns with check marks are shown. Click on a column name in the list to hide or show it in the table. or Click the settings button on the right side of the title bar to display the Settings dialog and select which columns to show in the table.

Tabbed views



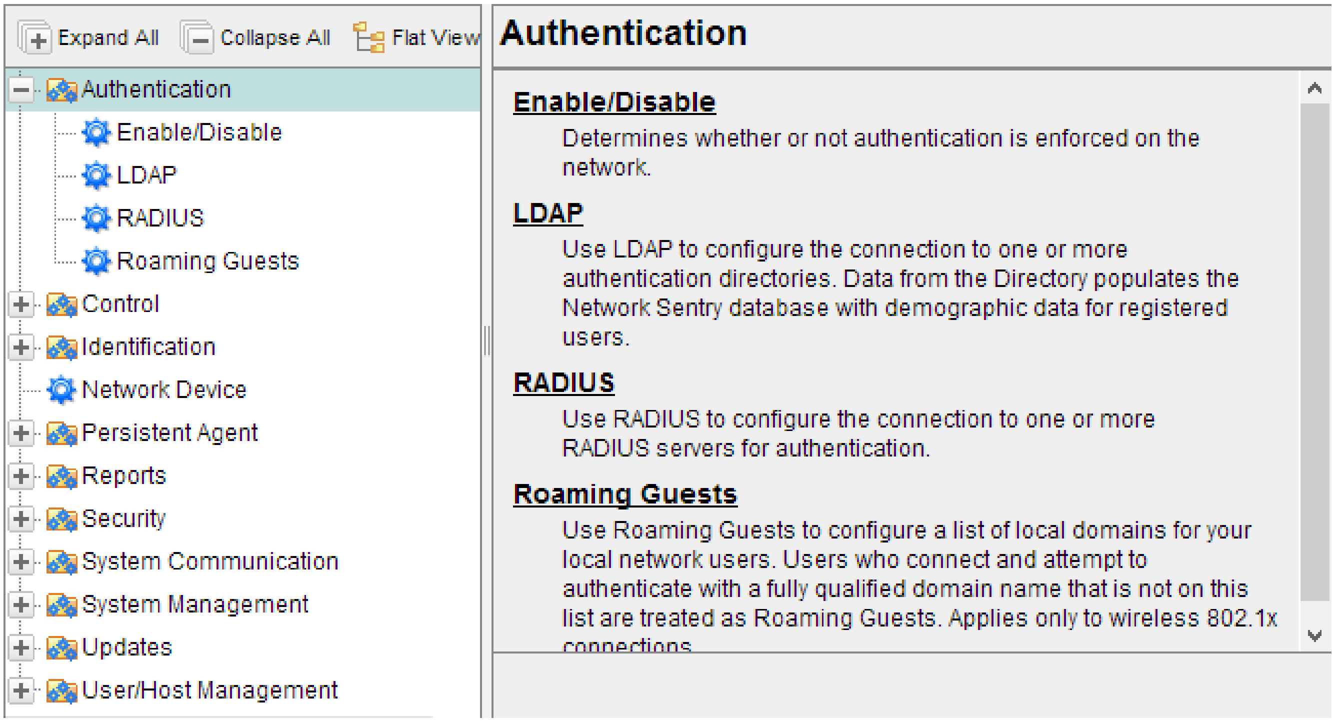
User/Host Profiles - Total: 5

Name	Where (Location)	Who/What by Group	Who/What by Attribute	When	
All Hosts	Any	Any	No	Always	
Catch All Profile	Any	Any	No	Always	
CatchAll User Profile	Any	Any	No	Always	
Global Authentication Conversion	Forced Authentication, L2 Wireless Devices	Any	Yes	Always	Converte Policy - V 2014
Host Has Norton	Any	Any	No	Always	

Some FortiNAC views allow you to perform multiple related functions. These views are presented with tabs along the left side. You are not necessarily required to configure all of the tabs, they are made available for faster navigation:

- Use the Double Arrow button in the menu bar to open or close the column containing the tabs.
- Click the titles in the tabs to move from one view to another.
- In some cases there are sub-tabs, as shown above under **Portal**.

Tree views



Authentication

Enable/Disable

Determines whether or not authentication is enforced on the network.

LDAP

Use LDAP to configure the connection to one or more authentication directories. Data from the Directory populates the Network Sentry database with demographic data for registered users.

RADIUS

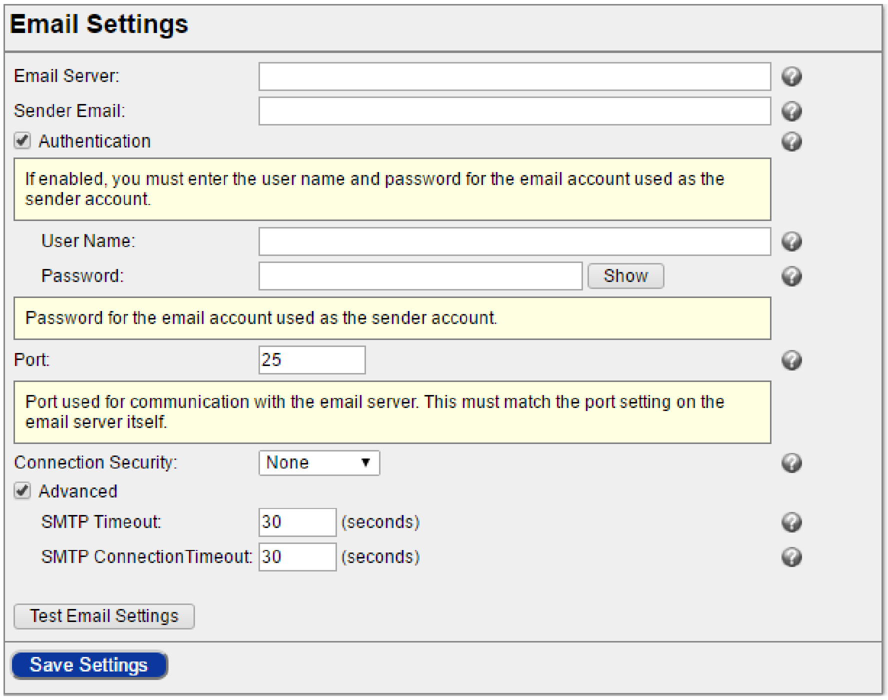
Use RADIUS to configure the connection to one or more RADIUS servers for authentication.

Roaming Guests

Use Roaming Guests to configure a list of local domains for your local network users. Users who connect and attempt to authenticate with a fully qualified domain name that is not on this list are treated as Roaming Guests. Applies only to wireless 802.1x connections.

Some complex FortiNAC views use a tree to display configuration options and related tasks. Click + to expand the branches of the tree or - to collapse them. In some cases, there is a Flat View feature that changes the display to list all options in the tree alphabetically.

Field level help



Email Settings

Email Server:

Sender Email:

☑ Authentication

If enabled, you must enter the user name and password for the email account used as the sender account.

User Name:

Password:

Password for the email account used as the sender account.

Port: 25

Port used for communication with the email server. This must match the port setting on the email server itself.

Connection Security: None

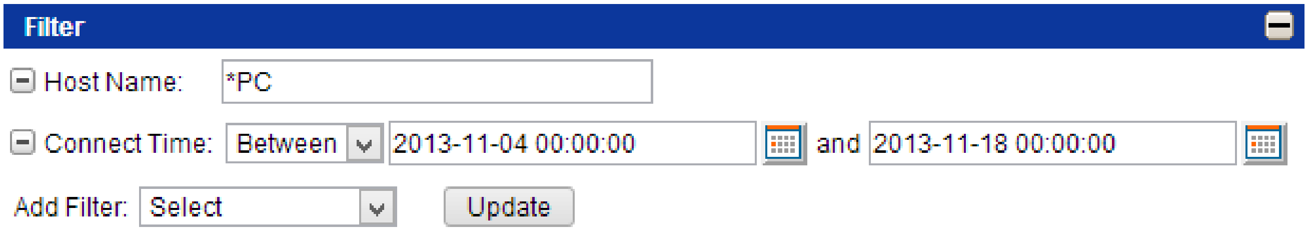
☑ Advanced

SMTP Timeout: 30 (seconds)

SMTP ConnectionTimeout: 30 (seconds)

Help is accessed from the menu bar by selecting **Help > Current View**. In some cases, where a task is complex, field level help has been added. To access help for a field, click the question mark to the right of that field as shown in the next figure.

Filters



Filter

Host Name: *PC

Connect Time: Between 2013-11-04 00:00:00 and 2013-11-18 00:00:00

Add Filter: Select

Views that allow filtering have additional fields displayed in a panel at the top of the screen. Filter fields are added one at a time from a list of possible pieces of data. Typically this is a list of the column titles that are displayed in the View. Possible fields vary depending on the View being accessed.

The Filter section can be opened or closed using the + and — symbols in the title bar. Wild card characters can be used in text based fields.

Using filters

1. Navigate to a view that has a filter panel at the top.
2. Click in the **Add Filter** field and select a data type to use as a filter, such as **Host Name**.

3. A field is displayed for the data to be used as a filter. In the example shown above, **PC* is entered as filter for **Host Name**. Enter the appropriate filter data.
4. Continue adding filter fields and filter data as needed.
5. Click **Update** to display the filtered data in the table.
6. To remove a filter, click the **-** symbol next to the field. Click **Update** to refresh the data in the table.

Filter types

Each view that has filters has options that are specific to that particular view. For example, Guest Contractor Accounts allows you to filter by account type. However, there are some filter options that are common to any views. The table below lists filters that are common across many views. Detailed filter information is available in the Help for each individual view.

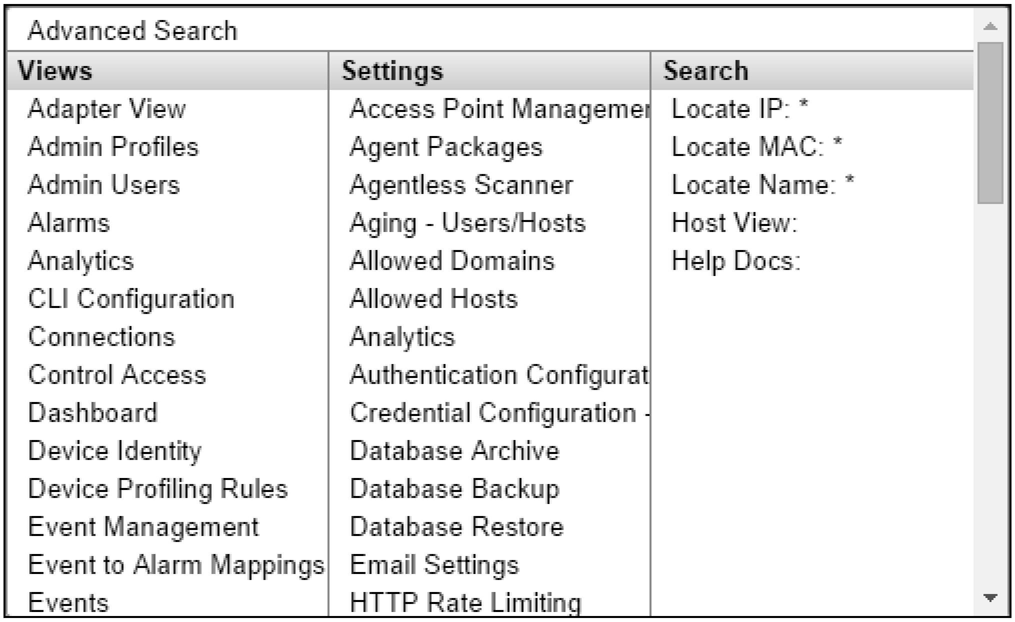
Type	Definition
Time	Filters that involve date and time: • **Last** — Searches for timestamps within the last X number of minutes, hours or days by counting backwards from the current date and time. • **Between** — Searches for timestamps between the Start and End time - entered in YYYY/MM/DD hh:mm AM/PM format. • **Month** — Searches for timestamps between the month's start and end dates. For example, if March is selected, the filter searches for timestamps between 03/01/2015 00:00:00 and 03/31/2015 23:59:59. • **After** — Searches for timestamps after the Start time entered in YYYY/MM/DD hh:mm AM/PM format. • **Before** — Searches for timestamps before the Start time entered in YYYY/MM/DD hh:mm AM/PM format. Use the calendar button at the end of each field to select a date.
Enabled	• **Enabled** — Record is enabled, such as a Guest Account. • **Disabled** — Record is disabled, such as a guest account.
Host Type	• **Registered** — Search includes only registered hosts or devices. • **Rogue** — Search includes only rogue or unregistered hosts or devices.
Authentication Type	• **Local** — Validates the user to a database on the local FortiNAC appliance. • **LDAP** — Validates the user to a directory database. FortiNAC uses the LDAP protocol to communicate to an organization’s directory. • **RADIUS** — Validates the user to a RADIUS server.
IP address	IP address of the connecting host or device.
Physical Address	MAC Address of the connecting host or device.
Location	Name of the device and port where the host or device connected.
Group	Name of the group containing that contains devices, ports, users or hosts.
Container	Name of the Container in which a device is a member.
Registered	Shows Registered and Unregistered Hosts

Wild cards

When searching using a text field you must enter specific search data, such as 192.168.10.5. Wild cards can be used in these fields. Possible wild cards include the following:

Option	Example
*	192.* in the IP address field searches for all IP addresses that begin with 192.
[...]	[192.168.10.10,172.168.5.22,192.168.5.10] Searches for each IP address in the series and returns multiple records. Any search field that starts and ends with square brackets "[]" and has one or more commas "," is treated as a list of values.
!	!192. in the IP address field searches for all IP addresses that do not contain 192.
![...]	![John, Frank, Bob] in the First Name field returns all records that do not contain John, Frank or Bob in the First Name field.
![...]	![Windows] in the Operating System field returns all records that do not contain Windows in the Operating System field.
<esc>!	<esc>!John in the First Name field returns records that match !John. The "<esc>" allows you to search for data that contains an exclamation point (!).
<esc>!	<esc>!Windows in the Operating System field returns records that match !Windows. The "<esc>" allows you to search for data that contains an exclamation point (!).

Search



The Search field displayed in the banner at the top of each page allows you to search both the Host View and the Help documents for any text such as, an IP address, a MAC address or in the case of Help a word. In addition, the title of all available windows in the system are displayed in the System Pages column allowing you to quickly navigate to a particular window without using the menus.

Wild card searches can be used. See Search and filter options on page 18 for details on using wild cards and locating hosts.

When searching for a particular word, such as, Dashboard, the search panel displays system windows that have the same title and simultaneously does a search in the Help. Click Help Docs to display Help with the results of the search in the left panel.

Search and filter options

There are several search and filter mechanisms used to locate Hosts, Adapters, Users or Applications. These four tabs share a single view and search mechanism. Options include: Quick Search and Custom Filters, which can be used once or saved for reuse.

When a search or filter is run, the search data or the name of the filter remains in the search field at the top of the window. If you then click on a different tab, that search is rerun in the context of the new tab.

Wild cards

When searching using a text field in a Custom Filter or the Quick Search field you must enter specific search data, such as 192.168.10.5. Wild cards can be used in these fields. Possible wild cards include the following:

Option	Example
*	192.* in the IP address field searches for all IP addresses that begin with 192.
[...]	[192.168.10.10,172.168.5.22,192.168.5.10] Searches for each IP address in the series and returns multiple records. Any search field that starts and ends with square brackets "[]" and has one or more commas "," is treated as a list of values.
!	!192. in the IP address field searches for all IP addresses that do not contain 192.
![...]	![John, Frank, Bob] in the First Name field returns all records that do not contain John, Frank or Bob in the First Name field.
<esc>!	<esc>!John in the First Name field returns records that match !John. The "<esc>" allows you to search for data that contains an exclamation point (!).

Quick search

The Quick Search field at the top of the window allows you to search based on a single piece of data, such as IP address, and display all matching records. The following fields are included in the Quick Search: IP address, MAC Address, Host Name, User First Name, User Last Name, Registered User, Logged On User, and User ID. To search by MAC Address you must use one of the following formats:

```
xx:xx:xx:xx:xx:xx
xxxxxxxxxxxx
```

```
xx.xx.xx.xx.xx.xx
xx-xx-xx-xx-xx-xx
xxxx.xxxx.xxxx
```

Wild card searches can also be done. If you are doing a wild card search for a MAC address you must include colons as separators, such as, 00:B6:5*. Without the separators the search option cannot distinguish that it is a MAC address.

If you are searching by IP address, you enter 192.168.5.1* and all records for IP addresses beginning with 192.168.5.1 are returned. See Wild cards on page 18.

The information displayed varies depending on the tab that is selected. As you click from tab to tab the search in the Quick Search field is applied automatically.

- Users Tab — Displays all users associated with a device that matches the IP range.
- Hosts Tab — Displays all hosts with an adapter that matches the IP range.
- Adapters Tab — Displays all adapters that match the IP range

To broaden the search, enter less information, such as *11*. This returns any IP, MAC, or Host Name containing 11 depending on the tab you have selected.

To use the Quick Search option:

1. Select **Hosts > Host View**.
2. Select either the Adapters, Hosts or Users Tab.
3. Enter a single piece data in the search field and press **Enter**. Wild card searches can be done.

Custom filter

The Custom Filter is the equivalent to an advanced search feature. It provides many fields that can be used in combination to narrow the list of Users, Adapters or Hosts displayed. A Custom Filter can be created and used just once or can be saved under a filter name. The file can be Private, only the current user can see them or shared with all administrators. The new filter then displays in the drop-down menu and separated into two sections, a Private and Shared. They can be accessed by clicking the arrow on the Quick Search field at the top of the window. Custom Filters can be modified, copied or deleted as needed. You can also export Custom Filters to a .txt file which allows Custom Filters to be imported and used by other Admin users.

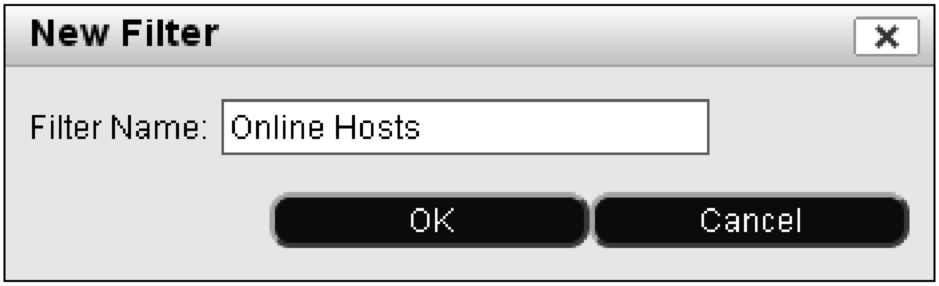
Use your mouse to hover over a saved filter in the drop-down menu and display a tooltip with details about that filter. There is currently only one default Custom Filter, Online Hosts, that displays a list of hosts that are connected to the network.

Create and save a custom filter

1. Select **Hosts > Host View**.
2. Select either the Adapters, Hosts, Users, or Applications Tab.
3. Click the arrow on the right side of the Quick Search field at the top of the window.
4. From the drop-down menu select **New Filter**.
5. Enter the name of the new filter and click **OK**.

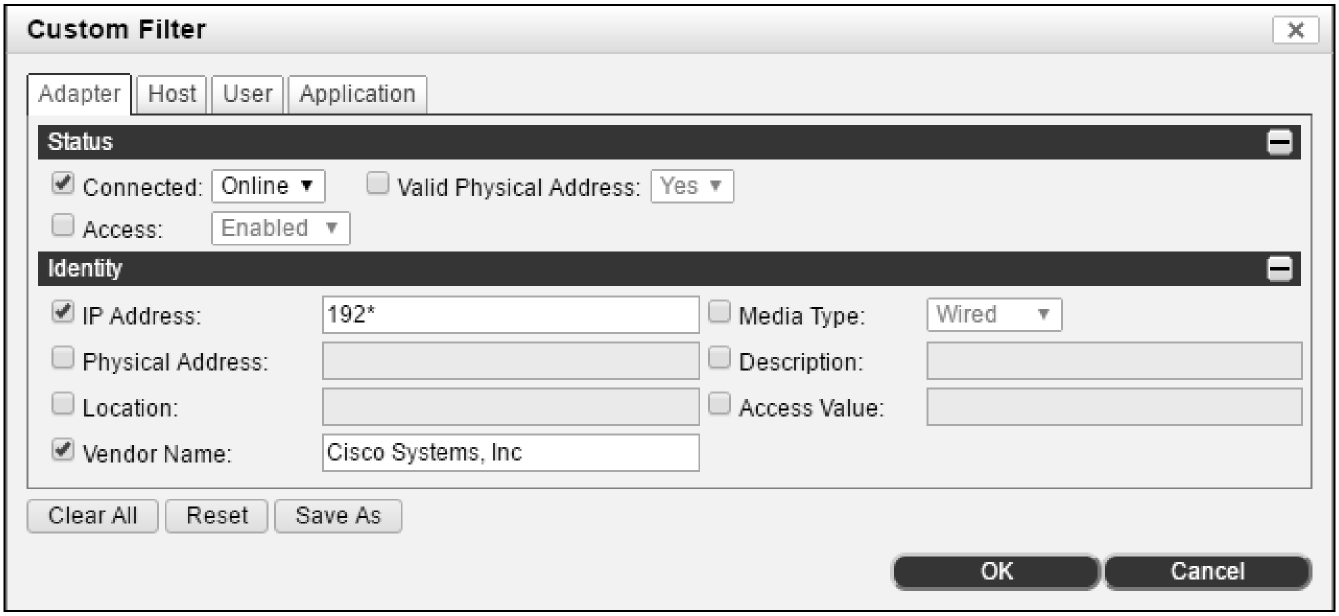
Filter names do not support more than 20 characters.

Continue with the topic below to configure the filter.


New Filter

Filter Name: Online Hosts

Configure a custom filter


Custom Filter

Status

☑ Connected: Online ▾ ☐ Valid Physical Address: Yes ▾

☐ Access: Enabled ▾

Identity

☑ IP Address: 192* ☐ Media Type: Wired ▾

☐ Physical Address: ☐ Description:

☐ Location: ☐ Access Value:

☑ Vendor Name: Cisco Systems, Inc

This window is used in two ways. First if you have selected New Filter from the menu off of the Quick Search drop-down, you can configure the filter and FortiNAC saves it for future use. Second, if you have selected Custom Filter from the menu off of the Quick Search, you can configure this filter and use it just one time.

This dialog box is common to the Adapter, Host and User Views. Custom filter entries on any of these tabs will persist if you navigate between these views.

1. Once you have the Filter window displayed, enable the fields to be included in the filter by marking them with a check mark.
2. For each enabled field you must provide additional information. For example, if you select the Connected field, you must choose either On Line or Off Line.
3. For text fields, such as the IP address field, you must enter the search data, such as 192.168.10.5. Wild cards can be used in these fields. See Wild cards on page 18.
4. To erase all selections, click the **Clear All** button.

5. If you have opened a saved filter and started to modify it, use the **Reset** button to return the filter to its original settings.
6. Click **OK** to run the configured filter. If this filter was assigned a name, the settings will be saved.
7. Immediately after the filter is run, the filter name displays at the top of the view in the Quick Search field. To modify the filter, click the Edit link to the left of the Quick Search field. This modifies the filter whether it was saved or just configured and run one time.

Edit a custom filter

1. Select **Hosts > Host View**.
2. Select either the Adapters, Hosts, Users, or Applications Tab.
3. Click the arrow on the right side of the Quick Search field at the top of the window.
4. On the drop-down menu locate the custom filter to be edited and click the pencil or edit icon to the right of the filter name.
5. When the Filter window displays, modify the filter as needed.
6. Click **OK** to save your changes.

Delete a custom filter

1. Select **Hosts > Host View**.
2. Select either the Adapters, Hosts, Users or Applications Tab.
3. Click the arrow on the right side of the Quick Search field at the top of the window.
4. On the drop-down menu locate the custom filter to be deleted and click the red X to the right of the filter name.
5. When the confirmation message displays, click **Yes**.

Export a custom filter

1. Select **Hosts > Host View**.
2. Select either the Adapters, Hosts, Users, or Applications Tab.
3. Click the arrow on the right side of the Quick Search field at the top of the window.
4. On the drop-down menu select **Import/Export**, and then click **Export**.
5. In the Export Filters dialog, select the filters you want to export. Use Ctrl or Shift to select multiple filters.
6. Click **OK**. The filters are downloaded to a .txt file to your default download directory.

Import a custom filter

1. Select **Hosts > Host View**.
2. Select either the Adapters, Hosts, Users, or Applications Tab.
3. Click the arrow on the right side of the Quick Search field at the top of the window.
4. On the drop-down menu select **Import/Export**, and then click **Import**.
5. Click Choose File to find and select the .txt file containing the filters.
6. Click **OK** to import the filters. The filters appears in the list.

Find containers or devices

The Find button at the top of the tree in the Topology View opens a search field allowing you to search for Containers or Devices. Search options include the following:

- Container Name
- Device Name
- Device IP address
- Device MAC Address

When text or numbers are entered in the search field, FortiNAC searches for anything in the Topology View containing that text. For example, if you entered Com in the search field, FortiNAC would find the device named 3Com4330. Find is case sensitive and wild cards cannot be used.

Menus

The main Menu bar is located across the top of the window at all times. If you access a view that has a series of options, such as the Host View, you will see a menu column down the left side of the window. For example, when you access the Host View, the menu bar on the left contains links for Adapters, Hosts and Users. Click a menu option to navigate to a view. Click Help > Current View to access the online help or to access the About box. Click Logout in the top right corner to logout of the Administrative interface.

Bookmarks

Use Bookmarks to create a personalized list of frequently visited views. In addition the Bookmarks menu contains default links, such as Locate, that are used by Administrative Users who have limited access to FortiNAC.

Bookmarks menu	Topic
Manage Bookmarks	Manage bookmarks on page 25
Dashboard	Dashboard on page 37
Locate	Locate on page 58
Manage Hosts & Ports	Manage hosts and ports on page 54
Send Message	Send a message to group/all hosts on page 551
Custom	Bookmarks created by the logged in Admin UI user.

Users

Users menu	Topic
Admin Users	Admin users on page 683
Guest/Contractor Accounts	Guest or contractor accounts on page 592
Self Registration Requests	Guest self-registration on page 609

Users menu	Topic
User View	User view on page 637
Admin Profiles	Admin profiles on page 578
Guest/Contractor Templates	Guest/contractor templates on page 566

Hosts

Hosts menu	Topic
Adapter View	Adapter view on page 817
Device Identity	Device identity on page 828
Host View	Host view on page 793
Profiled Devices	Profiled devices on page 367
Scan Results	Scan results view on page 925
Device Profiling Rules	Rules on page 350

Network devices

Network devices menu	Topic
Topology	Topology view on page 712
CLI Configuration	CLI configuration on page 928
L2 Polling (Resync Hosts)	L2 polling (resync hosts) on page 748
L3 Polling (IP --> MAC)	L3 polling (IP address to MAC address) on page 750
Network Devices	Network devices on page 833
Patch Servers	Patch management on page 178

Logs

Logs menu	Topic
Admin Auditing	Admin auditing on page 847
Alarms	Alarms view on page 887
Connections	Connections view on page 927
Port Changes	Port changes view on page 942
Events	Events view on page 867
Security Alarms	Security alarms on page 631

Logs menu	Topic
	Available when Automated Threat Response (ATR) is enabled within your current license package.
Security Events	Security events on page 634 Available when ATR is enabled within your current license package.
Analytics	Launches the FortiNAC/Analytics reporting package in a separate browser. Refer to the help for that product for additional information.
Reports	Reports view on page 897
Event to Alarm Mappings	Map events to alarms on page 888
Event Management	Event management on page 856

Policy

Policy menu	Topic
Control Access	Control access on page 715
Network Device Roles	Role management on page 553
Policy Configuration	Policies on page 377
Roles	Role management on page 553
Passive Agent Configuration	Passive Agent on page 495
Persistent Agent Properties	Persistent Agent settings on page 133
Remediation Configuration	Remediation configurations on page 481

System

System menu	Topic
Quick Start	
Groups	Groups view on page 838
Portal Configuration	Portal configuration on page 248
Scheduler	Scheduler view on page 849
Settings	Settings on page 71

Help

Help menu	Topic
Current View	Displays the context sensitive help topic for the view that is currently displayed.
Customer Portal	Launches the Fortinet Customer Portal login.
Feedback	Launches your default email client and populates the email address with the address of the Fortinet documentation department.
Preferences	Admin user preferences on page 26
Legal	Software properties on page 27
About	The About box provides you with information about the specific version of the software that is installed on your FortiNAC system. Information includes the Version number for each component and the build date.

Manage bookmarks

Use the Bookmarks menu to create links to views you access frequently. Changes to Bookmarks are stored for each user individually based on user name. Bookmarks can be placed within user specified groups and sub-groups. Create Groups first and then add bookmarks.

In some cases, existing bookmarks will not work. This can be caused by the following:

- A software upgrade where names or locations of some views have been modified.
- A change in the user's permissions.
- The user has bookmarked a view that is normally launched by selecting an object, such as right clicking on a device to launch the Device Properties view. The Device Properties view requires information about the device in order to open, if this information is not available to the server the bookmark fails.

Add a bookmark group

1. Select **Bookmarks > Manage Bookmarks** and click **Add Group**.
2. The New Group dialog is displayed.
3. In the **Name** field enter a name for this group.
4. If this group will be a sub-group, click in the **Add to group** drop-down and select the group where this new group should be placed.
5. Click **OK** to save.

Add a bookmark

1. Use the menu bar at the top of the window to navigate to the screen you wish to bookmark.
2. Click the star in the banner next to the name of the view or select **Bookmarks > Manage Bookmarks** and click **Add Bookmark**.
3. The New Bookmark dialog is displayed.

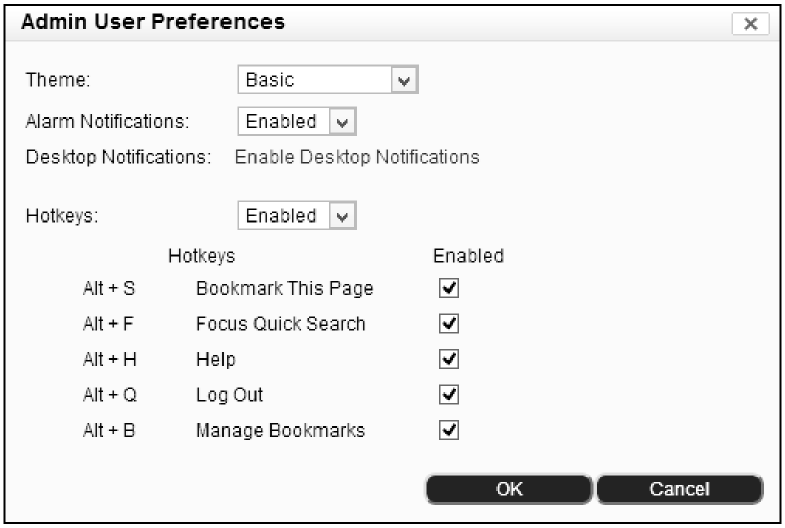
4. On the Bookmark dialog, the **Name** field is filled in with the name of the view displayed. This is the name that will be displayed on the Bookmarks menu. Edit the name if necessary.
5. The **URL** field is filled in with the name and location of the panel that is currently displayed. If you know the URL of another view you can edit this field, however, it is recommended that you navigate to the view itself to ensure accuracy.
6. In the **Open bookmark** in field select either Same Window or New Window. Same Window will change the current window to the new View. New Window will open another instance of the browser with the new view displayed.
7. If you would like to place this bookmark in a previously created group, click in the **Add to group** drop-down and select the group where this new bookmark should be placed.
8. Click **OK** to save.

Delete or edit a bookmark

1. Select **Bookmarks > Manage Bookmarks**.
2. The list of bookmarks is displayed.
3. To delete a bookmark, click the red **X** to the left of the bookmark name. The bookmark is deleted immediately.
4. To edit a bookmark, click the **Edit** icon to the left of the bookmark name.

Admin user preferences

Allows you to enable or disable Alarm and Desktop Notifications, and to enable or disable Alt key combinations for accessing menus. Allows you to modify the look and feel of the user interface for an Admin User. Settings are stored for the logged in user.



Admin User Preferences

Theme: Basic

Alarm Notifications: Enabled

Desktop Notifications: Enable Desktop Notifications

Hotkeys: Enabled

	Hotkeys	Enabled
Alt + S	Bookmark This Page	☑
Alt + F	Focus Quick Search	☑
Alt + H	Help	☑
Alt + Q	Log Out	☑
Alt + B	Manage Bookmarks	☑

1. Select **Help > Preferences**.
2. Use the **Theme** field to change the look and feel of the user interface.

If you have updated the User Theme for an Admin user, the Theme field in Admin User Preferences must be set to Custom to enable the new User Theme. This enables the theme for the logged in user, therefore, each user must log in individually and enable their theme. See User theme on page 689.

3. Use the **Alarm Notifications** to enable or disable the red number display in the menu bar that indicates when there are alarms. This also enables or disables the Alarm notifications that display on the login page.

If **Alarm Notifications** are disabled, **Desktop Notifications** are disabled by default.

4. To enable Desktop Notifications, click the blue link to the right that reads **Enable Desktop Notifications**. Settings in the browser are modified and you are asked to confirm that you want to allow notifications. If you enable Desktop Notifications but Cancel out of the Preferences window, Notifications remain enabled in the browser.

   To disable Desktop Notifications,view the **Help** for your particular browser or disable **Alarm Notifications**.

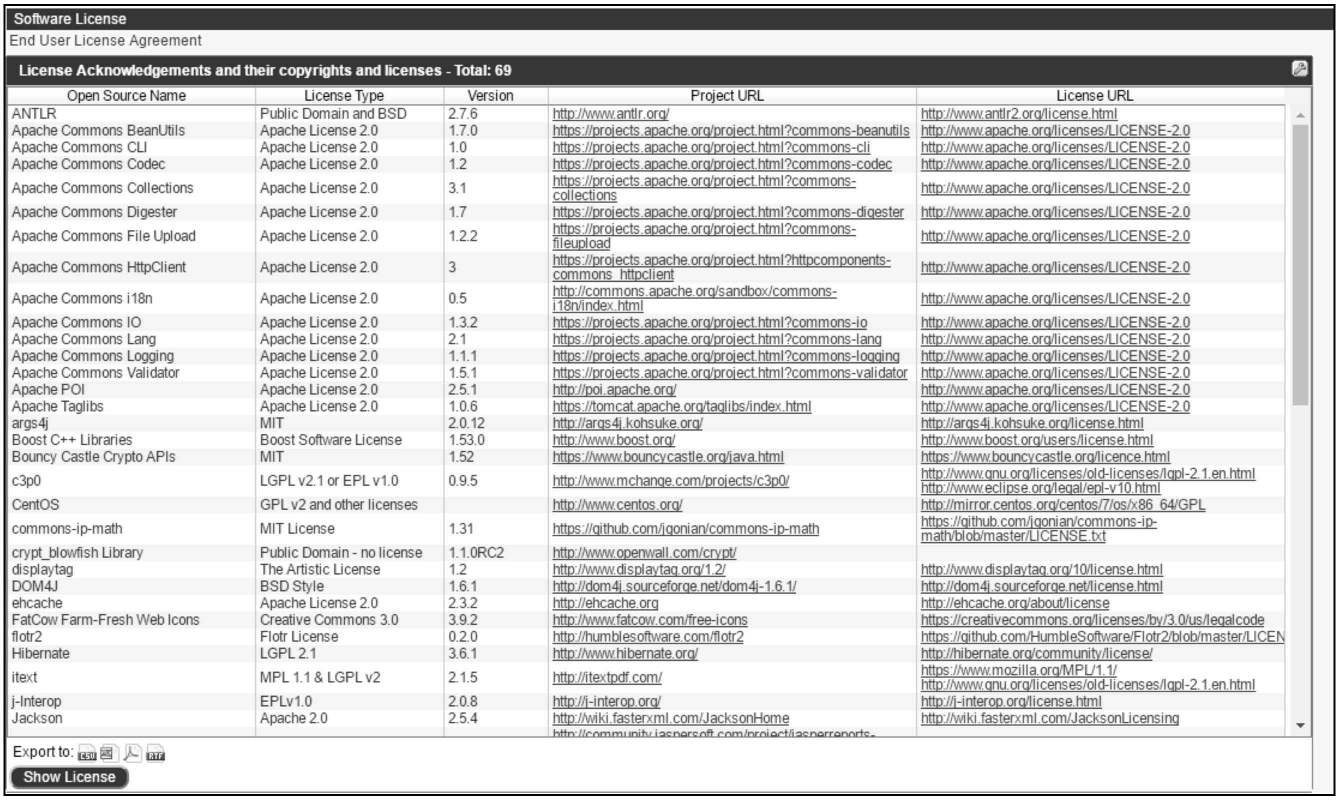
   If your browser does not support this option, the text Desktop Notifications are not supported by this browser. is displayed.

   Desktop Notifications are set on a per browser basis. They must be set again for each of these scenarios:

   - If you use http://8080 and then use https://8443
   - If you are in a High Availability environment and switch between the Shared IP address and the actual IP, address of the primary server.
   - If you have more than one FortiNAC appliance and you switch from one to another.
5. Use the **Hotkeys** options to enable or disable use of Alt key combinations to access menus or perform specific actions, such as logging out.
6. Click **OK** to save your settings.

Software properties

This option displays links to the FortiNAC End User License Agreement and associated copyright and license information.



End User License Agreement

License Acknowledgements and their copyrights and licenses - Total: 69

Open Source Name	License Type	Version	Project URL	License URL
ANTLR	Public Domain and BSD	2.7.6	http://www.antlr.org/	http://www.antlr2.org/license.html
Apache Commons BeanUtils	Apache License 2.0	1.7.0	https://projects.apache.org/project.html?commons-beanutils	http://www.apache.org/licenses/LICENSE-2.0
Apache Commons CLI	Apache License 2.0	1.0	https://projects.apache.org/project.html?commons-cli	http://www.apache.org/licenses/LICENSE-2.0
Apache Commons Codec	Apache License 2.0	1.2	https://projects.apache.org/project.html?commons-codec	http://www.apache.org/licenses/LICENSE-2.0
Apache Commons Collections	Apache License 2.0	3.1	https://projects.apache.org/project.html?commons-collections	http://www.apache.org/licenses/LICENSE-2.0
Apache Commons Digester	Apache License 2.0	1.7	https://projects.apache.org/project.html?commons-digester	http://www.apache.org/licenses/LICENSE-2.0
Apache Commons File Upload	Apache License 2.0	1.2.2	https://projects.apache.org/project.html?commons-fileupload	http://www.apache.org/licenses/LICENSE-2.0
Apache Commons HttpClient	Apache License 2.0	3	https://projects.apache.org/project.html?httpcomponents-commons_httpclient	http://www.apache.org/licenses/LICENSE-2.0
Apache Commons i18n	Apache License 2.0	0.5	http://commons.apache.org/sandbox/commons-i18n/index.html	http://www.apache.org/licenses/LICENSE-2.0
Apache Commons IO	Apache License 2.0	1.3.2	https://projects.apache.org/project.html?commons-io	http://www.apache.org/licenses/LICENSE-2.0
Apache Commons Lang	Apache License 2.0	2.1	https://projects.apache.org/project.html?commons-lang	http://www.apache.org/licenses/LICENSE-2.0
Apache Commons Logging	Apache License 2.0	1.1.1	https://projects.apache.org/project.html?commons-logging	http://www.apache.org/licenses/LICENSE-2.0
Apache Commons Validator	Apache License 2.0	1.5.1	https://projects.apache.org/project.html?commons-validator	http://www.apache.org/licenses/LICENSE-2.0
Apache POI	Apache License 2.0	2.5.1	http://poi.apache.org/	http://www.apache.org/licenses/LICENSE-2.0
Apache Taglibs	Apache License 2.0	1.0.6	https://tomcat.apache.org/taglibs/index.html	http://www.apache.org/licenses/LICENSE-2.0
args4j	MIT	2.0.12	http://args4j.kohsuke.org/	http://args4j.kohsuke.org/license.html
Boost C++ Libraries	Boost Software License	1.53.0	http://www.boost.org/	http://www.boost.org/users/license.html
Bouncy Castle Crypto APIs	MIT	1.52	https://www.bouncycastle.org/java.html	https://www.bouncycastle.org/licence.html
c3p0	LGPL v2.1 or EPL v1.0	0.9.5	http://www.mchange.com/projects/c3p0/	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.en.html http://www.eclipse.org/legal/epl-v10.html
CentOS	GPL v2 and other licenses		http://www.centos.org/	http://mirror.centos.org/centos/7/os/x86_64/GPL
commons-ip-math	MIT License	1.31	https://github.com/jgonian/commons-ip-math	https://github.com/jgonian/commons-ip-math/blob/master/LICENSE.txt
crypt_blowfish Library	Public Domain - no license	1.1.0RC2	http://www.openwall.com/crypt/	
displaytag	The Artistic License	1.2	http://www.displaytag.org/1.2/	http://www.displaytag.org/10/license.html
DOM4J	BSD Style	1.6.1	http://dom4j.sourceforge.net/dom4j-1.6.1/	http://dom4j.sourceforge.net/license.html
ehcache	Apache License 2.0	2.3.2	http://ehcache.org	http://ehcache.org/about/license
FatCow Farm-Fresh Web Icons	Creative Commons 3.0	3.9.2	http://www.fatcow.com/free-icons	https://creativecommons.org/licenses/by/3.0/us/legalcode
flotr2	Flotr License	0.2.0	http://humblesoftware.com/flotr2	https://github.com/HumbleSoftware/Flotr2/blob/master/LICEN
Hibernate	LGPL 2.1	3.6.1	http://www.hibernate.org/	http://hibernate.org/community/license/
itext	MPL 1.1 & LGPL v2	2.1.5	http://itextpdf.com/	https://www.mozilla.org/MPL/1.1/ http://www.gnu.org/licenses/old-licenses/lgpl-2.1.en.html
j-Interop	EPLv1.0	2.0.8	http://j-interop.org/	http://j-interop.org/license.html
Jackson	Apache 2.0	2.5.4	http://wiki.fasterxml.com/JacksonHome	http://wiki.fasterxml.com/JacksonLicensing
			http://community.jaspersoft.com/project/jasperreports-	

Passwords

There are several types of passwords that are used in conjunction with FortiNAC, such as passwords for CLI, SSH, Configuration Wizard, or Admin UI access. Each type of password has its own set of rules or conventions.

CLI/SSH and configuration wizard passwords

CLI/SSH and Configuration Wizard passwords must be eight characters or longer and contain a lowercase letter, an uppercase letter, a number, and one of the following symbols:

Required Symbols		
! exclamation point	@ at	_ underscore
# pound	$ dollar	~ tilde
^ caret	- hyphen	* asterisk
% percent	? question mark	

The symbols listed below are not permitted in CLI/SSH and Configuration Wizard passwords.

Prohibited Symbols		
(open parenthesis	; semicolon	{ open curly bracket
) close parenthesis	: colon	} close curly bracket
‘ back quote	“ double quote	[open square bracket
& ampersand	’ single quote	] close square bracket
+ plus	< less than	, comma
= equal	> greater than	. period
| pipe	\ back slash	/ forward slash

Admin CLI and root CLI passwords are limited to 64 characters.

Administrator passwords

Spaces are permitted in passwords with local authentication. Any other authentication will depend on the vendor.

Administrator passwords for FortiNAC stored in the FortiNAC database must conform to the following:

Permitted Characters	
Letters (upper and lower case)	A, B, C... (and a, b, c...)
Numbers	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Symbols	All characters not defined as letters or numbers. Including: ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : < > ? , . /

Prohibited Symbols	
’ single quote	“ double quote

Time stamps and time zones

Time for both the display and the database is stored in Coordinated Universal Time (UTC) and is adjusted based on the time zone setting in your browser. UTC corresponds roughly to Greenwich Mean time. Therefore, if the time zone for your browser is set to Eastern Standard Time, the program subtracts five hours from UTC time as it prints and displays the date and time for you.

Database

In the database, time is stored in UTC time, but the raw data is stored using a Unix convention. Date and time are represented as a Unix timestamp: the number of seconds elapsed since 1 January 1970 00:00:00 Greenwich Mean Time.

Display and export

Date and time are shown and exported as mm/dd/yy hh:mm AM or PM and time zone. For example the time stamp for a record could be 08/27/10 04:15 PM EDT.

Analytics

To open the Analytics reporting software, click the Analytics icon in the upper-right corner of FortiNAC:

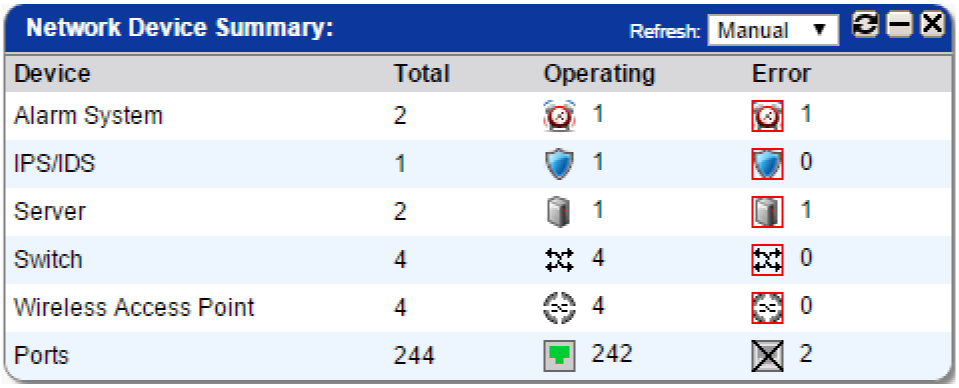
If Analytics is configured, the Analytics login window will appear.

If Analytics is not configured, a dialog will appear that allows you to enter the Analytics Activation Key and the fully Qualified Domain Name of the server where your FortiNAC/Analytics database resides.

Icons

Icons in FortiNAC represent different devices and users as they connect to and access the network. Host Icons are displayed in the Hosts View and the Topology View on the Ports tab. System Icons are displayed in the Topology View. Device Icons are displayed either in Hosts View, Profiled Devices, Dashboard or Topology View depending on where they are being managed. Host Icons in particular have many states.

The screen shot below from the Dashboard's Network Device Summary Panel illustrates the possible device icons shown in that view.



Network Device Summary:

Refresh: Manual

Device	Total	Operating	Error
Alarm System	2	1	1
IPS/IDS	1	1	0
Server	2	1	1
Switch	4	4	0
Wireless Access Point	4	4	0
Ports	244	🟩 242	☒ 2

Icons in FortiNAC represent different devices and users as they connect to and access the network. Host Icons are displayed in the Hosts View. Device Icons are displayed either in Hosts View or the Device Summary Panel on the Dashboard. Host Icons in particular have many states.

To indicate the state of a device or a host, the icons are modified slightly by superimposing an image on top, such as a red box to indicate that the item has been disabled. States can be cumulative. For example, you could see an "X" over a host icon. This indicates that the host has been disabled but is still online. The table below provides a legend for those states.

Icon state

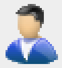
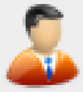
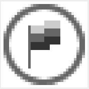
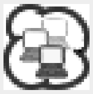
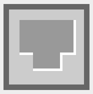
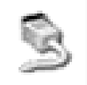
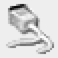
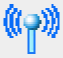
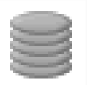
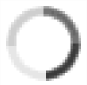
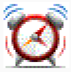
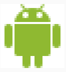
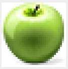
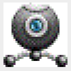
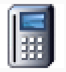
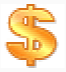
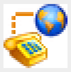
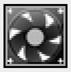
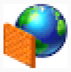
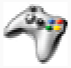
State	Definition	State	Definition
Hosts, adapters or users view			
💻	**Online / Enabled**—No image over icon indicates that the item, such as a Host or Adapter is online.	💻	**Offline / Enabled**—Icon pixelated indicates that the item, such as a Host or Adapter is offline.
☒	**Online / Disabled**—Host or User was disabled but is online. This could be due to a misconfiguration of a switch or port or because the host was online at the time it was disabled. Defined as a Violation in some summary windows.	☒	**Offline / Disabled**—Host or User is disabled and is not online.
➡	**Go To** — Allows you to select an icon on the User, Host or Adapter View and navigate to corresponding information on another view. For example, if you have a host selected on the Host view, and you click the Go To on the Adapter icon, the Adapter view is displayed with the appropriate adapter selected.	🎮	**Offline Device**—A device being managed through the Host View is not connected to the network, such as a gaming device or an IP phone.
A	**Not Authenticated**—Located at the upper-left corner of the icon. User has not yet authenticated. There is a delay between when the user's computer is connected to the network and when it is placed in the Authentication VLAN.	+	**Security Risk**—Located at the upper-right corner of the icon. Host has been moved to remediation.
+	**Pending At Risk**—Located at the upper-right corner of the icon. Host has failed a scan that is set to delayed remediation for x number of days. Icon indicates that the host has not yet been marked "at risk" but will be after the delay set in the scan has elapsed.		
Topology view			

State	Definition	State	Definition
	No image over icon=Contact Established	□	Device Contact Unknown. Indicates that FortiNAC has not made initial contact with the device. Upon initial contact, FortiNAC queries the device and verifies the device type.
□	Device Contact Lost		
◎ ◎ ◎	Wireless switch **Blue** — Initial contact has not been made **Red** — Contact Lost **Gray** — Contact Established	⚑ ⚑ ⚑	Container **Blue** — Initial contact has not been made with one or more devices in the container **Red** — Contact lost with one or more devices in the container **Gray** — Contact established with all devices in the container
🟩 ▨ ☒	Port Admin status is on and Link status is up, indicating Host or device connected Admin status is on and Link status is down, indicating that nothing is connected Admin status is Off.		

The icons shown in the table below represent hosts, users and devices that are either online or in a good state, such as hosts that are Safe.

Icon list

Icon	Definition	Icon	Definition
Adapter, host and user icons			
▦	Adapter	?	Rogue Host
💻	Registered Host	☎	IP Phone
💼	Contractor	📒	Guest

Icon	Definition	Icon	Definition
	User		Administrator User
System icons			
	Container		Multi Access Point (multiple hosts connected to one port, and none of the ports are phones)
	New Registered Host/Phone (one registered host and one phone are connected to a port)		New Rogue Host/Phone (one rogue host and one phone are connected to a port)
	New Cloud/Phone Icon Used when one of the following is true: More than one phone and one registered host connected to a port More than one registered host and one phone connected to a port More than one registered host and more than one phones connected to a port		Wired Port
	Link to a neighboring device		Process Plug-In
	Port Aggregate Uplink		SSID — Wireless Connection
	Directory		Process
Device icons			
	Alarm System		Android
	Apple Device		Camera
	Card Reader		Cash Register
	Dialup Server		Environmental
	Firewall		Gaming Device

Icon	Definition	Icon	Definition
	Generic Monitoring System		Health Care Device
	Hub		Internet TV
	IP Phone		IPS/IDS
	Linux		macOS
	Mobile or Apple iOS or Android		Generic Network Device
	PBX		Pingable Device
	Printer		Router
	Server		Switch
?	Unknown Device		Unix
	UPS		Vending Machine
	VPN Connection	W	Windows
	Wireless Switch		

Certificates

SSL Certificates can be used to secure many different types of connections for FortiNAC. The table below outlines the uses and requirements for these certificates.

Applies to all Certificates imported into or saved on FortiNAC appliances.

Certificates that use SHA2 encryption are not supported.

Valid Certificates are certificates that were obtained from a signing authority, such as, VeriSign.

Update the list of Allowed Domains with the domain of the certificate vendor. See Allowed domains on page 114.

Make sure that your network has a VLAN that allows hosts in isolation to access the internet when the host attempts to reach one of the sites in the Allowed Domains list.

It is recommended that you set the home page to a HTTP URL instead of a HTTPS URL to avoid receiving a certificate warning when opening your browser in IE while in the registration VLAN.

Connection	Types	Required	Format	Location	If No Certificate
Admin UI	Self-Signed or Valid	No		/bsc/services	Works with or without a certificate.
Portal	Self-Signed or Valid	No	PEM	Imported	Works with or without a certificate.
Persistent Agent	Self-Signed or Valid	Yes Agent 3.0 or higher		Imported	Use agents lower than 3.0.
Dissolvable Agent	Self-Signed or Valid	Yes Agent 3.0 or higher		Imported	Use agents lower than 3.0.
Mobile Agent	Valid	Yes		Imported	No workaround, must use certificate.
LDAP Directory	Valid	No		/bsc/campusMgr	Do not select SSL or TLS protocols on the Directory Configuration view.
RADIUS Server	Valid	Yes with 802.1x and PEAP.		Proprietary	Use security options WEP, WPA or WPA2 , which use PSK, instead of the enterprise versions which use PEAP.
Supplicant Configuration	Valid	Yes for Windows hosts if RADIUS server has certificate and uses 802.1x and PEAP.	PEM or binary	Imported	Use security options WEP, WPA or WPA2 , which use PSK, instead of the enterprise versions which use PEAP. Or Windows hosts will have poor user experience with connection delays during Supplicant Configuration implementation.
Palo Alto Integration		Yes		N/A FortiNAC automatically imports from Palo Alto	Required

Associated certificate documentation

Connection	Topic
Admin UI	See SSL certificates on page 523.
Portal	See Portal SSL on page 158.
Persistent Agent	See SSL certificates on page 523.
Dissolvable Agent	
Mobile Agent	
LDAP Directory	See Create a keystore for SSL or TLS on page 96
RADIUS Server	See the documentation for your RADIUS server.
Supplicant Configuration	See Supplicant EasyConnect policies on page 471.
Palo Alto Integration	See Add or modify the Palo Alto User-ID agent as a pingable on page 728.

Dashboard

The Dashboard is the first window displayed for administrators logging into FortiNAC. It can be accessed from the Bookmarks Menu. Depending on the permissions of each administrative user, some menus may not appear.

Dashboard panels display to provide you with additional information at a glance. Much of this data can be accessed from other parts of the system. Each panel can be closed and later restored using the Add Panel button. Panels can be moved by dragging and dropping the panel to a new location. See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.

Changes to the setup of the dashboard, such as panel position, panels displayed, panel expanded/collapsed state, panel refresh interval and filters are saved for the logged in user. These user preferences are stored in the database and are honored regardless of where the user logs into FortiNAC. Changes to thresholds on the Performance panel are global and affect all users.

The Device Summary, Host Summary, User Summary and License Information panels allow you to drill down to more detailed data by clicking on one of the icons displayed. For example, click on the Registered Host Icon to display a list of registered hosts. From that list click on the MAC Address of a single host to display the Host Properties window for that host.

Data displayed in the panels listed below is sample data and may not be the same as data displayed on your Dashboard.

The Dashboard contains the following panels:

- Alarm on page 38
- Host summary on page 41
- Views on page 52
- Network device summary on page 42
- License information on page 42
- Security summary on page 49
- Persistent Agent summary on page 45
- Scans on page 46
- Performance on page 43
- Summary on page 47
- User summary on page 52

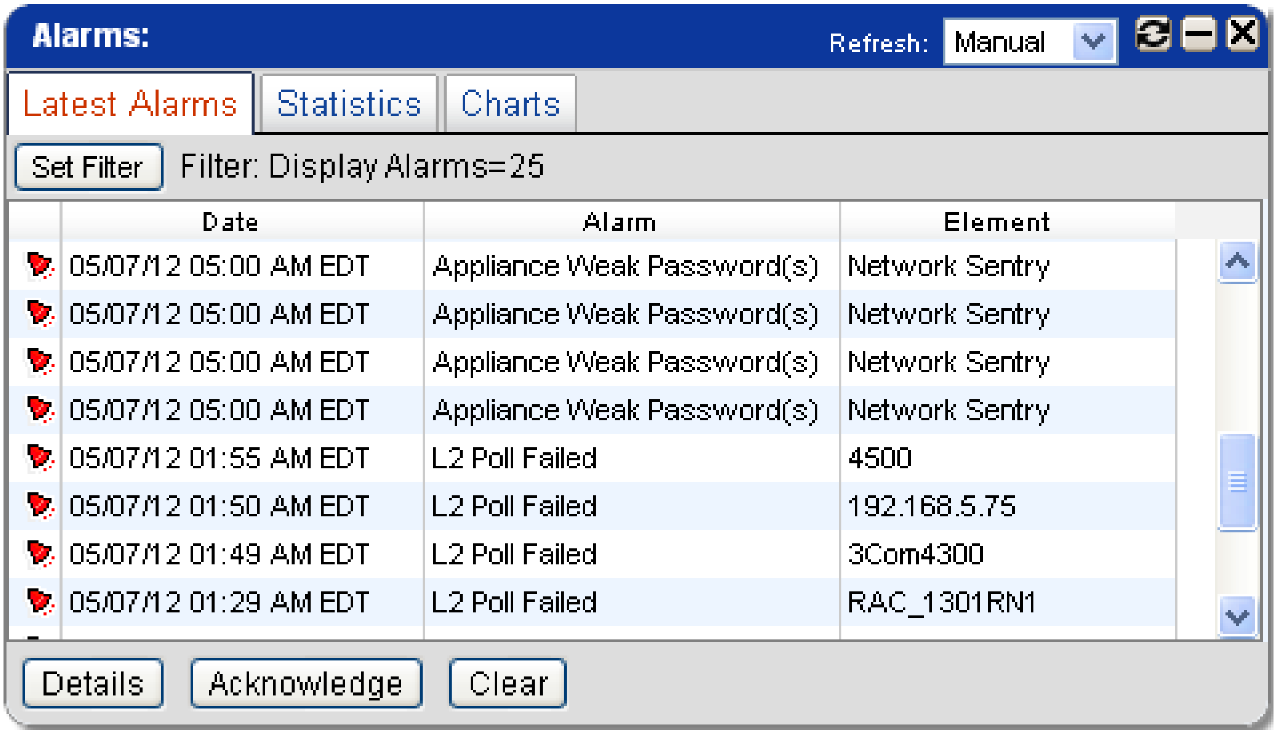
Add a panel

Use this option to add or restore closed panels to the dashboard.

1. Click the **Add Panel** button at the top of the dashboard window.
2. Select a panel from the list. To select more than one panel hold down the Ctrl key and click on the panel names.
3. Click **OK** to display the panels on the dashboard.

Alarm

The Alarm panel displays a subset of the information available on the Alarms View. It provides an at a glance view of alarms that have been triggered by events. The list is filtered to limit the number and type of alarms displayed. You can Acknowledge or Clear alarms and view alarm details. See Alarms view on page 887 and Add or modify alarm mapping on page 892 for additional information.



Filter: Display Alarms=25

Date	Alarm	Element
05/07/12 05:00 AM EDT	Appliance Weak Password(s)	Network Sentry
05/07/12 05:00 AM EDT	Appliance Weak Password(s)	Network Sentry
05/07/12 05:00 AM EDT	Appliance Weak Password(s)	Network Sentry
05/07/12 05:00 AM EDT	Appliance Weak Password(s)	Network Sentry
05/07/12 01:55 AM EDT	L2 Poll Failed	4500
05/07/12 01:50 AM EDT	L2 Poll Failed	192.168.5.75
05/07/12 01:49 AM EDT	L2 Poll Failed	3Com4300
05/07/12 01:29 AM EDT	L2 Poll Failed	RAC_1301RN1

Latest alarms tab

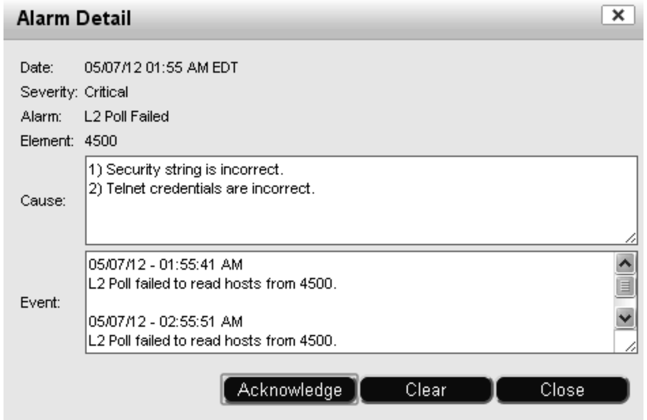
The Latest Alarms tab displays each alarm with date, time, and the elements affected. Elements include items such as, MAC Address or IP address. Click the Acknowledge button to indicate that you are aware of the selected alarm. Click the Clear button to remove the selected alarm from the database.

Set filter

1. Click the **Set Filter** button on the Latest Alarms Tab.
2. In the Filter window, click in the **Display Latest** drop-down list and select the number of alarms to display. The maximum is 100.
3. To filter by Severity, mark the **Severity** check box with a check mark to enable it and select the severity level from the drop-down list. Levels include Critical, Minor, Warning and Informational.
4. To display **Acknowledged Alarms**, mark that check box with a check mark to enable it.
5. Click **OK**. Filter settings are displayed on the Alarms panel to the right of the Set Filter button.

Filter settings are stored for each user.

View details



Date: 05/07/12 01:55 AM EDT

Severity: Critical

Alarm: L2 Poll Failed

Element: 4500

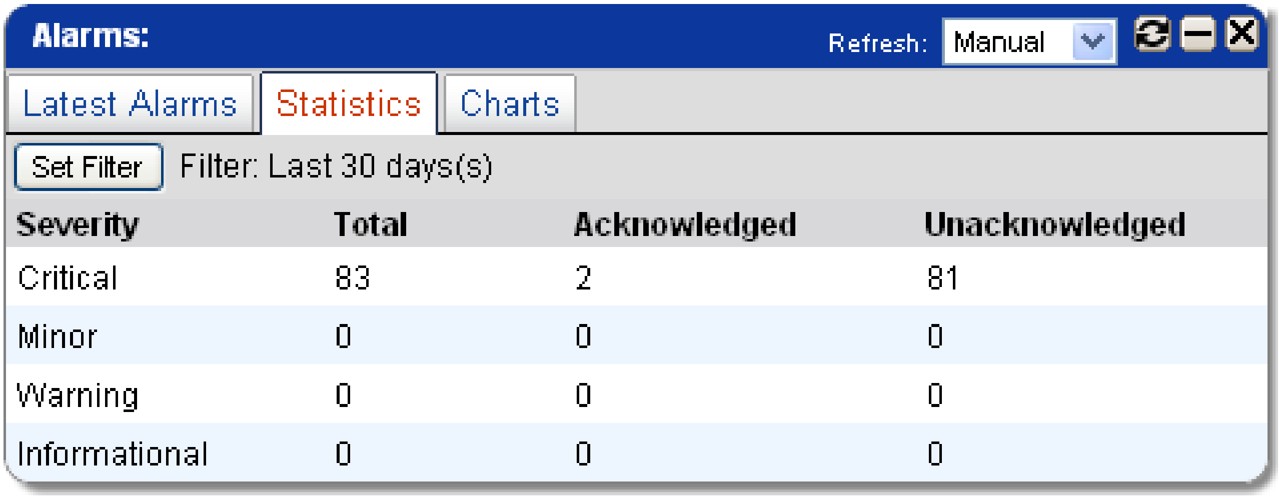
Cause:
1) Security string is incorrect.
2) Telnet credentials are incorrect.

Event:
05/07/12 - 01:55:41 AM
L2 Poll failed to read hosts from 4500.

05/07/12 - 02:55:51 AM
L2 Poll failed to read hosts from 4500.

1. Select an alarm from the list displayed in the Latest Alarms tab.
2. Click the **Details** button.
3. Click **Acknowledge** to mark the alarm as acknowledged.
4. Click **Clear** to remove the alarm from the database.
5. Click **Close** to return to the Dashboard.

Statistics tab



Filter: Last 30 days(s)

Severity	Total	Acknowledged	Unacknowledged
Critical	83	2	81
Minor	0	0	0
Warning	0	0	0
Informational	0	0	0

The Statistics tab displays alarm totals by severity. In addition, each total is broken down into Acknowledged and Unacknowledged alarms. Alarms can be marked as Acknowledged to indicate that a user is aware of the alarm. You can clear alarms that are no longer needed. Cleared alarms are not included in totals.

The Set Filter button allows you to choose the number of days of data that will be tallied by this Statistics screen. Depending on the age time selected in the FortiNAC Properties window and your archive and purge schedule, you may not be able to view data for the number of days selected on the Statistics tab. For example, the default age time for events and alarms is seven days. If you select nine days on the Statistics tab, you may not be able to see data for all nine days. See Database archive on page 210 for information on age time.

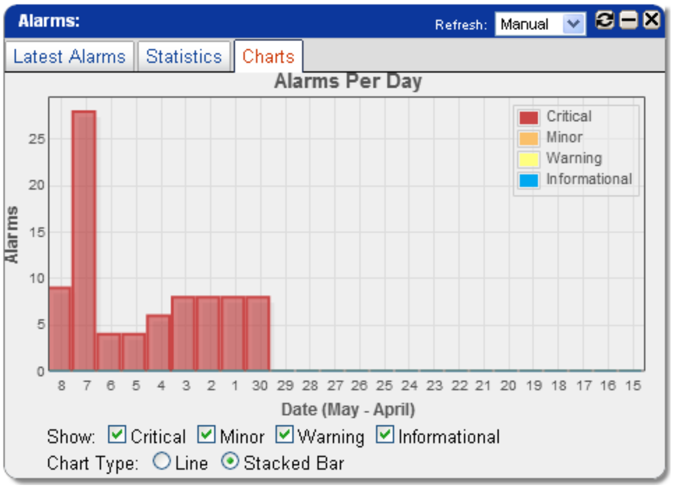
Filter settings are stored for each Admin user.

Set filter

1. Click the Set Filter button on the Statistics tab.
2. Type the number of days to go back and collect data.
3. Click OK.

If the number of days is too large, you may see a warning indicating the number of days selected for the age time in the FortiNAC Properties window. If the Age Time for purging alarm data is set to 7 days and you select 30 days for the filter, the panel will display data for as many days as it can access within the range selected.

Charts tab

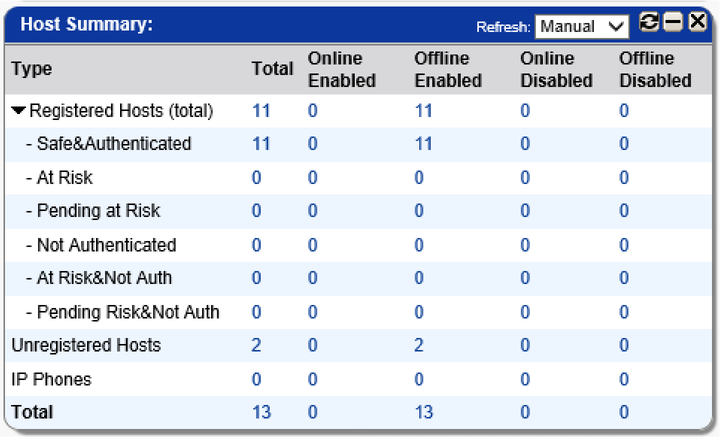


Show: ☑ Critical ☑ Minor ☑ Warning ☑ Informational

Chart Type: ○ Line ● Stacked Bar

The Charts tab provides a chart of alarms per day for the last 24 days. Depending on the age time settings in the FortiNAC Properties window and the archive and purge schedule, you may not have 24 days of data available. Use the **Show** check boxes across the bottom of the chart to select the alarms to display. The graphical representation of the alarms can be either a line or a stacked bar. Use the **Chart Type** options at the bottom of the window to change the graphic.

Host summary

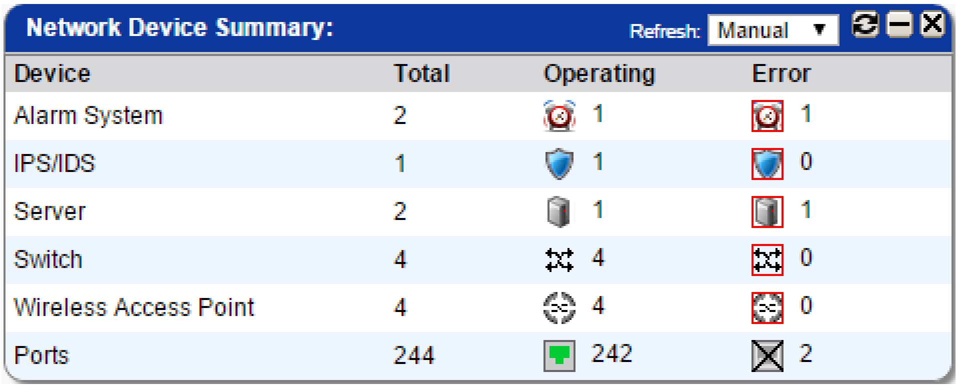


Type	Total	Online Enabled	Offline Enabled	Online Disabled	Offline Disabled
Registered Hosts (total)	11	0	11	0	0
- Safe&Authenticated	11	0	11	0	0
- At Risk	0	0	0	0	0
- Pending at Risk	0	0	0	0	0
- Not Authenticated	0	0	0	0	0
- At Risk&Not Auth	0	0	0	0	0
- Pending Risk&Not Auth	0	0	0	0	0
Unregistered Hosts	2	0	2	0	0
IP Phones	0	0	0	0	0
Total	13	0	13	0	0

This dashboard panel displays a table of information about the hosts on your network. Click the number in the Total column to display that list of hosts in the Host View.

Field	Definition
Registered Hosts	The total number of registered hosts. Total includes hosts registered to users and hosts registered as devices that are managed in Host View or in both Host View and Topology View. The total is broken out by the number that are Online, Offline, in Violation, Disabled, Online at Risk, and Offline At Risk. Click the expansion arrow to view registered hosts broken down by the host state. States include: **Safe & Authenticated** — Hosts that have not failed a scan and the associated user has authenticated against the local database, RADIUS or LDAP directory. **At Risk** — Host has failed a scan or has manually been marked at risk. **Pending At Risk** — Host has failed a scan but its At Risk status is delayed based on the delayed remediation setting in the Endpoint Compliance Policy used. **Not Authenticated** — Associated user has not authenticated against the local database, RADIUS or LDAP directory. **At Risk & Not Authenticated** — Host has failed a scan or has been marked At Risk and the associated user has not authenticated against the local database, RADIUS or LDAP directory. **Pending Risk & Not Authenticated** — Host has failed a scan but its At Risk status is delayed based on the delayed remediation setting in the Endpoint Compliance Policy used and the associated user has not authenticated against the local database, RADIUS or LDAP directory.
Unregistered Hosts	The total number of unregistered hosts. The total is broken out by the number that are Online, Offline, in Violation, Disabled, Online at Risk, and Offline At Risk.
IP Phones	Total number of IP Phones on the network. Total is broken out by the number that are online and offline.
Total	Shows the combined total for all hosts registered and rogues.

Network device summary



Network Device Summary:

Refresh: Manual

Device	Total	Operating	Error
Alarm System	2	1	1
IPS/IDS	1	1	0
Server	2	1	1
Switch	4	4	0
Wireless Access Point	4	4	0
Ports	244	242	2

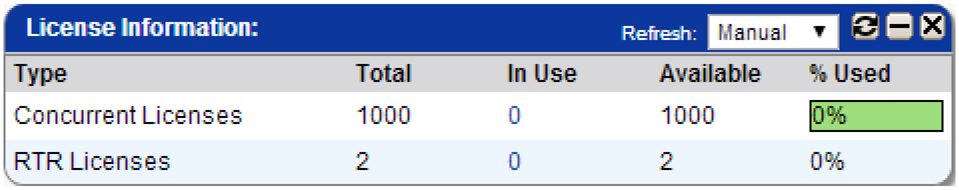
This Dashboard Panel displays a table of the total number of devices connected to your network by type. Totals are broken out by Operating (devices currently in operation) and Error (devices that currently have errors). Click on an icon to display a list of actual devices.

Details list view

FortiNAC provides summary views of device types with their corresponding icons. The total number of each type of device is also displayed. You can access this summary from the Dashboard.

If you click on an icon within one of the summaries a detailed list of that item type is displayed. For example, if you click on the Switch icon, a list of all of the switches on your network is displayed. You can then click on an individual switch and display the Properties window for that switch.

License information



License Information:

Refresh: Manual

Type	Total	In Use	Available	% Used
Concurrent Licenses	1000	0	1000	0%
RTR Licenses	2	0	2	0%

This dashboard panel displays the total number of licenses purchased. In addition, this summary indicates the number of licenses being used at any given time. Events can be generated and set to trigger alarms when license usage reaches or exceeds 75% of total licenses and when usage reaches 100% of total licenses. These are default thresholds. Thresholds used to calculate % Used information can be modified from the License Information panel by clicking on the colored bar. Thresholds can also be modified from the Events Management window. See Event thresholds on page 858 for instructions.

The color bars in the % Used column change as you exceed certain licensing thresholds. Colors are as follows:

- Green—the percentage used is below the threshold.
- Yellow—the percentage used is at or above the threshold.
- Red—the percentage used is at 100%.

Licenses in use

To determine how licenses are consumed within FortiNAC click the number displayed in the In Use column on the License Information panel. A list of the exact element consuming each license is displayed.

Data displayed in the License Usage Panel can be exported in CSV, Excel, PDF or RTF formats. Click the appropriate icon at the bottom of the window to export.

See Licenses on page 7 for additional license information.

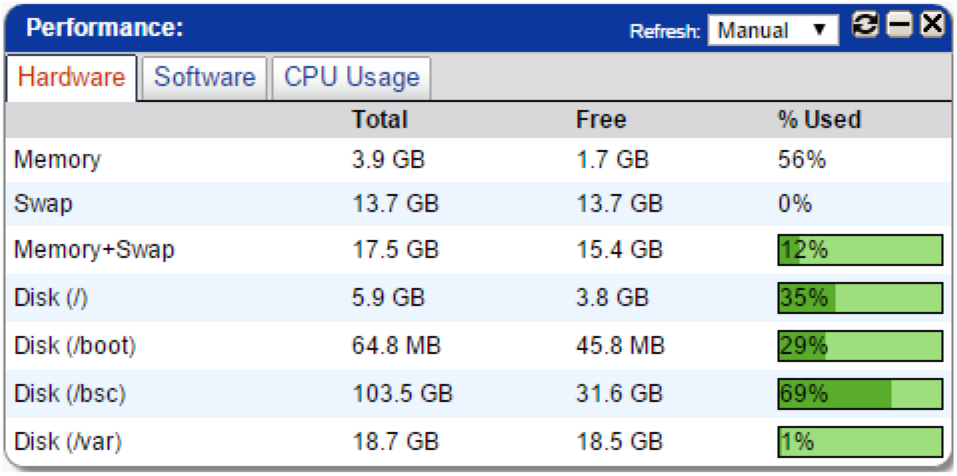
Performance

This dashboard panel displays performance information for your software, appliance size and CPU. For the software and sizing performance calculations you can modify the thresholds by clicking in the colored percentage bar.

Thresholds used to calculate % Used or % Capacity information can be modified from the Performance panel. Hover over the colored bars to display threshold settings. Click on the colored bar to modify threshold settings. Thresholds can also be modified from the Events Management window. See Event thresholds on page 858. Threshold changes are global and affect all users.

Color	Definition
Green	Percentage used is below the warning threshold.
Yellow	Percentage used is above the warning threshold, but below the critical threshold.
Red	Percentage used is above the critical threshold.

Hardware

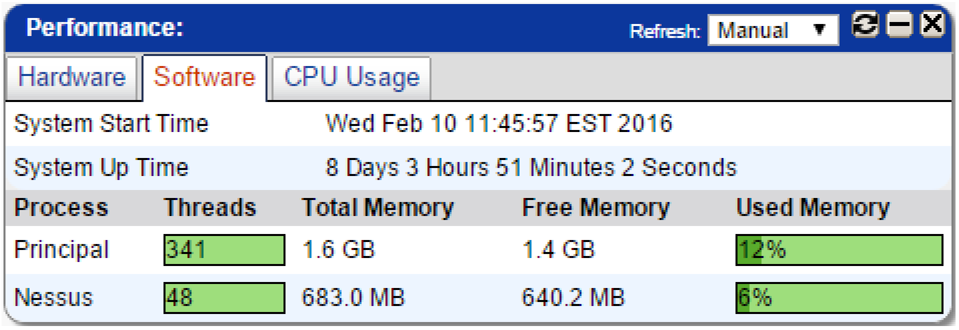


	Total	Free	% Used
Memory	3.9 GB	1.7 GB	56%
Swap	13.7 GB	13.7 GB	0%
Memory+Swap	17.5 GB	15.4 GB	12%
Disk (/)	5.9 GB	3.8 GB	35%
Disk (/boot)	64.8 MB	45.8 MB	29%
Disk (/bsc)	103.5 GB	31.6 GB	69%
Disk (/var)	18.7 GB	18.5 GB	1%

The system uses as much RAM as is available. The underlying operating system is optimized to use RAM as efficiently as possible. Swap space is configurable, but only by Customer Support. The sum total of space available in RAM and available in swap represents the total amount of virtual memory available on the system.

The disk space representing each directory on the file system is displayed. Thresholds used to calculate Memory+Swap and Disk Used percentages can be modified from the Performance panel by clicking on the colored bar.

Software



System Start Time Wed Feb 10 11:45:57 EST 2016

System Up Time 8 Days 3 Hours 51 Minutes 2 Seconds

Process	Threads	Total Memory	Free Memory	Used Memory
Principal	341	1.6 GB	1.4 GB	12%
Nessus	48	683.0 MB	640.2 MB	6%

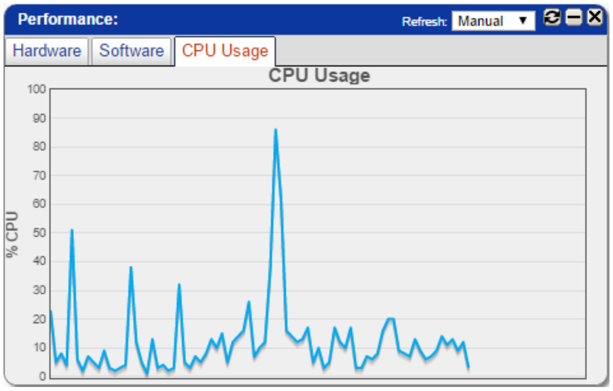
Memory is allocated to each of the internal loader processes in the FortiNAC appliance, such as the "master loader". The amount of memory allocated to these processes varies from platform to platform, and is configurable, but only by Customer Support.

Thresholds used to calculate Threads and Used Memory percentages can be modified from the Performance panel by clicking on one of the colored bars.

Settings

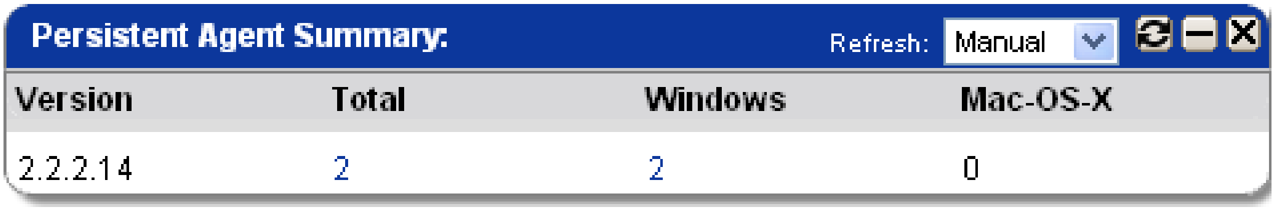
Field	Definition
System Start Time	Time the software was started.
System Up Time	Amount of time the software has been running.
Process	Processes that are currently running. If a process is not running it is not displayed. Possible processes include: Principal Nessus
Threads	Number of threads being used by a particular process. The thread count for master loader is: Minimum: warning: 500 critical: 575. These numbers may automatically increase depending on the capabilities of the hardware or virtual machine.
Total Memory	Total Memory allocated for each process.
Free Memory	Portion of Total Memory not being used for each process.
Used Memory	Percentage of total memory being used for each process. The amount of memory allocated.

CPU usage



The graph contained in this tab displays the percentage of CPU Usage. The data contained within the graph is not stored and is based on data points retrieved at each refresh interval. In an environment with a pair of servers, there are separate lines for the FortiNAC Control Server and FortiNAC Application Server.

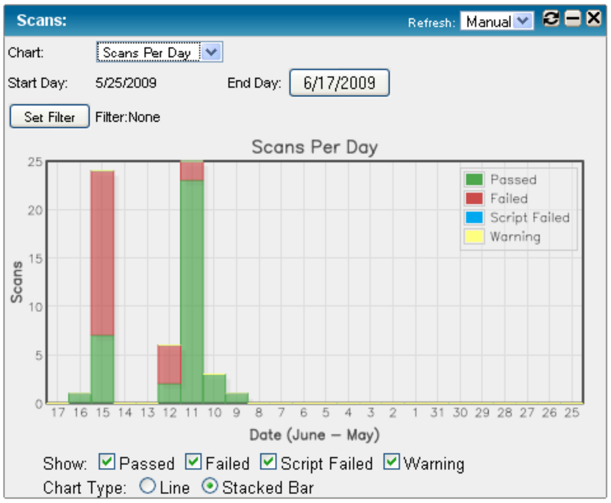
Persistent Agent summary



Version	Total	Windows	Mac-OS-X
2.2.2.14	2	2	0

This dashboard panel details the number of hosts at each agent version, broken out by operating system. You may have some hosts that use the Dissolvable Agent and are not counted on this window. If you have been using the Global Agent Update option, this summary panel helps you determine how many agents have been updated and how many remain at the previous version. Click the blue number in the Total or operating system column to display the list of hosts running that particular version of the Persistent Agent in the Host View.

Scans



Scans: Refresh: Manual

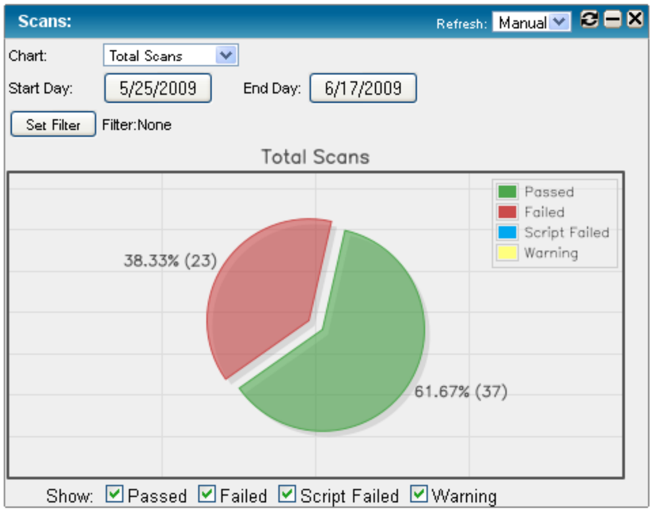
Chart: Scans Per Day

Start Day: 5/25/2009 End Day: 6/17/2009

Set Filter Filter:None

Show: ☑ Passed ☑ Failed ☑ Script Failed ☑ Warning

Chart Type: ○ Line ● Stacked Bar



Scans: Refresh: Manual

Chart: Total Scans

Start Day: 5/25/2009 End Day: 6/17/2009

Set Filter Filter:None

Show: ☑ Passed ☑ Failed ☑ Script Failed ☑ Warning

This dashboard panel contains a graph of host scans done per hour, per day or total scans based on a date range. Additional filters allow you to limit the data as needed. This data is similar to the data displayed in the Scan Results View. However, it is retrieved from a different database table that is not affected by the scheduled archive and purge of scans. As a result the Scan Results View and the Scans Panel may display different data. See Scan results view on page 925 for additional information.

Display scans

1. Click in the **Chart** drop-down and select the scans to be displayed. Options include **Scans Per Day**, **Scans Per Hour**,or **Total Scans**.
2. Enter date information for the scan chart selected. Date information required varies depending on the chart you selected:
   - If you selected Scans Per Day, enter the end date of the date range. The panel automatically calculates back 24 days. Days begin/end at midnight.
   - If you selected Scans Per Hour, enter a single date. The panel displays 24 hours.
   - If you selected Total Scans, enter a start and end date. The panel aggregates the totals across the entire date range.
3. Use the check boxes across the bottom of the panel to limit the number of scans by results. Options include:
   - **Passed**—Scans that ran and the host passed.
   - **Failed**—Scans that ran and the host failed. This includes scans that are set to Failure Pending.
   - **Script Failed**—Scan tried to run but failed before determining the host's state.
   - **Warning**—Scan determined that the host failed the scan policy and an administrator received a warning.

Hosts may need to be scanned more than once if they fail the initial scan. Therefore, each scan does not represent a single host.

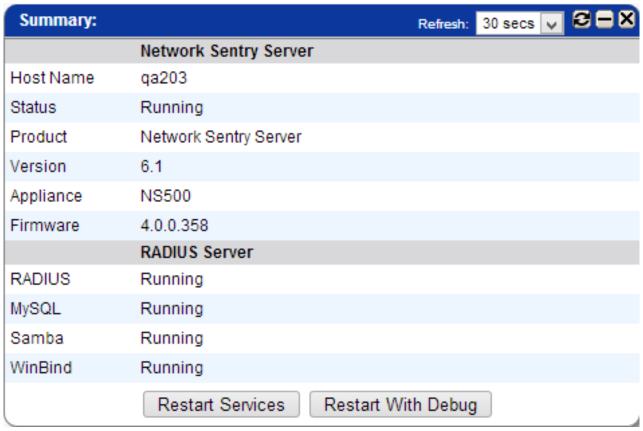
4. To filter data displayed on the panel, click the Set Filter button.

5. Enable one or more filters by marking the boxes with a check mark.
6. For each filter selected, choose an option in the drop-down menu. See the table below for definitions:

Field	Definition
Type	
SMA	Scans performed by the Dissolvable Agent.
System	Scans performed by the System based on the following scripts: • **ForceCSARescan**—Forces the Target Group of hosts using the Dissolvable agent to be rescanned by setting the hosts in the group to At-Risk. • **ForcePersistentAgent—**Forces the Target Group of hosts using the Persistent agent to be rescanned by setting the hosts in the group to At-Risk. • **PassAllClients—**Sets the Target Group of hosts to Safe. • **FailAllClients—**Sets the Target Group of hosts to At Risk.
SMA Agent	Scans performed by the Persistent Agent.
Agent Monitor	Custom scans that may run at a different interval than the scan with which they are associated.
Platform	
Windows MAC Linux	Filters scans based on the host's operating system.
Scan	
<Scan Name>	Filters scans based on the name of the scan used to evaluate the host.

7. Click **OK** to save. Filter options are saved for each admin user.

Summary



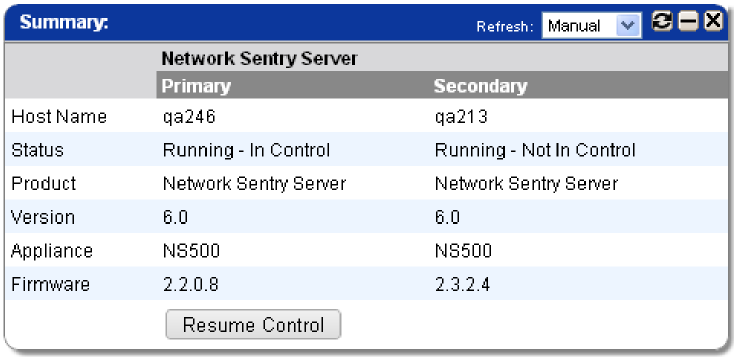
Summary:

Refresh: 30 secs

	Network Sentry Server
Host Name	qa203
Status	Running
Product	Network Sentry Server
Version	6.1
Appliance	NS500
Firmware	4.0.0.358
	RADIUS Server
RADIUS	Running
MySQL	Running
Samba	Running
WinBind	Running

This dashboard panel displays information about your servers.

If you are running in a High Availability Environment, a Resume Control button is displayed to allow you to restart the primary server and resynchronize the data. This button is only enabled if the Secondary Server is in control.



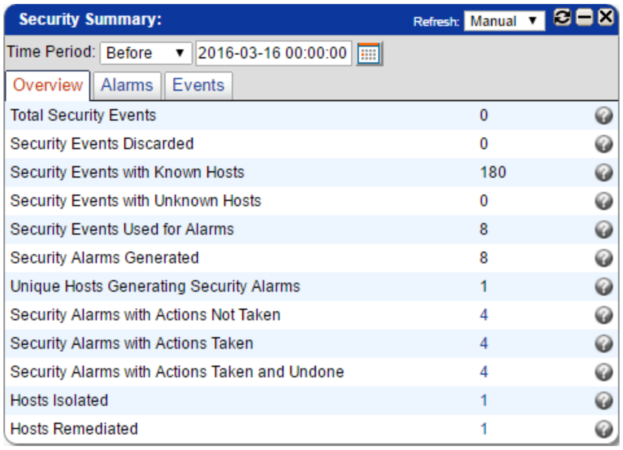
	Network Sentry Server	
	Primary	Secondary
Host Name	qa246	qa213
Status	Running - In Control	Running - Not In Control
Product	Network Sentry Server	Network Sentry Server
Version	6.0	6.0
Appliance	NS500	NS500
Firmware	2.2.0.8	2.3.2.4

Field	Definition
Host Name	Name of the appliance on which FortiNAC is running.
Status	Indicates the current status of each appliance displayed. Statuses include: • **Running** — Appliance and software are running. • **Not Reachable** — Dashboard cannot communicate with the server. • **Management Down** — Appliance is running but the software is down. • **Running - Idle** — Appliance and software are up and running but there is currently no activity. • **Running - In Control** — Appliance and software are up and running. This appliance is in control vs. an appliance that may be the secondary appliance for high availability. • **Running - Not In Control** — Applies in a High Availability environment, where a secondary server is ready to take over in the event of a failure on the primary server. Indicates that the appliance and software are running, but are not in control.
Product	Software that is installed and running on the appliance or virtual machine.
Version	Version number of the software listed under Product.
Appliance	Model number is displayed.
Firmware	Version number of the internal release specific software installed on the displayed appliance or virtual machine.
RADIUS Server	Displays only if the integrated FortiNAC RADIUS server feature is enabled. If enabled, associated services and corresponding status are displayed. Services include RADIUS, MySQL, Samba and WinBind.
Restart Services	Restarts all of the RADIUS server services.
Restart With Debug	Restarts all of the RADIUS server services and enabled debug output in the RADIUS Server logs.

Security summary

This dashboard panel displays a table of information about incoming security events that satisfied a security trigger, and the alarms that were created.

Overview



Security Summary: Refresh: Manual

Time Period: Before 2016-03-16 00:00:00

Overview | Alarms | Events

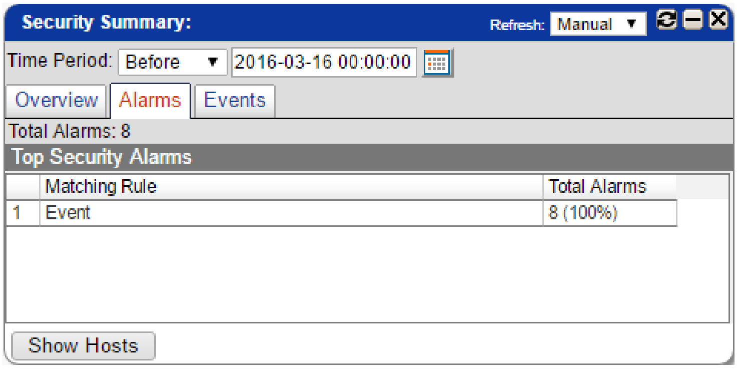
Total Security Events	0
Security Events Discarded	0
Security Events with Known Hosts	180
Security Events with Unknown Hosts	0
Security Events Used for Alarms	8
Security Alarms Generated	8
Unique Hosts Generating Security Alarms	1
Security Alarms with Actions Not Taken	4
Security Alarms with Actions Taken	4
Security Alarms with Actions Taken and Undone	4
Hosts Isolated	1
Hosts Remediated	1

The Overview tab displays general statistics about security events and alarms that were generated, as well as the number of hosts that were isolated and/or remediated as a result of actions taken based on the security alarms.

Field	Definition
Total Security Events	The number of valid security events received during the specified time period. (Valid security events must have a Source IP address).
Security Events Discarded	The number of security events that were not recorded during the specified time period because there were no enabled Security Triggers that matched the event.
Security Events with Known Hosts	The number of security events recorded during the specified time period that have a valid Source MAC (i.e., the server was able to resolve the Source IP to a MAC Address).
Security Events with Unknown Hosts	The number of security events recorded during the specified time period that have no Source MAC (i.e., the server was not able to resolve the Source IP to a MAC Address).
Security Events Used for Alarms	The number of security events recorded during the specified time period that were used to generate alarms.
Security Alarms Generated	The number of security alarms generated during the specified time period.
Unique Hosts Generating Security Alarms	The number of different hosts that generated security alarms during the specified time period.

Field	Definition
Security Alarms with Actions Not Taken	The number of security alarms generated during the specified time period for which the corresponding action was not taken. Click the number of security alarms to view the alarms in Security Alarms view.
Security Alarms with Actions Taken	The number of security alarms generated during the specified time period for which the corresponding alarm action was taken. Click the number of security alarms to view the alarms in Security Alarms view.
Security Alarms with Actions Taken and Undone	The number of security alarms generated during the specified time period for which the corresponding alarm action was both taken and undone. Click the number of security alarms to view the alarms in Security Alarms view.
Hosts Isolated	The number of hosts which have been isolated as the result of a security alarm generated during the specified time period. Click the number of hosts to display the hosts which were isolated. Note that the list only shows hosts that are still being managed by FortiNAC.
Hosts Remediated	The number of hosts which have been remediated as the result of a security alarm generated during the specified time period. Click the number of hosts to display the hosts which were remediated. Note that the list only shows hosts that are still being managed by FortiNAC.

Alarms



Refresh: Manual

Time Period: Before 2016-03-16 00:00:00

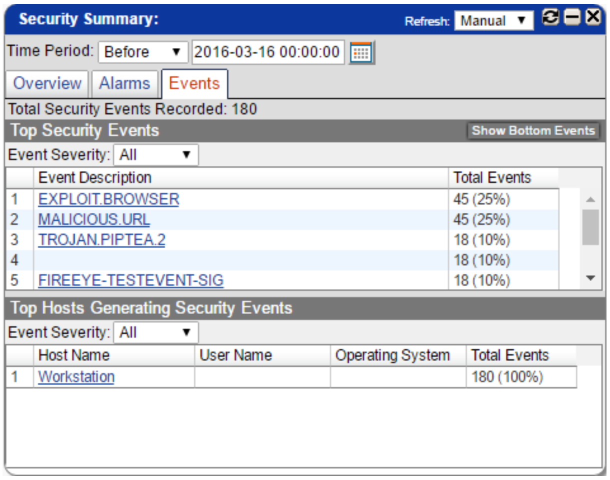
Total Alarms: 8

	Matching Rule	Total Alarms
1	Event	8 (100%)

The Alarms tab displays up to 20 of the most frequent security alarms that occurred during the selected time period.

Field	Definition
Matching Rule	The security rule that was satisfied which triggered the security alarm(s).
Total Alarms	The total number of security alarms that were triggered by the security rule.
Show Hosts	Opens a dialog showing the details of each host that generated the security alarm. You can also access the Host View from the Show Hosts dialog. See Host view on page 793.

Events



Refresh: Manual

Time Period: Before 2016-03-16 00:00:00

Total Security Events Recorded: 180

Event Severity: All

	Event Description	Total Events
1	EXPLOIT.BROWSER	45 (25%)
2	MALICIOUS.URL	45 (25%)
3	TROJAN.PIPTEA.2	18 (10%)
4		18 (10%)
5	FIREEYE-TESTEVENT-SIG	18 (10%)

Event Severity: All

	Host Name	User Name	Operating System	Total Events
1	Workstation			180 (100%)

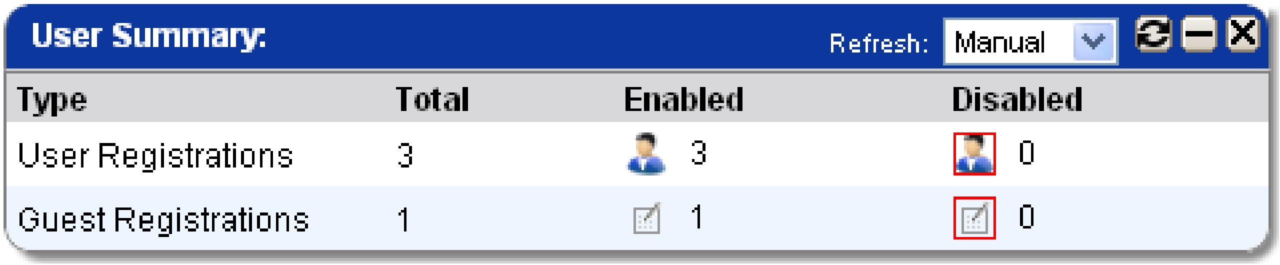
The Events tab displays up to 20 of the most frequent or least frequent security events that occurred during the selected time period.

The Top Hosts Generating Security Events section displays up to 20 hosts that have generated the most security events during the selected time period.

Field	Definition
Total Security Events Recorded	The total number of security events that occurred during the selected time period.
Show Top/Bottom Events	Click Show Top Events to display the most frequently occurring security events during the selected time period. Click Show Bottom Events to display the least frequently occurring security events during the selected time period.
Top security events	
Event Severity	Enables you to display security events by severity level. Select All, Critical, High, Medium, or Low.
Event Description	A description of the security event that you can click to view more information about the security event in Security Events view.
Total Events	The total number of each type of security event that occurred during the specified time period. The percentage of Total Security Events Recorded of which the security event type comprises is also displayed.
Top hosts generating security events	
Event Severity	Enables you to display security events by severity level. Select All, Critical, High, Medium, or Low.
Host Name	The name of the host that generated the security event. Click the host name to view details of the host in Host View.

Field	Definition
User Name	The name of the logged on user for the host.
Operating System	The operating system of the host.
Total Events	The total number of security events generated by the host that occurred during the specified time period. The percentage of Total Security Events Recorded of which the security events generated by the host comprise is also displayed.

User summary

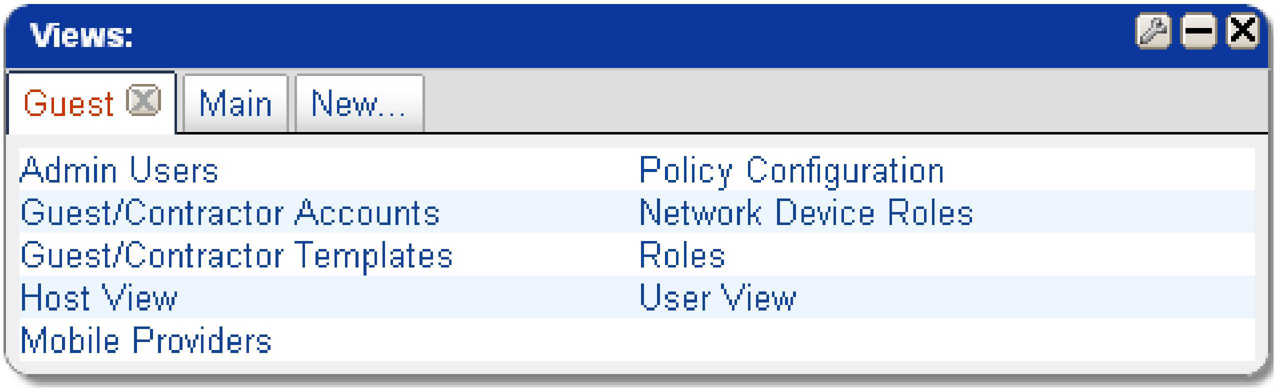


Type	Total	Enabled	Disabled
User Registrations	3	3	0
Guest Registrations	1	1	0

This dashboard panel displays a table of information about the users on your network. Click an icon to display additional user information in the User View.

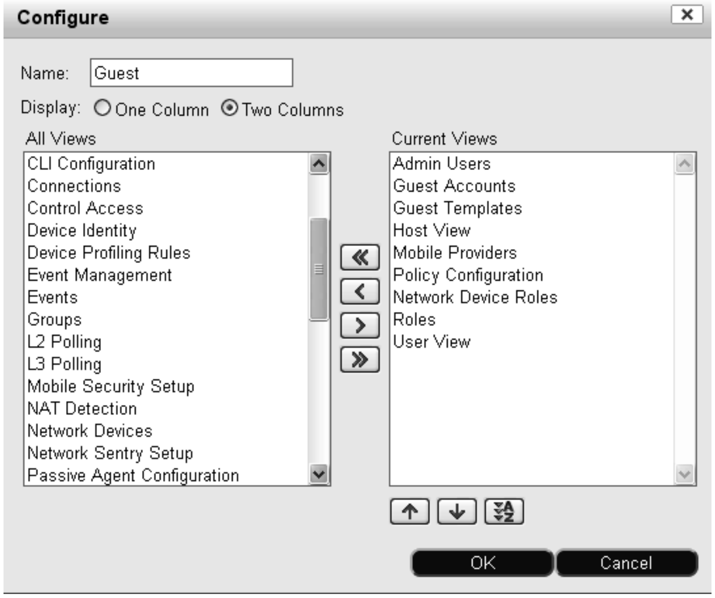
Field	Definition
User Registrations	The total number of users registered on the network, also shown by the number that are Enabled and Disabled.
Guest Registrations	The total number of guest/contractor users. The total is broken out by the number of guests that are Enabled and Disabled.

Views



This dashboard panel displays a list of links to "Views" used to access and modify system data. For example, clicking Host View allows you to view and manage a list of existing Hosts. This panel is configurable. Definitions of the links display either in the right hand column for the single column configuration or in a tool tip triggered by hovering over the link in the two column configuration. The first time the Views Panel is displayed, all possible links are included.

Configure the panel



Name: Guest

Display: ○ One Column ● Two Columns

All Views

- CLI Configuration
- Connections
- Control Access
- Device Identity
- Device Profiling Rules
- Event Management
- Events
- Groups
- L2 Polling
- L3 Polling
- Mobile Security Setup
- NAT Detection
- Network Devices
- Network Sentry Setup
- Passive Agent Configuration

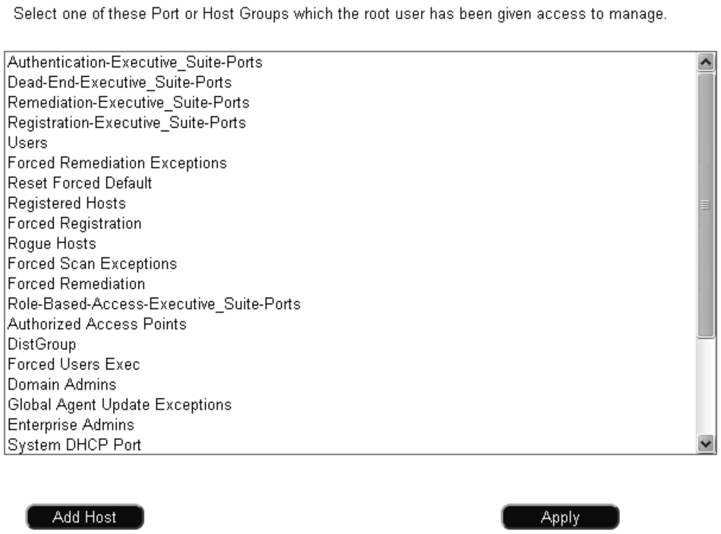
Current Views

- Admin Users
- Guest Accounts
- Guest Templates
- Host View
- Mobile Providers
- Policy Configuration
- Network Device Roles
- Roles
- User View

You can configure the Views panel to display links to the menu options from the Menu bar. You can break the list of links up into multiple tabs or keep everything on the Main tab.

1. On the **View Panel**, select the tab to be configured.
2. To create a new tab, select **New**. The Configure Window displays.
3. To configure an existing tab, select it and click the Configuration button at the top of the panel. The Configure window displays.
4. Click the **Name** field to create or edit the name for the tab.
5. In the **Display** section select either **One Column** or **Two Columns**. If you display links in one column, a definition for each link displays to the right of the link. If you display links in two columns, a definition for each link displays as a tool tip when you hover over the link.
6. The **All Views** list displays a list of possible links to views within FortiNAC. Use the arrows to move selected links into or out of the Current Views section. Links displayed in Current Views are included in the Views Panel.
7. To change the display order of your links, select a link in the Current Views list and click the up and down arrows.
8. Click the **AZ** button to sort links alphabetically.
9. Click **OK** to save changes to the selected Views tab.

Manage hosts and ports



Select one of these Port or Host Groups which the root user has been given access to manage.

Authentication-Executive_Suite-Ports
Dead-End-Executive_Suite-Ports
Remediation-Executive_Suite-Ports
Registration-Executive_Suite-Ports
Users
Forced Remediation Exceptions
Reset Forced Default
Registered Hosts
Forced Registration
Rogue Hosts
Forced Scan Exceptions
Forced Remediation
Role-Based-Access-Executive_Suite-Ports
Authorized Access Points
DistGroup
Forced Users Exec
Domain Admins
Global Agent Update Exceptions
Enterprise Admins
System DHCP Port

Manage Hosts & Ports contains a list of host and port groups. This view works in conjunction with Administrative groups to limit Admin user access. When you add an Admin user to an Administrative group, only the groups that the Admin user has permission to manage are listed in the Manage Hosts & Ports tab. Select a group from the list and click Apply to view or manage the members of the group. Click Add Hosts to add hosts to the database.

Add hosts

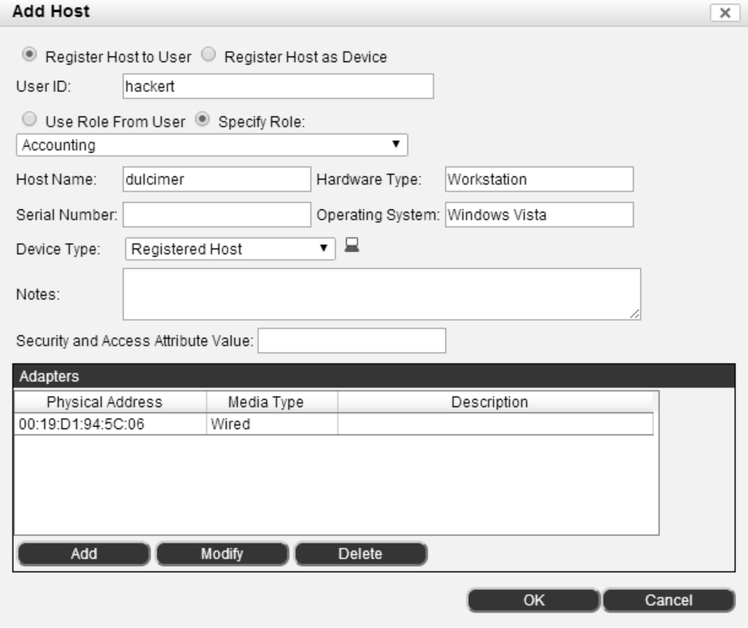
Administrative Users who do not have full access to the Admin user interface can add hosts in the Manage Hosts And Ports View. The Administrative User's Admin Profile must have permission for Manage Hosts & Ports with Access and Add/Modify enabled.

Access add hosts

1. Select **Bookmarks > Manage Hosts & Ports**.
2. Click the **Add Hosts** button at the bottom of the window.

Hosts added through this process are either registered to a user or registered as a device.

Host registered to a user



● Register Host to User ○ Register Host as Device

User ID: hackert

○ Use Role From User ● Specify Role:

Accounting

Host Name: dulcimer Hardware Type: Workstation

Serial Number: Operating System: Windows Vista

Device Type: Registered Host

Notes:

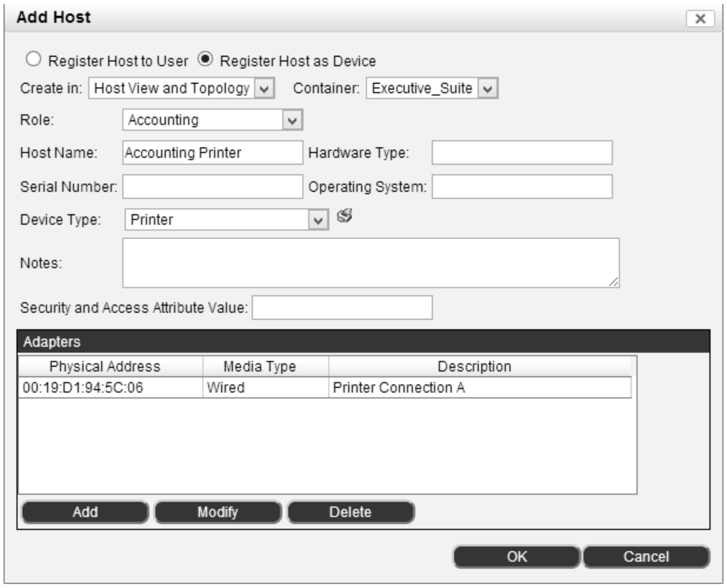
Security and Access Attribute Value:

Adapters

Physical Address	Media Type	Description
00:19:D1:94:5C:06	Wired	

A host registered to a user is associated with that user and inherits network access parameters from the user. The host contributes to the Allowed Hosts count for the user. If the host is registered here, the user will not have to go through the registration process elsewhere, such as the captive portal.

Host registered as a device



○ Register Host to User ● Register Host as Device

Create in: Host View and Topology Container: Executive_Suite

Role: Accounting

Host Name: Accounting Printer Hardware Type:

Serial Number: Operating System:

Device Type: Printer

Notes:

Security and Access Attribute Value:

Adapters

Physical Address	Media Type	Description
00:19:D1:94:5C:06	Wired	Printer Connection A

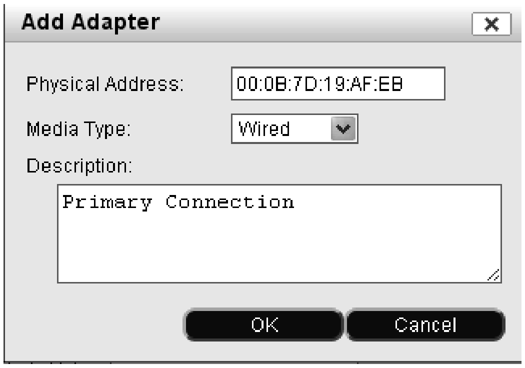
A host registered as a device can be displayed in the Host View or both the Host View and Topology View. Typically hosts registered as devices are items such as IP phones, security cameras, alarm systems or printers.

Settings

Field	Definitions
Register host to user	
User ID	ID of the user who owns this host. As you type a list of matching user IDs drops down. For example if you type ab, user IDs that start with ab are displayed. If the user ID does not exist in the database, but does exist in the directory used to authenticate users, the user is created at the same time. If the user does not exist either in the directory or in your database, you cannot save the host. If registering this host to a User exceeds the number of Allowed Hosts for that user, a message is displayed indicating that Allowed Hosts has been automatically incremented and the host is registered to the user.
Register host as device	
Create In	Indicates where the device should be displayed. Options include Host View or Host View And Topology View.
Container	If the host is created in both Host View and Topology View, you must choose a Topology View container to contain the host. Containers in Topology are used to group devices.
General	
Role	Roles are attributes of hosts and users that can be used as filters in User/Host Profiles. If the host is registered to a user, there are two options for selecting the host role: • **Use Role From User** — Indicates that the host role is inherited from the registered user associated with the host. • **Specify Role** — Indicates that the host role is manually selected. This enables a drop-down list of possible roles from which you can choose. If the host is registered as a device in Topology View only, its role is used to control network access or can be used to apply a CLI configuration. For example, a CLI configuration could be used to reduce the baud rate of a device when it connects to the network.
Host Name	Name of the host being registered.
Hardware Type	Type of hardware such as Printer, Server or Workstation.
Serial Number	Serial number on the device. May be of assistance if the device is ever stolen.
Operating System	Operating system on the host, such as Windows XP or macOS. Only hosts with a valid operating system can be rescanned. Valid operating systems are Windows, Mac, and Linux.
Device Type	Indicates the type of device being disinterested registering a host to a user this field defaults to Registered Host. It could also be set to a gaming or mobile device. When registering as a device, this might be set to devices that are not typically associated with an owner, such as a printer or an alarm system. An icon representing the device selected displays beside the Device Type field.

Field	Definitions
	If the device is an Access Point and you register it in Host View, it is removed from the Host View and moved to Topology View after the first poll. It is also removed from the Concurrent License count once it is recognized as an Access Point.
Notes	Free form notes entered by the Administrator.
Security and Access Attribute Value	This value can be included in a filter when determining the Security Policy that should scan this host when it connects to the network. If a directory is in use and a user is associated with this host, the value comes from the directory when it is synchronized with the database. Otherwise the value can be entered manually.
Adapters	Lists the adapters or network interfaces that exist on this host. By listing all adapter's on the host here, you establish that these adapters are siblings. Number of adapters per host is limited to **five**. See Edit adapters below. **Physical Address** — MAC Address of the adapter **Media Type** — Indicates whether the adapter is wired or wireless.

Edit adapters



Physical Address: 00:0B:7D:19:AF:EB

Media Type: Wired

Description: Primary Connection

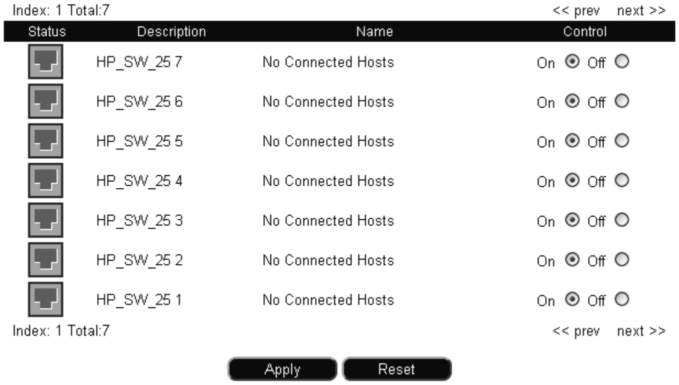
1. Go to the Adapter section of the Add or Modify Host Window.
2. To Add an Adapter: Click the **Add** button and provide the **Physical Address** and the **Media Type**, such as wired or wireless.
3. To Modify an Adapter: Select an Adapter and click the Modify button. Change the Media Type as needed. To change the Physical Address you must delete the adapter and add it again.
4. To Delete an Adapter: Click on the Adapter to select it and click **Delete**.
5. Click **OK** to save.

The number of adapters per host is limited to five.

View hosts and ports

1. Select **Bookmarks > Manage Hosts & Ports**.
2. Click the appropriate host group and then click Apply.
3. A list of hosts contained in the selected group is displayed. The host information shown includes Status, Name, IP address, Description of the device and port where the host is connected, and On/Off control for the port.
4. Click the host name to view the Properties on page 801.
5. Click the Description to view the Port properties on page 784.
6. Click On or Off to turn the port on or off.
7. Click Apply if any changes are made to the On/Off status of the port.

View and manage ports



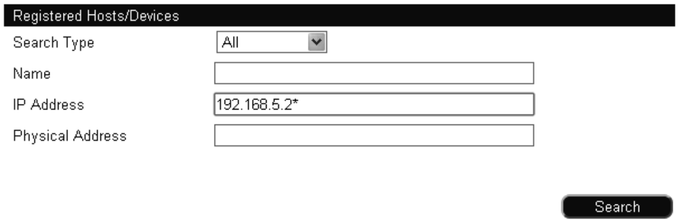
Index: 1 Total:7 << prev next >>

Status	Description	Name	Control
▣	HP_SW_25 7	No Connected Hosts	On ● Off ○
▣	HP_SW_25 6	No Connected Hosts	On ● Off ○
▣	HP_SW_25 5	No Connected Hosts	On ● Off ○
▣	HP_SW_25 4	No Connected Hosts	On ● Off ○
▣	HP_SW_25 3	No Connected Hosts	On ● Off ○
▣	HP_SW_25 2	No Connected Hosts	On ● Off ○
▣	HP_SW_25 1	No Connected Hosts	On ● Off ○

Index: 1 Total:7 << prev next >>

1. Select **Bookmarks > Manage Hosts & Ports**.
2. Click a port group and then click **Apply**.
3. A list of ports contained in the selected group is displayed. The port information shown includes Status, Description of the port, Name of the connected host (if any), and On/Off control for the port.
4. Click the **Status** icon to view the Connection details for the port.
5. Click the **Description** to view the Port properties on page 784.
6. Click **On** or **Off** to turn the port on or off.
7. Click **Apply** if any changes are made to the On/Off status of the port.

Locate



Registered Hosts/Devices

Search Type	All
Name	
IP Address	192.168.5.2*
Physical Address	

Click **Bookmarks > Locate** on the Dashboard to locate devices, users or hosts. Enter information in any or all of the fields.

Locate devices or hosts

1. Select **Bookmarks > Locate**.
2. Select a search type.

Search Type	Description
All	This option searches for both devices and hosts. To reduce the number of returned records, use the Devices or Host/User searches.
Devices	Use this option to locate network devices.
Host/User	Use this option to locate hosts or users.

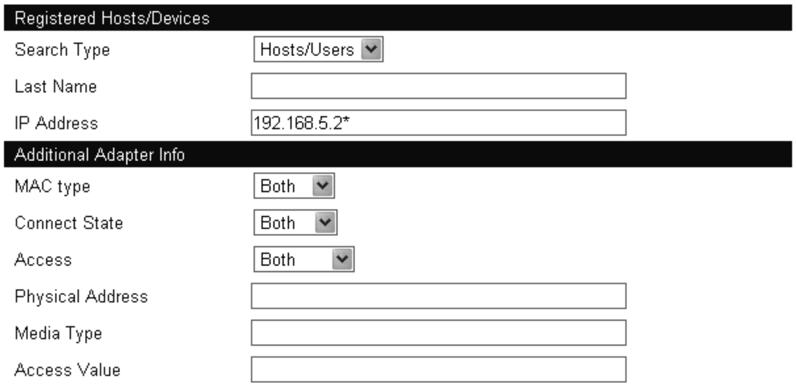
3. Enter the search criteria.

To reduce the potential for a significant number of records being returned in the Search Results, you must enter a value into one of the search fields.

If the Search Type is set to All and you enter data in the Name field, FortiNAC searches for User Last Names and Network Device Names.

4. Click **Search**.

Locate hosts and users



Registered Hosts/Devices

Search Type	Hosts/Users
Last Name	
IP Address	192.168.5.2*

Additional Adapter Info

MAC type	Both
Connect State	Both
Access	Both
Physical Address	
Media Type	
Access Value	

This window can be used to search your database for hosts and users of many types. Guests, contractors and conference attendees are also considered users and can be located using this window or through the Guest/Contractor Accounts window. See Guest or contractor accounts on page 592.

You cannot locate guest or contractor accounts until the account is automatically created on the specified date. For example, a contractor account scheduled for March 1 cannot be located until that date.

Use the Locate window to:

- Check that a record for a host exists.
- See where the host is on the network.
- Check the Connect Status and Access of the host.
- Search for a Registered Host by MAC address to see where it is on the system.
- Use wild cards to search for hosts or users. See Wild cards on page 17 for additional information.

Locate hosts

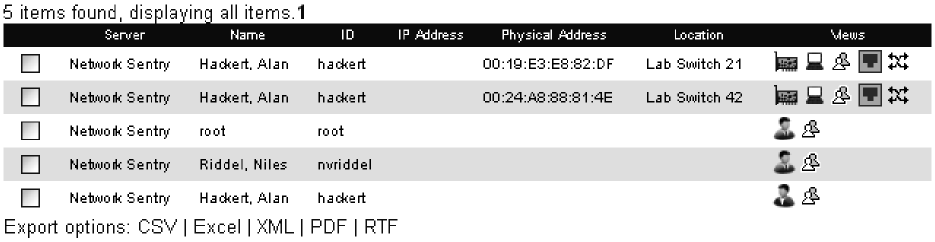
1. Select **Bookmarks > Locate**.
2. Select **Hosts/Users** from the **Search Type** drop-down list.
3. Enter the **Search** criteria.
4. Click **Search**.

Search fields

Field	Description
Registered hosts/devices	
Last Name	Last name of a user associated with the registered host or the vendor name of a rogue host.
IP address	IP address of the host.
Additional adapter info	
MAC Type	MAC Type for the host. The available options are: Invalid, Valid or Both.
Connect State	Connect State of the adapter. Options include: Both, Off line or On line.
Access	Access state of the adapter. Options include, Enabled, Disabled or Both.
Physical Address	MAC Address of the adapter on the host.
Media Type	Searches the Media Type field in the Adapter Properties. Typically this would be either wired or wireless.
Access Value	Name or number of the Network Access identifier given to this adapter based on the state of the host and the device to which the adapter is connected, such as VLAN ID, VLAN Name or Aruba Role.
Additional host info	
Host Name	Name of the host.
Agent Version	Version number of the Persistent, Mobile or Dissolvable Agent on the host.
Operating System	Operating system on the host.

Field	Description
Hardware	Hardware type of the host.
Host Type	Narrow the search by a specific type of host: All, IP Phone, Registered or Rogue.
Authenticated State	Include hosts on which a user has Authenticated, Not-authenticated or Both.
Security State	Include hosts that are Safe, At Risk, Pending At Risk or All. Note: Search results for Safe hosts include Pending At Risk hosts. Pending At Risk is a sub-set of Safe hosts.
Persistent Agent	The Persistent Agent usage of the host. Options include: • **No Agent** — Hosts with no agent. • **Agent** — Hosts using the Persistent Agent. • **Both** — Includes both hosts that have the Persistent Agent or no Agent.
Connect State	The Connect State of the adapter. Options include: Both, Off line or On line.
Access	The Access state of the host. Options include, Enabled, Disabled or Both.
Host Role	Name of the Role assigned to the host. Roles are used to group hosts and are used as filters in User/Host Profiles.
Security & Access Value	Directory Attribute used as a filter when determining which policies apply to hosts. Data contained in this field is copied from the user's account in the directory to the Security and Access value field on the User, Host and Adapter Properties. It can also be entered manually.
Additional user info	
First Name	First name of the user associated with the host.
User ID	Unique alphanumeric ID. Typically comes from the directory but if you are not using a directory, this field can be created manually.
Title	User's title, this could be a form of address or their title within the organization.
Admin Profile	Searches both Admin Users and network users. Options include: Any or a list of your Admin Profiles. To search network users and guests or contractors, select Any.
Sponsor	If the administrative user performing the search has Sponsor privileges, his User Name may be filled in this field. Depending on permissions, a Sponsor's search may be limited to the hosts he created and then registered. Sponsors with the ability to view all accounts can use this field to find hosts created and then registered by a specific Sponsor by entering that Sponsor's User Name in this field.
User Role	Name of the Role assigned to the user. Roles are used to group users and as filters in User/Host Profiles.
Access	The Access state of the user. Options include, Enabled, Disabled or Both.
Security & Access Value	Directory Attribute used as a filter in User/Host Profiles when determining which Policies apply to hosts. Data contained in this field is copied from the user's account in the directory to the Security and Access value field on the User, Host and Adapter Properties. It can also be entered manually.

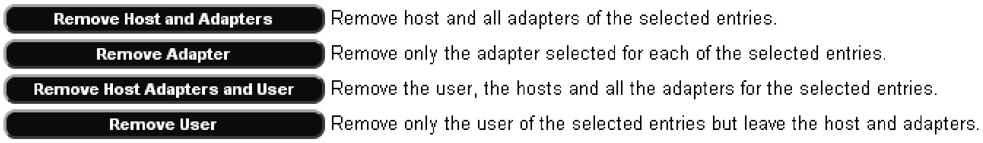
Search results



5 items found, displaying all items.1

	Server	Name	ID	IP Address	Physical Address	Location	Views
☐	Network Sentry	Hackert, Alan	hackert		00:19:E3:E8:82:DF	Lab Switch 21	
☐	Network Sentry	Hackert, Alan	hackert		00:24:A8:88:81:4E	Lab Switch 42	
☐	Network Sentry	root	root				
☐	Network Sentry	Riddel, Niles	nvriddel				
☐	Network Sentry	Hackert, Alan	hackert				

Export options: CSV | Excel | XML | PDF | RTF



Remove Host and Adapters Remove host and all adapters of the selected entries.

Remove Adapter Remove only the adapter selected for each of the selected entries.

Remove Host Adapters and User Remove the user, the hosts and all the adapters for the selected entries.

Remove User Remove only the user of the selected entries but leave the host and adapters.

Search results displays the host and user information and provides access to other host-specific information such as Adapter Properties, Host Properties, Group Membership, Port Properties, and Device Properties. Admin Users can delete hosts, adapters and users from this view.

Column	Description
Server	Server managing the host.
Name	Last name of the user (from the user record), host name or Vendor name. This column could contain any combination of this data.
ID	ID of the host or user.
IP address	IP address of the host.
Physical Address	MAC address of the host.
Location	Device the host is connected to, such as a switch or a router.
Views	Icons that provide access to other related information. Click an icon to go to that view from the results window. Options include: Adapter Properties, Host Properties, Group Membership, Ports Properties and Device Properties.
Remove Buttons	Click the one or more check boxes in the left column to select items for deletion. Selected are removed items from the server where they were being managed. Note: Only Administrator users can delete. Remove options are as follows: • **Remove Host And Adapters** — Deletes the selected host and all corresponding adapters. If a host has a wired and a wireless adapter, both are removed from the database. • **Remove Adapter** — Deletes only the selected adapter but leaves the host record, other adapter records and the user record in the database. • **Remove Host Adapters And User** — Deletes everything associated with the selected host from the database. • **Remove User** — Deletes the user associated with the selected host from the database.

Edit hosts

After searching for hosts using the Locate view, you are presented with a list of results. From within that list you can delete hosts, users and adapters, edit group membership and view adapter properties.

Delete hosts

1. Login as an Administrator user.
2. Select **Bookmarks > Locate**.
3. Enter the search criteria in the Locate view.
4. In the search results, select the check box next to the record(s) to be deleted.
5. Click the appropriate **Remove** button at the bottom of the window. See the button definitions shown in .

View or modify group membership

1. Select **Bookmarks > Locate**.
2. Enter the search criteria in the Locate view.
3. Go to the **Views** column in the search results and click the **Group Membership** icon.
4. The groups that contain this host or user are displayed.
5. Add or remove groups as needed and click **Apply** to save changes.

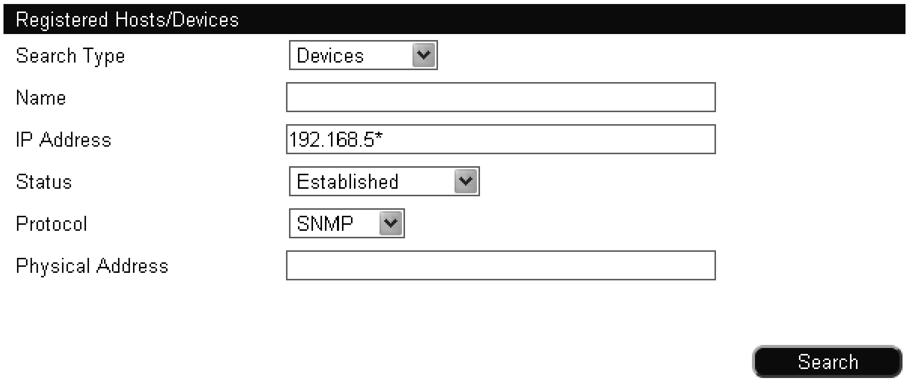
If an item is placed in a subgroup, it can only be removed when viewing the membership of that subgroup. It cannot be removed from the parent group containing the subgroup.

For example, the L2 Network Devices Group contains the Wired Devices and Wireless Devices subgroups. The Wired Devices subgroup contains four 3COM switches. The Wireless Devices subgroup contains two Cisco switches.The L2 Network Devices Group membership list shows all six switches, but to remove one of the 3COM switches you must go to the Wired Devices membership list.

View properties

1. Select **Bookmarks > Locate**.
2. Enter the search criteria in the Locate view.
3. Go to the **Views** column in the search results and click the **Properties** icon.
4. The properties for the selected adapter, host or user are displayed.

Locate devices



Registered Hosts/Devices

Search Type	Devices
Name	
IP Address	192.168.5*
Status	Established
Protocol	SNMP
Physical Address	

1. Select **Bookmarks > Locate**.
2. Select **Devices** from the **Search Type** drop-down list.
3. Enter the Search criteria.
4. Click **Search**.

Device search fields

Field	Definition
Name	Name of the device.
IP address	IP address of the device.
Status	The status of the device: **Any** — Show device regardless of current status. **Management Lost** — System is still in contact with the server, but the server is not managing anything. **Lost** — Cannot ping a known device. **Unknown** — Very brief status that only occurs while pinging a new device. Once the device responds to the ping the status changes. **Established** — Device can be pinged and is in contact.
Protocol	Protocol used to communicate with the device. Options include: Pingable, SNMP or Both.
Physical Address	Physical Address (MAC) of the device. If you enter a value for this option in the All or Device search, all of the device ports with a matching MAC address are shown in the results. If you do not enter a MAC address, only the device model is shown in the results.

Results

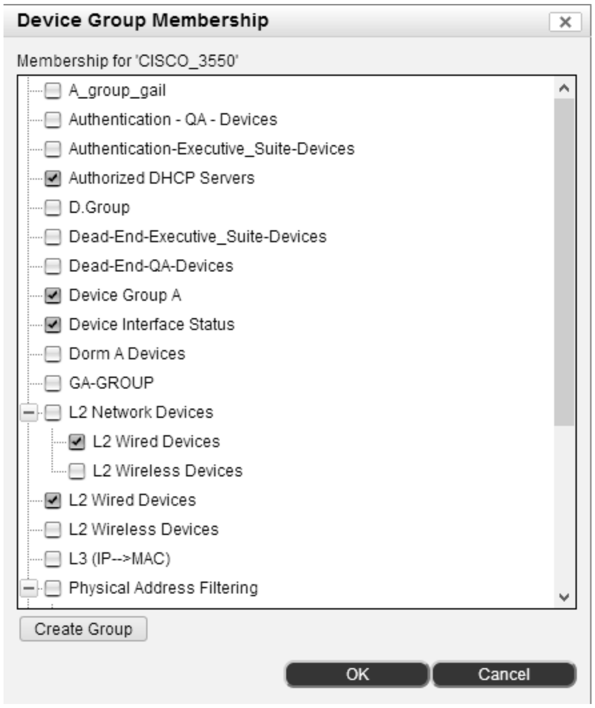
Device Search results displays the devices found and provides access to other device specific information such as Device Properties, Device Group Membership, and Ports and Hosts.

Field	Definition
Server	Name of the FortiNAC Control Server where the device is located.
Name	Name of the device.
IP address	IP address of the device.
Physical Address	MAC address of the device.
Type	Device type (vendor name/model).
Status	Contact status of the device.
Views	Icons that provide access to device specific views. Click an icon to go to that view from the results window. Options include: Device Properties, Device Group Membership and Ports and Hosts.

Edit devices

After searching for devices using the Locate View, you are presented with a list of results. From within that list you can edit device group membership, view device properties and view the port and hosts associated with the selected device.

View/modify device group membership



Membership for 'CISCO_3550'

- ☐ A_group_gail
- ☐ Authentication - QA - Devices
- ☐ Authentication-Executive_Suite-Devices
- ☑ Authorized DHCP Servers
- ☐ D.Group
- ☐ Dead-End-Executive_Suite-Devices
- ☐ Dead-End-QA-Devices
- ☑ Device Group A
- ☑ Device Interface Status
- ☐ Dorm A Devices
- ☐ GA-GROUP
- ☐ L2 Network Devices
  - ☑ L2 Wired Devices
  - ☐ L2 Wireless Devices
- ☑ L2 Wired Devices
- ☐ L2 Wireless Devices
- ☐ L3 (IP-->MAC)
- ☐ Physical Address Filtering

1. Select **Bookmarks > Locate**.
2. Enter the search criteria in the Locate Devices view.
3. Go to the **Views** column in the search results and click the **Group Membership** icon.

4. The group properties for the selected device are displayed.
5. Add or remove groups as needed and click **Apply** to save changes.

If an item is placed in a subgroup, it can only be removed when viewing the membership of that subgroup. It cannot be removed from the parent group containing the subgroup.

For example, the L2 Network Devices Group contains the Wired Devices and Wireless Devices subgroups. The Wired Devices subgroup contains four 3COM switches. The Wireless Devices subgroup contains two Cisco switches. The L2 Network Devices Group membership list shows all six switches, but to remove one of the 3COM switches you must go to the Wired Devices membership list.

View device properties

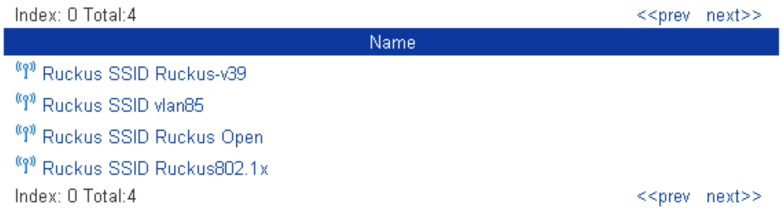
1. Select **Bookmarks > Locate**.
2. Enter the search criteria in the Locate Devices view.
3. Go to the **Views** column in the search results and click the **Device Properties** icon.
4. The properties for the selected device are displayed.

View device ports and hosts

The Device Ports and Hosts results contain VLAN (Current and Default) and Host (Name and IP) information for each port on the device.

1. Select **Bookmarks > Locate**.
2. Enter the search criteria in the Locate Devices view.
3. Go to the **Views** column in the search results and click the **Ports and Hosts** icon.
4. The ports and hosts for the selected device are displayed.

View SSIDs



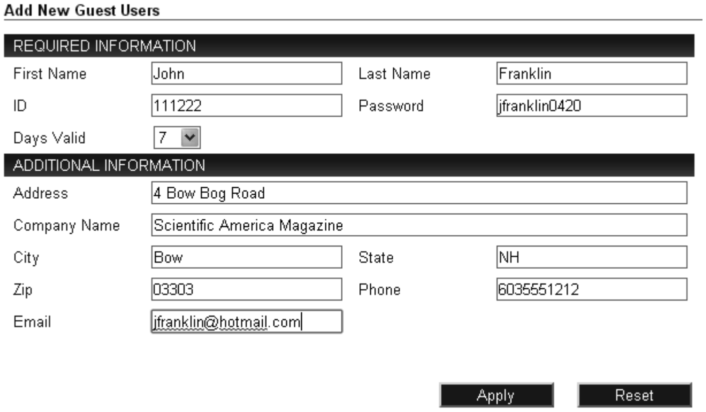
Index: 0 Total:4 <<prev next>>

Name
Ruckus SSID Ruckus-v39
Ruckus SSID vlan85
Ruckus SSID Ruckus Open
Ruckus SSID Ruckus802.1x

Index: 0 Total:4 <<prev next>>

All SSIDs on the device are listed with the current and default VLAN setting. If a host is connected on a port, the adapter MAC Address and IP information are also displayed.

Guest accounts



Add New Guest Users

REQUIRED INFORMATION

First Name	John	Last Name	Franklin
ID	111222	Password	jfranklin0420
Days Valid	7		

ADDITIONAL INFORMATION

Address	4 Bow Bog Road		
Company Name	Scientific America Magazine		
City	Bow	State	NH
Zip	03303	Phone	6035551212
Email	jfranklin@hotmail.com		

This option allows you to create accounts for guests visiting your facility. It provides a user name and password for each guest. Guests are authenticated through FortiNAC. Administrators, Operators and Help Desk Users all have permission to create guest accounts.

The Guest Account option is not available if you are using the Guest Manager feature. The Guest Manager feature provides extensive guest creation and management options.

Add a guest account

Guest accounts can be viewed and modified in the Users View. Guest accounts are provided with a default Security and Access value of "guest" allowing you to use this as a filter for User/Host Profiles. When a guest matches a profile the guest receives the Endpoint Compliance Policy associated with that profile. You can use the same User/Host Profile to assign a Network Access Policy and assign guest hosts to a VLAN. See Endpoint compliance policies on page 415 and Network access policies on page 407 for additional information.

1. Select **Bookmarks > Guest Account**.
2. If you do not see a Guest Account option it may be because the Guest Manager feature is enabled.
3. Enter the guest's **First** and **Last** names. The Last Name field is the guest's user name at login and is required.
4. Enter an **ID**. This field is required.
5. Enter a **Password**. This field is required.
6. Select the number of days this account will be valid from the Days Valid drop-down. Options are 1, 7 or 28. This controls the number of days that the guest record remains in the database. After the selected number of days has elapsed the guest's record is deleted.
7. The information in the **Additional Information** section of the window is optional. Complete any fields required by your organization.
8. Click **Apply** to save the guest account.

When a guest connects to the network and reaches the login page, the last name is used as the user name. If you are using the Version 1 Portal pages, you can edit the .html files directly to modify the labels on the fields on the login page.

If you have disabled the Version 1 Portal pages and are using the portal pages that shipped with FortiNAC, the field labels can be modified using the Content Editor in the Portal Configuration window.

Portal page requirements

If you are using your Version 1 Portal pages and you already have guest pages set up, you do not need to make any modifications. If you have disabled the Version 1 Portal pages and chosen to use the Portal pages provided with FortiNAC, there are a few fields that must be edited to allow guests to login using accounts created with the Guest Account tab on the Dashboard. These options do not apply to guest accounts created with Guest Manager.

If you are using local authentication for guests, do not enable the First Name and Last Name fields on the Custom Login Form. Information entered by guests at login in these fields is added to the database and will modify their authentication credentials. Guests would no longer be able to log in with their original credentials.

Configure guest login

The Guest Login designated in the Portal Configuration Content Editor is used to configure settings for Guest Manager. If you are not using Guest Manager you must disable that login and enable the Custom Registration login.

1. Select **System > Portal Configuration**.
2. Click the **Show Advanced Settings** check box to display all of the configuration tabs.
3. Click on the **Content Editor** tab.
4. Click on **Registration** in the left hand pane to expand it.
5. Click on **Login Menu** within Registration. The properties for that page are displayed in the right pane.
6. Scroll down to the **Guest Login Enabled** check box and remove the check mark.
7. Scroll to the **Custom Registration Enabled** check box and mark it with a check mark.
8. Scroll to the **Custom Registration Link Text** field and enter the text for the link to the Guest Login page, such as Guest Login or Guest Registration.
9. Scroll to the **Custom Registration Title** field and enter the text that should display above the link to the Guest Login page.
10. Click **Apply** to save your changes. When changes are made to the portal pages there is a delay before the changes are displayed.

Configure guest authentication

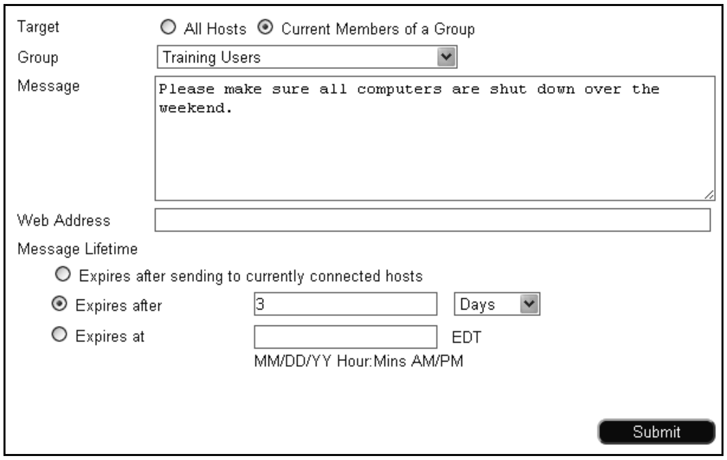
1. Select **System > Portal Configuration**.
2. Click the **Show Advanced Settings** check box to display all of the configuration tabs.
3. Click on the **Content Editor** tab.
4. Click on **Global** in the left hand pane to expand it.
5. Click on **Settings** within Global. The properties for that page are displayed in the right pane.
6. Scroll down to **Custom Login Type** and select **Local** from the drop-down menu.
7. Click **Apply** to save your changes. When changes are made to the portal pages there is a delay before the changes are displayed.

Modify user name field label

When Guest Accounts are created, the guest's last name is considered the User Name for login. The Login page asks for User Name and Password. You can either advise your guests that their last name is their user name or you can modify the Login page and set the label appropriately.

1. Select **System > Portal Configuration**.
2. Click the **Show Advanced Settings** check box to display all of the configuration tabs.
3. Click on the **Content Editor** tab.
4. Click on **Registration** in the left hand pane to expand it.
5. Click on **Custom Login Form** within Registration. The properties for that page are displayed in the right pane.
6. Scroll to the **User Name Field Label** field and change the label to Last Name or some other user-specified name.
7. Click **Apply** to save your changes. When changes are made to the portal pages there is a delay before the changes are displayed.

Send messages to hosts



Target ○ All Hosts ● Current Members of a Group

Group Training Users

Message Please make sure all computers are shut down over the weekend.

Web Address

Message Lifetime

○ Expires after sending to currently connected hosts

● Expires after 3 Days

○ Expires at EDT

MM/DD/YY Hour:Mins AM/PM

Use the Send Message option on the Bookmarks menu to send a real-time message to all hosts. This provides a method for you to get a message directly to the desktop of the selected hosts.

User can send messages to hosts with the Persistent Agent or Mobile Agent installed.

See Send a message to a host on page 814 in the Host Properties section for details on sending a message to an individual host.

1. Select **Bookmarks > Send Message**.
2. Click **All Hosts** to send the message to all hosts, or click Group and select a group of hosts to receive the message.

The message is sent only to the members of the selected group. Hosts who register and are assigned to the group after the message is sent will not receive the message, even if the message is still active.

3. Enter the message in the **Message** block.
4. If desired, enter a **Web Address** that will be sent as part of the message. Make sure the web address includes the http:// or ftp:// or other information. The page must also be in a location that the host(s) can access from their current VLAN, such as Remediation, Quarantine, Dead End, or other.
5. Click the radio button next to a **Message Lifetime** option and enter the information.

The server can only send messages to hosts with which it is communicating. If you have entered an expiration date and time, hosts who connect or communicate before that date and time also receive the message.

Message Lifetime Options	Description
Expires after sending to currently connected hosts	The message expires immediately after it has been sent.
Expires after	The message expires after the specified amount of time. Enter a number and select the timeframe of Minutes, Days, or Hours. The message remains active on the server for the selected timeframe. The server sends the message the next time it communicates with a host as long as communication occurs before the message expires.
Expires at	The message expires on the specified date and time. The format is MM/DD/YY hh:mm AM/PM. The message remains active on the server until the specified date and time. The server sends the message the next time it communicates with a host as long as communication occurs before the message expires.

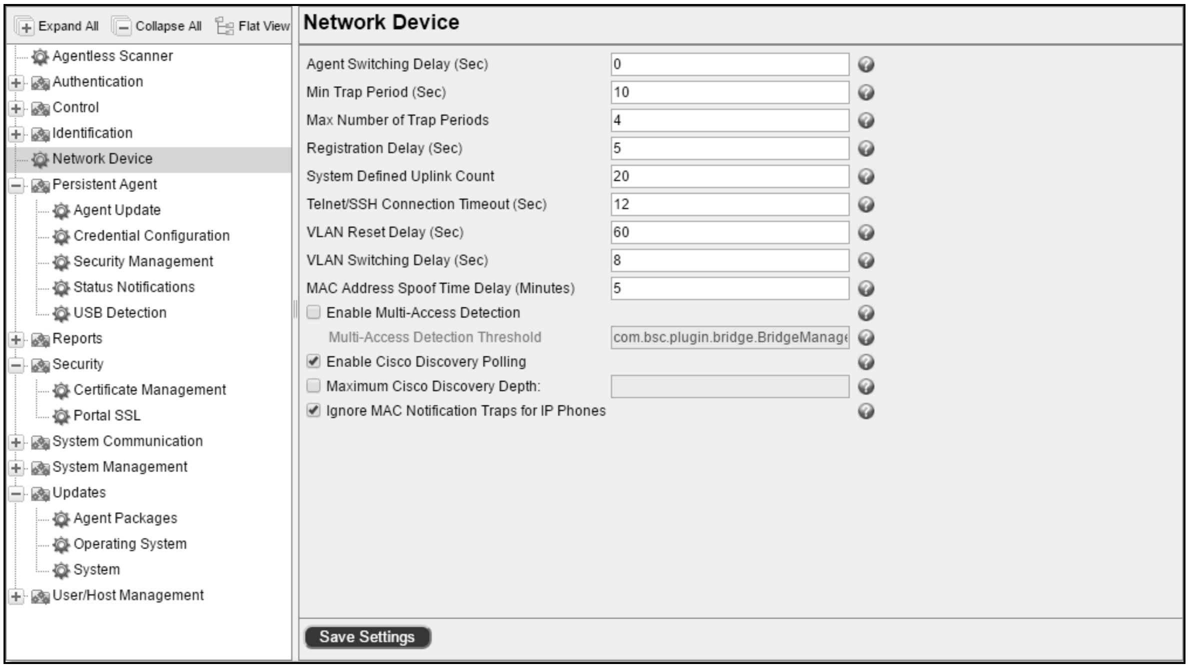
6. Click **Submit**.

Settings

The Settings View provides access to global system configuration options, such as Aging properties to remove hosts and users from the database or email settings for emailing users and administrators.

The Settings View is navigated using the tree control on the left side. The top level of the hierarchy represents the general configuration area, such as Authentication or System Communication. These areas are used to group similar functions. When a top level option such as Authentication is selected, the panel on the right contains a list of links to options that can be configured. For example, if Authentication is selected, the links provided include: Google, LDAP and RADIUS, and Roaming Guests. These options are also displayed below Authentication in the tree.

Use the **Flat View** button above the tree to list all of the options in alphabetical order instead of grouped in folders. Use the **+ Expand All** and **- Collapse All** buttons at the top of the tree to open and close all of the folders. Click on the **+** symbol next to a folder to open it. Click on the **-** symbol to close the folder. Click on an option to display the corresponding configuration panel on the right.



Network Device

Agent Switching Delay (Sec) 0
Min Trap Period (Sec) 10
Max Number of Trap Periods 4
Registration Delay (Sec) 5
System Defined Uplink Count 20
Telnet/SSH Connection Timeout (Sec) 12
VLAN Reset Delay (Sec) 60
VLAN Switching Delay (Sec) 8
MAC Address Spoof Time Delay (Minutes) 5
☐ Enable Multi-Access Detection
Multi-Access Detection Threshold com.bsc.plugin.bridge.BridgeManage
☑ Enable Cisco Discovery Polling
☐ Maximum Cisco Discovery Depth:
☑ Ignore MAC Notification Traps for IP Phones

Options

Option	Description
Authentication	
Google	Use Google to configure the connection to authenticate using a Google account. See Google authentication on page 76
LDAP	Configure the connection with one or more LDAP directories for user authentication. See Directories on page 79 and Configuration on page 82.

Option	Description
RADIUS	Set up RADIUS servers for authentication. See RADIUS on page 102.
Roaming Guests	Set up a list of local domains. Users with login credentials that contain domains outside the list are treated as Roaming Guests. See Roaming guests on page 110.
Control	
Access Point Management	Provides the ability to manage hosts connected to hubs using DHCP as a means to control or restrict host access. See Access point management on page 112.
Allowed Domains	Specify the domains and Production DNS Server that isolated hosts use to gain access to network locations. See Allowed domains on page 114.
Quarantine	When Quarantine VLAN Switching is set to Enable and the ports are in the Forced Remediation Group,FortiNAC switches unregistered hosts that are being scanned to the Quarantine VLAN until the scan process is completed. See Quarantine on page 117.
Identification	
NAT Detection	Enter the IP ranges where FortiNAC will allow NAT'd hosts. IP addresses outside this range could be NAT'd hosts and can generate an event and an alarm to notify the network administrator. See NAT detection on page 118.
Rogue DHCP Server Detection	Monitors approved DHCP servers operation and detects rogue DHCP servers on the network using a dedicated interface on the FortiNAC appliance. It defines a scheduled task to run and search specific VLANs and discover all active entities serving IP addresses. This task compares the discovered DHCP servers against a list of authorized DHCP servers and triggers corresponding events when there is no match. See Rogue DHCP server detection on page 122.
Vendor OUIs	Allows you to modify the Vendor OUI database, which is used to determine whether or not a MAC address is valid or by Device Profiler to profile devices by OUI. The database is updated periodically through the Auto Definition update process. See Vendor OUIs on page 127.
Network Device	
Network Device	Set global properties that are specific to network devices and VLANs. See Network device on page 130.
Persistent Agent	
Agent Update	Enable Persistent Agent updates by Operating System, schedule agent updates and add hosts to the list of Update Exceptions. You can update agents on both platforms simultaneously or separately.

Option	Description
	See Global updates on page 134
Credential Configuration	Configure how credentials are verified for hosts who use the Persistent Agent. See Credential configuration on page 139.
Security Management	Configure the FortiNAC server name of the server for Persistent Agent communication, enable or disable display notifications to the host, configure Header and footer text for the Persistent Agent Authentication page and Status messages in the message box on the user's desktop. See Security management on page 140.
Status Notifications	Configure how users are notified of their host status when the Persistent Agent contacts the FortiNAC server. See Status notifications on page 145.
Reports	
Local Reporting	Set record limits for reports to prevent the server from being overloaded. See Reports on page 155.
Analytics	Configure the connection between the FortiNAC server and the cloud reporting Analytics server. This connection allows an agent on the FortiNAC server to push data for reporting to an external server based on a user-defined schedule. See Reports on page 155.
Security	
Portal SSL	Enable or disable the use of SSL Certificates in the Portal or for Agent server communications. See Portal SSL on page 158.
System Communication	
Email Settings	Enter settings for your email server. This allows FortiNAC to send email to Administrators and network users. See Email settings on page 169.
Log Receivers	Configure a list of servers to receive event and alarm messages from FortiNAC. See Log receivers on page 169.
MDM Services	Configure one or more Mobile Device Management (MDM) servers that integrate with FortiNAC. See MDM services on page 172.
Mobile Providers	Displays the default set of Mobile Providers included in the database. FortiNAC uses the Mobile Providers list to send SMS messages to guests and administrators . The list can be modified as needed. See Mobile providers on page 175.
Patch Management	The Patch Management feature allows integration with Patch servers such as BigFix or PatchLink. See Patch management on page 178.

Option	Description
Proxy Settings	Configure FortiNAC to direct web traffic to a proxy server in order to download OS updates and auto-definition updates.
SNMP	Set the SNMP protocol for devices that query FortiNAC for information. It is also used to set the SNMP protocol to accept SNMPv3 traps that register hosts and users. See SNMP on page 186.
Syslog Files	Syslog Files that you create and store are used by FortiNAC to parse the information received from these external devices and generate an event. The event can contain any or all of the fields contained in the syslog output and can be mapped to an Alarm and an Alarm action. See Syslog management on page 190 and Map events to alarms on page 888.
Trap MIB Files	Enter configurations to interpret SNMP trap MIB information sent from a device and associate it with events and alarms in FortiNAC. See Trap MIB files on page 202 and Map events to alarms on page 888.
System Management	
Database Archive	Set the age time for archived data files and configure the schedule for the Archive and Purge task. See Database archive on page 210.
Database Backup/Restore	Schedule database backups, configure how many days to store local backups, and restore a database backup. Note that this restores backups on the FortiNAC server, not backups on a remote server. See Backup/restore a database on page 213.
High Availability	Configuration for Primary and Secondary appliances for High Availability. Saving changes to these settings restarts both the Primary and Secondary servers. See High availability on page 217.
License Management	View or modify the license key for this server or an associated Application server. See License management on page 215
NTP And Time Zone	Reset the time zone and NTP server for your FortiNAC appliances. Typically the time zone and NTP server are configured using the Configuration Wizard during the initial appliance set up. Requires a server restart to take effect. See The NTP server is used to synchronize the clock on the FortiNAC appliance. FortiNAC contacts the NTP server periodically to synchronize its clock with the NTP servers. NTP server keeps time in UTC or Coordinated Universal Time, which corresponds roughly to Greenwich Mean time. on page 216.
Power Management	Reboot or power off the FortiNAC server. In the case of a FortiNAC Control Server / Application Server pair, reboot or power off each server individually. See Power management on page 219.
Remote Backup Configuration	Configure Scheduled Backups to use a remote server via FTP and/or SSH. See Backup to a remote server on page 220.

Option	Description
System Backups	Create a backup of all system files that are used to configure FortiNAC. See System backups on page 223.
Updates	
Agent Packages	Displays a list of the Dissolvable, Persistent and Passive Agent versions available on your FortiNAC appliance. Download new agents and add them to FortiNAC as they become available from Fortinet using the Download button. Download an Administrative template for GPO configuration to your PC from the FortiNACappliance using the links at the top of the view. See Agent packages on page 226.
Operating System	Use Operating System Updates to download and install updates to the operating system on FortiNAC servers. See Updating CentOS on page 235.
System	Use System Updates to configure download settings, download updates from Fortinet, install updates and view the updates log. See System update on page 238.
User/Host Management	
Aging	Configure default settings to age users and hosts out of the database. See Aging on page 242.
Allowed Hosts	Configure the default number of hosts that can be registered to a user. See Allowed hosts on page 244.
Device Profiler	Enable or Disable creating rogues from DHCP packets heard on the network. See Device profiler on page 245.
MAC Address Exclusion	Lists the MAC addresses that can be ignored by FortiNAC when they connect to the network. These addresses will not be treated as rogues and will be allowed on the production network. See MAC address exclusion on page 245.

Authentication

Authentication groups together options to configure the connection to authenticate using a Google account, to configure an LDAP directory to authenticate users, to configure RADIUS servers to authenticate users, and to configure a list of local domains for your local network users.

Enabling authentication allows the Administrator to determine whether or not hosts connecting to the network will be forced to authenticate. Hosts can be forced to reauthenticate after a specified period of time.

Once a host is registered the host connecting via a wired connection may or may not have to authenticate depending on what port is being used. Hosts connecting via a wireless connection will be forced to authenticate if an Authentication VLAN has been established. See Wireless integration on page 969 for more information.

Switches used in the Forced Authentication process must have a value entered for the Authentication VLAN in the model configuration. The ports on these switches must be added to the Forced Authentication group. See Groups view on page 838 for details on adding ports to a group.

Options

Option	Definition
Google	Use Google to configure the connection to authenticate using a Google account. See Google authentication on page 76.
LDAP	Use LDAP to configure the connection to one or more authentication directories. Data from the Directory populates the FortiNAC database with demographic data for registered users. See Directories on page 79.
RADIUS	Use RADIUS to configure the connection to one or more RADIUS servers for authentication. See RADIUS on page 102.
Roaming Guests	Use Roaming Guests to configure a list of local domains for your local network users. Users who connect and attempt to authenticate with a fully qualified domain name that is not on this list are treated as Roaming Guests. Applies only to wireless 802.1x connections. See Roaming guests on page 110.

Automatic authentication

For appliances with firmware 2.2.0.8 and above, hosts can be automatically authenticated during registration. This requires the use of either the Dissolvable or Persistent Agent. For details on the agents see the and Using the Persistent Agent on page 514 sections.

Dissolvable Agent

1. Enable Authentication. See Add or modify a policy on page 406 for details.
2. When the host downloads and runs the Dissolvable agent the host is automatically authenticated.

Persistent Agent

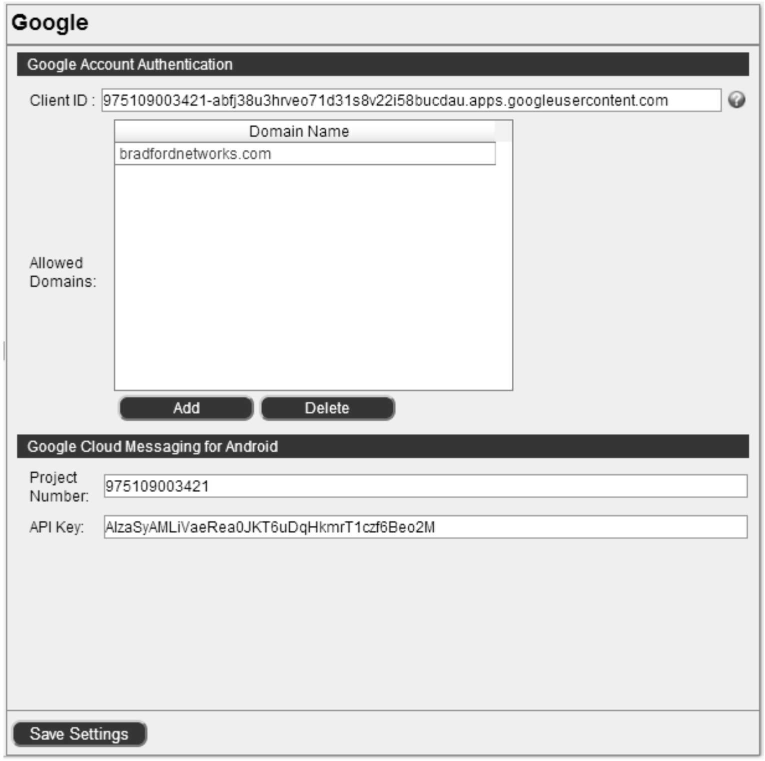
1. Enable Authentication. See Add or modify a policy on page 406for details.
2. When the host downloads and installs the Persistent Agent the host is automatically authenticated.

Google authentication

Google authentication allows users to authenticate using a Google account. When the settings are configured, the user logs into the network using the Google Sign In button instead of a username and password. When the user is authenticated, the user's email address (username and domain) is passed to FortiNAC to authenticate the user with the information.

Google Cloud Messaging for Android allows users to configure push notifications for the Mobile Agent.

You must first configure Google Authentication through the Google Developer's Console. See Google Developer's Console on page 78. Use the settings obtained during this process to configure Google Account Authentication.


Google
Google Account Authentication
Domain Name
Add
Delete
Google Cloud Messaging for Android
Save Settings

Client ID : 975109003421-abfj38u3hrveo71d31s8v22i58bucdau.apps.googleusercontent.com

Allowed Domains: bradfordnetworks.com

Project Number: 975109003421

API Key: AIzaSyAMLiVaeRea0JKT6uDqHkmrT1czf6Beo2M

Settings

Field	Definition
Google account authentication	
Client ID	The value provided by Google that allows FortiNAC to perform Google Authentication. The Client ID is generated during Google Authentication configuration using the Google Developers Console.
Allowed domains	The domains that have access to the network through Google Authentication.
Google Cloud Messaging for Android™	
Project number	The project number is generated during Google Authentication configuration. When the device registers with FortiNAC, the Project number is sent to the agent on the device, which is then used to identify FortiNAC when the agent registers with Google to receive messages.
API key	The API key is a unique code that identifies FortiNAC to Google.

Google Developer's Console

These instructions are current as of 6/21/2019. See https://developers.google.com/console/help/new/ for more information.

1. Log into https://console.developers.google.com using the Google account that you wish to use for FortiNAC integration.
2. Create a project (project number): https://support.google.com/cloud/answer/6251787?hl=en&ref_topic=6158848
3. Assign the project name.
4. Enter a unique project ID (e.g., FortiNAC<organization name>).

   Note the project number, which is required during FortiNAC configuration.

5. Enable APIs: https://support.google.com/cloud/answer/6158841?hl=en&ref_topic=6262490
   - Enable Google + API.
   - Enable Google Cloud Messaging for Android API.
6. Configure 0Auth Client ID: https://support.google.com/cloud/answer/6158849?hl=en&ref_topic=6262490
   - Application Type, selection will be **Web Application**.
   - Authorized Javascript Origins: enter the URL for your FortiNAC Portal (this will be the origin of all Google Authentication attempts).
   - Authorized Redirect URI: leave blank.

   Note the Client ID, which is required during FortiNAC configuration. Be sure to use the Client ID associated with the web application you created.

7. Configure the Server API Keys: https://support.google.com/cloud/answer/6158862?hl=en&ref_topic=6262490
   - Enter the effective external IP address of FortiNAC, and then click the Create button.

   Note the API Key, which is required during FortiNAC configuration.

Add or modify account settings

1. Click **System > Settings**.
2. Expand the **Authentication** folder.
3. Select **Google** from the tree.
4. Enter the Client ID obtained during Google Authentication configuration. See Google Developer's Console on page 78.
5. Click **Add** to enter the domains that will have access to the network.

It is not recommended that you use a common domain name, such as "google.com", because this will allow anyone with a generic Google account to have access to your network.

6. In addition, add the following domains to the Allowed Domains list. These domains will allow access in isolation in order to authenticate through Google:
   - mail.google.com
   - apis.google.com
   - googleapis.com
   - schemas.google.com
   - accounts.google.com
   - ssl.gstatic.com
   - oauth.googleusercontent.com
   - googlehosted.googleusercontent.com
7. Click **Save Settings**.
8. Click **System > Portal Configuration**.
9. Expand the **Global** folder.
10. Select **Settings** from the tree.
11. Select **Google** from the **Standard User Login Type** drop-down menu to enable Google to be the default login type for standard users.
12. Click **Apply**.

The Google Sign In button will appear on the portal when the user accesses the network.

Enable push notifications from Google Cloud Messaging

1. Click **System > Settings**.
2. Expand the **Authentication** folder.
3. Select **Google** from the tree.
4. Under **Google Cloud Messaging for Android**, enter the **Project Number** and **API Key** obtained during Google Authentication configuration.
5. Click **Save Settings**.

Directories

Use the Authentication Directories View to configure the connection with one or more LDAP directories. If you plan to use local authentication via the FortiNAC database or RADIUS authentication then this step is not necessary.

A directory is a database that contains the records of an organization’s members. You can organize the members into groups within the directory. If configured in FortiNAC the Directory can be used to authenticate network users. If you have chosen LDAP authentication in the Portal Configuration window, you must configure a Directory in FortiNAC. See Portal configuration on page 248 or Configure authentication credentials on page 272.

The Directory configuration validates the user and populates the user record in the FortiNAC databases with user-specific information before they are allowed access to the network. FortiNAC uses the LDAP protocol to communicate to an organization’s directory.

A user's record is made up of fields that contain information about the user such as first name, last name, and email address. The name of a field in a directory is defined by a schema. For example, the schema specifies that a user's first name is stored in a field with an attribute name of "givenName". This attribute name is used when retrieving a user's first name from the record. Attribute names can vary from directory to directory, so FortiNAC allows you to define your own fields. Users in an “ou” in the Directory are populated into a group in FortiNAC if the Distinguished Name (DN) attribute is entered in the Directory group attribute mappings view.

When an Admin Group is created in FortiNAC with the same name as a group being synchronized from a Directory, the Admin Group members will remain the same as the Directory group members. Therefore, if you add a non-Directory user to the Admin Group and then synchronize the Directory, the non-Directory user is removed from the Admin Group because the user is not a member of the Directory group.

Authenticate using a domain name

If you chose to authenticate using a domain name, you must consider the following:

- When a domain name is specified in the Directory Configuration view and the login includes the matching domain, authentication first uses both the user name and the domain name. If this authentication fails, no further authentications are attempted.
- When a domain name is specified in the Directory Configuration view and the login includes a domain that does not match the Directory Configuration view, the authentication immediately fails.
- When no domain is specified in the Directory Configuration view and the login includes a domain, authentication first uses the user name and the domain name. If this authentication fails, a second authentication is attempted using only the user name.
- Domain names must be an exact match. For example, if the Directory Configuration view specifies the domain as somedomain.com, a login of john.smith@it.somedomain.com is not authenticated because the domain specified is not an exact match.
- The table below provides a summary of the various formats which FortiNAC uses to interpret the Fully Qualified User Name and to identify the user portion (which can sometimes be a host), the domain portion and the separator.

Fully Qualified Username	User	Domain
user	user	no domain specified
user@domain.com	user	domain.com
user@domain	user	domain
domain\user	user	domain
domain.com\user	user	domain.com
host/machinename.domain.com	host/machinename	domain.com

The user portion can be further delimited by dots (e.g., first.last@hostname.domain.com).

Authenticate using domain names and multiple directories

If you are using multiple directories to authenticate users, you must consider the following:

- When one directory is configured and no domain is specified in the Directory Configuration view, authentication is attempted using the one directory.
- When multiple directories are configured and no domain is specified in the Directory Configuration view, authentication is attempted to all directories that are in the database. The order in which the directories are processed cannot be controlled, and the first directory that yields a successful authentication is used. Therefore, if settings such as Security & Access Attribute Value, Role, etc., are not identical between all configured directories, a user's network access can vary based on which directory settings are in effect. These settings will depend on the most recent Directory Sync.
- When multiple directories are configured, authentication is attempted against all directories without Domain configurations, or with Domain configurations matching the domain, if one is supplied. If a Domain is configured for the directory, the user must supply a matching value for their domain in order for authentication to be attempted to that directory.

Requirements

The following steps provide a basic outline for the procedures required to setup the Directory and its communication with FortiNAC.

1. Enable ping on the Directory Server itself. This allows FortiNAC to ping the Directory server and prevents the server Icon in the Network Device Summary panel on the dashboard from displaying an error as if it had lost contact when, in fact, it is in contact via LDAP.

   If you plan to use the top level (root) of the Directory tree as a Group search branch, make sure that you use Config Wizard to configure DNS in FortiNAC so that the IP address of the Directory can be resolved to the Directory's hostname. In addition, the IP address must be resolved by the Primary DNS server.

2. Set up the connection between the Directory application and FortiNAC. This step provides login information allowing FortiNAC to connect and communicate with the Directory. See Configuration on page 82.
3. Map directory data fields to FortiNAC data fields. This step allows you to import user and group information into your database.
4. Configure User and Group Search Branches.
5. Data in your directory can change frequently. Users could be added, removed or modified. Those changes need to be incorporated into your FortiNAC database. Create a schedule to synchronize the directory with the FortiNAC database. See Schedule synchronization on page 93.
6. If choosing to use SSL or TLS security protocols for communications with the LDAP directory, installing a security certificate isn't necessary in most cases. However, if needed, see Create a keystore for SSL or TLS on page 96.
7. If you choose to use logon/logoff scripts to register the host when a user logs on or off a domain, see Passive registration on page 96.

You may need to access your Directory using a separate interface to acquire login, group and user information.

If you create new users in the Directory, be sure not to assign a User ID that is the same as an existing user account or guest account in the FortiNAC database. Having duplicate User ID's will prevent one or both of the users from accessing the network.

Structure and synchronization

When synchronizing FortiNAC with a directory there are specific configuration tasks that must be completed. FortiNAC does not have a view into the structure of your directory, however, you must understand this structure to complete the configuration.

You may have your own application to view the attributes of your directory or there are some available on the Internet, such as, Active Directory Explorer, LDAP Administrator or Apache Directory.

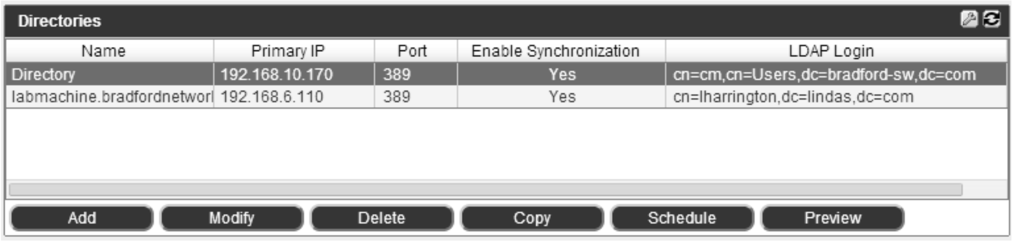
Configuration

The Directory Configuration window allows you to configure the connection to the directory, user attributes that you would like to import, User Search Branches and Group Search Branches. Each configuration section has specific information that must be entered to allow FortiNAC to connect with the Directory and import users and groups.

Use the Schedule button to configure the intervals for synchronizing the database with the selected Directory. Use the Preview button to review data in the selected Directory. Use the Copy button to pre-populate directory configuration fields for a new directory connection. Refer to for Settings.

Prior versions of FortiNAC did not always require a Physical Address for the Directory server. If you are modifying an existing Directory Configuration and that configuration does not have a Physical Address for the Directory server, you will not be able to save your changes until the Physical Address has been added.

Directory Configuration can be accessed from **System > Settings > Authentication > LDAP**.

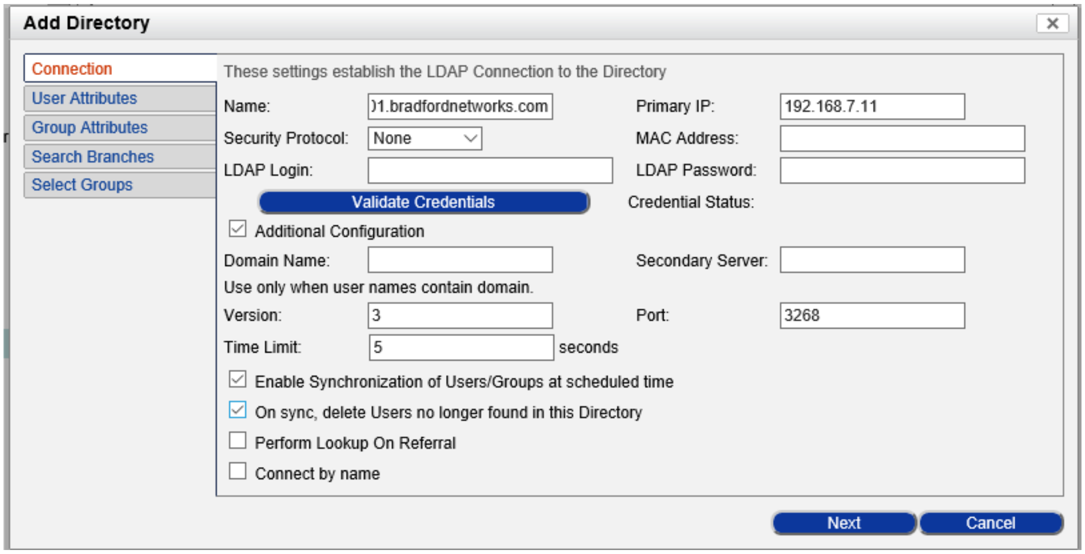


Directories

Name	Primary IP	Port	Enable Synchronization	LDAP Login
Directory	192.168.10.170	389	Yes	cn=cm,cn=Users,dc=bradford-sw,dc=com
labmachine.bradfordnetwor	192.168.6.110	389	Yes	cn=lharrington,dc=lindas,dc=com

Connection tab

The Connection tab contains the parameters required for communication with the Directory. Not all fields are required. Be sure to enter information only in those fields that apply to your directory.



Add Directory

Connection

User Attributes

Group Attributes

Search Branches

Select Groups

These settings establish the LDAP Connection to the Directory

Name:)1.bradfordnetworks.com

Primary IP: 192.168.7.11

Security Protocol: None

MAC Address:

LDAP Login:

LDAP Password:

Validate Credentials

Credential Status:

☑ Additional Configuration

Domain Name:

Secondary Server:

Use only when user names contain domain.

Version: 3

Port: 3268

Time Limit: 5 seconds

☑ Enable Synchronization of Users/Groups at scheduled time

☑ On sync, delete Users no longer found in this Directory

☐ Perform Lookup On Referral

☐ Connect by name

Settings

Field	Description
Name	Name of the server where the directory is hosted.
Primary IP	IP address of the primary directory server. The server will be added as a pingable device.
Security Protocol	The security protocol used when communicating with the server containing your directory. Options are SSL, STARTTLS, and None. See Create a keystore for SSL or TLS on page 96 for instructions on importing and storing certificates. If SSL or STARTTLS are chosen you must have a security certificate from a Certificate Authority. The certificate should be stored in the following directory on your appliance/bsc/campusMgr/
MAC Address	Physical Address of the primary directory server. This field is required.
LDAP Login	User login name FortiNAC uses to access the LDAP server.
LDAP Password	Password for the user login.
Validate Credentials	Click to verify that directory credentials are correct.
Credential Status	Displays the results of clicking the Validate Credentials button. Messages such as Credentials Verified or Failed to Validate can be displayed.
Additional Configuration	Displays the fields listed below in this table.
Domain Name	If this field contains a domain name, users must include the domain name in their login to be authenticated against this directory. **Example:**

Field	Description
	Valid formats for login are: user, user@domain.com and domain\user. Setting a value here requires all users to supply a domain name during login. When no domain is specified in the Directory Configuration view and the login includes a domain, authentication first uses the user name and the domain name. If this authentication fails, a second authentication is attempted using only the user name.
Secondary Server	FQDN or IP address of the secondary directory server. This server would be accessed in the event that the Primary server was unavailable. This server is added as a pingable device.
Version	Directory version. Default = 3
Port	Communication port used by the directory. The default port is based on the security protocol. To use a port other than the default, type the desired port number into this field. Common port values/protocols are: • None = 389 • SSL = 636 • STARTTLS = 389
Time Limit	Time in seconds that FortiNAC waits for a response from the directory. Default = 5. The number of seconds may need to be increased in the Directory or in FortiNAC if the exception “Time Limit Exceeded” begins to be noted more often.
Enable Synchronization of Users/Groups At Scheduled Time	Check this box to synchronize the FortiNAC database with either the Primary or the Secondary Directory servers based on a schedule in the Scheduler View.
on sync, delete Users no longer found in this directory	When checked, users that have been removed from the directory will be removed from the FortiNAC database when the scheduled resynchronization takes place.
Perform Lookup On Referral	Referrals allow administrators to set up search paths for collecting results from multiple servers. If you have configured your directory for referrals and you want to do authentication on the referred directory servers, enable this option.
Connect by Name	Automatically checked when StartTLS is selected as the Security Protocol. FortiNAC connects to LDAP using the the Name field of the Directory Configuration with a URL such as ldap://dc.example.com to connect to the primary server. When not selected, FortiNAC will connect to LDAP using the Primary IP address field of the Directory Configuration with a URL such as ldap://10.0.0.2.

The Administrator must enter the specific connection information for the Directory server used for user authentication. The Security information required varies depending on the type of directory you are using. Be sure to enter only the data required for your directory type.

The Directories View can be accessed either from **System > Settings > Authentication > LDAP**.

1. Click **System > Settings**.
2. Click the **Authentication** folder in the tree control.
3. Click **LDAP** to display the Directories window.
4. To Modify a directory, select a directory in the list and click **Modify**.

5. To Add a directory, click **Add**.
6. A list of directories found on your network is displayed. Click on the name of the directory to be added. If the directory is not listed, click **Enter Manually**. Directories are found based on SRV records on your corporate DNS.
7. Use the information in the Settings table above to enter connection information.
8. Click the **Connection** tab and enter connection information.
9. Click **Validate Credentials** to verify the connection.
10. If FortiNAC is able to successfully connect to the Directory a **Credentials Verified** message is displayed in the Credential Status field.
11. To ensure that the user data is available to FortiNAC, you must also complete the User Attributes, Group Attributes, Search Branches and Select Groups tabs.
12. Click **Next** to continue.

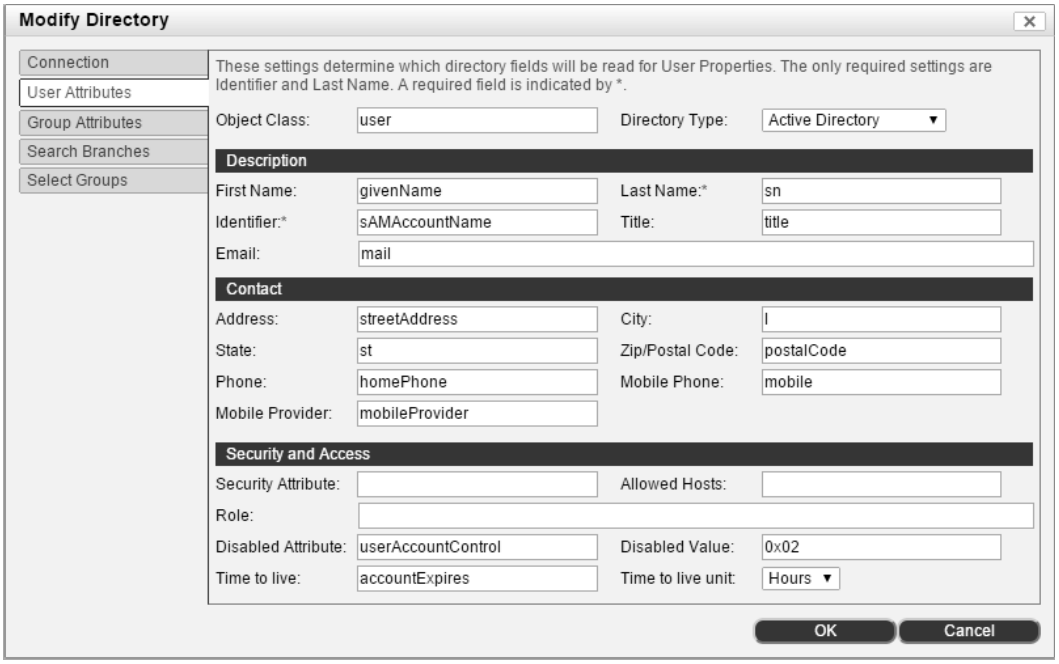
User attributes tab

To add users from an LDAP compliant directory, the customer user database schema must be mapped to the FortiNAC user data. Attributes can be mapped for users and groups by selecting the tabs on the left side of the window.

If a user in the directory has multiple attributes with the same attribute ID, FortiNAC uses the first one it finds. For example, if a record looked like the one shown below, FortiNAC would use staff.

```
eduPersonalAffiliation=staff
eduPersonalAffiliation=employee
eduPersonalAffiliation=alum
eduPersonalAffiliation=student
```

The Attribute Mappings for the user are entered on the User Attributes Tab. The AD attributes are mapped on this form for User Description, Contact, Hardware, and Security and Access. This allows FortiNAC to retrieve the user information based on the User Search Branches configured on the Search Branches tab.



These settings determine which directory fields will be read for User Properties. The only required settings are Identifier and Last Name. A required field is indicated by *.

Object Class:	user	Directory Type:	Active Directory ▼

Description

First Name:	givenName	Last Name:*	sn
Identifier:*	sAMAccountName	Title:	title
Email:	mail		

Contact

Address:	streetAddress	City:	l
State:	st	Zip/Postal Code:	postalCode
Phone:	homePhone	Mobile Phone:	mobile
Mobile Provider:	mobileProvider		

Security and Access

Security Attribute:		Allowed Hosts:	
Role:			
Disabled Attribute:	userAccountControl	Disabled Value:	0x02
Time to live:	accountExpires	Time to live unit:	Hours ▼

Configure user attributes

When adding a directory FortiNAC attempts to determine the directory type and populates the attribute fields based on the directory type. Do not modify the Directory Type unless it is incorrect. Do not modify the attributes unless they are incorrect.

The value of an attribute being mapped cannot exceed 255 characters in order for the attribute to be retrieved by FortiNAC.

1. To access User Attributes for an existing Directory select System > Settings.
2. If you are adding a new Directory, the User Attributes tab is displayed when you click Next after completing the Connection tab.
3. The Directory Type drop-down indicates the type of directory being configured. This will scan the directory based on the type selected and pre-populate some of the fields. The directory type should already be listed for you. If the directory type is not listed or you know the field names for your directory, this step is not required.
4. Enter the user attribute mappings.
5. The Last Name and Identifier (ID) fields are required entries. User records in the directory must have data entered in the selected ID and last name fields.
6. To ensure that the user data is available to FortiNAC, you must also complete the Group Attributes, Search Branches and Select Groups tabs.
7. Click Next to continue.

Directory attributes

If you are using Active Directory, keep in mind that Active Directory only allows access via LDAP to users whose primary group is the Domain Users group.

User Attributes	Active Directory	Novell
Object Class	user	person
Description		
First Name	givenName	givenName
Last Name *	sn	sn
Identifier *	sAMAccountName	cn
Title	title	
E-mail	userPrincipalName	
Contact		
Address	streetAddress	mailstop
City	l	city
State	st	S
Zip/Postal Code	postalCode	
Phone	telephoneNumber	Telephone Number
Mobile Phone	mobile	
Mobile Provider	otherMobile The provider contained in the Mobile Provider field in the Directory must match a provider in the FortiNAC database or SMS messages cannot be sent to that user's Mobile phone. Depending on the configuration of your directory, otherMobile may not be the location of the Mobile Provider field.	
Security and access		
Security Attribute	The Directory Attribute that can be used in a filter. Data contained in this field is copied to the Security and Access value field on the User Properties and the Host Properties record for each user and associated host when the directory synchronizes with the database.	
Allowed Hosts	The number of host records each individual user may have in FortiNAC.	
Role	Name of the Directory Attribute used to associate a user with a role.	

User Attributes	Active Directory	Novell
	Matching roles must be created in FortiNAC with the exact same spelling and case as the roles that exist in the directory based on the selected attribute. See Roles view on page 557. When assigning Roles to users, the use of Directory attributes over Directory groups is recommended. Under no circumstances should you use both methods to assign roles.	
Disabled Attribute	Setting this attribute allows the AD Administrator to disable users in Active Directory and have all instances of the user automatically disabled in FortiNAC when the next scheduled resync occurs. Attribute = userAccountControl Disabled users are able to access the network until FortiNAC resynchronizes with the Active Directory. To immediately disable all instances of the user in FortiNAC, go the Scheduler View and run the Synchronize Users with Directory task. See Scheduler view on page 849 for more information.	
Disabled Value	When the value for the Disabled Attribute for the user equals the Disabled Value, FortiNAC disables all instances of a user when the next scheduled resync with AD occurs. The user must have previously been disabled in AD. The Disabled Value may vary from directory to directory. Check a user that is currently disabled in the directory to see what the disabled value should be. Enter that value in the Disabled Value field. If "Disabled Value" starts with a "0x", a bitwise comparison is done between the value in the directory and this field. Otherwise, without the "0x" prefix, it will only do an exact match numeric comparison.	

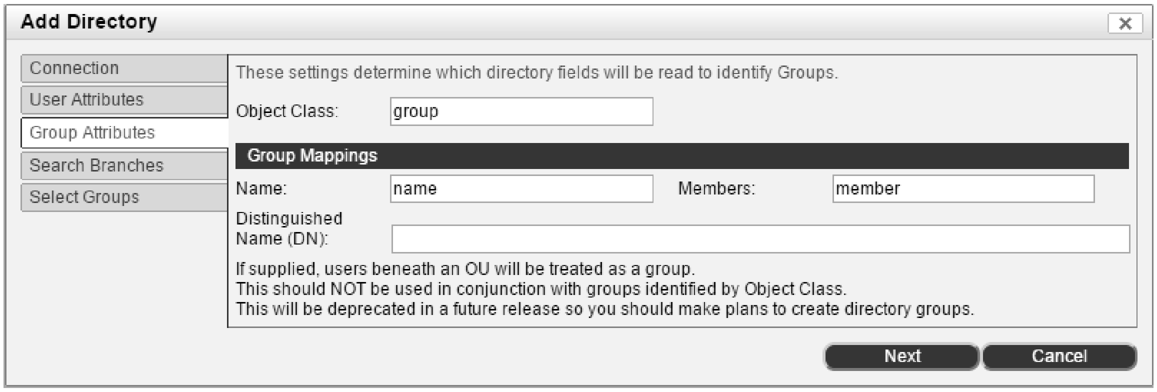
User Attributes	Active Directory	Novell
	If you are using Active Directory, it is possible for the Disabled Value to vary from user to user. The value is affected by other account settings selected within the directory, such as, Password Never Expires or User Must Change Password At Next Login. You may only be able to set the Disabled Value for users that have identical account settings. See https://support.microsoft.com/en-us/kb/305144 for more information on these values.	
Time To Live	The name of the directory attribute that contains the numerical value for the user age time. If the attribute does not have a value the user age time is not set by the directory. Age time can also be set using the FortiNAC Properties window or on the User Properties window for an individual user. All of these options simply modify the Expiration Date in the User Properties window. See User properties on page 649. The value of the attribute in the Time To Live field must be set to the name of the custom attribute that is configured in the directory as the numerical value of hours or days for which the user is valid.	
Time to Live Unit	The time unit set in the User Properties age time if the Time to Live attribute contains a value. Options: Hours or Days	

Group attributes tab

The Attribute Mappings for groups are entered on the Group Tab. The AD attributes are mapped on this form for Object Class, Group Name and Members. This allows FortiNAC to retrieve the group information based on the Group Search Branch configured on the Search Branches Tab. Groups created in the directory are imported into FortiNAC each time the Directory Synchronization task is run either manually or by the Scheduler.

Active Directory size limitations for the number of users per group may cause issues with group based operations. Only the users up to the limitation are affected by group based operations. Size limitations vary depending on the version of Active Directory used and the settings in the MaxValRange and MaxPageSize directory fields.

The value of an attribute being mapped cannot exceed 255 characters in order for the attribute to be retrieved by FortiNAC.



These settings determine which directory fields will be read to identify Groups.

Object Class: group

Name: name

Members: member

Distinguished Name (DN):

If supplied, users beneath an OU will be treated as a group.
This should NOT be used in conjunction with groups identified by Object Class.
This will be deprecated in a future release so you should make plans to create directory groups.

Configure group attributes

1. To access Group Attributes for an existing Directory, select **System > Settings**.
2. If you are adding a new Directory, the Group Attributes tab is displayed when you click **Next** after completing the User Attributes tab.
3. Enter the group attribute mappings:

Group Attributes	Active Directory	Novell
Object Class	group	groupOfMembers
Group Name	name	cn
Group Members	member	member
Distinguished Name (DN)		

The DN is not to be used in conjunction with groups identified by Object Class.

4. To ensure that the user data is available to FortiNAC, you must also complete the Search Branches and Select Groups tabs.
5. Click **Next** to continue.

Search branches tab

The Search Branches tab is where the Administrator enters the specific User and Group Search Branches information for the Directory server. This tells FortiNAC where the user and group information is located in the Directory.

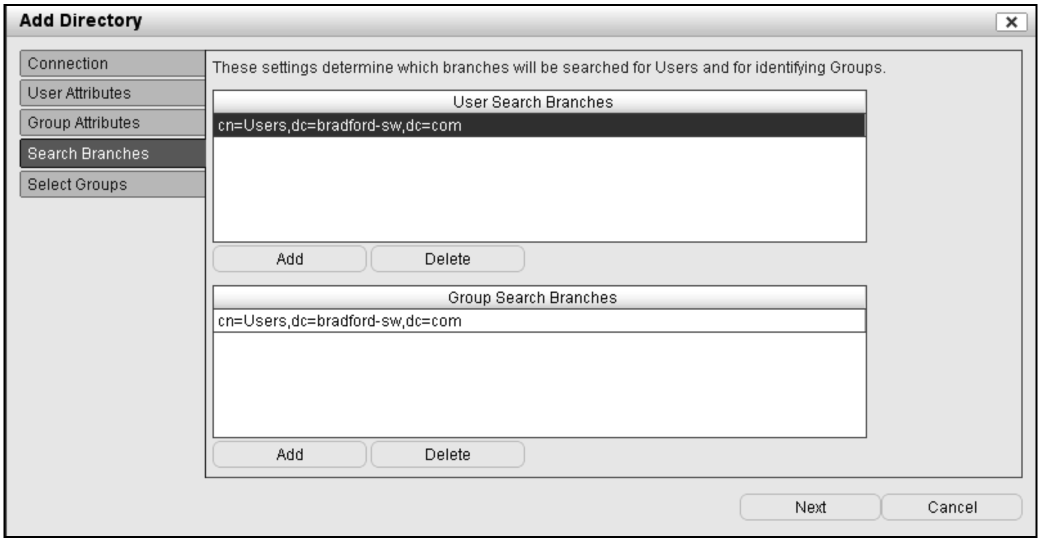
Active Directory size limitations for the number of users per group may cause issues with group based operations. Only the users up to the limitation are affected by group based operations. Size limitations vary depending on the version of Active Directory used and the settings in the MaxValRange and MaxPageSize directory fields.

The example shown in the figure below is for Active Directory. In this example the segments represent the following:

cn=Users—The abbreviation cn stands for Common Name. In this case, it is the name of the branch or folder in Active Directory that should be searched for users. The name of that branch could be anything, such as, Employees or Students.

dc=example—The abbreviation dc stands for Domain Component. In this case it is the second level domain name, such as, yahoo in yahoo.com.

dc=com—The abbreviation dc stands for Domain Component. In this case it is the first level domain name, such as, com in google.com or edu in marshalluniversity.edu or org in npr.org.



These settings determine which branches will be searched for Users and for identifying Groups.

User Search Branches

cn=Users,dc=bradford-sw,dc=com

Group Search Branches

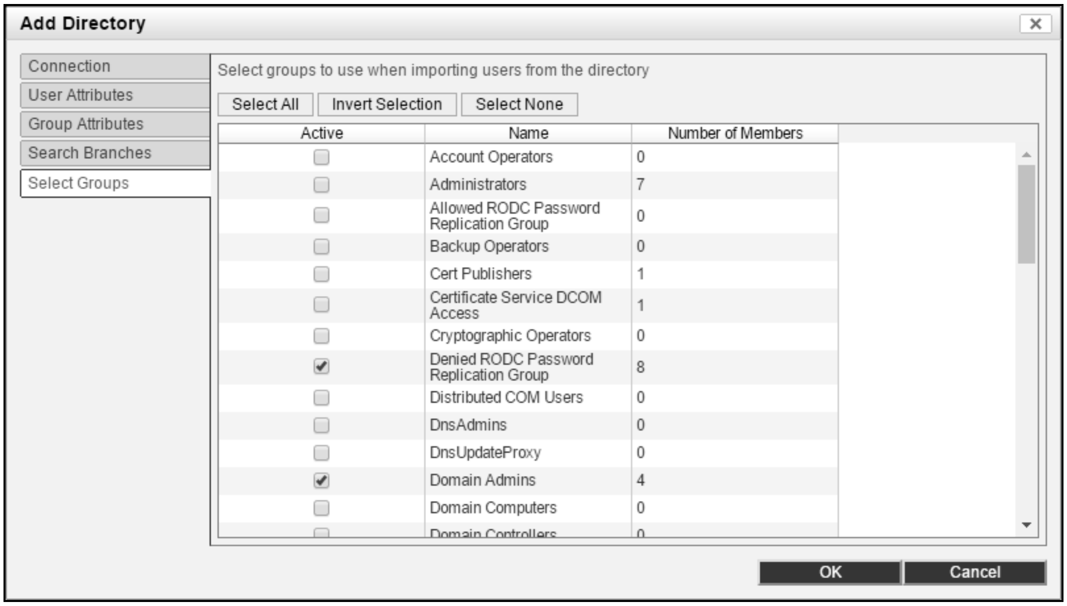
cn=Users,dc=bradford-sw,dc=com

Configure search branches

1. To access Search Branches for an existing Directory, select **System > Settings**.
2. To modify an entry in the Search Branches list, select the entry and click **Modify**.
3. To remove an entry in the Search Branches list select the entry to be removed and click **Delete**.
4. If you are adding a new Directory, the Search Branches tab is displayed when you click **Next** after completing the Group Attributes tab.
5. Click **Add** to add new search branch information. Available search branches are listed, however you can enter your own information. If the list of available search branches is too long to display, type the first few letters of the branch needed to narrow the list.
6. In the Add dialog, enter or select the **Search Branch** and then click **OK**.
7. To ensure that the user data is available to FortiNAC, you must also complete the Select Groups tab.
8. Click **Next** to save search branch information.

Select groups tab

Use the Select Groups tab to choose groups of users to be included when the directory and the FortiNAC database are synchronized. Users that do not already exist in FortiNAC are not imported. However, user data for users already in the database is updated each time the Synchronization task is run. Only the user records for users in the selected groups are updated. Users in the directory that are not in a selected group are ignored during Synchronization.



Select groups to use when importing users from the directory

Active	Name	Number of Members
□	Account Operators	0
□	Administrators	7
□	Allowed RODC Password Replication Group	0
□	Backup Operators	0
□	Cert Publishers	1
□	Certificate Service DCOM Access	1
□	Cryptographic Operators	0
☑	Denied RODC Password Replication Group	8
□	Distributed COM Users	0
□	DnsAdmins	0
□	DnsUpdateProxy	0
☑	Domain Admins	4
□	Domain Computers	0
□	Domain Controllers	0

Configure group selections

1. To access Group Selections for an existing Directory, select **System > Settings**.
2. If you are adding a new Directory, the Select Groups tab is displayed when you click **Next** after completing the Search Branches tab.
3. Mark the Groups of users that should be included when the Directory and the database are synchronized by checking the box in the **Active** column. If you do not check any boxes, all Groups will be included.
4. Click **OK** to save the directory configuration.
5. An initial Synchronization is done immediately when you save the Directory. It is recommended that you set up a schedule for synchronizing the Directory See Schedule synchronization on page 93.

Delete a directory

1. Click **System > Settings**.
2. Click the **Authentication** folder in the tree control.
3. Click **LDAP** to display the Directories window.
4. Select a directory configuration in the list and click **Delete**.
5. Confirm that you wish to delete the directory configuration.

Schedule synchronization

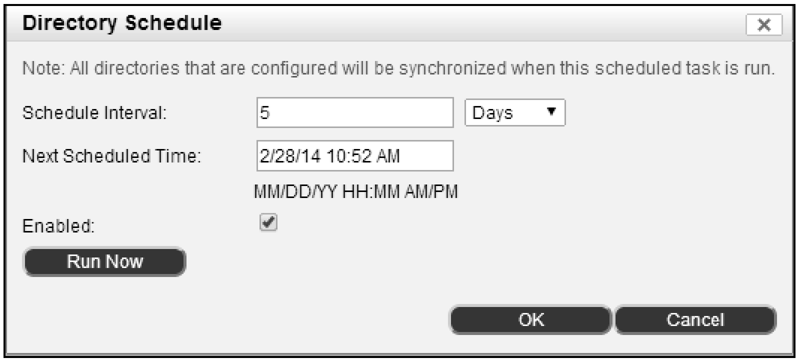
The Schedule button on the Directories View allows the Administrator to select a date/time and poll interval for the directory synchronization task. The scheduled task may also be paused and run manually later. This process adds the **Synchronize Users with Directory** task to the Scheduler View.

When the Directory and FortiNAC are synchronized changes made to users in the Directory are written to corresponding user records in the database. Users from the Directory are only added to the FortiNAC database when they connect to the network and register. Directory groups are added to the FortiNAC database each time a synchronization occurs. Groups created in the directory are displayed in FortiNAC on the Groups View. Specific directory groups can be disabled from Attribute Mappings.

If you are using a directory for authentication, user data is updated from the directory based on the User ID during synchronization. This is true regardless of how the user is created and whether the user is locally authenticated or authenticated through the directory. If the User ID on the user record matches a User ID in the directory, the FortiNAC database is updated with the directory data.

When an Admin Group is created in FortiNAC with the same name as a group being synchronized from a Directory, the Admin Group members will remain the same as the Directory group members. Therefore, if you add a non-Directory user to the Admin Group and then synchronize the Directory, the non-Directory user is removed from the Admin Group because the user is not a member of the Directory group.

The Directory Schedule is global and applies to all directories listed. Separate schedules cannot be entered for each directory.


Directory Schedule

Note: All directories that are configured will be synchronized when this scheduled task is run.

Schedule Interval: 5 Days

Next Scheduled Time: 2/28/14 10:52 AM

MM/DD/YY HH:MM AM/PM

Enabled: ☑

Settings

Field	Definition
Schedule Interval	Poll interval for the scheduled task. Options are Minutes, Hours, or Days.
Next Scheduled Time	The next date/time the scheduled synchronization task will run. Entered in the format MM/DD/YY HH:MM AM/PM.
Enabled	When unselected, the scheduled synchronization task is stopped and does not run automatically. To run the task manually click Run Now.

Field	Definition
Run Now	Runs the Synchronization task immediately.

Schedule directory resynchronization

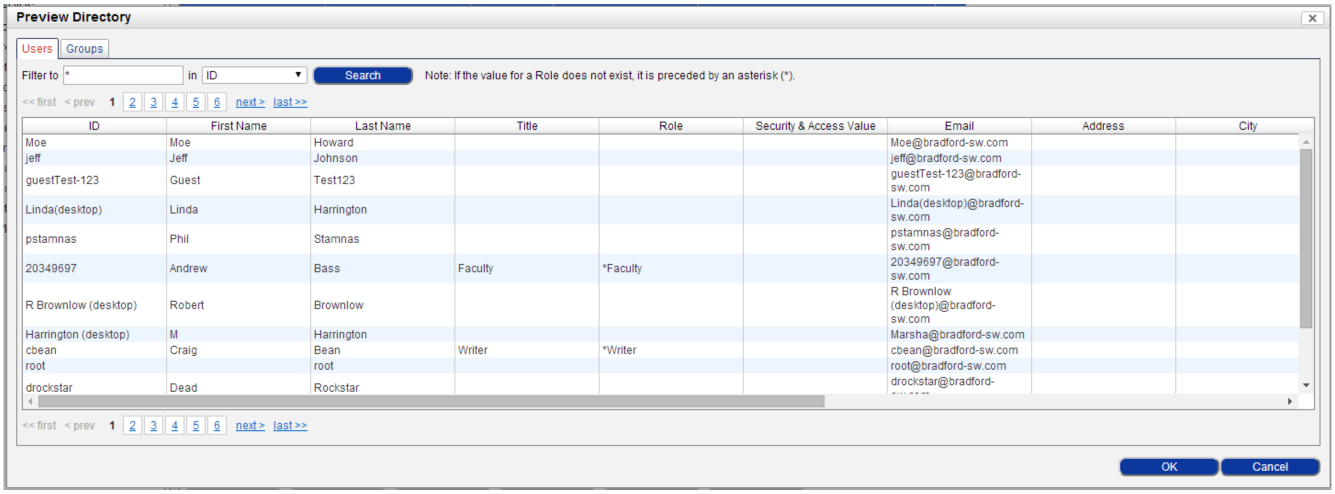
1. Click **System > Settings**.
2. Select a directory in the list and click **Schedule**.
3. Set a **Schedule Interval** by entering a number and selecting Minutes, Hours, or Days from the drop-down menu.
4. Click in the **Next Scheduled Time** field and enter the **date/time** to run the synchronization task.
5. To stop the scheduled task, remove the check mark from click in the **Enabled** box.

   If the scheduled task is disabled, the Administrator can go to the Scheduler view and run the task manually to synchronize the directory with FortiNAC. See Scheduler view on page 849 for details.
6. To run the scheduled task immediately, click Run Now.
7. Click OK to save the schedule.

Preview

Use Preview to view the list of users that are found in the directory. User records in the directory are not listed until a parameter is selected and its associated value is entered in the Filter field.

The Directory Configuration must be completed before any records can be previewed.



Filter to * in ID

Note: If the value for a Role does not exist, it is preceded by an asterisk (*).

ID	First Name	Last Name	Title	Role	Security & Access Value	Email	Address	City
Moe	Moe	Howard				Moe@bradford-sw.com		
jeff	Jeff	Johnson				jeff@bradford-sw.com		
guestTest-123	Guest	Test123				guestTest-123@bradford-sw.com		
Linda(desktop)	Linda	Harrington				Linda(desktop)@bradford-sw.com		
pstamnas	Phil	Stamnas				pstamnas@bradford-sw.com		
20349697	Andrew	Bass	Faculty	*Faculty		20349697@bradford-sw.com		
R Brownlow (desktop)	Robert	Brownlow				R Brownlow (desktop)@bradford-sw.com		
Harrington (desktop)	M	Harrington				Marsha@bradford-sw.com		
cbean	Craig	Bean	Writer	*Writer		cbean@bradford-sw.com		
root		root				root@bradford-sw.com		
drockstar	Dead	Rockstar				drockstar@bradford-		

View user and group records

1. Click **System > Settings**.
2. Select a directory in the list and click **Preview**.
3. Enter search criteria in the first text field, such as an ID or Last Name. Searches are not case-sensitive.

Use asterisks (*) as wild cards in text fields if you know only a portion of a name. The wild card represents any characters. For example, enter F* in the text field and select the First Name parameter to locate all records where F is the first character in the First Name field.

4. Select a **parameter** from the drop-down list.
5. Click **Search**.

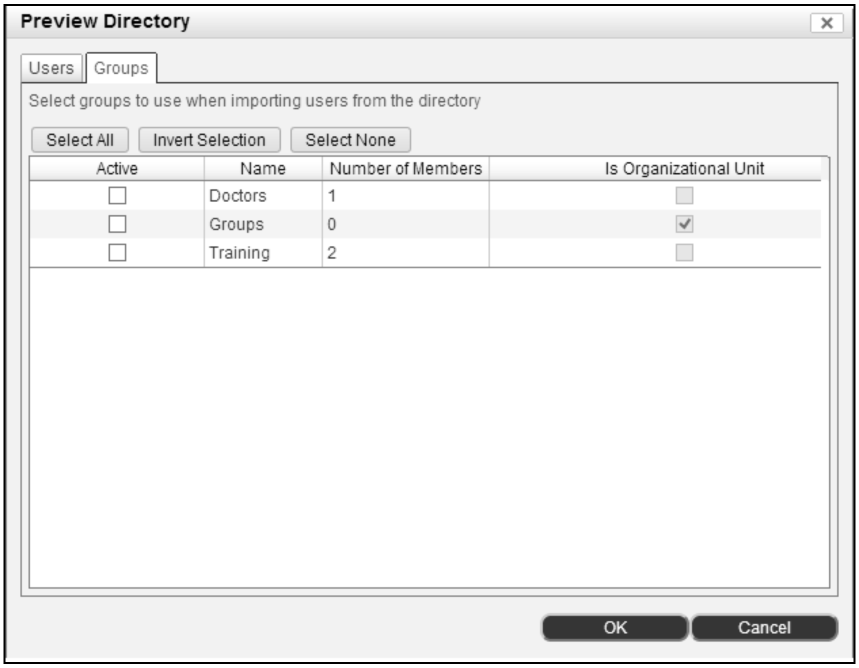
An asterisk in the Role column next to an attribute value indicates that the role name has not been configured in FortiNAC. If the role does exist in FortiNAC, the attribute value appears in the Role column without an asterisk.

Entering just the wild card in the text field returns every record in the directory and may cause time or size limit exceeded errors to occur depending on the total number of records.

This is a view only list and is NOT imported into FortiNAC. The user information is only imported into the FortiNAC database as the user registers. The Sync Directory task in the Scheduler View is used to update user information already in the FortiNAC database with any changes made in the Directory database. See Scheduler view on page 849 for additional information.

6. Click the Groups tab to view the groups in the Directory and select the groups to import.
   All the groups in the Directory are listed along with the number of member records contained in each group.

Selecting groups is part of the process of adding a Directory configuration, therefore, groups may already be selected.



Select groups to use when importing users from the directory

Active	Name	Number of Members	Is Organizational Unit
□	Doctors	1	□
□	Groups	0	☑
□	Training	2	□

7. To import groups of user records from the Directory to the FortiNAC database when the Directory Synchronization scheduled task runs select the groups to be imported by checking the box(es) next to the group name.
8. A check mark in the **Is Organizational Unit** column indicates that the group is an OU or a container for other groups.
9. Click **OK**.

Create a keystore for SSL or TLS

If you choose to use SSL or TLS security protocols for communications with your LDAP directory, you must have a security certificate. You must obtain a valid certificate from a Certificate Authority. That certificate must be saved to a specific directory on your FortiNAC appliance.

SSL or TLS protocols are selected on the Directory Configuration window when you set up the connection to your LDAP directory. Follow the steps below to import your certificate. You should be logged in as root to follow this procedure.

1. When you have received your certificate from the Certificate Authority, copy the file to the */bsc/campusMgr/* directory on your FortiNAC server.
2. Use the keytool command to import the certificate into a keystore file.
3. For example, if your certificate file is named MainCertificate.der, you would type the following:

```
keytool -import -trustcacerts -alias <MyLDAP> -file MainCertificate.der -keystore .keystore
```

Depending on the file extension of your certificate file, you may need to modify the command shown above. For additional information on using the keytool key and certificate management tool go to the Sun web site java.sun.com.

4. When the script responds with the **Trust this certificate?** prompt, type **Yes** and press **Enter**.
5. At the prompt for the keystore password, type in the following password and press **Enter** *^8Bradford%23*
6. To view the certificate, navigate to the /bsc/campusMgr/ directory and type the following:

```
keytool -list -v -keystore .keystore
```

7. Type the password used to import the certificate and press **Enter**.

The keystore is cached on startup. Therefore, it is recommended that you restart FortiNAC after making any changes to the keystore.

Passive registration

You can configure FortiNAC to automatically run logon and logoff scripts and register the host when a user logs on or off a domain. This process allows users to be tracked as they use various hosts on the network. The registration process is not visible to the user. Logon and logoff scripts are provided, but must be customized for your configuration.

To use login or logout scripts, you must be using an LDAP directory for authentication and it must be configured in FortiNAC. See Requirements on page 81 for an overview on configuring your Directory.

Make sure that Authentication is enabled. See Authentication on page 75.

Host registration vs device registration

Host registration associates the host with a user. Device registration has no associated user and the host is registered by its host name. Both types of hosts are displayed in the Host View.

Customize login and logout scripts

FortiNAC allows you to register hosts using login and logout scripts. These scripts are provided for you on the appliance. They contain variables that must be modified to match your environment and requirements. Scripts are located in the following directory:

```
/bsc/campusMgr/ui/runTime/config/ldap
```

Scripts that should be modified include *sendLogIn.vbs, sendLogOut.vbs*. It is recommended that you review the comments contained within the script. They contain the most up to date information about variables that can be used and additional parameters that can be set.

To use the scripts they must be copied to the directory server, such as your Active Directory Server. After they have been copied, use the information in the Variables on page 98 and Trap parameters on page 99 tables below to modify the necessary parameters.

To receive traps from the scripts, you must have the latest versions of **snmptrap.exe** and **libsnmp.dll** on the directory server in the same directory that contains the scripts. These two files are part of a package that can be downloaded and installed on your directory server from http://www.net-snmp.org/download.html . Select the latest binaries. From the list of download files select the file that is in the following format: *net-snmp-<version number>.exe*.

Registration types

There are two types of registration that can be done using scripts. A host can be registered as a host with an associated user or as a device with no identity. When a host is registered as a device, the host name of the device is used. Hosts can also be left as rogues.

If you are registering shared hosts, such as computers in a lab, you may want to modify the script to register the computers as devices.

Registration Type	Settings

Host / User	Register the host as a host by user name.
	REG_ROGUE = "0"
	REG_BY_USER = "1"

Device	Register the host as a device by host name.
	REG_ROGUE = "0"
	REG_BY_USER = "0"

Registration examples

In the two examples above, the login script was set to register by user. Both the host and the user are shown, first from the User View and second from the Host View. The host shows as Type - Registered, indicating that it is registered to a user. The host is associated with or Registered To the user.

In the two examples above, the login script was set to register by device. Both the host and the user are shown, but there is no association between the host and the user. The User View example shows Type - Logged On, indicating that the user is logged onto this host but that the host is not Registered to a user. The Registered To field is blank. The Host View represents the actual computer. The User View represents the temporary user who logged into the host.

Variables

Variable	Definition
Required variables	

ACTION	Indicates whether this script is for logon or logoff.
	Type = Integer
	Logoff = 0
	Logon = 1
	Logon Started = 2
	Example: ACTION = "1"

REG_ROGUE	When Register is enabled, host is registered either by user name or as a device by host name based on the Register by User setting. If Do not register is enabled, the host remains a rogue. Type = Integer Register = 0 Do not register = 1 Example: REG_ROGUE = "0"
WHITELIST	If enabled, adds the host to the Forced User Authentication Exceptions group. A user logging in on a host in this group is not forced to authenticate. Default is disabled. Type = Integer Do not add = 0 Add = 1 Example: WHITELIST = "0"
REG_BY_USER	Registers the host by user name as a host or by host name as a device. Type = Integer Register as device = 0 Register by user name = 1 Example: REG_BY_USER = "0"
DIRECTORY_SERVER	Your Active Directory server. If you have more than one Active Directory server for failover, it is recommended that you use your domain name instead of the IP address. Example: DIRECTORY_SERVER = "192.168.102.2" Example: DIRECTORY_SERVER = "example.com"
DIRECTORY_SHARED	Active Directory server's shared directory where the login/logoff scripts, snmptrap.exe and libsnmp.dll files are stored. If you have more than one Active Directory server for failover, it is recommended that you use your domain name instead of the IP address. Example: DIRECTORY_SHARED ="\\192.168.102.2\sysvol\eng.local\scripts\" Example: DIRECTORY_SHARED ="\\example.com\sysvol\eng.local\scripts\"
Novell specific variables	

Variable	Definition
USE_ENV_USERNAME	Indicates whether or not the user name should come from another variable. To enable, set this to True. If you are **not** using Novell or if the User Name entered at login is sufficient, set this to False. Example: USE_ENV_USERNAME = False
ENV_USERNAME_ VARIABLE	The variable containing the User Name. This information is used only if USE_ENV_ USERNAME is set to True. Example: ENV_USERNAME_VARIABLE = "%NWUSERNAME%"
Optional changes - sample	
Wscript.Sleep 5000	Add before the last "End If" statement. This makes the script wait 5 seconds allowing more time for processes to start or finish. REM End If Wscript.Sleep 5000 End If Next End Function

You may choose to make other modifications to the script to accommodate requirements outside FortiNAC. For example, you may choose to add a timer that waits a few seconds before ending the script.

Trap parameters

The login and logout scripts send a trap to FortiNAC that contains the values of the variables listed above along with registration parameters from the user. To receive traps from the scripts, you must have the latest versions of **snmptrap.exe** and **libsnmp.dll** on the directory server in the same directory that contains the scripts. These two files are part of a package that can be downloaded and installed on your directory server from http://www.net-snmp.org/download.html . Select the latest binaries. From the list of download files select the file that is in the following format: *net-snmp-<version number>.exe*.

OID	Description	Definition
1.1	Action	Value of the Action variable.
1.2	User Name	User name of the person logging in or out. Type = String
1.3	Host Name	Name of the host used to log in or out. Type = String
1.4	Host IP	IP address of the host used to log in or out. Type = IP address
1.5	Host MAC	MAC address of the host used to log in or out. Type = String
1.8	Operating System	Operating System of the host used to log in or out. Type = String

OID	Description	Definition
1.10	Register Rogue	Value of the Reg_Rogue variable.
1.11	Whitelist	Value of the Whitelist variable.
1.12	Register by User	Value of the Register by User variable.

Active Directory setup

Passive registration can be set up for one or more groups of users.

1. Copy the following files from the runtime area

   `<Host Name>/ui/runTime/config/ldap`

   to the AD shared directory, generally located at:

   `/WINNT/SYSVOL/<domainname>/sysvol/scripts`

   Files to be copied:

   `sendLogIn.vbs, sendLogOut.vbs`

   Permissions should be set such that all users may read and execute on all the files.

2. To receive traps from the scripts, you must have the latest versions of **snmptrap.exe** and **libsnmp.dll** on the directory server in the same directory that contains the scripts. These two files are part of a package that can be downloaded and installed on your directory server from http://www.net-snmp.org/download.html . Select the latest binaries. From the list of download files select the file that is in the following format: *net-snmp-<version number>.exe*.
3. If you have not already done so, customize the scripts so that they take into account your network setup. See Customize login and logout scripts on page 97 for detailed information.
4. Configure AD to use the following scripts:

   `sendLogIn.vbs` and `sendLogOut.vbs`

   a. Start the Active Directory Users & Computers application.

   b. Click the **domain name** in the Tree panel to select it.

   c. Right-click and select **Properties**.

   d. In the Properties window, click the Group Policy tab.

   e. Double-click the policy (Default Domain Policy) that will enable the scripts.

   f. In the **Group Policy** window click the plus sign (+) next to the **User Configuration** folder, then click the plus sign (+) next to the **Windows Settings** folder, and click **Scripts (Logon/Logoff)**.

   g. In the right panel of the Group Policy view, double-click the logon script to launch the Logon Properties view. Click the **Add** button, then click the **Browse** button and navigate to the sysvol folder where files were copied in step 1. Select the following: `sendLogIn.vbs`

   h. Once the script file has been added, click **OK**.

   i. In the right panel of the Group Policy view, double-click the logoff script to launch the Logoff Properties view. Click the **Add** button, then click the **Browse** button and navigate to the sysvol folder where the files were copied in step 1. Select the following: `sendLogOut.vbs`

   j. Once the script file has been added, click **OK**.
5. In the Group Policy view, click **New** to add a new policy for each group of users.

For FortiNAC users change the name to **CM_Policies**.

For Guest users change the name to **Guest_Policies**.

6. Double-click the new policy. The Group Policy window will appear.
7. In the **Group Policy** window click the plus sign (+) next to the **User Configuration** folder, then click the plus sign (+) next to the **Windows Settings** folder, and click **Scripts (Logon/Logoff)**.
   a. In the right panel of the Group Policy view, double-click the logon script to launch the Logon Properties view. Click the **Add** button, then click the **Browse** button and navigate to the NETLOGON directory on the domain controller. Select the following: `sendLogIn.vbs`
   b. Once the script file has been added, click **OK**.
   c. In the right panel of the Group Policy view, double-click the logoff script to launch the Logoff Properties view. Click the **Add** button, then click the **Browse** button and navigate to the NETLOGON directory on the domain controller. Select the following: `sendLogOut.vbs`
   d. Once the script file has been added, click **OK**.
8. In the **Group Policy** window for the Group Policy created in step 3 Click the plus sign (+) in front of the User Configuration folder.
9. Click the plus sign (+) in front of the Administrative Templates folder, and then click the plus sign (+) in front of the System folder. Click the Logon/Logoff folder.
10. Enable the following policies by double-clicking on them, clicking **Enable**, and then clicking **OK**.

```
Run logon scripts visible
Run logoff scripts visible
Run logon scripts synchronously
```

Visible mode only needs to be enabled for the testing period. Once the Administrator has determined that the logon/logoff scripts are working, running in visible mode can be disabled.

11. Roll the policy changes to the host. AD has built-in delays so reboot the hosts if the scripts fail to run. The delay can be shortened by setting the "Group Policy refresh interval for user" to a shorter time period. The policy is located in the User Configuration folder.

Novell setup

This setup can be used for network users. The following steps are only necessary on a PC platform:

1. Copy the files listed below from FortiNAC /bsc/campusMgr/ui/runTime/config/ldap to the directory from which the scripts are run.

   `sendLogIn.vbs` and `sendLogOut.vbs`

   Set the permissions on all copied files to read and execute for all.
2. To receive traps from the scripts, you must have the latest versions of **snmptrap.exe** and **libsnmp.dll** on the directory server in the same directory that contains the scripts. These two files are part of a package that can be downloaded and installed on your directory server from http://www.net-snmp.org/download.html . Select the latest binaries. From the list of download files select the file that is in the following format: *net-snmp-<version number>.exe*.
3. Configure the "Login Script" attribute in all users and groups within the directory to use the following:

   `sendLogIn.vbs`

   This is done by setting the "Login Script" attribute to either sendLogIn.vbs or gscLogin.vbs depending on your users.

   See Novell's users guide for detailed instructions: http://www.novell.com/documentation/edir873/index.html

RADIUS

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service. A RADIUS server enables external authentication for users connected to FortiNAC-managed network devices. This type of server is often used in a wireless environment.

FortiNAC uses RADIUS authentication to external RADIUS servers for several purposes including:

- Authenticating users attaching to managed network devices using 802.1x.
- Authenticating VPN users.
- Authenticating users accessing FortiNAC's own captive portal process.
- Authenticating administrative users logging onto the FortiNAC system.

FortiNAC works with all the known RADIUS server products, including FreeRADIUS, Steel Belted RADIUS, Microsoft IAS, Cisco ACS, and RADIATOR. To support these uses, RADIUS server profiles must be created in FortiNAC, which can then be assigned as the authentication method for the FortiNAC system or a specific device.

You can create an unlimited number of RADIUS server profiles. Several configuration options are available:

- System-wide—Default Primary and Secondary Profiles assigned at the system level are used for both captive portal and administrative user authentication.
- In an 802.1x environment:
  - Profiles can be assigned for each individual device.
  - Profiles can be assigned for individual SSIDs.
  - Profiles can be mapped to domains. User names contain a domain name prefix of the user logging onto the network.
  - Profiles can be mapped to a blank domain which would encompass any authenticating user who does not have a domain name prefix as part of his user name.

Manage settings

The RADIUS Settings View allows you to add or modify RADIUS server profiles for individual network devices. For devices using 802.1x, accept the default primary and secondary RADIUS servers or you can select profiles for each device within its Model or Global Model Configuration view. See Model configuration on page 767 for additional information.

The ability to map a domain name to a RADIUS server profile also functions within the context of 802.1x. It provides RADIUS server selection based on the domain of the authenticating user. Users authenticating from different Microsoft domains can be directed to separate RADIUS servers configured for those domains.

Users authenticating from a domain, can only authenticate via the RADIUS server profile configured for that domain. Multiple RADIUS server profiles can be configured for each domain and searched for the authenticating user. RADIUS servers are searched in order from the top of the list of servers down. .

RADIUS Settings can be accessed from **System > Settings** or from **System > Quick Start > Authentication Settings**, however configuration steps point you to **System > Settings**.

FortiNAC's capacity for processing RADIUS requests is approximately 60 requests per second. Capacity is affected by the use of other features in the program such as the Persistent Agent or MAC Notification Traps. Any requests that are not immediately processed are placed in queue. After 5 seconds any unprocessed requests are discarded. If you are in an environment where you expect to receive more than 60 RADIUS requests per second you may need additional FortiNAC appliances to handle the load.

802.1x environments

When using 802.1x in a FortiNAC managed environment, it is necessary to configure the network devices, FortiNAC and the production RADIUS server(s) so that all can communicate successfully. This requires at a minimum that all three components have the same RADIUS secret key value defined, since FortiNAC does not modify 802.1x packets as they pass from the network device through to the terminating RADIUS server. The same restriction exists when using Domain mapping.

For instance, many wireless devices that support 802.1x allow a RADIUS server definition for each configured SSID. In such an environment, if two users are connected to the same SSID but to different domains, the RADIUS secret used in both authentication requests would be identical. The users are both using the same RADIUS profile on the wireless device. Assuming FortiNAC were configured to use different terminating RADIUS servers for each domain, it would forward the requests and both servers would need to use the same secret value in order to validate the packets.

Order of precedence

When one or more RADIUS servers are used for authentication coupled with different methods of configuration, it can be difficult to determine which server will be used. The uses for RADIUS servers are as follows:

- Authenticating FortiNAC Admin Users.
- Authenticating network users accessing the network through a VPN.
- Authenticating network users who come in through the captive portal.
- Devices that have no RADIUS servers configured in the model configuration.
- Devices that have specific RADIUS servers configured in the model configuration.
- SSIDs that have no RADIUS servers configured and inherit from the parent device.
- SSIDs that have specific RADIUS servers configured.

Unless a specific RADIUS server is configured for a particular device or SSID, these options use the default Primary and Secondary RADIUS servers. However, if RADIUS server profiles are mapped to domains and the authenticating user's username contains a domain name prefix, then the RADIUS server mapped to the domain takes precedence. The order of precedence to determine which RADIUS server is used is as follows:

1. If domain mappings exist and an entry matches the domain prefix contained within the user name of a connecting user, then the RADIUS server mapped to the domain is used. Multiple servers can be mapped to a single domain. If the user is not found on the first RADIUS server in the list, FortiNAC checks each server mapped to the domain in turn until the user is found.
2. If a blank domain has been mapped and an authenticating user does not have a domain prefix in the user name, then the server or servers mapped to the blank domain are used.

   If you create a domain mapping for a RADIUS server with a blank domain name this always takes precedence over the default Primary and Secondary RADIUS servers because all users who do not use domain name to log in will match this mapping.
3. If no domain mappings exist, the RADIUS server profile chosen for the originating SSID is used.

4. If no SSID mapping exists, the RADIUS server profile chosen for the originating device is used.
5. If no device specific server selection exists, the system-wide default Primary and Secondary server settings are used.

Configure profiles

Access the RADIUS Settings from **System > Settings > Authentication** or **System > Quick Start > Authentication Settings**. Add a profile for each RADIUS Server. The first RADIUS Server added becomes the primary server by default. As more, servers are added, you can modify which server is the primary.

The encryption method for user names and passwords passed between FortiNAC and the RADIUS server must be set to PAP. This affects the following accounts or user names and passwords created on the RADIUS server:

- The validation account created for communication with FortiNAC and entered in the RADIUS Server Profile configuration.
- Network users that access the network via the captive portal and are authenticated through RADIUS.
- Admin UI users authenticated through RADIUS.
- VPN Users authenticated through RADIUS.

You should be able to communicate with a RADIUS Server in order to add it to the list. For example, if a RADIUS Server is not currently connected to the network and FortiNAC cannot contact it, you will be asked if you want to add the server anyway.

Add a profile

1. Click **System > Settings**.
2. Expand the **Authentication** folder and click **RADIUS**. The RADIUS Servers window displays.
3. Click **Add**.
4. Enter the parameters for the RADIUS Server profile.
5. Click the **RADIUS Secret** field to enter the RADIUS secret.
6. Enter the User Name.
7. Click the **Password** field to enter the Password information.

Field	Definition
Profile Name	Name displayed in the RADIUS server list.
Host Name/IP address	Host name or IP address of the RADIUS server. If you are generating certificates using a NSRADIUS appliance, the Fully Qualified Domain Name is required.
RADIUS Secret	Encryption key used by the RADIUS server to send authentication information.
Authentication Port	Port number through which the RADIUS server communicates.

Field	Definition
Accounting Port	Port number that the RADIUS server uses for the accounting features, if they are used. If your RADIUS server does not use accounting features, leave the check box blank.
Server Is NSRADIUS Appliance	Indicates that this is a NSRADIUS Server. Check this box if you have purchased a NSRADIUS server as part of your FortiNAC configuration. Option displays only if a NSRADIUS license is installed on the FortiNAC or control server, and when there is no NSRADIUS Server already configured. REST API credentials are required for the Portal Certificate page to generate and download certificates.
REST API User	User name for the admin user created on the NSRADIUS server. This user name will be used to communicate with the REST API on the NSRADIUS Server. It is recommended that you configure the REST API user.
REST API Password	Password for the NSRADIUS admin user that will allow the FortiNAC server to communicate with the REST API on the NSRADIUS Server. Appears when the Server Is NSRADIUS Appliance check box is selected.
Last Modified By	User name of the last user to modify the RADIUS Server.
Last Modified Date	Date and time of the last modification to this RADIUS Server.
Validation Account	
User Name	User name for verifying access to the RADIUS Server. This field is required, but only used when there are multiple RADIUS Servers configured. You must create an account on the RADIUS Server that is used by FortiNAC to communicate with that Server. The encryption method must be set to PAP.
Password	Password for verifying access to the RADIUS server. This field is required.

8. New servers are saved automatically.
9. Repeat as needed for additional RADIUS servers.

Modify a profile

1. Click **System > Settings**.
2. Expand the **Authentication** folder and click **RADIUS**.
3. Select the RADIUS Server profile and click **Modify**.
4. Make the changes. Changes are saved automatically.

Delete a profile

1. Click **System > Settings**.
2. Expand the **Authentication** folder and click **RADIUS**.
3. Select the RADIUS Server profile and click **Delete**.

Set defaults

Once you have added the RADIUS Server profiles, specify the default primary RADIUS server and secondary RADIUS server to be used in the event of a primary server failure. These servers are used for authentication unless you specify other RADIUS Servers in the SSID Configuration, Device Model or Global Model Configuration views, or by mapping RADIUS servers to domains. The default servers are also used for web-portal authentication, when it is configured for RADIUS.

You may want to deploy multiple RADIUS servers to handle requests if the primary server should fail. Within the FortiNAC managed environment, you can define many servers, and you have the option to choose different servers, both a primary and a secondary, for each device.

The first RADIUS Server added is the default for the Primary RADIUS Server until it is changed manually.

1. Click **System > Settings**.
2. Expand the **Authentication** folder and click **RADIUS**.
3. The RADIUS Server Defaults and RADIUS Domain Mappings windows display.
4. In the RADIUS Server Defaults window select the Default Primary and Secondary server names from the drop-down lists.
5. Click **Apply** to save your changes.

Set domain mappings

If you plan to use the user domain for RADIUS server selection, you must create mappings for the desired domains. First make sure that you have added the RADIUS Server profiles. Then, choose one or more RADIUS servers per domain to authenticate users who connect through a specific domain.

If more than one RADIUS server is entered for a single domain, FortiNAC sends the authentication request to the first server in the domain that matches the user's domain. If the RADIUS server does not recognize the user FortiNAC sends the request to the next server in the list with a matching domain and so on until the user is authenticated. If one of the servers does not respond at all FortiNAC sends the request to the next server in the list.

If you have users that do not log in through the domain but need to be authenticated by one of your RADIUS servers, you can enter Domain Mappings with a blank domain field.

If you map RADIUS servers to a blank domain, the Primary and Secondary servers will never be used because anyone logging in without domain information will match the blank domain.

RADIUS servers mapped to domains take precedence over all other RADIUS server settings.

You must use the Fully Qualified Domain Name or the server will not be able to authenticate users connecting to the network.

Add mapping

1. Click **System > Settings**.
2. Expand the **Authentication** folder and click **RADIUS**.
3. The RADIUS Server Defaults and RADIUS Domain Mappings windows display.
4. In the RADIUS Domain Mappings window click Add.
5. Enter the Fully Qualified Domain Name to be used for authentication. For example, bbc.com or myuniversity.edu. Users can then log in with any of the following user name formats:
    - User@FQDN (bob@bbc.com)
    - FQDN\User (bbc.com\bob)
6. Select the RADIUS Server profile name from the drop-down list.
7. Your changes are saved automatically.

Delete mapping

1. Click **System > Settings**.
2. Expand the **Authentication** folder and click **RADIUS**.
3. The RADIUS Server Defaults and RADIUS Domain Mappings windows display.
4. In the RADIUS Domain Mappings window select the mapping to be removed.
5. Click **Delete**.

Configure local domain list

Configure the list of local domains. This allows FortiNAC to distinguish between local users and Roaming Guests. See Roaming guests on page 110 for a detailed description.

Add local domains

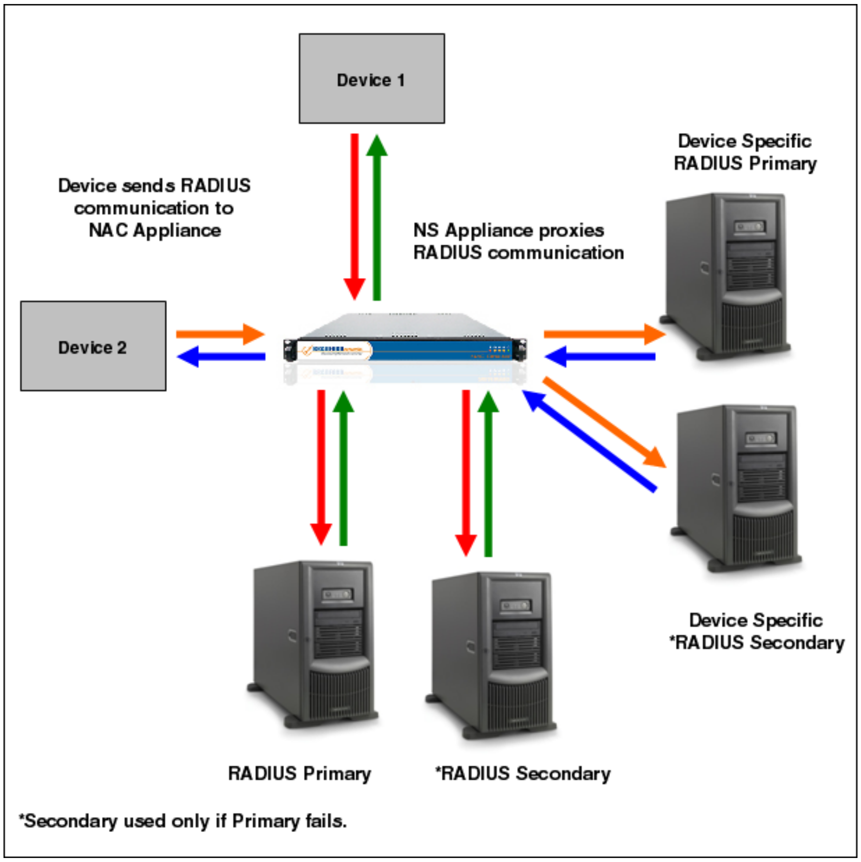
1. Click **System > Quick Start > Authentication Settings**.
2. Select **RADIUS Settings**.
3. Scroll down to the RADIUS Local Domain List section.
4. Click **Add**.
5. Enter a domain name.
6. Click **OK**.
7. Continue adding domain names until all local domains have been added.

Failover process

In FortiNAC you can have primary and secondary RADIUS servers that are the system-wide default for RADIUS requests. You can also have other RADIUS servers that are listed as the primary and secondary server for requests coming through a specific device.

All of these RADIUS servers must be configured in FortiNAC and must be running in parallel. It is required that each RADIUS server be configured with a user name and password that will be used by FortiNAC as a Validation Account to test for RADIUS server availability. That user name and password must also be entered into the RADIUS server configuration within FortiNAC allowing a test message to be sent to the RADIUS server.

If one or both of your RADIUS servers were to fail, there is a failover process that is followed. No events or alarms are generated when a RADIUS server fails. There are two types of failure in this process. The first is a failure by the RADIUS server to respond to a RADIUS communication sent from a device and proxied by FortiNAC. This does not indicate that the RADIUS server is not running, simply that it did not accept or respond to the communication. The second type is a failure caused because the RADIUS server is down and FortiNAC cannot communicate with it.



Failover

1. FortiNAC receives a RADIUS communication.
2. The RADIUS communication is proxied to the configured primary RADIUS server.
3. The primary server responds.
4. If the primary server does not respond, the original RADIUS communication is not processed nor is any response sent to the device. FortiNAC contacts the primary RADIUS server with the validation account to validate RADIUS communication.
5. If the primary server responds to FortiNAC, then the primary RADIUS server continues to be used for subsequent incoming RADIUS communications.
6. If the primary server does not respond to FortiNAC, FortiNAC begins sending new RADIUS communications to the secondary RADIUS server.
7. The secondary server responds.

8. If the secondary server does not respond, the RADIUS communication in progress is not processed nor is any response sent to the device. FortiNAC contacts the secondary RADIUS server with the validation account to validate RADIUS communication.
9. If the secondary server responds to FortiNAC, then it continues to be used for subsequent RADIUS communications until contact is re-established with the primary server.

Recovery

1. If the primary server fails FortiNAC continues to attempt to communicate with the primary RADIUS server at six second intervals. This setting is not configurable.
2. The secondary server continues to be used until a response is received from the primary RADIUS server. The primary server is used for subsequent RADIUS communications.
3. If both the primary and the secondary servers have failed, FortiNAC continuously attempts to contact both the primary and the secondary RADIUS servers at six second intervals. The primary server is considered to be "in charge" at that point even though neither server is responding.
4. As soon as either RADIUS server responds, FortiNAC begins sending RADIUS communications to that server.
5. If it is the secondary server that responded, FortiNAC continues trying to contact the primary server. When the primary server responds, it is used for subsequent RADIUS communications.
6. If it is the primary server that responded, FortiNAC uses the primary server for subsequent RADIUS communications.

Validate redundant RADIUS

Validate that your redundant RADIUS servers are functioning properly. That is, when the Primary RADIUS server fails, control passes successfully to the Secondary, which then continues handling authentication messages until control can successfully be returned to the Primary RADIUS server.

To test redundancy, keep the following details in mind:

- The RADIUS server is actually a service running on a server.
- Primary and Secondary RADIUS servers run on separate servers (computers) not on the FortiNAC appliance.
- For this test RADIUS requests are generated by logging in a host through the Captive Portal.

Test setup

1. Log in to the CLI on your FortiNAC appliance and enable debug by typing *campusmgrdebug -name RadiusManager true.*
2. Make sure both RADIUS servers are up and running, so communication is proxied to the Primary.
3. Monitor the output.master file in the /bsc/campusMgr/master_loader directory on the FortiNAC Control Server for the RADIUS messages that are generated by this test.

Force a failover

1. Turn off the Primary RADIUS service.
2. Send a RADIUS request (use a computer to log in through the portal).
3. Verify that the Primary RADIUS server fails to respond. You will see that it retries, and finally times out.
4. Verify that a RADIUS request is initiated using the Validation Account (specified in the RADIUS configuration in the Admin UI for the FortiNAC appliance) and that this also fails. You should see a message in the output.master file similar to “Contact Message being sent".

5. Verify that the Primary RADIUS server is added to the Failover list - you can read that FortiNAC is adding the Primary RADIUS server to the list, and when a new request comes in you will see that FortiNAC checks this list by reading the output.
6. Confirm that requests are sent repeatedly to the Primary RADIUS server to see if it is up and running (e.g., every 5 - 6 seconds).
7. Send a RADIUS request by logging in through the portal again.
8. Confirm that the Secondary RADIUS server responds correctly.

Restore the primary server

1. Turn the Primary RADIUS service back on.
2. Send a RADIUS request by logging in through the portal.
3. Confirm that the Primary RADIUS server responds correctly.

Disable both servers, then restore the primary

1. Turn off both RADIUS services.
2. Send a RADIUS request by logging in through the portal.
3. Verify that requests are sent repeatedly to both the Primary and Secondary RADIUS servers.
4. Turn on the Primary RADIUS server.
5. Send a RADIUS request by logging in through the portal.
6. Confirm that the Primary RADIUS server responds correctly.

Disable both servers, then restore the secondary

1. Turn off both RADIUS services.
2. Turn on the Secondary RADIUS server.
3. Send a RADIUS request by logging in through the portal.
4. Confirm that the Secondary RADIUS server responds correctly.

Roaming guests

Use Roaming Guests to configure a list of local domains for your local network users. Users who connect and attempt to authenticate with a fully qualified domain name that is NOT on this list are treated as Roaming Guests. This feature was developed to accommodate organizations that meet at each other's sites frequently, such as an educational consortium or a business development group. Supports Eduroam for participating universities.

This feature can only be used for wireless 802.1x connections.

RADIUS configuration

Configure your local RADIUS server with the remote RADIUS servers to which it should proxy authentication requests for users who are not part of one of your local domains.

Model configuration

Modify the Model Configuration of any wireless device to which your roaming guests will connect. Specific treatment can be configured for Roaming Guests in the Model Configuration. This controls network access, such as the VLAN in which the host is placed, or access can be denied for Roaming Guests on a particular device. See the information for the Host State field in Model configuration on page 767.

Roaming Guests cannot be controlled at the SSID level only at the device level.

Local domains

Configure the list of local domains. This allows FortiNAC to distinguish between local users and Roaming Guests. See Add Local Domains below for instructions.

Notes

- Roaming Guests may require a supplicant for the wireless connection. This supplicant cannot be configured by FortiNAC. Easy Connect Supplicant Policies cannot be used for Roaming Guests because Roaming Guests are placed in a special network based on the settings in the Model Configuration before the host could be evaluated and assigned a Supplicant Policy.
- Device Profiler automatic registration settings are suspended for Roaming Guests.
- Roaming Guests age out of the database in 24 hours.
- If a Roaming Guest logs into a host registered to a local user, the host is treated like a Roaming Guest.
- If a Roaming Guest logs into an existing Roaming Guest host, they are treated as a Roaming Guest.
- If a Roaming Guest has a Persistent Agent installed on their host from their own FortiNAC system, there is no impact on your FortiNAC server.

Connection process

When a Roaming Guest connects to the network, the process is as follows:

1. FortiNAC proxies the request to a local corporate RADIUS server.
2. The local RADIUS server queries the appropriate remote RADIUS server for the domain name contained in the login information. The remote RADIUS servers must be configured within your corporate RADIUS server to allow the authentication request to be proxied to the correct server.
3. The remote RADIUS server replies to the local corporate RADIUS server.
4. That reply is sent to FortiNAC.
5. FortiNAC registers the host in the database as a device and allows the user to connect to the network. The user is shown as a logged in user.
6. Users are placed in a special Group called Roaming Guest Users.
7. Hosts are placed in a special Group called Roaming Guest Hosts.

Add local domains

1. Click **System > Settings**.
2. Expand the **Authentication** folder.
3. Select **Roaming Guests** from the tree.

4. Click **Add**.
5. Enter a domain name.
6. Click **OK**.

Control

Control groups together options that determine whether or not hosts can access the network or the internet when they are a rogue or are in remediation. Options include:

Option	Definition
Access Point Management	Manage hosts connected to hubs using DHCP as a means to control or restrict host access. See Access point management on page 112.
Allowed Domains	Specify the domains and Production DNS Server that isolated hosts use to gain access to network locations. For example, if hosts are in isolation because they do not have the latest virus definitions for their virus software, they would need to be able to access the web site for their virus software to download virus definitions. See Allowed domains on page 114.
Web Proxy Integration	Configure FortiNAC to work with a web proxy. See Web proxy on page 116.
Quarantine	Globally enables or disables Quarantine VLAN switching and allows the Administrator to set the Risk State for all hosts to Safe. See Quarantine on page 117.

Access point management

Access Point Management provides the ability to manage hosts connected to hubs using DHCP as a means to control or restrict host access.

If the Access Point (AP) was discovered using Device Discovery and the AP supports bridging, FortiNAC automatically puts the AP model in the Bridging Devices group and the interface that the AP is connected to shows up as a link.

For FortiNAC to manage the hosts connecting through the AP the AP must show up connected to an interface of the upstream switch.

Configure an AP

1. Put the Port that the AP is connected to into the Access Point Management group.
2. Remove the AP from the Bridging Devices group.
3. Undo any uplink setting on the interfaces/ports that the APs are connected to within FortiNAC.

a. From Topology click the device to select it.
b. Click the interface/port that is identified as an uplink to select it, then right-click and select Port Properties.
c. Turn the User Defined Uplink off, then click Apply.
d. Right-click the switch model and select Resync Interfaces.

The link goes away and either the AP or a Cloud is connected to the interface/port.

This process has to be done for models that were placed in the Bridging Group that have an AP connected. Each interface/port where an AP is connected on those models needs to be modified so that Access Point Management is applied.

FortiNAC does the following:

- Assigns authorized hosts an IP address from the allocated IP address pool (this allocation is done in the dhcpd.conf file that is updated using the Configuration Wizard)
- Assigns unauthorized hosts an IP address from the allocated IP address pool for all unauthorized hosts (this allocation is done in the dhcpd.conf file that is updated using the Configuration Wizard)
- Updates the DHCP server configuration with authorized IP addresses and the associated MAC Address
- Directs authorized hosts to a valid DNS to allow network access
- Directs unauthorized hosts to FortiNAC’s Access Point Management DNS
- Verifies whether or not the host accessing the network through an access point has a valid IP address in the DHCP lease file
- Generates a Static-IP-Address event if a host’s IP address is not listed in the DHCP lease file maintained by FortiNAC
- Takes action on the Static-IP-Address event when the event is mapped to an alarm and action through the Alarm Mapping functionality

StaticIPAddress event

FortiNAC detects static IP addresses and generates a StaticIPAddress event. When a host connects, FortiNAC checks the DHCP lease file maintained by FortiNAC. If the host’s MAC address is in the DHCP leasefile, FortiNAC allows the host to connect. If the host’s MAC address is not in the DHCP lease file, FortiNAC generates the StaticIPAddress event. You can map this event to an alarm and have action taken on the host. See Map events to alarms on page 888 for details on using this feature.

Configure access point management

Before configuring Access Point Management in FortiNAC make sure that the Access Point Management view with appropriate VLAN ID and IP address ranges has been configured in the Configuration Wizard. See the *Appliance Installation Guide* for directions.

If a host is manually rescanned by selecting rescan on the Host Health tab or an existing scan is manually set to Failed while the host is on the production network, the host remains on the production network until the lease for the IP address expires or the host disconnects from the network. There is no mechanism to move the host to Isolation when it is connected to the network in an Access Point Management environment.

1. Click **System > Settings**.
2. Expand the **Control** folder and click Access Point Management.
3. Click the check box next to **Enable Access Point Management**.
4. In the **Configuration Update** field enter the number of seconds that will lapse between updates to the DHCP Configuration file.

5. Click **Add** below the IP address table to add ranges of possible IP addresses. This table only needs to be configured if detecting hosts with Static IP addresses is required.

   The IP address ranges entered should include all the possible IP addresses that were made available on the network for access point management when the Configuration Wizard was run.
6. Enter the **Starting** and **Ending** IP addresses of a range of possible IP addresses.
7. Click **OK**.
8. Repeat step 6 through step 8 to enter all the ranges of possible IP addresses.
9. Click **Save Settings** to save all changes to the Access Point Management view.
10. Click **System > Groups** view and click the **Access-Point-Management** group to select it.
11. Right-click and select **Modify**.
12. The All Members panel in the Modify Group dialog displays a list of Topology containers. Click the + sign next to the container that has the managed switch, and then click the **+** sign next to the device. Select the port where the access point is connected.
13. Click the right arrow to move the port to the **Selected Members** column.
14. Click **OK**.
15. On the Groups View, with the group still selected, click the **Show Members** button and verify that the port is in the group.
16. To disable hosts on the access point, set a port on the switch to a secure or static port based on the type of switch in use. This is not the port where the Access Point connects; it is another port on the same switch. See Secure port/static port overview on page 776 for additional information.

    Some switches may require the command line interface rather than the FortiNAC User Interface.

When a Restricted host connects a fake DNS is given. This will resolve to the FortiNAC Application Server DNS.

The Application Server DNS directs to a page which redirects the host to a preconfigured URL, based on host state (At Risk or Unregistered, for example) Registration, Remediation, Quarantine, or Dead End.

Allowed domains

Use the Allowed Domains View to specify the domains and Production DNS Server that isolated hosts use to gain access to network locations. For example, if hosts are in isolation because they do not have the latest virus definitions for their virus software, they would need to be able to access the web site for their virus software to download virus definitions.

If you have used a valid SSL certificate to secure the portal, add the domain of the certificate authority to the Domains list, such as verisign.com. This allows the host's browser to validate the certificate.

Field	Definition
IP address	The IP address(es) of the Production DNS Server(s). If the **Prevent the DNS server from making iterative queries** check box is enabled, FortiNAC would no longer perform iterative queries to external authoritative servers. If the DNS server does not find the domain, the DNS server will not continue to perform queries to authoritative name servers. The only DNS requests the FortiNAC server will make on behalf of endpoints are to the specified DNS forwarding IPs.

Field	Definition
Proxy Auto Config	Optional. If you use a Proxy server, this populates the wpad.dat file with the information that allows a host to learn about the Proxy server. This also adds the Domains listed to allow hosts in Isolation to reach sites related to Anti-Virus or Operating System updates required. See Web proxy on page 116 for additional information.
Domains	A list of authorized domains that an isolated host is permitted to access, such as microsoft.com.
Revert To Defaults	Reset the values to the factory settings.

Configure a production DNS server

Enter the IP address(es) of the Production DNS Server(s) for isolated hosts to have access to network Resources.

1. Select **System > Settings**.
2. Expand the **Control** folder and click **Allowed Domains**.
3. Click in the **IP address** field and enter the IP address of the production DNS server. Separate multiple IP addresses with a semicolon (;).
4. Click **Save Settings** to save all of your changes.

Add a domain

Wildcards such as * cannot be used when entering Domain names. You can enter a large domain that contains sub-domains. For example, if you enter Microsoft.com, users can access all domains for Microsoft. However, if you enter a sub-domain, such as downloads.microsoft.com, then users can only access that specific domain.

1. Select **System > Settings**.
2. Expand the **Control** folder and click **Allowed Domains**.
3. In the Domains section of the window, click **Add**.
4. Enter the domain name and click **OK**. Repeat to add additional domains.
5. Click **Save Settings**.

Delete a domain

1. Select **System > Settings**.
2. Expand the **Control** folder and click **Allowed Domains**.
3. In the **Domains** section of the window, click the domain name to select it.
4. Click **Delete**.
5. Click **Save Settings**.

Revert to the default domains list

To revert to the default list of domains and reset the Production DNS IP address:

1. Select **System > Settings**.
2. Expand the **Control** folder and click **Allowed Domains**.
3. Click the **Revert to Defaults** button at the bottom of the **Domains** section.
4. Click **Save Settings**.

Web proxy

If you have a proxy server in your environment, you must configure FortiNAC to direct web traffic to that server when hosts are in isolation. Isolated hosts may need to reach web sites related to their Anti-Virus or Operating System to install updates before being allowed on the production network. If the FortiNAC proxy server configuration is not set up, attempts by isolated hosts to reach these web sites will fail.

Browsers configured with a static Proxy Server cannot be reconfigured by FortiNAC. Proxy settings must be dynamic.

FortiNAC cannot integrate with a pre-configured IP address based proxy.

This document describes a method for hosts on the network to learn about and use a proxy server configured by a network administrator. Each host is configured automatically to use the proxy server instead of needing to be configured manually. If any hosts have already been configured to use a specific proxy server, then this feature will not reconfigure the host.

The web proxy feature can be configured to redirect hosts to a proxy server based on the web site requested. This is only for hosts that have Automatic Proxy Detection enabled.

To redirect hosts you must enable the Proxy Auto Config check box and enter the Proxy server information on the Domains tab of the Portal Configuration View.

If the host requests a web site by IP address, it cannot be redirected to a proxy server. Only requests based on the name or URL of the web site are redirected to a proxy server.

Requirements

• Firmware version 3.x or higher

• FortiNAC version 6.0.3 or higher

• Hosts must have automatic proxy detection enabled in the browser.

Configure proxy server integration

1. Select **System > Settings**.
2. Expand the **Control** folder and click **Allowed Domains**.
3. Click in the **IP address** field and enter the IP address of the Production DNS Server. Separate multiple IP addresses with a semicolon (;).
4. Mark the **Enable Proxy Auto Config** check box with a check mark to enable it.
5. In the field below the check box enter your proxy server information. More than one server can be entered separated by semi-colons (;). Formats can be as follows:
    - **DIRECT** — Fetch the object directly from the content HTTP server denoted by its URL bypassing the proxy server. This can be used as a fall back option in the event that the proxy server cannot be reached. It should be placed at the end of the list of servers.

- **PROXY name:port** — Fetch the object via the proxy HTTP server at the given location (name and port)
- **SOCKS name:port** — Fetch the object via the SOCKS server at the given location (name and port)

Examples:

PROXY 10.0.0.1:8080;

PROXY proxy.example.com:8080

PROXY proxy.example.com:8080; PROXY 10.0.0.2:8080; DIRECT

6. Click Save Settings.

This process updates a special domains file on your FortiNAC Server or Application Server. The contents of that file and the contents of the wpad.dat.custom file are used to generate wpad.dat. Proxy auto-detection using wpad.dat is a widely supported mechanism to deliver a Proxy Auto-Config ("PAC") file, and the only mechanism FortiNAC supports. No other configuration is required.

The wpad.dat.custom file is never overwritten and allows you to make customizations for your particular proxy environment. This file can be edited and is incorporated into the wpad.dat file when that file is generated. The wpad.dat.custom file is stored on your FortiNAC Server or Application Server in the following directory:

```
/bsc/www/portal/ROOT/
```

Quarantine

Quarantine allows the Administrator to set the Risk State for all hosts to Safe. In the event that a scan profile generates significant false negatives which results in multiple hosts being set to At Risk, rather than set each individual host to Safe, this option allows the Administrator to globally change all hosts. Once that has been done, then the scan can be reconfigured and hosts rescanned.

Quarantine VLAN switching can be globally enabled or disabled from the Quarantine view.

1. Click **System > Settings > Control > Quarantine**.
2. Mark the **Enable Quarantine VLAN Switching** check box with a check mark to enable it.
3. If you need to set all hosts to safe, click the **Apply** button.
4. Click **Save Settings**.

Settings

Option	Definition
Quarantine VLAN Switching	When Quarantine VLAN Switching is set to Enable and the ports are in the Forced Remediation Group, the appliance switches unregistered hosts that are being scanned to the Quarantine VLAN until the scan process is completed. Registered hosts are scanned in the production VLAN. Once the scan is finished and the registered host has passed, the host remains in the production VLAN. If the host fails the scan, it is moved to the Quarantine VLAN to remediate. When set to Disable, all hosts remain in the production VLAN during the scan process even if the host fails the scan. Default =Enable
Set all hosts 'Risk State' to 'Safe'	Changes all hosts to Safe.

Identification

Identification groups together methods of detecting and identifying rogue hosts. Options include:

Option	Definition
Device Types	Displays icons representing each device type in the system, and allows you to add, modify, and delete custom device type icons.
NAT Detection	Lists the IP ranges where FortiNAC will allow NAT'd hosts. IP addresses outside this range could be NAT'd hosts and can generate an event and an alarm to notify the network administrator. See NAT detection on page 118.
Rogue DHCP Server Detection	Monitors approved DHCP servers operation and detects rogue DHCP servers on the network using a dedicated interface on the FortiNAC appliance. It defines a scheduled task to run and search specific VLANs and discover all active entities serving IP addresses. This task compares the discovered DHCP servers against a list of authorized DHCP servers and triggers corresponding events when there is no match. See Rogue DHCP server detection on page 122.
Vendor OUIs	Allows you to modify the Vendor OUI database, which is used to determine whether or not a MAC address is valid or by Device Profiler to profile devices by OUI. The database is updated periodically through the Auto Definition update process. See Vendor OUIs on page 127.

NAT detection

A NATing device is a device (e.g., a router) that sits on your network and performs Network Address Translation (NAT) to share network resources with one or more devices behind the NATing device. This could be a security risk to your network. An administrator can see the NATing device by its IP, however, the other devices behind it remain hidden.

NAT Detection has the ability to identify the following:

- A host/device that has a NIC card with an IP that is does not match the IP address of the device connected directly to the port.
- A user is MAC spoofing, where the user registers the host and then sets the NATing device's MAC address to the host's MAC address

The key to NAT detection is identifying the authorized IP ranges (i.e., for Production, Remediation etc.). The Dissolvable or Persistent agent gathers host IP and MAC address information. The NAT device will be within the authorized range, but the host behind it is served an IP by the NAT device and its IP is outside the range. This mismatch triggers events and alarms that indicate that a NATing device is being used.

The information gathered by the agent is returned to the FortiNAC server and analyzed as follows:

- FortiNAC determines whether or not the IP address of the device connected directly to the port is within the range specified for NAT detection.
- If the IP address is within the NAT detection range, then FortiNAC verifies that one of the IP addresses returned by the Agent matches the IP address of the device connected directly to the port. The agent can only return the IP

addresses of the host, not the NAT device. If none of the IP addresses of the host sent match the IP address of the device on the port, then a "Possible NAT User" event is generated.

If a network user sets local or self-signed IP addresses on the host that is behind the NAT device, no event is triggered.

- The agent also returns the MAC addresses of the interfaces on the host. If FortiNAC detects that the device connected to the port and the interfaces on the host have the same MAC address, it generates a "Possible NAT Device, MAC Spoofed" event.

By mapping alarms to notify management when these events occur, you can identify and remove NATing devices from your network.

If you want to allow a router with hosts connected behind it to access your network, you must enable NAT Detection by entering the IP Ranges within which using a NAT device is permitted and detected. If NAT Detection is not enabled, or the router is given an IP address that is not within a NAT detection range, both the router and the host behind it are left in registration. The administrator is not notified that a NAT device is connected.

To run NAT Detection, the following requirements must be met:

- Hosts must use either the Dissolvable or the Persistent Agent
- At least one Security Policy must be defined to use the Dissolvable or Persistent Agent
- Designate the IP address ranges that FortiNAC should monitor.
- Map the NAT detection events to alarms with an appropriate action (e.g., notify management). See Map events to alarms on page 888 for details.

If you have a host trying to connect through a router, and that router is not in an IP address range being checked for NAT Detection, that host will be stuck in Registration. Create IP address Ranges in NAT Detection that encompass any of IP address the router could be given.

Add or modify IP ranges

You must enter a separate range of IP addresses for each subnet.

Example:

Range 1 = 192.168.5.2 - 192.168.5.255

Range 2 = 192.168.6.2 - 192.168.6.255

Do not enter a single range spanning both of the above 192.168.5.2 - 192.168.6.255

1. Click **System > Settings**.
2. Expand the **Identification** folder and click **NAT Detection**.
3. Click **Add**.
4. Enter the starting and ending IP addresses for the range and click **Add**.
5. Repeat for additional ranges of IP addresses.

Remove an IP range

1. Click **System > Settings**.
2. Expand the **Identification** folder and click **NAT Detection**.
3. Select an IP range to be deleted.
4. Click **Delete**.

NAT detection configurations and results

NAT detection configuration and corresponding results can be complex. Below are a series of examples detailing common scenarios and the results shown in FortiNAC.

The IP addresses used in the examples below are only for illustration purposes. They are not the specific IP addresses you will see on your own network.

For the purposes of the examples assume the following:

- Network IP Range for Production = 10.10.5.50 - 10.10.5.99
- Network IP Range for Registration = 10.10.5.100 - 10.10.5.200
- NAT Detection has been configured with the following IP Ranges:
  - 10.10.5.50 - 10.10.5.99
  - 10.10.5.100 - 10.10.5.200

Scenario 1: NAT detection enabled, using endpoint compliance policy and agent

1. The user connects a router to a port on your network and then connects a host to the router.
2. Neither the router nor the host are registered.
3. The router is placed in Registration and is given a Registration IP address of 10.10.5.101. The host is given IP address 192.168.1.1 by the router.
4. The user goes through the registration process and is assigned an Endpoint Compliance Policy.

NAT Detection requires that the host have an agent installed.

5. The IP address of the router is within one of the IP ranges set up for NAT Detection. The IP address of the host is sent by the agent to FortiNAC. FortiNAC determines that the host IP address is outside the IP ranges set up for NAT Detection. This process triggers a "NAT Device Registered" event.
6. When the host itself is registered a "Possible NAT User" event is triggered.
7. On the Host View the router has been registered as a NAT Device to the user. The router has an IP address in the Production range, such as 10.10.5.51. The Registered To field displays User Name - NAT Device, such as Doe, John - NAT Device. The Host icon is displayed and shows as on-line.
8. On the Host View the PC behind the router is registered as a host to the user. The Host's IP address displays as a production IP address, such as 10.10.5.50. However, the host actually still has the IP served by the router of 192.168.1.1. The Registered To field displays only the user name, such as Doe, John. The Host icon is displayed and shows as offline even though the host is on-line.

Scenario 2: NAT detection enabled, not using endpoint compliance policy or agent

1. The user connects a router to a port on your network and then connects a host to the router.
2. Neither the router nor the host are registered.
3. The router is placed in Registration and is given a Registration IP address of 10.10.5.101. The host is given IP address 192.168.1.1 by the router.
4. The user goes through the registration process.
5. On the Host View the router has been registered as a PC to the user. The host connected to the router is not shown because FortiNAC is unaware of the host's existence behind the router.
6. Events associated with a NAT device are not generated.
7. Eventually the router is moved to Production and the host can access the network and the Internet. This may require the user to release and renew the IP address on the router by disconnecting and reconnecting the router to the port.

Scenario 3: NAT detection disabled, not using endpoint compliance policy or agent

1. The user connects a router to a port on your network and then connects a host to the router.
2. Neither the router nor the host are registered.
3. The router is placed in Registration and is given a Registration IP address of 10.10.5.101. The host is given IP address 192.168.1.1 by the router.
4. The user goes through the Registration process, but there is no Endpoint Compliance Policy required. The user does not download an agent.
5. The only IP address information provided to FortiNAC is the information returned from the switch where the router is connected when it is polled.
6. The router is assigned a Production IP address, such as 10.10.5.55.
7. The host behind the router continues to use the 192.168.1.1 IP address assigned by the router.
8. On the Host View the router has been registered to the user, but FortiNAC is unaware that this device is a NAT Device. The Registered To field displays User Name, such as Doe, John . The Host icon is displayed and shows as on-line.
9. FortiNAC is not aware of the host behind the router, therefore, its information is not displayed. The user of this host can access the network and the Internet.
10. In this scenario the user may need to release/renew the IP address on both the host and the router to access the Internet.

Scenario 4: NAT detection disabled, using endpoint compliance policy and agent

1. The user connects a router to a port on your network and then connects a host to the router.
2. Neither the router nor the host are registered.
3. The router is placed in Registration and is given a Registration IP address of 10.10.5.101. The host is given IP address 192.168.1.1 by the router.
4. The user goes through the Registration process and is assigned an Endpoint Compliance Policy which includes downloading and installing either the Dissolvable or the Persistent Agent.
5. The router is not registered and is trapped in the registration VLAN. The host is registered but is also trapped in the registration VLAN because it is connected to the router.
6. In the Host View, the router continues to display as a rogue. The host is registered but shows as offline.

Rogue DHCP server detection

Rogue DHCP Detection monitors approved DHCP servers operation and detects rogue DHCP servers on the network. This feature uses a dedicated interface on the FortiNAC appliance. It defines a scheduled task to run and search specific VLANs and discover all active entities serving IP addresses. When the Rogue DHCP Detection task runs, it will switch the port designated as the System DHCP Port to each of the VLANs designated. During the switch to each VLAN, the port admin state is set to down then back to up after the configuration to the new VLAN ID. This task compares the discovered DHCP servers against a list of authorized DHCP servers and triggers corresponding events when there is no match. These are suspected unauthorized DHCP servers and are managed according to the alarms that are mapped to the events.

Implementation

- To perform Rogue DHCP Server Detection with FortiNACa dedicated network interface is required. Installation of an additional Network Card may be required.
- The interface on the FortiNAC appliance used for Rogue DHCP Server Detection must be configured with an IP address. This should be an unused IP address from an unused subnet on your network. Configure the IP address through the CLI by modifying the `vlanInterfaces` file in `/bsc/siteConfiguration`. If you are unfamiliar with this file, contact Customer Support for assistance.
- The interface on the FortiNAC appliance used for Rogue DHCP Server Detection must be configured in FortiNAC.
- The Authorized DHCP Servers must be added to the Authorized DHCP Servers group.
- The DHCP Port must be indicated in the System DHCP Port group.
- Polling VLANs for Rogue DHCP servers must be scheduled.

If IP Helper is being utilized on the network an additional configuration step will be required to make FortiNAC aware of the Authorized DHCP Servers.

Rogue DHCP events and alarms

Event	Definition
Rogue Host DHCP Server Application	A host is serving IP addresses (i.e., a DHCP response was seen from a host).
Rogue Device DHCP Server Application	A device is serving IP addresses.

These events can be mapped to alarms. Alarms can be set to notify an administrator when they are triggered. Alarms can also be viewed on the Alarms Panel in the Dashboard. For more information on events and alarms, e-mail notifications, SMS notifications, and how to map events to alarms see Map events to alarms on page 888.

Configure an IP address for a new interface

To modify an IP address for the eth0 or eth1 interface, use the Configuration Wizard.

To add an IP to an interface (other than the eth0 and eth1 interface), add an entry to the appropriate interface in the `vlanInterfaces` file and run the `network restart` command as follows:

1. Access the CLI on the FortiNAC Server or Application Server.
2. Navigate to the `siteConfiguration` directory.
   ```
   cd /bsc/siteConfiguration
   ```
3. Edit the `vlanInterfaces` file.
4. Add the new IP address to the appropriate interface. The following example adds IPADDR_1 to eth2:
   ```
   ifcfg-eth2|IPADDR='188.11.32.2', NETMASK='
   255.255.255.0',STARTMODE='onboot',BOOTPROTO='static',
   IPADDR_1='188.11.32.3',NETMASK_1='255.255.255.0',LABEL_1='1'
   ```
5. Run the following command(s).
   ```
   service bsc-network start
   service network restart
   ```

Server detection configuration

Rogue DHCP Server Detection Configuration allows you to indicate which interface on the appliance is used for scanning VLANS. The interface used varies depending on the configuration of your FortiNAC environment.

All FortiNAC Appliances

The eth0 interface is always used for management and cannot be used for rogue DHCP detection.

FortiNAC Server

On a FortiNAC Server, eth1 is typically used for the captive portal, leaving eth2 for Rogue DHCP Server Detection.

FortiNAC Control Server/Application Server Pair

On a FortiNAC Application Server / Control Server pair, the captive portal is typically on eth1 on the Application Server. You could use could use eth1 on the Control Server for Rogue DHCP Server Detection. You may need to add a network card to your server to provide an interface for Rogue DHCP Server Detection.

Once you have determined the interface to use for Rogue DHCP Server Detection, it must be configured with an IP address. The IP address should be an unused address from an unused subnet on your network. To configure the IP address go to the CLI on the server and modify the `vlanInterfaces` file in `/bsc/siteConfiguration`. When the interface has been configured, enter it on this view.

If you are using Rogue DHCP Server Detection in a High Availability environment, both the primary and secondary servers must have the same Interface setting. In addition, the ports to which the Interfaces connect must be added to the System DHCP Port group. See Modify a group on page 841 for details.

In the event of a failover, it is important that these fields be setup correctly or DHCP monitoring will not run.

Settings

Field	Definition
Interface	Ethernet interface used by the FortiNAC appliance for Rogue DHCP Server Configuration, such as eth2.
Authorized DHCP Servers	Device group containing the list of servers that are authorized to serve DHCP. The Authorized DHCP Servers group can be modified here or on the Groups View.
System DHCP Ports	Port group containing the port where the FortiNAC interface is connected to the network. The System DHCP Ports group can be modified here or on the Groups View.
VLANs To Scan For Rogue DHCP Servers	ID and Name of the VLANs that should be scanned for Rogue DHCP servers. If a VLAN is not entered in the list, it is not scanned for Rogue DHCP servers. Only the VLANs entered here are scanned.
Schedule DHCP Server Verification	Use a scheduled task to set the poll interval and scheduled time to poll the selected VLANs for rogue DHCP servers.

Configure server detection

1. Click **System > Settings**.
2. Expand the **Identification** folder.
3. Select **Rogue DHCP Server Detection** from the tree.
4. In the **Interface** field enter the ethernet interface used by the FortiNAC appliance for Rogue DHCP Server Configuration.
5. Click the **Modify** button next to **Authorized DHCP Servers** to add the servers that are allowed to serve DHCP into the Authorized DHCP Server group.
6. On the Modify Group dialog click the **Container** where the servers are located to expand the list. Mark each server with a check mark and click the right arrow button in the center of the screen to move the selected servers to the Selected Members column.
7. Click **OK** to save the changes to the group.
8. Click the **Modify** button next to **System DHCP Ports** to update the System DHCP Ports group with the port where the FortiNAC interface is connected to the network.
9. On the Modify Group dialog click the **Container** where the switch is located.
10. Click the switch where the FortiNAC Rogue DHCP Detection Server interface is connected. A list of the ports on the selected switch appears below the switch.

Select the switch and port where the FortiNAC network card is connected, such as eth1 or eth2. This is the connection that will handle the scanning for Rogue DHCP Servers. Do NOT select the DHCP Server itself or the port the DHCP Server is connected to. Do NOT select the switch or port where the FortiNAC eth0 network card is connected.

11. Select the **Port** where the Rogue DHCP Detection server is connected and click the right arrow button to move the port to the Selected Members column.
12. Click **OK** to save the changes to the group.
13. In the **VLANs To Scan For Rogue DHCP Servers** section, click **Add**.
14. In the **Add** dialog enter the ID and Name of the VLANs that should be scanned for Rogue DHCP servers and click

OK.

If a VLAN is not entered in the list, it is not scanned for Rogue DHCP servers. Only the VLANs entered here are scanned.

15. Click Save Settings.

Schedule DHCP server verification

Use the Schedule option to set the poll interval and scheduled time to poll the selected VLANs for rogue DHCP servers.

1. Click **System > Settings**.
2. Expand the **Identification** folder.
3. Select **Rogue DHCP Server Detection** from the tree.
4. Click **Modify Schedule**.
5. Select the **Enabled** check box.
6. Enter a name for the task in the Name field.
7. The **Description** field is optional. Enter a description of the task.
8. Action type and Action are pre-configured based on the task and cannot be modified.
9. From the **Schedule Type** drop down list, select either **Fixed Day** or **Repetitive** and set the day and time that the task is to be performed.
10. A **Fixed Day Task** is one in which you schedule a task to run on a combination of days of the week and times of the day, such as Mondays at 1:00 pm and Fridays at 10:00 am. Select the day(s) and time to run the task.
    a. Click the box next to the day(s) to select the day.
    b. Click the down arrows and select the hour, minutes, and AM or PM from the drop-down list for each day.
    c. To enter days/times more quickly, use the **Set Multiple Days** button to set multiple days with the same time.
    d. To remove all settings click the **Clear All** button.
11. A **Repetitive Task** is one that you schedule to start on a given day, at a certain time, for the number of times you specify, such as every 10 days starting today. The repetition rate can be set to any number of minutes, hours, or days.
    a. Enter the **Repetition Rate** using whole numbers.

       A repetition rate of zero causes the task to run only once.

    b. Click the down arrow and select **Minutes**, **Hours**, or **Days** from the drop-down list.
    c. Enter the date and time for the task to run in the **Next Scheduled Time** field using the format MM/DD/YY hh:mm AM/PM Time Zone.

       The new Repetition Rate does not take effect immediately. It starts the next time the scheduled task runs. For the new Repetition Rate take effect immediately, click the **Update** button.

    d. Click **Update** to update the **Next Scheduled Time** field or change the **Repetition Rate**.

12. Click **OK**.
13. Click **Save Settings**.

Schedule settings

Field	Definition
Remove local backups older than	Number of days for which you would like to keep backups. Anything older than the number of days entered, is removed the next time the scheduled task for backups runs. This setting removes backup files created on the FortiNAC server before they are copied to the remote server. Backups on the remote server are not removed. The timing of the scheduled backup task and the age of the files that are to be removed must be thought out carefully or you will remove all of your backups. For example, if the remove option is set to 5 days and your backup task runs every 15 days, you may inadvertently remove all of your backups. However, if the remove option is set to 15 days and the backup task runs every 5 days, then you would always have backup files.
Status	Indicates whether the task is Enabled or Disabled.
Schedule Interval	How often the scheduled task runs. Options are Minutes, Hours, or Days.
Next Scheduled Time	The next date and time the scheduled synchronization task will run. Entered in the format MM/DD/YY HH:MM AM/PM
Modify Schedule	Allows you to modify the scheduled activity.
Run Now	Runs the scheduled task immediately.

Rogue DHCP server detection with IP helper

When IP Helper is in use, an IP address for the Authorized DHCP Server is returned to FortiNAC for each VLAN. This IP address has a MAC address associated with it. FortiNAC compares the IP address it receives with the list of valid Authorized DHCP Server IP addresses. If the FortiNAC list does not contain the IP and the related MAC Address, it does not recognize the DHCP Server as authorized.

The following procedure must be completed to enable FortiNAC to recognize the returned Authorized DHCP Server IP addresses as valid.

1. Create a Pingable model in the Topology View for each IP Helper Address.
   a. In the Topology view, click the container where devices are located.
   b. Right-click and select **Add Pingable Device**.
   c. Enter the **Device Name**, **IP address**, **Protocol** (set to Pingable), and select the **Device Type** of Pingable.
   d. Click **Apply**.
2. Ensure that the Pingable model has a MAC address.
   a. Click the **Pingable model** in the Topology view to select it.
   b. Right-click and select **Properties**.
   c. Enter the **MAC address** associated with the IP address.

   d. Click **Apply**.
   e. Close the **Device Properties** window.
3. Place the Pingable model in the Authorized DHCP Server group.
   a. Select **System > Groups**.
   b. Click the **Authorized DHCP Servers** group to select it.
   c. Right-click and select **Modify**.
   d. Click the container where the Pingable models were created. A list of the devices in the container will be displayed in the below the container.
   e. Click the **Pingable model(s)** to mark them with a check mark.
   f. Click the right arrow to move your selections to the **Selected Members** column.
   g. Click **OK**.
   h. Select the Group in the Groups View, click the **Show Members** button and verify that all the Pingable models for the IP Helper IP addresses are listed.

Vendor OUIs

Use the Vendor OUI database to determine whether a particular MAC is valid. As new IEEE device information becomes available, the database needs to be updated to reflect the new codes. This prevents *invalid physical address* errors when devices with the new MACs are connected to the network. The AutoDef Synchronization scheduled task automatically updates the Vendor OUI database. See Scheduler view on page 849 for additional information on scheduling tasks.

You can search the Vendor OUI database, and add, modify, or remove Vendor OUIs. Vendor OUI Added and Vendor OUI Removed events are generated when you add or remove Vendor OUIs.

The Vendor Name appears in the Host view unless you enter a Vendor OUI alias. If you use a Vendor OUI alias to identify the type of device, you can quickly filter all devices with a specific alias. For example, you can manage gaming devices by adding the Vendor OUI to the database with the Vendor OUI alias of *Gaming Device.* Then you can use the Host view filter to find these records by name, change them to registered, and assign them a role without requiring the device to be assigned to a user.

Vendor OUIs are also used with the Device Profiler feature. Device Profiling Rules can use the Vendor OUI to help identify rogue devices connecting the network. Depending on the instructions associated with the rule, the device can be automatically assigned a device type and be placed in the Host View, the Topology View or both. See Device profiler on page 348 for additional information.

To access the Vendor OUI View select **System > Settings > Identification > Vendor OUIs**. See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.

Add a vendor OUI

1. Click **System > Settings**.
2. Expand the **Identification** folder and click **Vendor OUIs**.
3. Click **Add** at the bottom of the window.
4. Use the table below to enter the Vendor OUI information:

Field	Description
Vendor OUI	First 3 octets of a device's Physical Address. Enter in the hexadecimal format ##:##:## (For example, 00:1D:09)
Vendor Name	Name of the Vendor that owns the Vendor OUI.
Vendor Alias	Value entered displays as the Host Name in the Host view. This field is optional when adding a Vendor OUI.
Role	Role for devices associated with this Vendor OUI. Roles assigned by Device Profiler take precedence. If a device is registered via the Portal Page, then the role associated with the Vendor OUI is applied. See Role management on page 553.
Registration Type	Type of device registration that is specified through the AutoDef Synchronization update, such as a Camera, a Card Reader or a Gaming Device. In the Add/Modify Vendor Code dialog the current setting for the vendor code Registration Type is displayed. Options include Manual or a specific device type.
Registration Type Override	Used to specify a Registration Type that is different from the default supplied by the AutoDef Synchronization update. Options include Manual or a specific device type.
Description	User specified description of the Vendor OUI.
Last Modified By	User name of the last user to modify the Vendor OUI.
Last Modified Date	Date and time of the last modification to this Vendor OUI.
Right click options	
Delete	Deletes the selected Vendor OUI.
Modify	Opens the Modify Vendor OUI dialog.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.
Buttons	
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.

5. The **Description** field is optional and allows you to add notes about the OUI. This field is not displayed on the Vendor OUIs view.
6. Select the **Registration Type Override** for the device.
7. Click **OK**.

Modify a vendor OUI

1. Click **System > Settings**.
2. Expand the **Identification** folder and click **Vendor OUIs**.
3. Search for the appropriate Vendor OUI and select it. Click **Modify**.
4. Edit the Vendor OUI information
5. The **Description** field is optional.
6. Click **OK**.

Modify multiple vendor OUIs

Multiple Vendor OUIs can be modified at the same time to update fields such as Role or Description.

1. Click **System > Settings**.
2. Expand the **Identification** folder and click **Vendor OUIs**.
3. Search for the appropriate Vendor OUIs. Select all of the affected Vendor OUIs. If they are not part of a continuous list, hold down the CTRL key to select them.
4. Click **Modify**.
5. On the Modify dialog enable the check boxes next to the fields to be updated. Any field that is not enabled will not be affected.
6. Modify the data in the selected fields.
7. Click **OK**.

Delete a vendor OUI

1. Click **System > Settings**.
2. Expand the **Identification** folder and click **Vendor OUIs**.
3. Search for the Vendor OUI to be deleted and select it.
4. Click **Delete**.
5. A confirmation message is displayed. Click **Yes** to delete the OUI.

Register devices

To register devices, such as gaming devices, you must enter the Vendor OUIs in the Vendor OUI database. When the host connects the device to the network a rogue host record is created.

If you are using the Device Profiler feature, these devices may be processed by a Device Profiling Rule that registers them for you.

1. Enter the Vendor OUIs into the database.
2. When entering the Vendor OUI be sure to fill in the **Vendor Alias** field. This alias displays on the Host View when a device with this Vendor OUI connects to the network.
3. If this device requires a role, select a **Role** on the Vendor OUI window. This role is only applied to devices registered manually through the Portal Page.

4. In order to register a device you must make sure that the **Registration Type Override** field in the Vendor OUI window is set to reflect the correct device type. For example, if this Vendor OUI represents a gaming device, you would select Gaming Device from the list in this field.
5. Once the device is connected to the network, click **Hosts > Host View**.
6. Locate the record for the rogue device.
7. Select the record. Then, right-click and select **Register As Device**.

Device registration after vendor OUI database update

Devices whose Vendor OUIs are not in the database appear in the Host view as rogues when they connect to the network. Once you have entered the Vendor OUI in the database, the information in the Host view displays the Vendor OUI data as part of the rogue record. Use the Vendor Alias to identify the type of device, such as gaming device or security camera, for example. The Vendor Alias is displayed in the Host Name column of the Host view.

1. Add the Vendor OUI information to the database. Include the Vendor Alias to aid in grouping the devices.
2. Go to the Host View and use the filter tabs or column sort features to locate the devices.
3. Select the record(s) and change the device to Registered using the Register As Device option on the right-click menu.

Network device

Network Device allows you to set global properties that are specific to network devices and VLANs.

1. Click **System > Settings**.
2. Select **Network Device** from the tree.
3. Click a field and enter a setting. See the table below for settings.
4. Click **Save Settings**.

Settings

Field	Definition
Agent Switching Delay (Sec)	Number of seconds FortiNAC waits before a host that has failed the Persistent Agent Check will be switched to the Quarantine or Remediation VLAN. Default = 0 seconds
Minimum Trap Period (Sec)	Number of seconds FortiNAC waits after receiving a linkup trap before reading the forwarding table from the switch associated with the trap. Default setting = 10 seconds

Field	Definition
Max Number of Trap Periods	Maximum number of Trap Periods that the appliance waits before reading the switch forwarding tables. If the switch does not have the MAC address information for the port that generated the linkup trap, the appliance places the switch back into the queue. Once the Minimum Trap Period has expired, the forwarding table on the switch is read again. If another linkup trap is generated by the same switch the trap period time is reset. Default setting = 4 For example, if the Minimum Trap Period is set to 20 seconds and the Max Number of Trap Periods is set to 2, the longest the appliance will wait to read the switch forwarding tables is 40 seconds.
Registration Delay (Sec)	Number of seconds FortiNAC waits before switching a port to the production VLAN. This allows the user registering a host time to read the information on the Registration Success page. Default setting = 5 seconds If another host connects to the same switch during the Registration Delay time, the switch updates and the port is switched to the production VLAN without waiting for the delay time to expire.
System Defined Uplink Count	When the number of MAC addresses on a port exceeds this value the port is changed to an uplink. Setting this value to a higher number can help to indicate Multi-Access points. Default setting = 20 For example, setting this value to 7 changes the port to an uplink if a minihub with 8 ports is connected on the port. See Port properties on page 784.
Telnet Connection Timeout (Sec)	When using telnet to contact devices, this setting determines how long the server waits for a response from the device before timing out. Default = 12 seconds
VLAN Reset Delay (Sec)	Number of seconds FortiNAC waits before resetting the VLAN of a port that has no connected hosts or devices. The port must be a member of either the Reset to Registration group or the Reset to Default port group. If the port is a member of both groups, the Registration VLAN takes precedence. Default = 60 seconds

Field	Definition
VLAN Switching Delay (Sec)	Number of seconds FortiNAC waits between disabling and reenabling a port when switching it to another VLAN. Default setting = 8 seconds If this value is left as zero (0) the host may have an invalid IP on the new VLAN.
MAC Address Spoof Time Delay (Minutes)	The number of minutes after which, if the same MAC address has been detected on two devices/ports simultaneously, the Possible MAC Address Spoof event will be generated. The default is set to 5 minutes. A long age time in a host may cause the MAC address of the host to be falsely reported as connected to more than one device at the same time. For example, Host A is connected to Switch A with an age time of 10 minutes. Host A is moved to Switch B and FortiNAC updates the location. FortiNAC reads Switch A which still shows Host A as online because Host A has not yet aged out.
Enable Multi-Access Detection	When enabled, the appliance looks for multiple MAC addresses on ports each time a switch is read. Default = Disabled To have an event generated when multiple MAC addresses are detected on a port the Multi-Access Point Detected event must also be enabled. However, if the port is in the Authorized Access Points group an event is not generated. See Event management on page 856 to enable the Multi-Access Point Detected event. See System groups on page 843 to determine if the port is in the Authorized Access Points group.
Multi-Access Detection Threshold	The number of MAC addresses that are allowed on a port before a Multi-Access Point Detected event is generated.
Enable Cisco Discovery Protocol	When enabled, allows FortiNAC to query devices about other connected devices on the network. If a device has this discovery protocol enabled it gathers and stores information about devices it manages and devices it can contact on the network. Only devices with CDP enabled will respond to a CDP query. This is a global setting for the system. If this setting is enabled, devices can be set individually on the Polling Tab of the Device Properties View. If this setting is disabled, the device setting is ignored and the CDP feature is not used when polling a device. Devices that have the capacity for CDP must have the feature configured on the device's firmware. Default = Enabled
Maximum Cisco Discovery Depth	Limits the number of layers from the original device that will be queried using Cisco Discovery Protocol. For example, if the Depth is set to 1, then FortiNAC will only query for devices that are directly connected to the device with the starting IP address during the Discovery process. If the Depth is set to 2, then FortiNAC stops querying after it reaches the second level of devices away from the starting IP address.

Field	Definition
	See Discover devices on page 735.
Ignore MAC Notification Traps for IP Phones	When enabled, FortiNAC will not process MAC Notification Traps for IP Phones. This setting is enabled by default. Disabling this setting may cause FortiNAC to process large numbers of traps, resulting in decreased performance.

Persistent Agent settings

Persistent Agent groups together properties for the use and behavior of the Persistent Agent and the configuration for updating the Persistent Agent installed on existing hosts to a different version.

Navigate to **Policy > Persistent Agent Properties**.

Options

Option	Definition
Agent Update	Globally update hosts on your network that already have a Persistent Agent installed. See Global updates on page 134.
Credential Configuration	Configure how credentials are verified for hosts who use the Persistent Agent. See Credential configuration on page 139.
Security Management	Configure the following: Host Name of the server for Persistent Agent communication. Host group whose members receive the Host Name when they connect. Whether display notifications will be sent to the host. Header and footer text for the Persistent Agent Authentication page. Status messages in the message box on the user's desktop. See Security management on page 140.
Status Notifications	Use the Status Notifications view to configure how users are notified of their host status when the Persistent Agent contacts the FortiNAC server. See Status notifications on page 145.
Transport Configuration	Configure TCP and UDP communication between the FortiNAC server and the Persistent Agent. See Transport configurations on page 148.

Option	Definition
USB Detection	Use the USB Detection view allows to configure FortiNAC to be notified in the event that a USB device was plugged into a host on the network. See USB detection on page 151.

Global updates

Hosts on your network that already have a version of the Persistent Agent installed can be globally updated. The update is triggered when a host connects to the network and the current Persistent Agent begins to communicate with FortiNAC.

The Persistent Agent version number on the host is checked by FortiNAC. If the version is different than the one selected on the Agent Update window, an update is initiated.

Clients upgrading the Persistent Agent must have access to Port 80 on the FortiNAC appliances.

It is only the difference in version number that triggers the update. FortiNAC does not check to see if the existing number is higher or lower than the update. This allows you to go back to a previous Persistent Agent if necessary.

If the host has software installed to reset the host to its original configuration after a re-boot, the agent reverts to the previous version. The software must be disabled before updating the Agent.

Update failure

A maximum number of attempts to update limits the number of times FortiNAC tries to update the host. If the maximum number of attempts has already been met, then no update is sent.

To address this you have several options. If a large number of hosts have failed the update, use the **Reset Counter** button on the Agent Update window to set the counter for all hosts to 0. If only a few hosts have failed the update, the Agent Version can be updated individually. Another option is to increase the Maximum Attempts on the Agent Update window to force an update. However, if the original problem has not been addressed the update will probably fail again.

Reset hosts that failed to update

If you have a large number of hosts that failed to update successfully and the Maximum Global Update Attempts count for those hosts was exceeded, the counter can be reset allowing the system to try to update those hosts again. The counter is reset for all hosts in the database, however, the system will not attempt to update hosts that successfully updated earlier.

1. Click **System > Settings**.
2. Expand the **Persistent Agent** folder.
3. Select **Agent Update** from the tree.
4. Click the **Reset Counter** button.

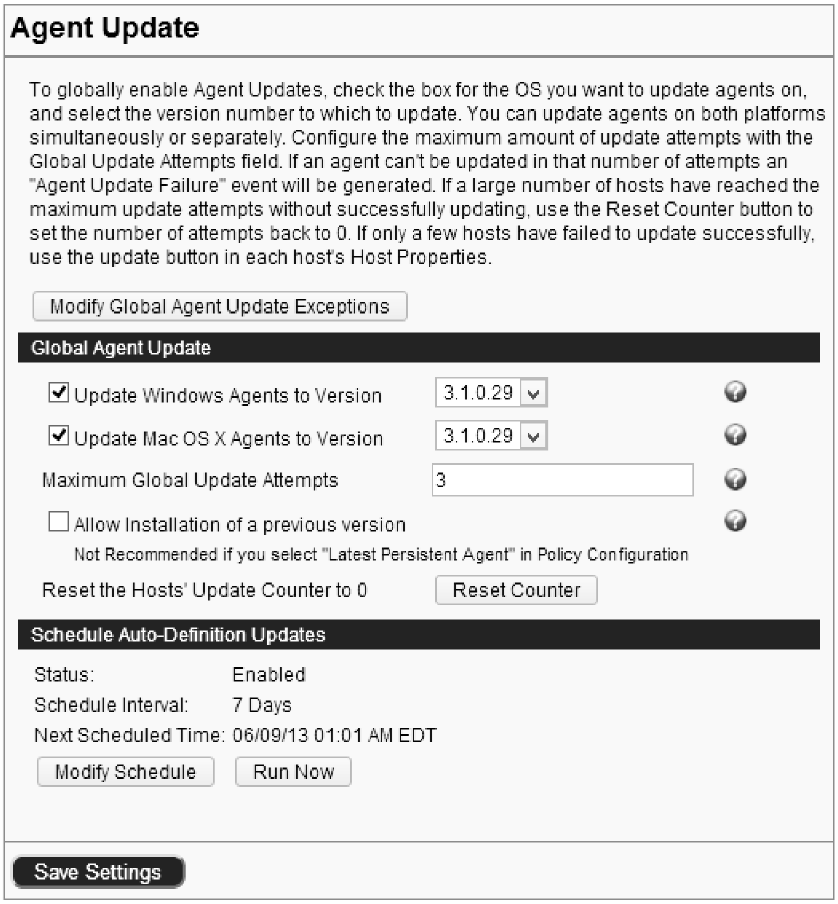
Event generation

When an update fails because the maximum number of attempts has been met, an **Agent Update Failure** event is generated. The default setting for this event is Enabled. See Enable and disable events on page 857 to modify the default setting. Enabled events are recorded and can be viewed. See Events view on page 867.

When an update is successful an **Agent Update Success** event is generated. The default setting for this event is Disabled. Disabled events are not recorded and cannot be viewed later.

Alarms can be associated with enabled events. See Map events to alarms on page 888. Alarms can be configured to send e-mail notifications or simply display on the Dashboard in the Alarm panel.

Set up global updates



Agent Update

To globally enable Agent Updates, check the box for the OS you want to update agents on, and select the version number to which to update. You can update agents on both platforms simultaneously or separately. Configure the maximum amount of update attempts with the Global Update Attempts field. If an agent can't be updated in that number of attempts an "Agent Update Failure" event will be generated. If a large number of hosts have reached the maximum update attempts without successfully updating, use the Reset Counter button to set the number of attempts back to 0. If only a few hosts have failed to update successfully, use the update button in each host's Host Properties.

Global Agent Update

☑ Update Windows Agents to Version: 3.1.0.29

☑ Update Mac OS X Agents to Version: 3.1.0.29

Maximum Global Update Attempts: 3

☐ Allow Installation of a previous version

Not Recommended if you select "Latest Persistent Agent" in Policy Configuration

Reset the Hosts' Update Counter to 0

Schedule Auto-Definition Updates

Status: Enabled
Schedule Interval: 7 Days
Next Scheduled Time: 06/09/13 01:01 AM EDT

1. Click **System > Settings**.
2. Expand the **Persistent Agent** folder.
3. Select **Agent Update** from the tree.

4. Click the check box(es) to enable an update.
5. Click in the drop-down box and select the Persistent Agent Version for the update.
6. Click in the **Maximum Global Update Attempts** field and enter the number of times the update feature should attempt to update the Persistent Agent for each host.
7. If you need to trigger the installation of an earlier version of the Agent, click **Allow Installation of a Previous Version** and make sure the correct version is selected in the version fields. Typically this would remain unchecked because you would want to move to the newest version of the Agent.

If you have selected **Latest Persistent Agent** as the agent to download on the Endpoint Compliance Configuration window for any configuration, you should not check this option.

Your hosts could end up in a situation where the latest agent is installed based on the Endpoint Compliance Policy used when the host is registered, then an older agent is installed because this option is checked and the agent selected is older than the latest agent.

8. Click **Save Settings**.

Settings

Field	Definition
Modify Global Agent Update Exceptions	Opens the Global Agent Update Exceptions Group and allows you to add or remove hosts. This group can also be modified from the Groups View. Hosts in this group are never automatically updated. See the **Exclude Hosts From the Update** section below this table.
Update Windows Agents To Version	If enabled, Windows hosts with a Persistent Agent installed will be updated if the version number on the agent currently installed is different than the version selected in the drop-down list. A lower agent version will not be installed unless the **Allow Installation of a Previous Version** option is checked.
Update macOS Agents To Version	If enabled, macOS hosts with a Persistent Agent installed will be updated if the version number on the agent currently installed is different than the version selected in the drop-down list. A lower agent version will not be installed unless the **Allow Installation of a Previous Version** option is checked.
Maximum Global Update Attempts	Number of times FortiNAC should attempt to update the Persistent Agent for each host. If the maximum is reached and some hosts have not been updated, use the **Reset Counter** button to clear the number of attempts for all hosts and try again.
Allow Installation Of A Previous Version	If enabled, FortiNAC will update the agent on a host even if the installed agent is a higher version than the agent selected for update.
Reset The Hosts Update Counter To 0	The **Reset Counter** button clears the number of update attempts from the Host record for all hosts. This allows FortiNAC to attempt to update hosts that were not successfully updated previously. See the **Reset Hosts That Failed To Update** section above this table.

Field	Definition
Schedule Auto-Definition Updates	Allows you to schedule updates that include: • Information on the latest Anti-Virus definitions • Support for new versions of Anti-Virus • Support for new operating system versions • Any new Vendor OUIs released by the IEEE Standards Association • New or modified Custom Scan options

Exclude hosts from updates

A special group, **Global Agent Update Exceptions**, has been created to stop selected hosts from being automatically updated. Any host in this group is not updated. This is controlled by MAC Address. If a host has more than one MAC Address, as long as any one of its MAC Addresses is listed in this group the host is not updated.

The user name of the person who logs into this host displays along with the MAC Address in the Group window. However, the user name is actually ignored for update purposes. If a user logs into a second different host, the second host is updated because none of its MAC Addresses match the anything in the Global Agent Update Exceptions group.

1. Click **System > Settings**.
2. Expand the **Persistent Agent** folder.
3. Select **Agent Update** from the tree.
4. Click the **Modify Global Agent Update Exceptions** button.
5. In the Group dialog, select one or more hosts from the column on the left.
6. Click the right arrow in the center of the dialog to move them to the Selected Members column.
7. Click **OK** to save.

This group can also be modified from the Groups View.

Verify the number of updated hosts

Since hosts are only updated when they connect to the network, updating all hosts could take some time. To see how many hosts have been updated, go to the Dashboard and look at the Persistent Agent Summary panel. This displays the total number of hosts registered and breaks that number up into groups by version number and operating system. If the panel is not displayed, use the Add Panel link to restore it to the Dashboard.

Schedule auto-definition updates

This feature allows you to automatically update the Virus Definition or Signature information for the anti-virus software that is permitted in Scans within your Endpoint Compliance Policies.

When new versions of an operating system and anti-virus are added using the Auto-Def Schedule feature, they are not automatically selected in existing scans. You must go to each scan and enable the new options if you choose to scan for them.

The scans you configure with Endpoint Compliance specify the definition requirements for anti-virus programs as well as operating systems. The default setting for the definition version information for all supported anti-virus products is updated when the scheduled Automatic Definition Synchronizer task runs.

This task applies the update to all configured scans. The version information is maintained by Fortinet and is updated on a weekly basis. It is recommended that this task be scheduled to run weekly. If you change the default information in a scan for a specific operating system or anti-virus software, the scheduled task will not overwrite that change.

To have the most recent version information appear in the Scan, go to the Scan containing the modified operating system or anti-virus program, deselect the program and click OK. Open the Scan again and reselect the program. Click OK again to restore all the default settings for the selected program.

Automatic updates rely on the configuration of communications settings between the FortiNAC server and the updates server. See System update on page 238 for information on configuring communications.

Configure Schedule

1. Click **System > Settings**.
2. Expand the **Persistent Agent** folder.
3. Select **Agent Update** from the tree.
4. Click **Modify Schedule**.
5. Select the **Enabled** check box.
6. Enter a name for the task in the Name field.
7. The **Description** field is optional. Enter a description of the task.
8. Action type and Action are pre-configured based on the task and cannot be modified.
9. From the **Schedule Type** drop down list, select either **Fixed Day** or **Repetitive** and set the day and time that the task is to be performed.
10. A **Fixed Day Task** is one in which you schedule a task to run on a combination of days of the week and times of the day, such as Mondays at 1:00 pm and Fridays at 10:00 am. Select the day(s) and time to run the task.
    a. Click the box next to the day(s) to select the day.
    b. Click the down arrows and select the hour, minutes, and AM or PM from the drop-down list for each day.
    c. To enter days/times more quickly, use the **Set Multiple Days** button to set multiple days with the same time.
    d. To remove all settings click the **Clear All** button.
11. A **Repetitive Task** is one that you schedule to start on a given day, at a certain time, for the number of times you specify, such as every 10 days starting today. The repetition rate can be set to any number of minutes, hours, or days.
    a. Enter the **Repetition Rate** using whole numbers.

    A repetition rate of zero causes the task to run only once.

    b. Click the down arrow and select **Minutes**, **Hours**, or **Days** from the drop-down list.
    c. Enter the date and time for the task to run in the **Next Scheduled Time** field using the format MM/DD/YY

hh:mm AM/PM Time Zone.

The new Repetition Rate does not take effect immediately. It starts the next time the scheduled task runs. For the new Repetition Rate take effect immediately, click the **Update** button.

d. Click **Update** to update the Next Scheduled Time field or change the Repetition Rate.

12. Click **OK**.

Schedule settings

Field	Definition
Remove local backups older than	Number of days for which you would like to keep backups. Anything older than the number of days entered, is removed the next time the scheduled task for backups runs. This setting removes backup files created on the FortiNAC server before they are copied to the remote server. Backups on the remote server are not removed. The timing of the scheduled backup task and the age of the files that are to be removed must be thought out carefully or you will remove all of your backups. For example, if the remove option is set to 5 days and your backup task runs every 15 days, you may inadvertently remove all of your backups. However, if the remove option is set to 15 days and the backup task runs every 5 days, then you would always have backup files.
Status	Indicates whether the task is Enabled or Disabled.
Schedule Interval	How often the scheduled task runs. Options are Minutes, Hours, or Days.
Next Scheduled Time	The next date and time the scheduled synchronization task will run. Entered in the format MM/DD/YY HH:MM AM/PM
Modify Schedule	Allows you to modify the scheduled activity.
Run Now	Runs the scheduled task immediately.

Credential configuration

Use the Credential Configuration view to configure how credentials are verified for hosts who use the Persistent Agent.

This tab is only available for firmware version 2.2.0.x or greater.

1. Click **System > Settings**.
2. Do one of the following:
   a. In folder view, expand the **Persistent Agent folder** and select **Credential Configuration** from the tree.
   b. In flat view, select **Credential Configuration - Persistent Agent**.

3. Use the table below to configure Persistent Agent Credentials and click **Save Settings**.

Settings

Field	Definition
Enable Registration	If checked, any unregistered (rogue) hosts who use the Persistent Agent will be registered by the agent. Typically this is disabled when rogues are being registered by the Device Profiler. There is a method in Device Profiler that detects the presence of the Persistent Agent and can use that in combination with other criteria to register the host. When this option is unchecked, **Register as Device** and **Authentication Type** are disabled.
Register As Device	If checked, all unregistered (rogue) hosts who use the Persistent Agent are registered automatically when they connect to the network. Then name of the host is entered in the ID field in the host record. If unchecked, all unregistered (rogue) hosts who use the Persistent Agent are presented with a login screen to enter their credentials. The credentials are verified with the method selected in the Authentication Type field.
Authentication Type	The method used to verify the user credentials for access to the network: Local, LDAP, RADIUS or RADIUS/LDAP. The RADIUS/LDAP option indicates that the user is being authenticated by a RADIUS server but registered based on data in an LDAP server. If the user is successfully authenticated by the RADIUS server but does not exist in the LDAP database, FortiNAC will still create the user record in its own database. The authentication type selected must match the authentication method selected in the Portal Configuration window. Google authentication for the Persistent Agent is not supported.

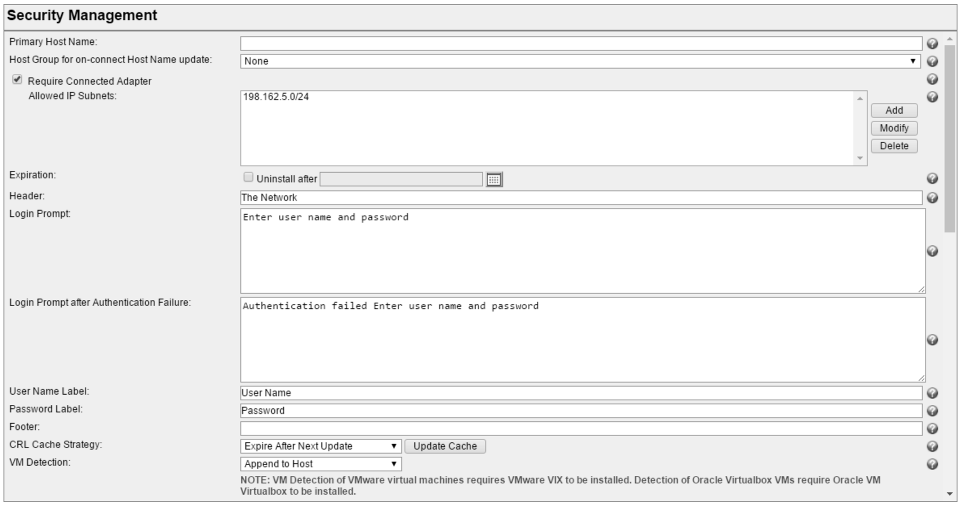
Security management

Use the Security Management view to set:

- The Host Name of the server for Persistent Agent communication.
- The Host group whose members receive the Host Name when they connect.
- Whether to require an adapter to be connected to a device managed by FortiNAC in order to communicate.
- Whether display notifications will be sent to the host.
- Header and footer text for the Persistent Agent Authentication page.
- The amount of time that a CRL will be cached before retrieving a new CRL.
- Status messages in the message box on the user's desktop.

You can also enter text for other message windows generated during Registration or Scanning.

To access the Persistent Agent Security Management properties, go to **Policy > Persistent Agent Properties**.



Security Management

Primary Host Name:

Host Group for on-connect Host Name update: None

☑ Require Connected Adapter

Allowed IP Subnets: 198.162.5.0/24

Expiration: □ Uninstall after

Header: The Network

Login Prompt: Enter user name and password

Login Prompt after Authentication Failure: Authentication failed Enter user name and password

User Name Label: User Name

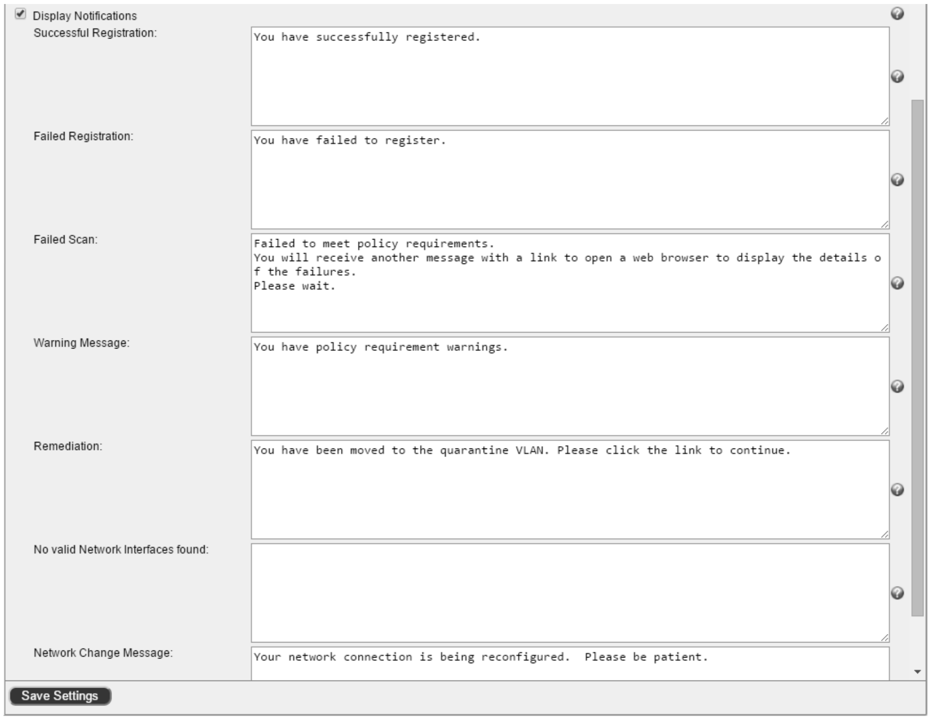
Password Label: Password

Footer:

CRL Cache Strategy: Expire After Next Update

VM Detection: Append to Host

NOTE: VM Detection of VMware virtual machines requires VMware VIX to be installed. Detection of Oracle Virtualbox VMs require Oracle VM Virtualbox to be installed.



☑ Display Notifications

Successful Registration: You have successfully registered.

Failed Registration: You have failed to register.

Failed Scan:

```
Failed to meet policy requirements.
You will receive another message with a link to open a web browser to display the details o
f the failures.
Please wait.
```

Warning Message: You have policy requirement warnings.

Remediation: You have been moved to the quarantine VLAN. Please click the link to continue.

No valid Network Interfaces found:

Network Change Message: Your network connection is being reconfigured. Please be patient.

Settings

Field	Definition
Primary Host Name	Fully qualified host name of the FortiNAC Application Server or the FortiNAC Server if you are not using a pair. It is pushed out to the connecting host(s) to ensure that the Persistent Agent is communicating with the correct host in a distributed environment. In a High Availability environment you must use the actual host name not the shared host name. This field is required for Agent Updates.
Secondary Host Name	This field is displayed only in a High Availability environment and is used only in a failover situation. Fully qualified host name of the secondary FortiNAC Application Server or the secondary FortiNAC Server if you are not using a pair. It is pushed out to the connecting host(s) to ensure that the Persistent Agent is communicating with the correct host in a distributed environment. Use the actual host name and not the shared host name. This field is required for Agent Updates.
Host Group for on-connect Host Name update	When hosts in this group connect to the network, they are given this Persistent Agent Host Name for communication between the host and the Persistent Agent server.
Require Connected Adapter	If enabled, the server will require one of the adapters reported by the agent to be connected to a device managed by FortiNAC in order to communicate. This eliminates the need to use ACLs to block access to a FortiNAC Application server when the host is connecting on a device managed by a different FortiNAC Control server/Application server pair. The agent must be configured with security enabled. Requires Persistent Agent 4.0.3 or higher.
Allowed IP Subnets	When you have a client that is not detected as connected (e.g., a VPN-connected client), the agents cannot connect to the server when the the Require Connected Adapter option is enabled. You can configure specific subnets to allow the server to accept connections from any host connecting from an IP address within one of the subnets or from any connected adapter. Any IP address that the agent connects from will be checked against these subnets. If the IP address is within the range, it will be allowed to connect. This applies to all hosts connecting from the specified ranges.
Expiration	If enabled, the Persistent Agent uninstalls itself from the host once date and time selected have passed. This option is only available for Persistent Agent Version 3.0 or higher.
Header	This text appears at the top of all message windows generated by the Persistent Agent.
Login Prompt	This text displays on the login window.

Field	Definition
Login Prompt after Authentication Failure	This text appears in the message block received when a user has not been authenticated.
User Name Label	Controls the text that appears next to the User Name field on the log in window.
Password Label	Controls the text that appears next to the Password field on the log in window.
Footer	This text appears at the bottom of all message windows generated by the Persistent Agent.
CRL Cache Strategy	Defines the amount of time that a CRL will be cached before retrieving a new CRL. • **Expire After Next Update**. This is the default setting. Retrieves a new copy of the CRL when the date defined by the Certificate Authority in the CRL has expired. • **Expire After This Update**. Select this option to define how long after the date defined as This Update in the CRL when a new CRL should be retrieved. **Note**: If the number of hours entered is fewer than the This Update time interval defined in the CRL, the CRL will be retrieved each time a scan occurs because the CRL will appear out of date. This may cause performance issues. • **Poll for Changes**. Sets the time interval to download a new CRL. • **Update Cache**. Lets you instantly retrieve a new CRL. This can be used when a certificate is revoked and you require a new CRL. Otherwise, the CRL is retrieved based on the defined Cache Strategy settings. See Certificate validation on page 518
Agent Contact Window on Host Connect	The time after host connection before an agent must connect or communicate successfully with the server. If this time expires without the agent having communicated, the "No Contact" flag is set and the "Persistent Agent Not Communicating" event is generated.
Agent Contact Window on Agent Disconnect	The time after the agent disconnects or communication is lost. If this time expires without the host disconnecting or the agent having communicated, the "No Contact" flag is set and the "Persistent Agent Not Communicating" event is generated.
VM Detection	**None**. When selected, a virtual machine that connects to the network as a bridged adapter is detected as a new device on the port. **Append to Host**. When selected, the virtual machine adapters are added to the host as additional adapters. When a Guest VM has been appended to the host as a virtual Guest adapter, the Guest VM will remain an adapter on that host until the Guest VM is manually deleted from the host, even if VM Detection is changed to **None** or **Register as New Host**. **Register as New Host**. When selected, the virtual machine is automatically registered as a new host belonging to the same user as the host running the virtual machine, allowing default registration. **VM Platform Support by OS**

<table>
<tr><th>Field</th><th>Definition</th></tr>
<tr><td></td><td>
<table>
<tr><th>Platform</th><th>Windows</th><th>OSX</th><th>Linux</th></tr>
<tr><td>Oracle VBox</td><td>Supported</td><td>Supported</td><td>Supported</td></tr>
<tr><td>VMware Workstation*</td><td>Supported</td><td>Not Supported</td><td>Supported</td></tr>
<tr><td>VMware Fusion</td><td>Not Supported</td><td>Supported</td><td>Not Supported</td></tr>
</table>
*VIX 1.5 must also be installed for Workstation Player
VM Detection of VMware virtual machines requires the virtual machine to be configured with a bridged network adapter.
VM Detection of VMware virtual machines requires VMware VIX to be installed.
Detection of Oracle Virtualbox VMs require Oracle VM Virtualbox to be installed.
Linux hosts must be configured to run the Persistent Agent Daemon process as the logged on user. To configure this, go to /etc/sysconfig/bndaemon and change DAEMON_USER from bndaemon to the current logged on user, and then restart the daemon service.
VM Detection requires Persistent Agent version 4.1.0 or greater.
FortiNAC will register a detected VM guest with the same registration as the VM host. However, the VM guest will not inherit the authentication state of the VM host, and the guest OS will be subject to any authentication policies currently in place. This means that the guest OS may require separate authentication.
</td></tr>
<tr><td>Display Notifications</td><td>Determines whether the popup notifications from the Persistent Agent such as "VLAN switch taking place", or "Renewing IP", will be displayed. When checked the notifications are displayed on the host.
If unchecked, the notification fields below are hidden on this configuration view and on the host.</td></tr>
<tr><td>Successful Registration</td><td>This text appears in the message block received when a host has successfully registered. If you do not enter text, the message box does not appear for successful registrations.</td></tr>
<tr><td>Failed Registration</td><td>This text appears in the message block received when a host has failed the registration process. If you do not enter text, the message box does not appear for failed registrations.</td></tr>
<tr><td>Failed Scan</td><td>This text appears in the message block received when a host has failed a scan. If you do not enter text, the message box does not appear for failed scans.</td></tr>
<tr><td>Warning Message</td><td>This text appears in the message block received when a host has warning messages generated from a scan. If you do not enter text, the message box does not appear for warning messages.</td></tr>
<tr><td>Remediation</td><td>This text appears in the message block received when a host has been placed in the Remediation VLAN. If you do not enter any text, the message box does not appear.</td></tr>
</table>

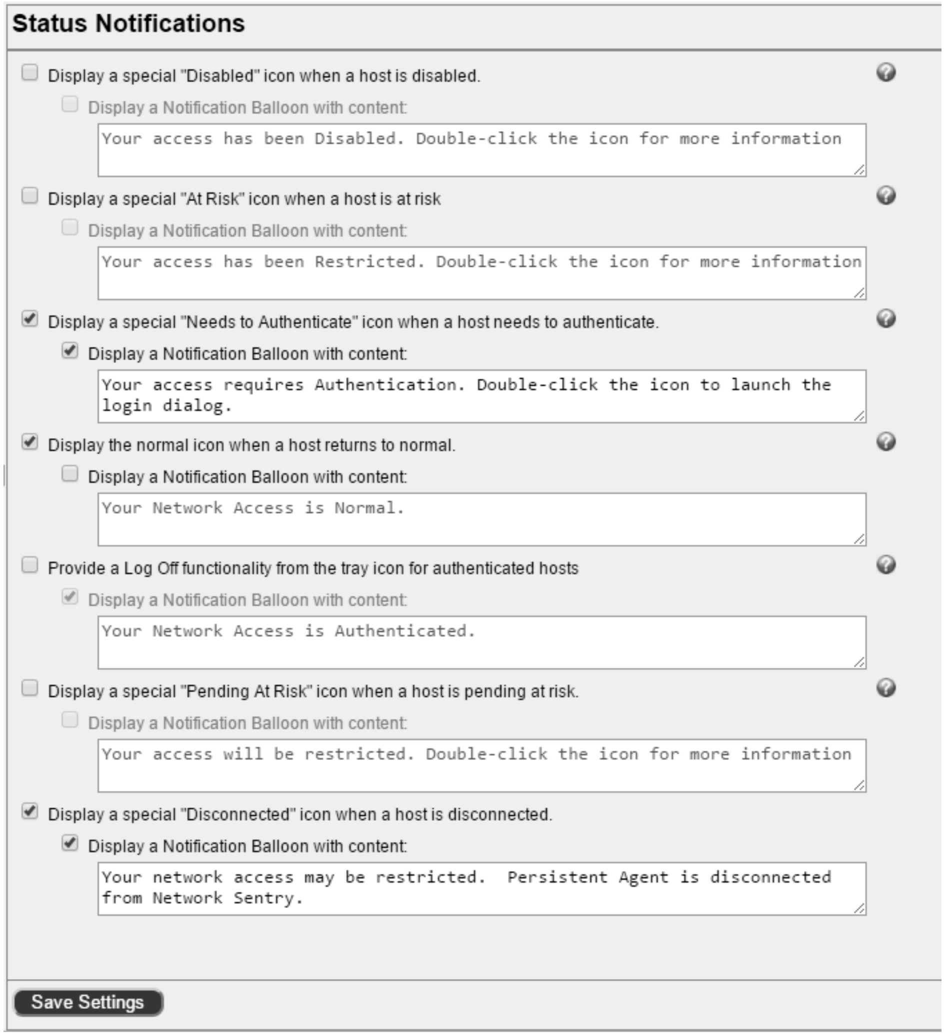
Field	Definition
No Valid Network Interfaces found	This text appears in the message block when the Persistent Agent cannot determine the MAC address of the interface used to connect to the network or if the MAC address for that interface is invalid. Default value for this field is blank. If you do not enter text, the message box does not appear for invalid MAC addresses.
Network Change Message	This text appears in the message block when the IP address for the host is being renewed. This can happen when the host is being moved from one VLAN to another.

Configure security management properties

1. Click **System > Settings**.
2. Expand the **Persistent Agent** folder.
3. Select **Security Management** from the tree.
4. Use the information in the Security Management Settings table above to complete the fields.
5. Click **Save Settings**.

Status notifications

Use the Status Notifications view to configure how users are notified of their host status when the Persistent Agent contacts the FortiNAC server. There are two levels of notification. The first enables or disables the display of a special icon shown in the System Tray based on the state of the host. If the first level is enabled, the second level enables or disables the display of Notification Balloons over the icon. These provide more detail to the user if there is an issue with network access.



Status Notifications

☐ Display a special "Disabled" icon when a host is disabled.

☐ Display a Notification Balloon with content:

```
Your access has been Disabled. Double-click the icon for more information
```

☐ Display a special "At Risk" icon when a host is at risk

☐ Display a Notification Balloon with content:

```
Your access has been Restricted. Double-click the icon for more information
```

☑ Display a special "Needs to Authenticate" icon when a host needs to authenticate.

☑ Display a Notification Balloon with content:

```
Your access requires Authentication. Double-click the icon to launch the
login dialog.
```

☑ Display the normal icon when a host returns to normal.

☐ Display a Notification Balloon with content:

```
Your Network Access is Normal.
```

☐ Provide a Log Off functionality from the tray icon for authenticated hosts

☑ Display a Notification Balloon with content:

```
Your Network Access is Authenticated.
```

☐ Display a special "Pending At Risk" icon when a host is pending at risk.

☐ Display a Notification Balloon with content:

```
Your access will be restricted. Double-click the icon for more information
```

☑ Display a special "Disconnected" icon when a host is disconnected.

☑ Display a Notification Balloon with content:

```
Your network access may be restricted.  Persistent Agent is disconnected
from Network Sentry.
```

Settings

Icon/Field	Definition
!	This icon displays in the host System Tray if special icon options have been enabled on the Status Notifications window. This icon represents the following host states: • Disabled • At Risk • Pending At Risk • Needs to Authenticate Icon can only be disabled using administrative templates.

Icon/Field	Definition
▣	This icon displays in the host System Tray. Indicates that the host has normal network access. If you require authentication, this icon also indicates that the user has been authenticated. Icon can only be disabled using administrative templates.
▣	This icon displays in the host System Tray. Indicates that the host has been disconnected from the network. Icon can only be disabled using administrative templates. This icon will display for Agent 3.5 and higher.
Display a special "Disabled" icon when a host is disabled.	Displays an icon in the System Tray indicating that the host has been disabled and does not have access to the network. The user must double-click on the icon or click on the notification balloon to open a web-browser with additional information.
Display a special "At Risk" icon when a host is at risk.	Displays an icon in the System Tray indicating that the host has been marked At Risk based on an Endpoint Compliance Policy scan. The user can double-click on the icon or click on the notification balloon to open a web-browser with additional information. For Persistent Agent with EasyConnect, it is recommended that you enable this check box to display a notification balloon that allows the user to access the web page to register upon failure to connect.
Display a special "Needs to Authenticate" icon when a host needs to authenticate.	Displays an icon in the System Tray indicating that the user on this host has not been authenticated. The user can double-click on the icon or click on the notification balloon to open a login window.
Display a normal icon when host returns to normal.	Displays an icon in the System Tray indicating that the host has normal network access and there are no issues.
Provide a Log Off functionality from the tray icon for authenticated hosts.	Allows authenticated users to log off the network by right-clicking the Persistent Agent icon and selecting Log Off the Network from the pop-up menu. This does not log the user out of Windows.
Display a special "Pending At Risk" icon when a host is pending at risk.	Displays an icon in the System Tray indicating that the host has been marked Pending At Risk based on an Endpoint Compliance Policy scan that has delayed remediation enabled. The user can double-click on the icon or click on the notification balloon to open a web-browser with additional information. See Delayed remediation for scanned hosts on page 431.

Icon/Field	Definition
Display a special "Disconnected" icon when a host is disconnected.	Displays an icon in the System Tray indicating that the host has been disconnected from the network. Requires Agent 3.5 or higher.
Display a Notification Balloon with content.	This option is provided for each icon and is available only when the Display Icon option above it has been enabled. If Notification Balloons are enabled enter the text you would like the user to see in a balloon when his host status changes. Balloons follow the Windows standards as far as the amount time they are displayed and disappearing when they are clicked. When a balloon is clicked it takes the user to either a web-browser with additional information or a login window.

Transport configurations

Packet Transport Configurations define the methods of communication available between FortiNAC and the Persistent Agent. Each Packet Transport Configuration is defined with a unique Name and a unique combination of Bind Address, Port, and Transport Type. If no Bind Address is specified, all addresses are bound for the supplied Port. The supplied port must be in the range of 1024 to 49151 and not already in use by another service within the operating system. If the Transport Type is TCP, a TLS Service Configuration must be defined to secure the communication. Changes made to Packet Transport Configurations do not take effect immediately. The enabled configurations will begin listening when the Persistent Agent services are reloaded or FortiNAC is restarted.

TLS Service Configurations define the Certificate, TLS Protocols, and Ciphers used for secure communication. The Certificate can be uploaded using the Certificate Management view. By checking "Automatically Update Ciphers and Protocols on Upgrade," the settings for both Ciphers and TLS Protocols will become managed by FortiNAC. Upon upgrade, the system will automatically configure the TLS Service Configuration to the latest recommended Ciphers and Protocols.

Packet transport settings

Field	Definition
Enabled	If true, a listener will be created for this configuration on the next load of the Persistent Agent services.
Name	Unique name used to identify the configuration.
Bind Address	An optional IPv4 or IPv6 to use when listening for packets. If no address is provided, all addresses are used.
Port	The port this configuration should open a socket using. System and Dynamic ports may not be used. Valid values are in the range of 1024 to 49151

Field	Definition
TLS Configuration	The selected configuration for security communication with the Persistent Agent. Only TCP Transports use a TLS Configuration
Transport Type	The communication protocol, either TCP or UDP, to use when communication with the Persistent Agent
Maximum Incoming Packets to Queue	The maximum number of unprocessed packets from the Persistent Agent to retain. Any packets received while the queue is full will be discarded.
Read Idle Timeout	The maximum amount of time, in seconds, without receiving from the agent before closing the connection.
Write Idle Timeout	The maximum amount of time, in seconds, before the server will send a packet to the agent to ensure the connection is still open.
Use Native Transport (Experimental)	Use native libraries for Sockets and TLS when possible. Enable this experimental feature only if recommended.
Last Modified By	User name of the last user to modify the configuration.
Last Modified Date	Date and time of the last modification to this configuration.
Right click options	
Modify	Modify the selected Packet Transport Configuration.
Delete	Deletes the selected Packet Transport Configuration.
Reload Services	Closes any existing sockets in the Persistent Agent server and creates a new series of sockets using the enabled Packet Transport Configurations. All unprocessed packets in the existing queues are dropped, allowing the Persistent Agent server to resume communication from a clean state.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.

TLS service settings

Field	Definition
Automatically Update Ciphers and Protocols on Upgrade	If true, the settings for both Ciphers and TLS Protocols will become managed by FortiNAC. Upon upgrade, the system will automatically configure the TLS Service Configuration to the latest recommended Ciphers and Protocols.
Name	Unique name used to identify the configuration.
Ciphers	The Cipher Suite to use when encoding messages using TLS. At least one Cipher must be selected. Ciphers must be supported by both client and server, so disabling Ciphers may prevent some Persistent Agents from communicating.

Field	Definition
TLS Protocol	The list of TLS Protocols to allow by the server. At least one TLS Protocol must be selected. TLS Protocols must be supported by both client and server, so disabling Protocols may prevent some Persistent Agents from communicating.
Certificate Alias	Select the Certificate to use when securing communication. Certificates may be uploaded using the Certificate Management view. See Certificate management on page 161.
Last Modified By	User name of the last user to modify the group.
Last Modified Date	Date and time of the last modification to this group.
Right click options	
Modify	Modify the selected TLS Service Configuration.
Delete	Deletes the selected TLS Service Configuration.
In Use	Provides a list of Packet Transport Configurations that currently reference the selected TLS Service Configuration.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.

Add or modify packet transport configuration

1. Click **System > Settings**.
2. Expand the **Persistent Agent** folder.
3. Select **Transport Configuration** from the tree.
4. To modify a record: Select a Packet Transport Configuration record from the table and click **Modify**.
5. To add a new record: Click **Add** at the bottom of the upper panel.
6. Use the Settings for the Persistent Agent Transport Configuration topic to enter the Packet Transport Configuration information.
7. Click **OK** to save.

After adding or modifying a Packet Transport Configuration, the services will continue to use the previous configuration until a reload is requested or FortiNAC is restarted.

Delete packet transport configuration

1. Click **System > Settings**.
2. Expand the **Persistent Agent** folder.
3. Select **Transport Configuration** from the tree.
4. Select a Packet Transport Configuration record from the table

5. Click **Delete** at the bottom of the panel.
6. Click **Yes** on the confirmation message.

Add or modify TLS service configuration

1. Click **System > Settings**.
2. Expand the **Persistent Agent** folder.
3. Select **Transport Configuration** from the tree.
4. To modify a record: Select a TLS Service Configuration record from the table and click **Modify**.
5. To add a new record: Click **Add** at the bottom of the lower panel.
6. Use the Settings for the Persistent Agent Transport Configuration topic to enter the TLS Service Configuration information.
7. Click **OK** to save.

After adding or modifying a TLS Service Configuration, the Packet Transport Configuration services will continue to use the previous configuration until a reload is requested or FortiNAC is restarted.

Delete TLS service configuration

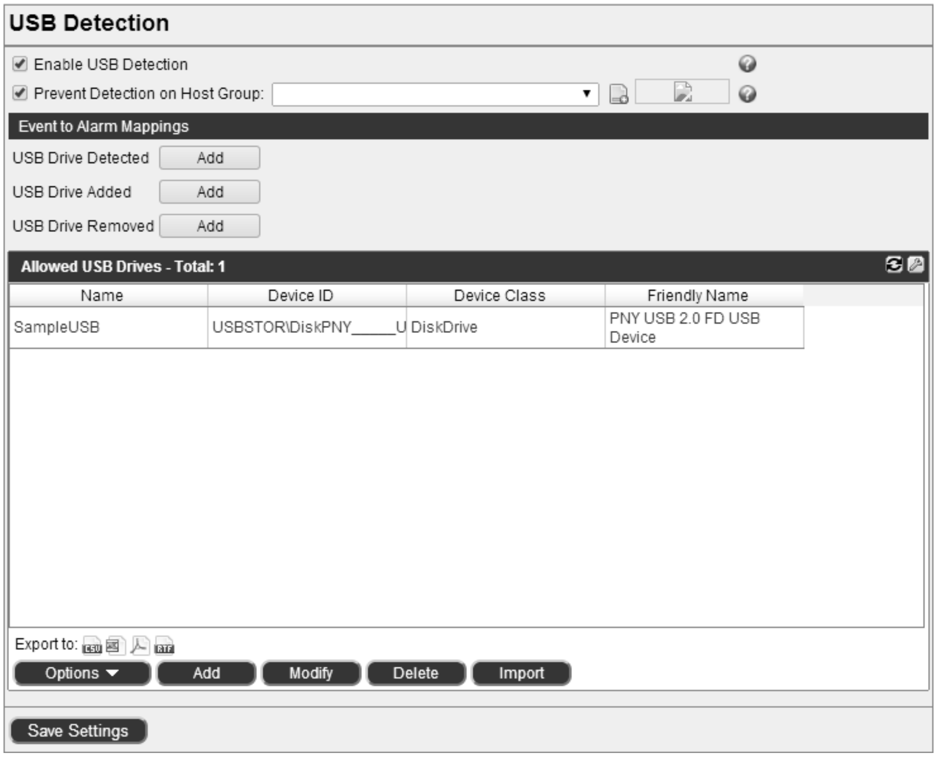
1. Click **System > Settings**.
2. Expand the **Persistent Agent** folder.
3. Select **Transport Configuration** from the tree.
4. Select a TLS Service Configuration record from the table
5. Click **Delete** at the bottom of the panel.
6. If one or more Packet Transport Configurations are associated with the TLS Service Configuration, you will not be able to delete it.
7. Click **Yes** on the confirmation message.

USB detection

The USB Detection view allows you to configure FortiNAC to be notified in the event that a USB device was plugged into a host on the network. When a USB drive is detected, FortiNAC events can be mapped to alarms to specify an action based on the host where the USB drive is connected. You can also indicate which drives should be ignored by the system, regardless of the hosts they are connected to.

This feature requires Agent 3.3 or higher.

This feature is only supported on Windows hosts.



USB Detection

☑ Enable USB Detection

☑ Prevent Detection on Host Group:

Event to Alarm Mappings

USB Drive Detected Add

USB Drive Added Add

USB Drive Removed Add

Allowed USB Drives - Total: 1

Name	Device ID	Device Class	Friendly Name
SampleUSB	USBSTOR\DiskPNY_____U	DiskDrive	PNY USB 2.0 FD USB Device

Settings

Icon/Field	Definition
Enable USB Detection	When enabled, if a USB drive is plugged into a host, the agent will detect the USB drive and notify FortiNAC.
Prevent Detection on Host Group	Select the host group where you wish to prevent USB detection. If the USB connects to a host within the selected host group, the USB is ignored and no event is generated. Click the Add icon to add a group. Click the Modify icon to modify the selected group.
Event to alarm mappings	
USB Drive Detected	Allows user to configure an event to alarm mapping for when the USB drive is present when the agent is started.
USB Drive Added	Allows user to configure an event to alarm mapping for when the USB drive is added while the agent is running.
USB Drive Removed	Allows user to configure an event to alarm mapping for when the USB drive is removed while the agent is running.
Allow USB drives	
Name	The name of the USB drive.
Device ID	The Device ID for the USB drive from the registry key.
Device Class	The Device Class for the USB drive from the registry key.

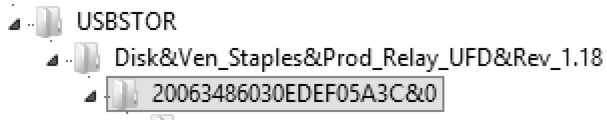
Icon/Field	Definition
Friendly Name	The Friendly Name for the USB drive from the registry key.
Right click options	
Delete	Deletes the selected USB drive.
Modify	Opens the Modify Allowed USB Drive dialog.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.
Buttons	
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.
Save Settings	Click to save the USB detection settings.

Add/modify an allowed USB drive

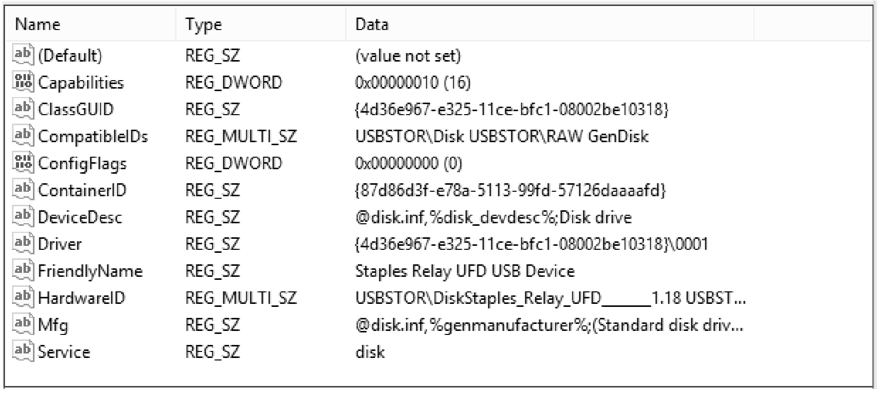
1. Click **System > Settings**.
2. Expand the **Persistent Agent** folder.
3. Select **USB Detection** from the tree.
4. Click the **Add** button or select an existing USB drive and click **Modify**.
5. Enter the name for FortiNAC to use to identify the USB drive that is being allowed.
6. Run *regedit.exe* to access the registry key.
7. Expand `HKEY_LOCAL_MACHINE>SYSTEM>CurrentControlSet>Enum>USBSTOR`

If `CurrentControlSet` is not available, you can also find USBSTOR in `ControlSet001`.

8. Expand the folder for the device containing the information you wish to add or modify, and click the key.



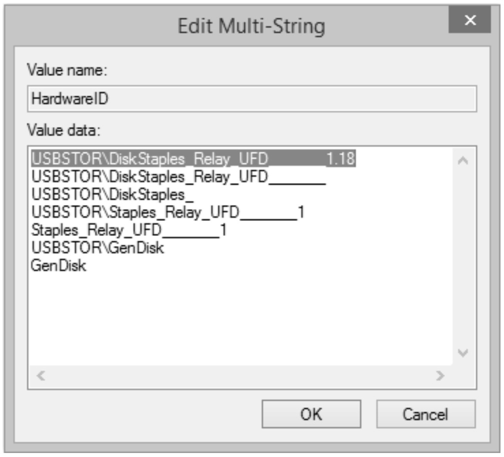
The key values appear.



Name	Type	Data
(Default)	REG_SZ	(value not set)
Capabilities	REG_DWORD	0x00000010 (16)
ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW GenDisk
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{87d86d3f-e78a-5113-99fd-57126daaaafd}
DeviceDesc	REG_SZ	@disk.inf,%disk_devdesc%;Disk drive
Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}\0001
FriendlyName	REG_SZ	Staples Relay UFD USB Device
HardwareID	REG_MULTI_SZ	USBSTOR\DiskStaples_Relay_UFD______1.18 USBST...
Mfg	REG_SZ	@disk.inf,%genmanufacturer%;(Standard disk driv...
Service	REG_SZ	disk

The asterisk (*) wildcard can be used at the beginning and end of all values you enter.

9. Enter the following values from the registry key:
   - Device ID: The first value from the Hardware ID key as defined in the Registry entry for the USB device in: HKEY_LOCAL_MACHINE>SYSTEM>CurrentControlSet>Enum>USBSTOR (e.g., UBSTOR\DiskStaples_Relay_UFD________1.18).



Edit Multi-String

Value name:

HardwareID

Value data:

```
USBSTOR\DiskStaples_Relay_UFD________1.18
USBSTOR\DiskStaples_Relay_UFD________
USBSTOR\DiskStaples_
USBSTOR\Staples_Relay_UFD________1
Staples_Relay_UFD________1
USBSTOR\GenDisk
GenDisk
```

   - Device Class: The value from the Class key as defined in the Registry entry for the USB device in: HKEY_LOCAL_MACHINE>SYSTEM>CurrentControlSet>Enum>USBSTOR

If the Class value is empty or is not present in the registry, leave the Class field blank. Otherwise, the rule will not match and an event will be generated.

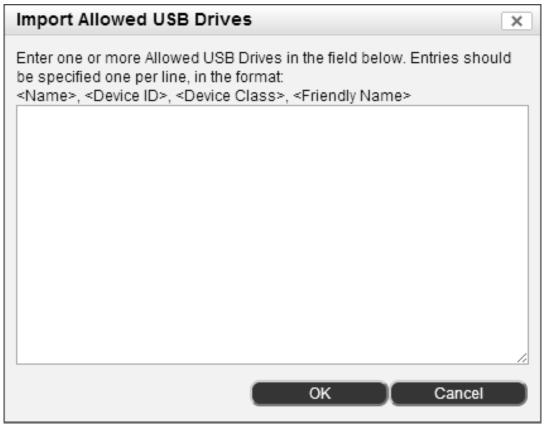
   - Friendly Name: The value from the Friendly Name key as defined in the Registry entry for the USB device in: HKEY_LOCAL_MACHINE>SYSTEM>CurrentControlSet>Enum>USBSTOR.

10. Click **OK**.

Import allowed USB drives

You can import multiple USB drives at a time to the list of Allowed USB drives.

1. Click **System > Settings**.
2. Expand the **Persistent Agent** folder.
3. Select **USB Detection** from the tree.
4. Click **Import**.



Enter one or more Allowed USB Drives in the field below. Entries should be specified one per line, in the format:
<Name>, <Device ID>, <Device Class>, <Friendly Name>

5. Enter the Name, Device ID, Device Class, and Friendly Name for each USB drive you wish to import in the specified format.
6. Click **OK**.

Delete an allowed USB drive

1. Select **System> Settings**.
2. Expand the **Persistent Agent** folder.
3. Select **USB Detection** from the tree.
4. Select a USB drive in the Allowed USB Drives list, and click **Delete**.
5. A confirmation message is displayed. Click **Yes** to continue.

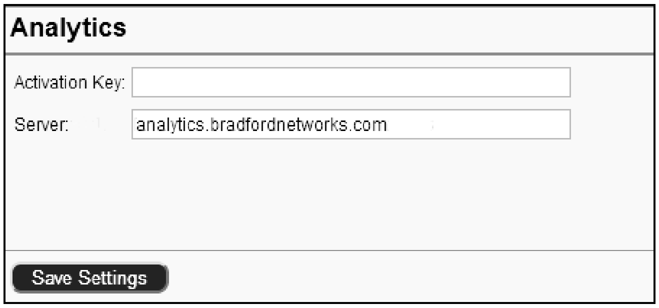
Reports

Reports groups together properties for reports that are generated directly from the FortiNAC database and the integration with Analytics which is an external reporting package.

Option	Definition
Analytics	Configures the connection between the FortiNAC server and the Analytics server. This connection allows an agent on the FortiNAC server to push data for reporting to an external server based on a user-defined schedule.
Local seporting	Use Local Reporting to set record limits for reports to prevent the server from being overloaded.

Analytics

Use analytics to configure the connection between the FortiNAC server and the cloud reporting Analytics server. This connection allows an agent on the FortiNAC server to push data for reporting to an external server based on a user-defined schedule. The schedule is set in the Analytics reporting software.



Analytics

Activation Key:

Server: analytics.bradfordnetworks.com

1. Click **System > Settings**.
2. Expand the **Reports** folder.
3. Select **Analytics** from the tree.
4. Use the Settings table below to enter the connection settings for the Analytics server.
5. Click **Save Settings**.

Settings

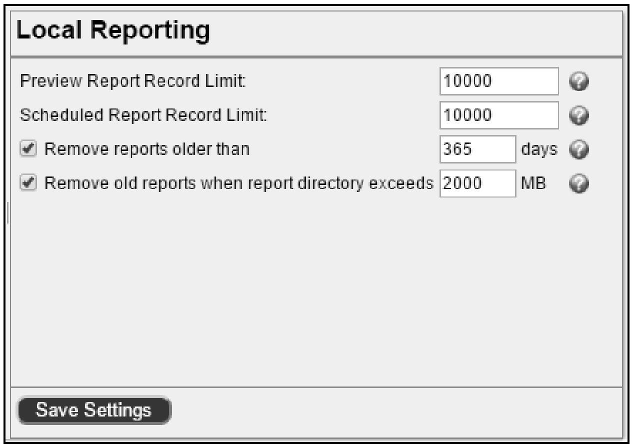
Field	Definition
Activation Key	Key that activates the license for FortiNAC/Analytics. When the license is activated, the agent on the FortiNAC server can begin sending data to the FortiNAC/Analytics database. See **Generate An Activation Key** below for instructions on creating a key.
Server	Fully Qualified Domain Name of the server where your FortiNAC/Analytics database resides. Default = analytics.bradfordnetworks.com

Generate an activation key

1. On the FortiNAC/Analytics server, log into the User Interface as Administrator.
2. Click the **Manage > Manage Client** on the menu bar.
3. Select the appropriate client from the list and click **Edit**.
4. On the Manage Clients view, click the **Generate** button under the **Access Key** field.
5. A license key is generated and displayed in the Access Key field.
6. Highlight the text and copy it to the Activation Key field in FortiNAC under **System > Settings > Reports > Analytics**.
7. Click **Save Settings**.

Local reporting

Use Local Reporting to set record limits for reports to prevent the server from being overloaded.



Local Reporting

Preview Report Record Limit: 10000

Scheduled Report Record Limit: 10000

☑ Remove reports older than 365 days

☑ Remove old reports when report directory exceeds 2000 MB

1. Click **System > Settings**.
2. Expand the **Reports** folder.
3. Select **Local Reporting** from the tree.
4. Modify the record limits as needed.
5. Click **Save Settings**.

Settings

Field	Definition
Preview Report Record Limit	Number of database records displayed in report preview window. Default = 10,000
Scheduled Report Record Limit	Number of database records displayed in a scheduled report. Default = 10,000
Remove reports older than	The number of days after which reports stored in the /home/cm/reports directory on your system are purged.
Remove old reports when report directory exceeds	All reports in the /home/cm/reports directory are purged when the size of the directory exceeds this value.

Security

Security groups together options for SSL Certificates.

Option	Definition
Portal SSL	Enable and disable SSL Security, generate a certificate request and upload certificates from a third party certificate authority. See Portal SSL on page 158.
Certificate Management	Provides the ability to manage certificates with different encoding schemes and file formats. See Certificate management on page 161.

Portal SSL

SSL Security allows you to enable and disable SSL Security, and enter the Fully Qualified Host Name.

Using a Valid SSL Certificate for captive portal security will not completely eliminate certificate errors, as you might wish. For example, if the host requests secure access using a URL such as https://www.google.com, the request will be redirected to the captive portal for FortiNAC as https. This maintains the https security level, but ultimately the certificate name will not match (the request will be for google.com and the response will be from FortiNAC's address) so there is a trust mismatch and the host will translate this to a possible hijacking attempt.

Alternately, if the host requests secure access using a URL, such as https://www.google.com, and if FortiNAC did not maintain the security level of HTTPS and returned HTTP instead, this would lead to an encryption error because the request was HTTPS and the response was http.

Settings

Field	Definition
SSL Mode	Determines how the web traffic is directed when it reaches the captive portal. The available settings are: - **Valid SSL Certificate**—Directs web traffic from port 80 to port 443 and presents a Certificate Authority Signed Valid SSL Certificate to the user. - **Self-Signed SSL Certificate**—Directs traffic from port 80 to port 443 and presents a Self-Signed SSL Certificate to the user. - **Disabled**—Directs all traffic to port 80.
Enable Shibboleth Integration with mod_shib	Enables the use of the Shibboleth Apache module if it has been configured on the FortiNAC Server or Application Server. This field does not display if Shibboleth is not configured on the server. The file HTTPAuthSMAAuthenticate.jsp does not need to exist on a system that is configured correctly to interact with Shibboleth. The FortiNAC tom-cat portal is configured to map requests with URIs that include "/common/HTTPAuthSMAAuthenticate.jsp" to /common/SMAAuthenticate.jsp.
Fully-Qualified Host Name	The fully qualified name of this appliance. If you have a FortiNAC Control Server and a FortiNAC Application Server pair, enter the fully qualified name of the FortiNAC Application Server.

Configure SSL security

There are two types of certificates used for the captive portal:

- **Valid SSL Certificate**—Issued by a Certificate Authority
- **Self-Signed SSL Certificate**—generated by the FortiNAC.

These options control the security level of the portal used for Registration, Remediation, Authentication, Dead End, and Quarantine contexts.

The web server listens on port 80 and port 443 for web traffic coming into the portal. The SSL Mode setting determines how the web traffic is directed when it reaches the captive portal. The available settings are:

- **Valid SSL Certificate**—Directs web traffic from port 80 to port 443 and presents a Certificate Authority Signed Valid SSL Certificate to the user. The certificate should be in PEM format.
- **Self-Signed SSL Certificate**—Directs traffic from port 80 to port 443 and presents a Self-Signed SSL Certificate to the user.
- **Disabled**—Directs all traffic to port 80.

If you choose to use the Valid SSL Certificate option you must obtain a certificate from a signing authority, such as, VeriSign. Until you have received your certificate, you can either use a Self-Signed SSL Certificate or set the SSL option to Disabled. When you have received the certificate, you must upload it to the web server.

Disable SSL mode

SSL Mode can be disabled if necessary. All web traffic coming to the captive portal will be directed to port 80.

1. Click **System > Settings**.
2. Expand the **Security** folder.
3. Select **Portal SSL** from the tree.
4. Select **Disabled** from the drop-down menu in the SSL Mode field.
5. Click **Save Settings**.

Apply a self-signed certificate

Self-Signed Certificates can be used to secure the captive portal and to secure communication between some Agents and the FortiNAC server until you purchase a Valid Third Party SSL Certificate.

All Mobile Agents and all Agents that are Version 3.x or higher require the use of a Valid Third Party Certificate. A Self-Signed Certificate cannot be used if any of these agents have been deployed.

Do not click Generate CSR to create a Self-Signed Certificate if you have already generated a request for a Valid Third Party SSL Certificate from a Certificate Authority. That process created a Self-Signed Certificate on the FortiNAC server. Clicking Generate CSR again creates a new Private Key that will not match the certificate returned from the Certificate Authority.

Use the existing self-signed SSL certificate

If you have generated the Private Key and the Certificate Request to obtain a certificate from a Certificate authority, a Self-Signed SSL Certificate was generated at the same time. Use the Self-Signed certificate until the Valid SSL Certificate is returned from the Certificate Authority.

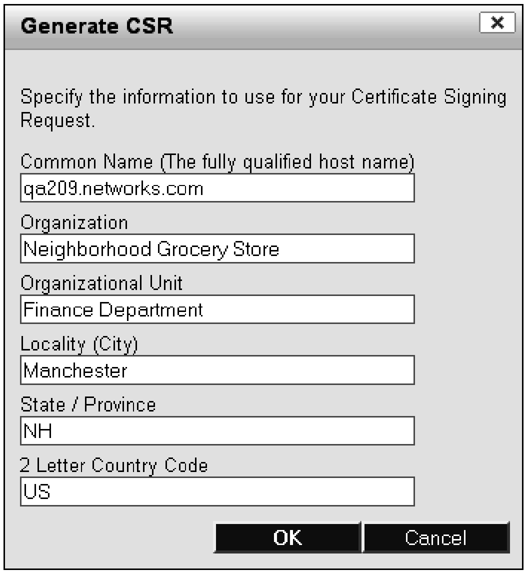
1. Click **System > Settings**.
2. Expand the **Security** folder.
3. Select **Portal SSL** from the tree.

4. In the SSL panel select **Self-Signed SSL Certificate** from the drop-down menu in the **SSL Mode** field.
5. Click **Save Settings**.

Generate a new self-signed SSL certificate

If you have never requested a certificate from a Certificate from a Certificate Authority and you would like to use a Self-Signed certificate to secure the portal, follow the instructions below:

1. Click **System > Settings**.
2. Expand the **Security** folder.
3. Select **Portal SSL** from the tree.
4. In the SSL panel enter the **Fully-Qualified Host Name**.
5. Click the **Generate CSR** button.
6. Enter the information for the Certificate in the dialog box.



Generate CSR

Specify the information to use for your Certificate Signing Request.

Common Name (The fully qualified host name): qa209.networks.com

Organization: Neighborhood Grocery Store

Organizational Unit: Finance Department

Locality (City): Manchester

State / Province: NH

2 Letter Country Code: US

The common name must exactly match the name entered on the General Tab.

7. Click OK.

   The Success dialog appears with the Private Key and the Certificate Request.
8. Click **Close** on the Success dialog.
9. Click **Save Settings**.

Apply a third-party SSL certificate

To secure the Admin UI with a trusted SSL Certificate, see SSL certificates on page 523.

SSL certificates for servers in an L3 HA environment

In an L3 HA environment redundant servers are on separate subnets, they do not share an IP address nor do they share a host name. If you need to secure the captive portal or agent server communications in such an environment, there are two options.

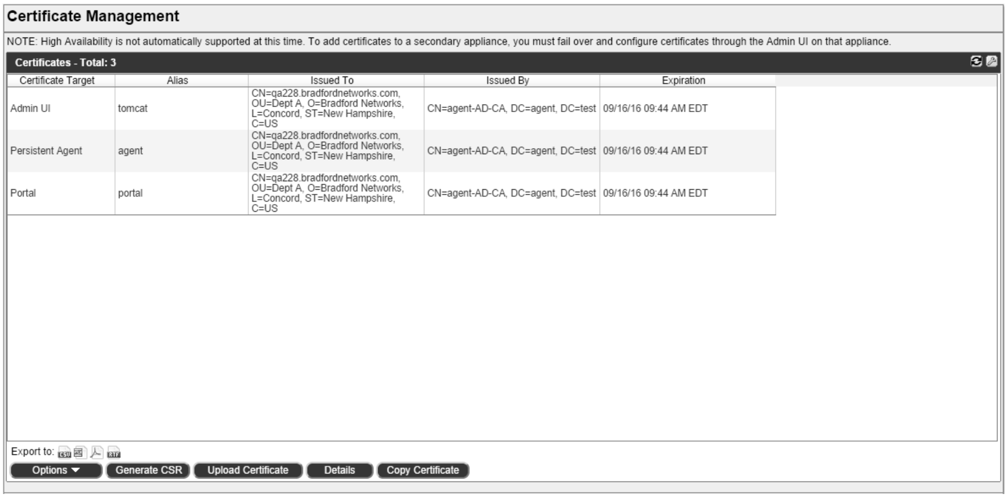
Wild card certificates can be used in a High Availability environment and the appropriate files will be replicated from the Primary to the Secondary server. Using a wild card certificate only the domain name is used and that portion of the Fully Qualified Host Name is the same for all servers, such as *.example.com.

However, in a High Availability configuration where primary and secondary servers are on separate subnets (L3 HA) and you do not wish to use a wild card certificate, you must request and import a separate certificate with the Fully-Qualified Host Name of each FortiNAC Server or FortiNAC Application server.

Certificate management

Certificate Management provides users with the ability to manage certificates with different encoding schemes and file formats. The Certificate Management view shows the certificates that are currently installed on FortiNAC. Users can create and install server certificates for the Admin UI.

High Availability is not automatically supported at this time. To add certificates to a secondary appliance, you must fail over and configure certificates through the Admin UI on that appliance.



Certificate Management

NOTE: High Availability is not automatically supported at this time. To add certificates to a secondary appliance, you must fail over and configure certificates through the Admin UI on that appliance.

Certificates - Total: 3

Certificate Target	Alias	Issued To	Issued By	Expiration
Admin UI	tomcat	CN=qa228.bradfordnetworks.com, OU=Dept A, O=Bradford Networks, L=Concord, ST=New Hampshire, C=US	CN=agent-AD-CA, DC=agent, DC=test	09/16/16 09:44 AM EDT
Persistent Agent	agent	CN=qa228.bradfordnetworks.com, OU=Dept A, O=Bradford Networks, L=Concord, ST=New Hampshire, C=US	CN=agent-AD-CA, DC=agent, DC=test	09/16/16 09:44 AM EDT
Portal	portal	CN=qa228.bradfordnetworks.com, OU=Dept A, O=Bradford Networks, L=Concord, ST=New Hampshire, C=US	CN=agent-AD-CA, DC=agent, DC=test	09/16/16 09:44 AM EDT

Settings

Field	Definition
Add Filter drop-down list	Allows you to select a field from the current view to filter information. Select the field from the drop-down list, and then enter the information you wish to filter. See Filters on page 15.
Update button	Displays the filtered data in the table.

Field	Definition
Certificate Target	The component where the certificate is applied.
Alias	Indicates how the certificate is stored in the underlying Keystore.
Issued To	The server that received the certificate. Displays information entered when generating the CSR.
Issued By	The CA that issued the certificate.
Expiration	The date when the certificate expires and a new certificate is required. Users can map events to alarms when the certificate will expire or has expired. See Map events to alarms on page 888.
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.
Buttons	
Generate CSR	Opens the Generate CSR window to enter the CSR details.
Upload Certificate	Opens the Upload Certificate window to find and select the key and certificate. See.
Details	Opens the details and private key information for the selected target.

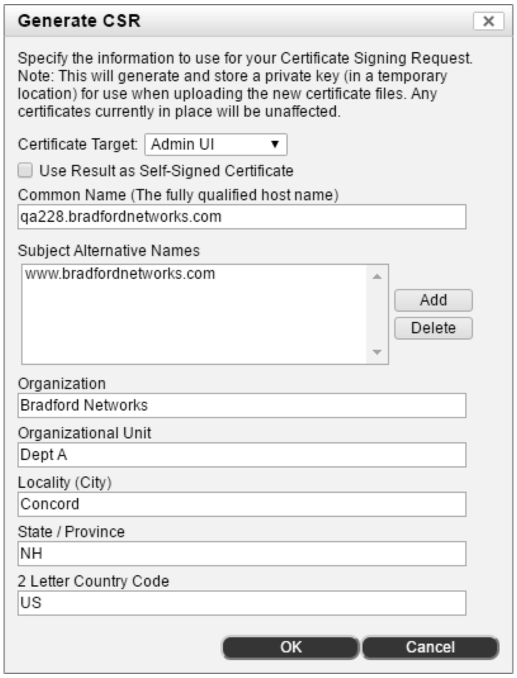
Obtaining a certificate from a Certificate Authority (CA)

If you do not have a certificate, you must obtain a certificate from a CA.

To obtain a valid third party SSL certificate from a CA, you must generate a CSR and send it to the CA.

To generate a CSR, and self-signed certificate:

1. Select **System > Settings**.
2. Expand the **Security** folder.
3. Select **Certificate Management** from the tree.
4. Click **Generate CSR**.



Generate CSR

Specify the information to use for your Certificate Signing Request. Note: This will generate and store a private key (in a temporary location) for use when uploading the new certificate files. Any certificates currently in place will be unaffected.

Certificate Target: Admin UI ▾

□ Use Result as Self-Signed Certificate

Common Name (The fully qualified host name)
qa228.bradfordnetworks.com

Subject Alternative Names
www.bradfordnetworks.com

Organization
Bradford Networks

Organizational Unit
Dept A

Locality (City)
Concord

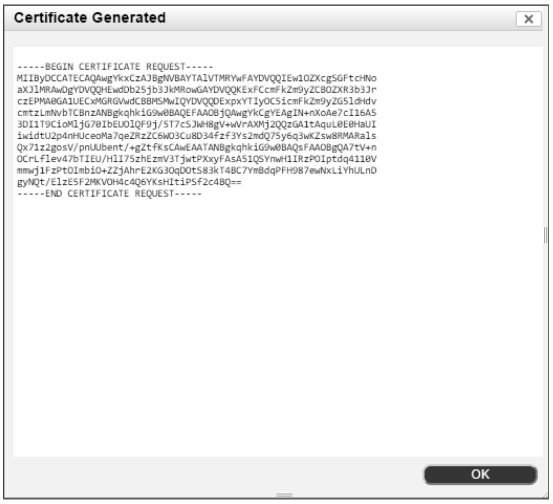
State / Province
NH

2 Letter Country Code
US

5. Select the certificate target (the type of certificate you want to generate).
   - Select **Admin UI** to generate a CSR for the administrative user interface.
   - Select **Persistent Agent** to generate a CSR for the PA communications.
   - Select **Portal** to generate a CSR to secure the captive portal and DA communications.
   - Select **RADIUS Server** to generate a CSR for integrated FortiNAC RADIUS server set to use 802.1x and PEAP.

> The Private Key that corresponds with the CSR is stored on the appliance. Once the SSL Certificate is uploaded, to view the Private Key, click the **Details** button and select the **Private Key** tab.

6. Enter the Common Name (Fully-Qualified Host Name). This is the Host Name to be secured by the certificate. If generating a wildcard CSR, enter the desired domain specifying the wildcard in the Common Name Field (Example: *.example.com).
7. Enter the Subject Alternative Names (leave blank if not requesting a SAN certificate). Click **Add** to enter each additional host name and/or IP address.
8. Enter the remaining information for the certificate in the dialog box:
   - **Organization**: The name of the server's organization.
   - **Organizational Unit**: The name of the server's unit (department).
   - **Locality (City)**: The city where the server is located.
   - **State/Province**: The state/province where the server is located.
   - **2 Letter Country Code**: The country code where the server is located.
9. Click **OK** to generate the CSR.



```
-----BEGIN CERTIFICATE REQUEST-----
MIIByDCCATECAQAwgYkxCzAJBgNVBAYTAlVTMRYwFAYDVQQIEw1OZXcgSGFtcHNo
aXJlMRAwDgYDVQQHEwdDb25jb3JkMRowGAYDVQQKExFCcmFkZm9yZCBOZXR3b3Jr
czEPMA0GA1UECxMGRGVwdCBBMSMwIQYDVQQDExpxYTIyOC5icmFkZm9yZG5ldHdv
cmtzLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAgIN+nXoAe7cI16A5
3DI1T9CioMljG70IbEUOlQF9j/5T7cSJWH8gV+wVrAXMj2QQzGA1tAquL0E0HaUI
iwidtU2p4nHUceoMa7qeZRzZC6WO3Cu8D34fzf3Ys2mdQ75y6q3wKZsw8RMARals
Qx71z2gosV/pnUUbent/+gZtfKsCAwEAATANBgkqhkiG9w0BAQsFAAOBgQA7tV+n
OCrLflev47bTIEU/HlI75zhEzmV3TjwtPXxyFAsA51QSYnwH1IRzPOIptdq4110V
mmwj1FzPtOImbiO+ZZjAhrE2KG3OqDOtS83kT4BC7YmBdqPFH987ewNxLiYhULnD
gyNQt/ElzE5F2MKVOH4c4Q6YKsHItiPSf2c4BQ==
-----END CERTIFICATE REQUEST-----
```

10. Copy the section with the certificate request to include the following:

```
-----BEGIN CERTIFICATE REQUEST-----
...Certificate Request Data...
-----END CERTIFICATE REQUEST-----
```

11. Paste it into a text file, and save the file with a .txt extension. Note the location of this file on your PC.

Make sure there are no spaces, characters or carriage returns added to the Certificate Request.

12. Send the Certificate Request file to the CA to request a Valid SSL Certificate.

Important Notes:

- Do not click OK in the Generate CSR screen after saving the Certificate Request file and sending to the CA. Each time OK is clicked on the Generate CSR screen, a new CSR and private key are created, overwriting any previous private key. Consequently, if a Certificate Request file has been submitted to the CA, and the OK button has been clicked since the original Certificate Request was generated, the returned certificate will not match the current private key, and a new request will have to be issued and sent to the CA.
- Not all Certificate Authorities ask for the same information when requesting a certificate. For example, some CA's ask for a server type (Apache, etc) while others do not. FortiNAC requires a non-encrypted certificate in one of the following formats:
  - PEM
  - DER
  - PKCS#7
  - P7B

  This will allow the certificate to be applied to any of the desired components.

  If the certificate is in PEM format, opening the certificate in a text editor should look something like the following format:

```
-----BEGIN CERTIFICATE1-----
fjkghwjernlsfuigylerkjlkfjnu23jnlkjbliu5ghl6kh4
fjkjlkfjnu23jnlkjbliu5ghl6khkghwjernlsfuigyler4
ghwjernlsfuigylerkjlkfjnu23jnlkjbliu5fjkghl6kh4
-----END CERTIFICTATE1-----
-----BEGIN CERTIFICATE2----
```

```
fjkghwjernlsfuigylerkjlkfjnu23jnlkjbliu5ghl6kh4
fjkjlkfjnu23jnlkjbliu5ghl6khkghwjernlsfuigyler4
ghwjernlsfuigylerkjlkfjnu23jnlkjbliu5fjkghl6kh4
-----END CERTIFCATE2-----
```

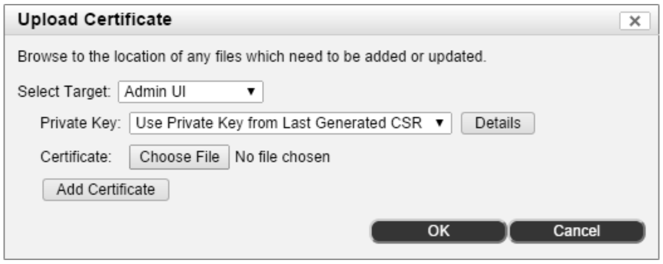
Certificate requests generated on FortiNAC use the SHA1 RSA encryption signature. However, certificates with SHA2 encryption can be requested using this CSR.

- Agent versions prior to 3.1.5 are not compatible with SHA2. Contact Support to verify appropriate SHA version based on current deployment.
  - Select **Admin UI** to generate a CSR for the administrative user interface.
  - Select **Persistent Agent** to generate a CSR for the PA communications.
  - Select **Portal** to generate a CSR to secure the captive portal and DA communications.

The Private Key that corresponds with the CSR is stored on the appliance. Once the SSL Certificate is uploaded, to view the Private Key, click the **Details** button and select the **Private Key** tab.

Upload the certificate

Upload the valid SSL certificate to the appliance when the certificate file is returned from the CA. Certificate files can be returned to you in one of several configurations. Depending upon the CA, one or multiple certificate files may be returned.



Upload Certificate

Browse to the location of any files which need to be added or updated.

Select Target: Admin UI

Private Key: Use Private Key from Last Generated CSR

Certificate: Choose File No file chosen

1. Save the file(s) received from the CA to your PC.
2. Select **System > Settings**.
3. Expand the **Security** folder.
4. Select **Certificate Management** from the tree.
5. Click **Upload Certificate**.
6. Select the target where the certificate will be uploaded:
   - Select **Admin UI** to install the certificate for the administrative user interface.
   - Select **Persistent Agent** to install certificate for the PA communications.
   - Select **Portal** to install the certificate to secure the captive portal.
7. Do one of the following:
   - Select **Use Private Key from Last Generated CSR** to use the key from the most recent CSR for the selected target.
   - Select **Reuse Private Key from Existing Certificate** to use the private key for the certificate currently in use. This option is for renewing an existing installed certificate.
   - Select **Upload Private Key** to upload a key stored outside FortiNAC. Click Choose to find and upload the private key.

8. Click the Choose File button to find and select the certificate to be uploaded. Users can also upload CA certificates and CA bundles.

   Upload any relevant intermediate certificate files needed for the creation of a complete certificate chain of authority. The Certificate Authority should be able to provide these files. Without a complete certificate chain of authority, the target functionality may produce error/warning messages.

9. Click the **Add Certificate** button if multiple certificates were returned. Use this to enter each additional certificate file.
10. Click **OK**.

Copying a certificate to another target

If the certificate is intended to be used for multiple targets, copy the certificate to the new target:

1. Highlight the target with the desired certificate installed.
2. Click **Copy Certificate**.
3. Select the new target from the drop-down menu.
4. Click **OK**.

Activating certificates

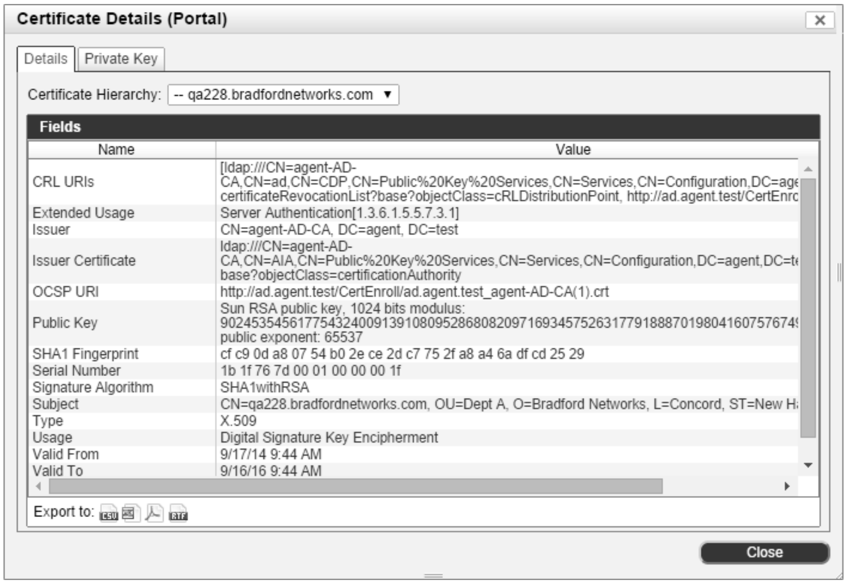
Certificates for the Administrative User Interface and Persistent Agent are activated automatically upon installation. No further action is required.

To begin using the certificate when connecting to the Portal, do the following:

1. Navigate to **System > Settings**.
2. Expand the **Security** folder, and then click **Portal SSL**.
3. In the **SSL Mode** field, select **Valid SSL Certificate**.
4. Click **Save Settings** (this may take several minutes).

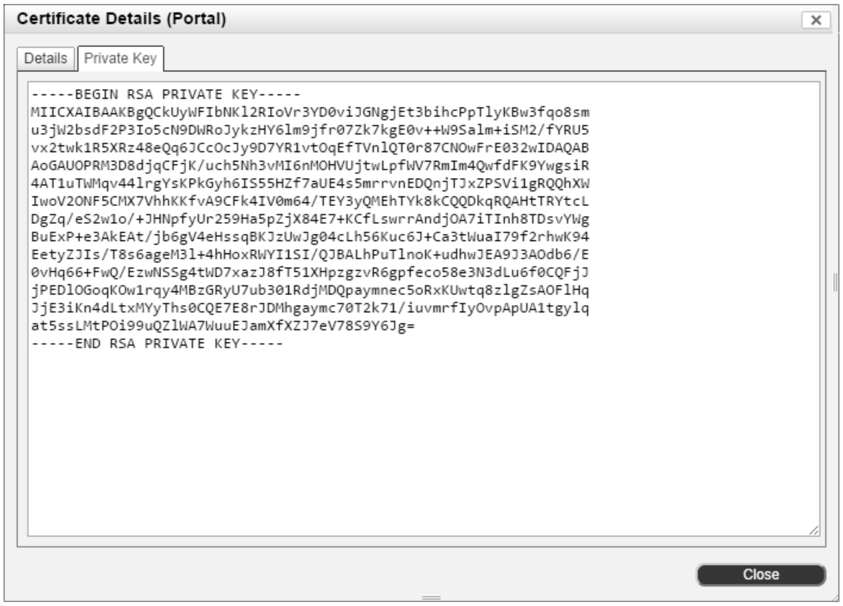
View the details and private key information for a certificate

Users can view the certificate details and private key information for the selected target.



Certificate Hierarchy: -- qa228.bradfordnetworks.com

Name	Value
CRL URIs	[ldap:///CN=agent-AD-CA,CN=ad,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=age certificateRevocationList?base?objectClass=cRLDistributionPoint, http://ad.agent.test/CertEnrc
Extended Usage	Server Authentication[1.3.6.1.5.5.7.3.1]
Issuer	CN=agent-AD-CA, DC=agent, DC=test
Issuer Certificate	ldap:///CN=agent-AD-CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=agent,DC=te base?objectClass=certificationAuthority
OCSP URI	http://ad.agent.test/CertEnroll/ad.agent.test_agent-AD-CA(1).crt
Public Key	Sun RSA public key, 1024 bits modulus: 90245354561775432400913910809528680820971693457526317791888701980416075767 public exponent: 65537
SHA1 Fingerprint	cf c9 0d a8 07 54 b0 2e ce 2d c7 75 2f a8 a4 6a df cd 25 29
Serial Number	1b 1f 76 7d 00 01 00 00 00 1f
Signature Algorithm	SHA1withRSA
Subject	CN=qa228.bradfordnetworks.com, OU=Dept A, O=Bradford Networks, L=Concord, ST=New H
Type	X.509
Usage	Digital Signature Key Encipherment
Valid From	9/17/14 9:44 AM
Valid To	9/16/16 9:44 AM



```
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQCkUyWFIbNKl2RIoVr3YD0viJGNgjEt3bihcPpTlyKBw3fqo8sm
u3jW2bsdF2P3Io5cN9DWRoJykzHY6lm9jfr07Zk7kgE0v++W9Salm+iSM2/fYRU5
vx2twk1R5XRz48eQq6JCcOcJy9D7YR1vtOqEfTVnlQT0r87CNOwFrE032wIDAQAB
AoGAUOPRM3D8djqCFjK/uch5Nh3vMI6nMOHVUjtwLpfWV7RmIm4QwfdFK9YwgsiR
4AT1uTWMqv44lrgYsKPkGyh6IS55HZf7aUE4s5mrrvnEDQnjTJxZPSVi1gRQQhXW
IwoV2ONF5CMX7VhhKKfvA9CFk4IV0m64/TEY3yQMEhTYk8kCQQDkqRQAHtTRYtcL
DgZq/eS2w1o/+JHNpfyUr259Ha5pZjX84E7+KCfLswrrAndjOA7iTInh8TDsvYWg
BuExP+e3AkEAt/jb6gV4eHssqBKJzUwJg04cLh56Kuc6J+Ca3tWuaI79f2rhwK94
EetyZJIs/T8s6ageM3l+4hHoxRWYI1SI/QJBALhPuTlnoK+udhwJEA9J3AOdb6/E
0vHq66+FwQ/EzwNSSg4tWD7xazJ8fT51XHpzgzvR6gpfeco58e3N3dLu6f0CQFjJ
jPEDlOGoqKOw1rqy4MBzGRyU7ub301RdjMDQpaymnec5oRxKUwtq8zlgZsAOFlHq
JjE3iKn4dLtxMYyThs0CQE7E8rJDMhgaymc70T2k71/iuvmrfIyOvpApUA1tgylq
at5ssLMtPOi99uQZlWA7WuuEJamXfXZJ7eV78S9Y6Jg=
-----END RSA PRIVATE KEY-----
```

1. Click **System > Settings**.
2. Expand the **Security** folder.
3. Select **Certificate Management** from the tree.
4. Click **Details**.

System communication

System Communication groups together features that allow FortiNAC to communicate with other devices or to send email and SMS messages to administrators and network users.

Option	Definition
Email Settings	Enter settings for your email server. This allows FortiNAC to send email to Administrators and network users. See Email settings on page 169.
Log Receivers	Configure a list of servers that to receive event and alarm messages from FortiNAC. See Log receivers on page 169.
MDM Services	Configure one or more Mobile Device Management (MDM) servers that integrate with FortiNAC. See MDM services on page 172.
Mobile Providers	Displays the default set of Mobile Providers included in the database. FortiNAC uses the Mobile Providers list to send SMS messages to guests and administrators . The list can be modified as needed. See Mobile providers on page 175.
Patch Management	The Patch Management feature allows integration with Patch servers such as BigFix or PatchLink. See Patch management on page 178.
Proxy Settings	Configure FortiNAC to direct web traffic to a proxy server in order to download OS updates and auto-definition updates.
SNMP	Set the SNMP protocol for devices that query FortiNAC for information. It is also used to set the SNMP protocol to accept SNMPv3 traps that register hosts and users. See SNMP on page 186.
Syslog Files	Syslog Files that you create and store are used by FortiNAC to parse the information received from these external devices and generate an event. The event can contain any or all of the fields contained in the syslog output and can be mapped to an Alarm and an Alarm action. See Syslog management on page 190 and Map events to alarms on page 888.
Security Event Parsers	Customize parsing of syslog messages for generating security events. See Security event parsers on page 198
Trap MIB Files	Enter configurations to interpret SNMP trap MIB information sent from a device and associate it with events and alarms in FortiNAC. See Trap MIB files on page 202 and Map events to alarms on page 888.
Threat Analysis Engines	Configure Threat Analysis Engines to be used when applications are submitted via an agent to FortiNAC.
Vulnerability Scanners	Configure and manage the connection to a Vulnerability Scanner, allowing FortiNAC to request and process scan results. See Vulnerability scanner on page 204.

Email settings

1. Click **System > Settings**.
2. Expand the **System Communication** folder.
3. Select **Email Settings** from the tree.
4. Use the table below to enter the necessary settings.
5. Click **Save Settings**.

Settings

Field	Definition
Email Server	Server used to send email notifications.
Sender Email	Email address that appears as the sender in email sent from FortiNAC. You may want to configure an alias for this email address to better inform the recipient that the message is being sent from FortiNAC.
Authentication	If enabled, you must enter the user name and password for the email account used as the sender account.
User Name	User Name for the email account used as the sender account.
Password	Password for the email account used as the sender account.
Port	Port used for communication with the email server. This must match the port setting on the email server itself.
Connection Security	Used to encrypt email communication between the FortiNAC server and the email server. This setting must match the setting configured on your email server. Options are: None, SSL/TLS or STARTTLS.
Advanced	When enabled, displays the SMTP Timeout and SMTP Connection Timeout fields.
SMTP Timeout	Defines how long FortiNAC will wait if the flow of data has stalled before it fails.
SMTP Connection Timeout	Lets you define the amount of time allowed to connect to the email server before it fails.
Test Email Settings	Click this button to send a test message to the email address entered in the Test Settings dialog.

Log receivers

Event and Alarm records may be stored offline on another host. The events and alarms are forwarded by using either a Syslog message or an SNMP Trap. See Log events to an external log host on page 860 and Map events to alarms on page 888 for more information. The host may be either an SNMP Trap receiver or a Syslog server. Use the Log Receivers view to add, modify, and remove external log hosts.

Add a log host server

1. Click **System > Settings**.
2. In the tree on the left select **System Communication > Log Receivers**.
3. Click **Add** to add a log host.
4. Select the type of server.
5. Enter the **IP address** of the server.
6. Enter the configuration parameters for the type of log host. The standard port information for each host type is automatically entered. See the table below for detailed information on each type of server.
7. Click **OK**.

Settings

Field	Definition
Type	Type of server that will receive Event and Alarm messages. Options include: Syslog CSV, SNMP Trap, and Syslog Command Event Format (CEF).
IP address	IP address of the server that will receive Event and Alarm messages.
Port	Connection port on the server. For Syslog CSV and Syslog CEF servers, the default = 514. For SNMP Trap servers the default =162

Field	Definition
Facility	Displays only when Syslog is selected as the Type. Allows you to configure the message type. The default is 4. Options include: • 0 kernel messages • 1 user-level messages • 2 mail system • 3 system daemons • 4 security/authorization messages • 5 messages generated internally by syslogd • 6 line printer subsystem • 7 network news subsystem • 8 UUCP subsystem • 9 clock daemon • 10 security/authorization messages • 11 FTP daemon • 12 NTP subsystem • 13 log audit • 14 log alert • 15 clock daemon • 16 local use 0 (local0) • 17 local use 1 (local1) • 18 local use 2 (local2) • 19 local use 3 (local3) • 20 local use 4 (local4) • 21 local use 5 (local5) • 22 local use 6 (local6) • 23 local use 7 (local7)
Security String	Displays only when SNMP is selected as the Type. The security string sent with the Event and Alarm message.

Modify connection information

1. Click **System > Settings**.
2. In the tree on the left, select **System Communication > Log Receivers**.
3. Select a log receiver from the list and click **Modify**.
4. Edit the log host information.
5. Click **OK**.

Delete an external log host

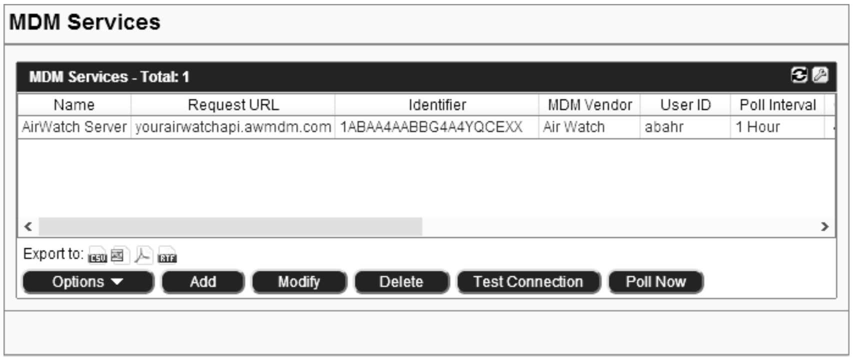
1. Click **System > Settings**.
2. In the tree on the left select **System Communication > Log Receivers**.

3. Select a Log Receiver from the list and click **Delete**.
4. Click **Yes** on the confirmation message.

MDM services

MDM Services allows you to configure the connection or integration between FortiNAC and a Mobile Device Management (MDM) system. FortiNAC and the MDM system work together sharing data via an API to secure the network. FortiNAC leverages the data in the MDM database and registers hosts using that data as they connect to the network.

Proxy communication is not supported.



MDM Services

MDM Services - Total: 1

Name	Request URL	Identifier	MDM Vendor	User ID	Poll Interval
AirWatch Server	yourairwatchapi.awmdm.com	1ABAA4AABBG4A4YQCEXX	Air Watch	abahr	1 Hour

Supported vendors

For information about supported vendors, see the Fortinet Documentation Library.

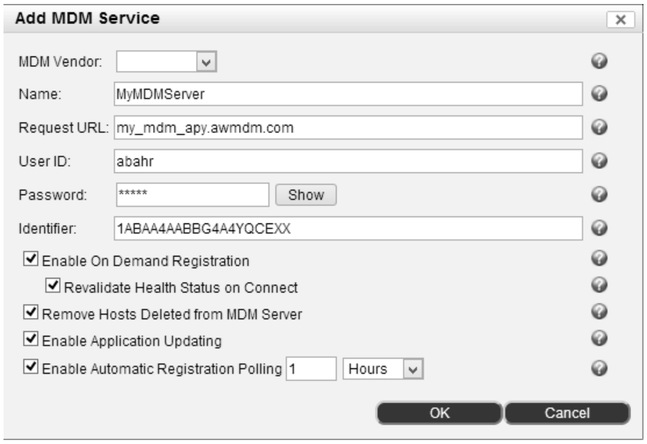
Settings

Field	Definition
MDM Vendor	Name of the vendor of the MDM system.
Name	Name of the connection configuration for the connection between an MDM system and FortiNAC.
Request URL	The URL for the API to which FortiNAC must connect to request data. This will be a unique URL based on your MDM system.
Identifier	A type of key used to identify FortiNAC to the MDM server. This field is not required for all MDM products. In the case of AirWatch, this is the API Key generated during the AirWatch Configuration. An API key is a unique code that identifies the FortiNAC server to AirWatch and is part of the authentication process for AirWatch.

Field	Definition
Application ID	Enter the application ID.
Platform ID	Enter the platform version number.
Application Version	Enter the application version number.
Access Key	Enter the application access key (API key).
User ID	User name of the account used by FortiNAC to log into the MDM system when requesting data.
Password	Password for the account used by FortiNAC to log into the MDM system when requesting data. This field displays only when adding a new MDM connection configuration. It is not displayed in the table of MDM servers.
Poll Interval	Indicates how often FortiNAC should poll the MDM system for information.
Last Poll	Date and time of the last poll.
Last Successful Poll	Date and time of the last poll that successfully retrieved data.
Create Date	Date that this connection configuration was set up.
On Demand Registration	If enabled, when an unknown host reaches the captive portal, FortiNAC queries the MDM server for information about that host. If the host exists in the MDM server, it is registered in FortiNAC using the data from the MDM server.
Revalidate Health Status On Connect	If enabled, when the host connects to the network FortiNAC queries the MDM server to determine if the host is compliant with MDM policies. **NOTE**: This setting is disabled by default. When enabled, the MDM may not be able to manage the rate of queries from FortiNAC, causing performance issues. Instead of enabling Revalidate Health Status On Connect, you can enable automatic registration polling to occur once a day, which will also retrieve Health Status, but with less frequency.
Remove Hosts	If enabled, when FortiNAC polls the MDM server it deletes hosts from the FortiNAC database if they have been removed or disabled on the MDM server.
Update Applications	If enabled, when FortiNAC polls the MDM server it retrieves and stores the Application Inventory for hosts that are in the FortiNAC database. **NOTE**: This setting is disabled by default. When enabled, the MDM may not be able to manage the rate of queries from FortiNAC, causing performance issues.
Last Modified By	User name of the last user to modify the connection configuration.
Last Modified Date	Date and time of the last modification to this connection configuration.
Right click options	
Delete	Deletes the MDM Service.
Modify	Opens the Modify MDM Service dialog.
Poll Now	Polls the MDM server immediately.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item.

Field	Definition
	For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.
Test Connection	Tests the connection between the selected MDM server and FortiNAC. Error messages indicate which fields are missing or incorrect.
Buttons	
Add	Opens the Add MDM Service dialog.
Modify	Opens the Modify MDM Service dialog.
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.
Test Connection	Tests the connection between the selected MDM server and FortiNAC. Error messages indicate which fields are missing or incorrect.
Poll Now	Polls the MDM server immediately.

Add or modify MDM service



Add MDM Service

MDM Vendor:	
Name:	MyMDMServer
Request URL:	my_mdm_apy.awmdm.com
User ID:	abahr
Password:	*****
Identifier:	1ABAA4AABBG4A4YQCEXX

☑ Enable On Demand Registration

☑ Revalidate Health Status on Connect

☑ Remove Hosts Deleted from MDM Server

☑ Enable Application Updating

☑ Enable Automatic Registration Polling 1 Hours

1. Click **System > Settings**.
2. Expand the **System Communication** folder.
3. Select **MDM Service** from the tree.
   a. To modify a record: Select a MDM Service record from the table and click **Modify**.
   b. To add a new record: Click **Add** at the bottom of the window.
4. Use the settings for the MDM Services to enter the MDM Service information.
5. Click **OK** to save.

When integrating an MDM with FortiNAC, if there is more than one FortiNAC with an NCM, it is only necessary to configure the integration on one of the FortiNAC Servers. The host records will be propagated on demand to the other FortiNAC Servers.

The Revalidate Health Status On Connect and Update Applications settings are disabled by default. When enabled, the MDM may not be able to manage the rate of queries from FortiNAC, causing performance issues.

Instead of enabling Revalidate Health Status On Connect, you can enable automatic registration polling to occur once a day, which will also retrieve Health Status, but with less frequency.

Delete MDM service

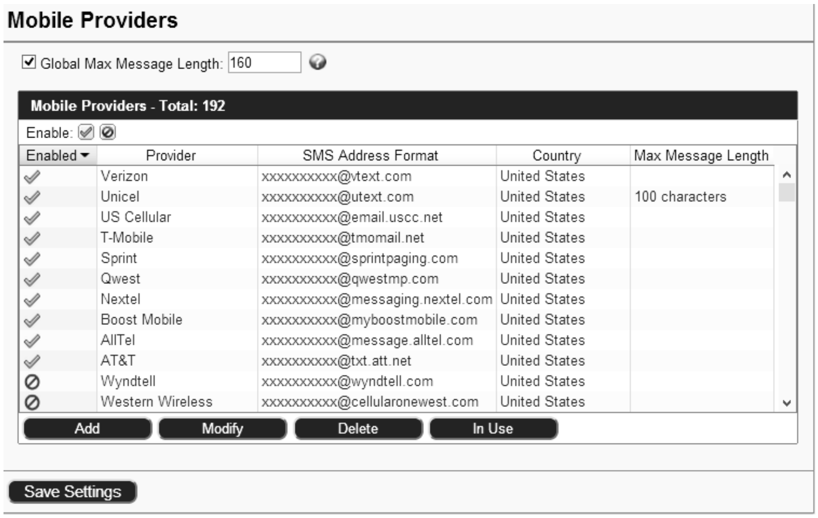
1. Click **System > Settings**.
2. Expand the **System Communication** folder.
3. Select **MDM Service** from the tree.
4. Select an **MDM Service** record from the table.
5. Click **Delete** at the bottom of the window.
6. Click **Yes** on the confirmation message.

Mobile providers

The Mobile Providers window displays the default set of providers included in the database. FortiNAC uses the Mobile Providers list to send SMS messages to guests and administrators by sending email to an address that is a combination of the Mobile Phone number and the Mobile Provider's email address.

This list is populated with some known Mobile Providers but is not comprehensive nor is it updated by Fortinet. You can add, delete or modify Mobile Providers as needed. Mobile Providers can be enabled or disabled individually to limit the number of providers displayed in drop-down lists when configuring guests, users and administrators.

See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.



Mobile Providers

☑ Global Max Message Length: 160

Mobile Providers - Total: 192

Enable: ✓ ⊘

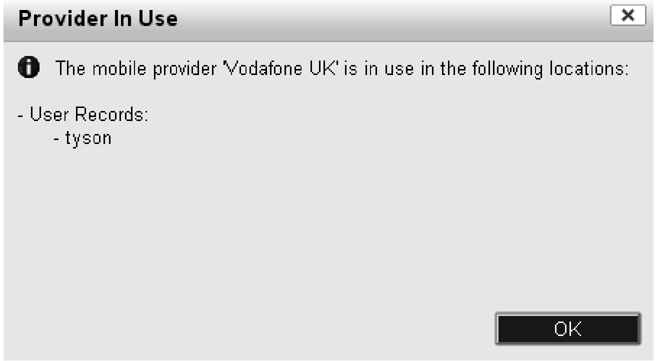
Enabled	Provider	SMS Address Format	Country	Max Message Length
✓	Verizon	xxxxxxxxxxx@vtext.com	United States	
✓	Unicel	xxxxxxxxxxx@utext.com	United States	100 characters
✓	US Cellular	xxxxxxxxxxx@email.uscc.net	United States	
✓	T-Mobile	xxxxxxxxxxx@tmomail.net	United States	
✓	Sprint	xxxxxxxxxxx@sprintpaging.com	United States	
✓	Qwest	xxxxxxxxxxx@qwestmp.com	United States	
✓	Nextel	xxxxxxxxxxx@messaging.nextel.com	United States	
✓	Boost Mobile	xxxxxxxxxxx@myboostmobile.com	United States	
✓	AllTel	xxxxxxxxxxx@message.alltel.com	United States	
✓	AT&T	xxxxxxxxxxx@txt.att.net	United States	
⊘	Wyndtell	xxxxxxxxxxx@wyndtell.com	United States	
⊘	Western Wireless	xxxxxxxxxxx@cellularonewest.com	United States	

Settings

Field	Definition
Global Max Message Length	Enable to set the maximum number of characters that will be included in a single SMS message sent from FortiNAC for all Mobile Providers. If the message is longer than the Max Message Length, it is divided up and sent in multiple messages. If an individual provider has a Max Message Length setting, it overrides the Global setting.
Enable Buttons	Enables or disables the selected provider. If a provider is disabled it is not displayed in the Mobile Provider selection list shown when configuring an Admin user or a guest. You cannot disable a provider that is in use or associated with a user in the database. Click the In Use button to determine which users have the selected provider.
Enabled	A green check mark indicates that the provider is enabled. A red circle indicates that the provider is disabled.
Provider	Name of the company that provides mobile phone services.
SMS Address Format	Format of the address used to send SMS messages via email. For example, for provider AllTel the format is xxxxxxxxxx@message.alltell.com, where the x's represent the user's mobile telephone number.
Country	Country to which this SMS Address corresponds. You may have providers that have a different SMS Address for each country in which they operate. You need a separate record for each one.
Right click options	
Delete	Deletes the selected Provider. Providers that are associated with Users cannot be deleted.
In Use	Select a provider and click In Use to determine if any one in the database has this provider listed in their user record.
Modify	Opens the Modify Mobile Provider window for the selected provider.

Provider in use

To find the list of users associated with a provider, select the provider and click the In Use button. A message is displayed indicating whether or not the provider is associated with any user or guest records. If users are associated with the provider, a list of User IDs is displayed.

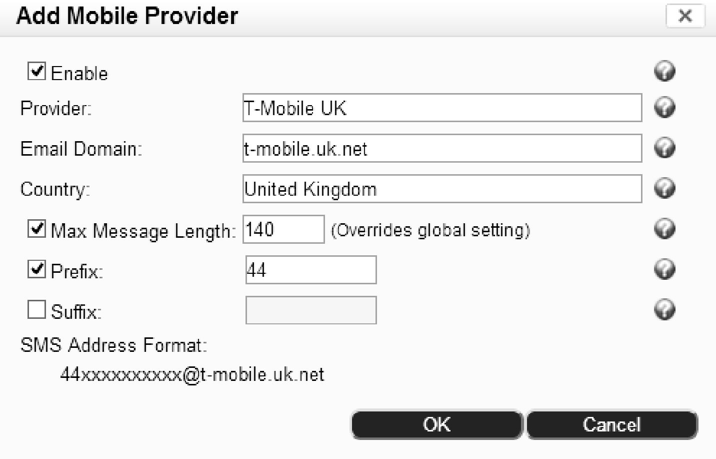


Provider In Use

The mobile provider 'Vodafone UK' is in use in the following locations:

- User Records:
  - tyson

Add or modify a provider



Add Mobile Provider

☑ Enable

Provider: T-Mobile UK

Email Domain: t-mobile.uk.net

Country: United Kingdom

☑ Max Message Length: 140 (Overrides global setting)

☑ Prefix: 44

☐ Suffix:

SMS Address Format:
44xxxxxxxxxx@t-mobile.uk.net

1. Click **System > Settings**.
2. Expand the **System Communication** folder.
3. Select **Mobile Providers** from the tree.
4. Click the **Add** button or select a provider and click **Modify**.
5. Use the table below to complete the provider information.
6. Click **OK** to save your changes.

Settings

Field	Definition
Enable	Enables/disables the provider. Enable/Disable can also be done from the Mobile Providers list.

Field	Definition
Provider	Name of the provider being configured. This name must be unique.
Email Domain	The provider's email domain, such as, nextel.messaging.com.
Country	Country to which this SMS Address corresponds. You may have providers that have a different SMS Address for each country in which they operate. You need a separate record for each one.
Max Message Length	Controls the number of characters included in a single message when messages are sent to this provider's customers. If the message length exceeds the Max Message Length, it is divided up in to multiple messages.
Prefix	Any numbers that are required before the user's mobile number. For example, you may have users that are in an adjacent country, therefore you may need to enter a number, such as 1, ahead of the mobile number.
Suffix	Any numbers required after the user's mobile number.
SMS Address Format	The format used for the address of the message recipient. FortiNAC sends SMS messages via email. The provider's email server sends the messages to the mobile phone number contained in the SMS Address. As you enter information in to the Add/Modify Provider dialog, the SMS Address is updated.

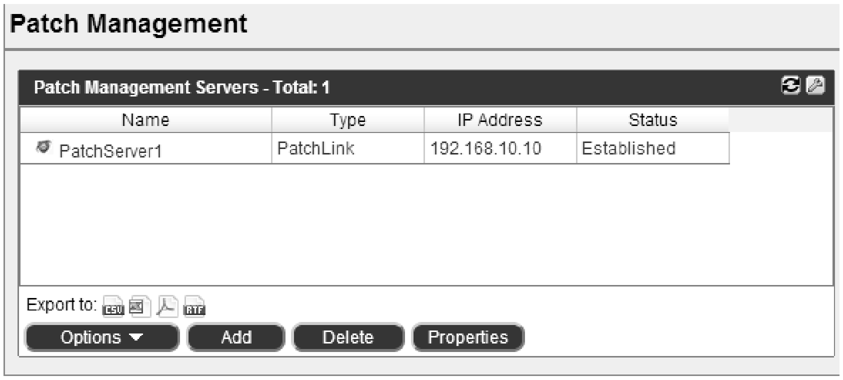
Delete a mobile provider

1. Click **System > Settings**.
2. Expand the **System Communication** folder.
3. Select **Mobile Providers** from the tree.
4. Select a provider and click **Delete**.
5. If users are associated with the provider, a list of user names is displayed. You cannot delete a Mobile Provider if that provider is listed in a User record. First modify the user record and then delete the provider.
6. If no users are associated with the provider, confirm that you want to delete the provider.

Patch management

The Patch Management feature allows integration with Patch servers such as BigFix or PatchLink. The endpoint’s posture is checked on the patch servers. When an endpoint is out-of-compliance, FortiNAC automatically moves the endpoint to a separate remediation network where the patch server solution automatically updates the non-compliant system.

See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.



Name	Type	IP Address	Status
PatchServer1	PatchLink	192.168.10.10	Established

Settings

Field	Definition
Name	Name of the server being configured.
Type	Type of patch server, such as BigFix or PatchLink.
IP address	IP address assigned to the patch server.
Status	Indicates whether or not contact has been established between FortiNAC and the patch server.
Right click options	
Configuration (BigFix Only)	Opens a new window to modify applied actions to BigFix Baseline results.
Delete	Deletes the selected Provider. Providers that are associated with Users cannot be deleted.
Properties	Displays Patch Management Server Properties and allows you to set the Polling Interval. Default = 2 minutes.
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.

Servers and hosts

The Persistent Agent is required on the host to support Patch Management. The Patch Management client must also be installed on the host. If the Patch Management client is installed on the host the Persistent Agent reports this during its routine messages to the server.

When a Patch Management Server is added to the Patch Management View, FortiNAC queries that server to determine whether or not the host is compliant.

- If the Patch Management Server is not reachable, an event and alarm are generated. The host is considered compliant and remains in the production network.
  - *BigFix event* - Communication lost with the BigFix Server Database
  - *PatchLink event* - Communication lost with the PatchLink Server
- If the Patch Management Server is reachable and determines that the host is not compliant, the host is moved to remediation. An event is generated to indicate that the host is not compliant.

  - *BigFix events* - BigFix High Violation, BigFix Medium Violation, BigFix Low Violation
  - *PatchLink event* - PatchLink Non Compliant
- If the Patch Management Server is reachable and determines the host is compliant and the host was previously NOT compliant, then an event is generated to indicate that the host is now compliant. The compliant event is only generated after a not compliant event has been generated.
  - *PatchLink event* - PatchLink Compliant

Alarms can be mapped to events to notify you when the event has been generated. Each of the events listed above could be mapped to an alarm. See Map events to alarms on page 888 for additional information.

PatchLink implementation

To setup communication between a PatchLink Server and FortiNAC you must do the following:

- The PatchLink NAC Integrator plug-in is required on the PatchLink server to allow PatchLink to respond to HTTP requests from FortiNAC.
- Your FortiNAC Server must have licenses for Integration Suite and Endpoint Compliance. Check the License Information panel on the Dashboard to make sure you have the correct licenses. See License management on page 215.
- Add the PatchLink Server to System > Settings > System Communication > Patch Management.
- Go to the PatchLink server properties and configure the Polling Interval. The default is 2 minutes.
- Network hosts must have the Persistent Agent installed. See Agent overview on page 491.
- Network hosts must have the PatchLink Agent installed. Refer to the PatchLink documentation for instructions on installing this agent.
- Enable the PatchLink Compliant and PatchLink Non Compliant events. See Enable and disable events on page 857.
- Create an Admin Scan specifically for PatchLink. These scans indicate the reason why a host was marked at risk. They are not actually scanning the host but provide a configuration or profile with which to associate the host state. Admin Scans are also used to mark hosts At Risk or Safe based on an alarm action triggered by a PatchLink event. See Add a scan on page 481.
- Map alarms to the PatchLink Compliant and PatchLink Non Compliant events. For each alarm, configure a Host security action associated with the PatchLink Admin Scan earlier and mark the host At Risk or Safe depending on the alarm triggered. See Add or modify alarm mapping on page 892.

PatchLink process

When PatchLink is integrated with FortiNAC as a patch management server a variety of communications occur between the two servers to make sure that hosts are compliant. The communication process is as follows:

1. The PatchLink Agent installed on the host sets a registry key value with an Agent ID value.

   Registry Example:

   NameValue:

   Name = PatchManagementID

   Value = 6AA80EB2-CFAA-466C-9A6B-85B5A918B162
2. The FortiNAC Persistent Agent installed on the host reads the registry key and reports the value set by the PatchLink Agent back to FortiNAC. This is stored in the database, but is not displayed in the Admin User Interface.
3. Based on the Polling interval set for the PatchLink server, FortiNAC gathers a list of hosts with values for PatchLink

in the database and sends an HTTP request to the PatchLink server for each host. For example, if the polling interval is set to 2 minutes, then every 2 minutes an HTTP request is sent for every host in the database with PatchLink data in the host record.

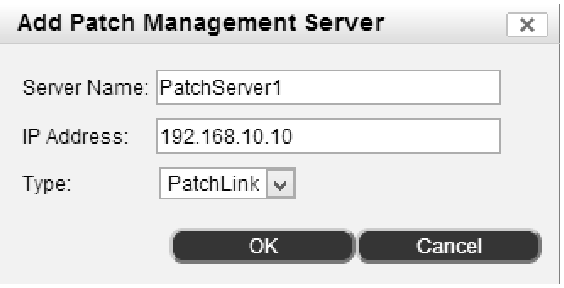
Request Example:

http://10.20.100.32/IntegrationPoint/EndpointSecurity_V1/Status.aspx?Agentid=A5F1D1F2-F045-4866-8903-7E920417BD62

4. The PatchLink server returns a response for each host indicating whether the host is compliant or non-compliant. For each response, either a PatchLink Compliant or a PatchLink Non Compliant event is triggered.
5. If alarms have been configured for these events, then hosts are marked either safe or at risk based on the event triggered.

Add servers

To integrate a Patch Management Server with FortiNAC it must be added to the Patch Management view.



Add Patch Management Server

Server Name: PatchServer1

IP Address: 192.168.10.10

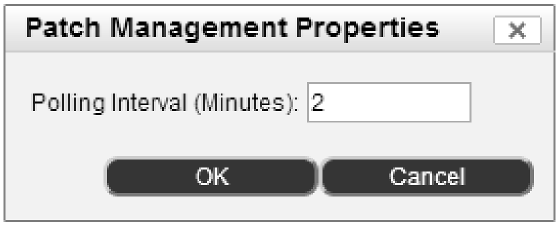
Type: PatchLink

1. Click **System > Settings > System Communication**.
2. Select **Patch Management**.
3. Click **Add**.
4. Enter a name for the server, the IP address, and select the patch server from the **Type** drop-down list.
5. Click **OK**.
6. If you select **BigFix** from the **Type** drop-down list, you are prompted to enter the BigFix database credentials, which lets FortiNAC connect directly to the data store of BigFix, allowing for BaseLine test results.

Read access is required.

PatchLink server configuration

Once the PatchLink server has been added to the Topology view, the polling interval must be entered into the properties view. The polling interval is the length of time FortiNAC will wait before polling the PatchLink Server for updated client status information.



Polling Interval (Minutes): 2

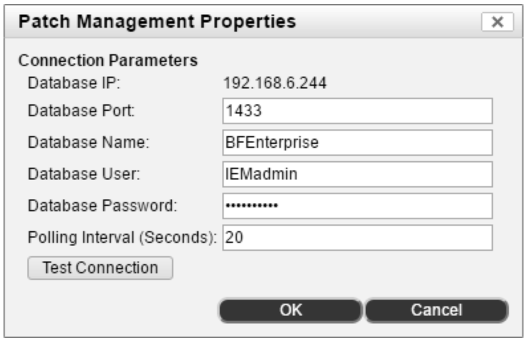
1. Click **Network Devices > Topology** and expand the **FortiNAC** and **Patch Management** icons.
2. Right-click on the **PatchLink Server** and select **Properties**.
3. Enter the polling interval.
4. Click **Apply**.

BigFix server properties

Once the BigFix patch management server has been added to the Patch Management Servers view, the connection parameters for the server and database must be entered to allow FortiNAC to communicate with the server and database.

The Persistent Agent must be installed to communicate with a Patch Management integration.

The BigFix Client must be installed and be connected to the BigFix Server before the Persistent Agent is installed.



Connection Parameters

Database IP:	192.168.6.244
Database Port:	1433
Database Name:	BFEnterprise
Database User:	IEMadmin
Database Password:	••••••••••
Polling Interval (Seconds):	20

1. Click **System > Settings > System Communication > Patch Management**.
2. Right-click on the **BigFix Patch Management Server** and select **Properties**.
3. Use the table below to enter the connection parameters for the server and database.
4. Click The BigFix Client must be installed and be connected to the BigFix Server before the Persistent Agent is installed.

Settings

Field	Description
Database IP	The IP address of the server where the database resides.
Database Port	The port on the server used for access to the database information.
Database Name	The name of the database.
Database User	The username used to access the database information.
Database Password	The password for access to the database for the entered database user.
Polling Interval (Sec)	The length of time between polls to the patch management server to retrieve data.
Test Connection	Allows you to test SQL Server credentials for Patch Management servers.

Once communication with the BigFix Patch Management server has been established the Administrator will use the BigFix server's Configuration view to view the status of host endpoint systems and select an action to take if the host is out of compliance.

BigFix configuration

The Configuration view contains a list of the Base-Line Names from the BigFix server. Each of the Base-Line Names has an associated Failure Action and Untested Action.

Although actions applied will affect all users that report as failed or untested, the report will only show online users being affected.

Field	Description
Base-Line Name	A list of required patches given in the BigFix database that the host must have to be in compliance. The list of hosts or groups that the Base-Line Name apply to are determined in the BigFix server.
Failure Action	The action that can be applied to an endpoint if it has failed the test for the Base-Line Name indicated.
Untested Action	The action that can be applied to an endpoint if it has not been tested against the Base-Line Name indicated.

The Administrative Action is an Admin scan that is created in Remediation Configuration. See Remediation configurations on page 481 for details on adding and using an Admin scan.

Admin scans must be created under Remediation Configuration before you can select them here. See Remediation configurations on page 481.

To apply a Failure or Untested Action on an endpoint:

1. Click **System > Settings > System Communication > Patch Management**.
2. Right-click on the **BigFix Patch Management Server** and select **Configuration**.
3. Select the **Severity** under **Failure Action** to apply that action to the hosts indicated in the **Base-Line Name** that have failed to meet the specified patch requirements.
4. Select the **Severity** under **Untested Action** to apply that action to the hosts indicated in the **Base-Line Name** that have not been tested to determine whether or not the specified patch requirements have been met.
5. Click **Apply**.

The severity creates an alarm that can be associated with actions, including Admin Scans. See Map events to alarms on page 888

In **Logs > Events To Alarm Mappings**, three events can be used for security related actions:

- BigFix Low Violation
- BigFix Medium Violation
- BigFix High Violation

When creating these events, an action may be applied to accompany the creation of the alarm. To use Admin Scans created in the Remediation Configuration, do the following:

1. Select **Host Security Action**.
2. Select the **Admin Scan** for which the host state will be modified.

When applying a severity to results of a baseline action, the online hosts that are affected will be in the Baseline Host Report. To access this report, select Hosts next to the severity being applied.

BigFix Baseline Host

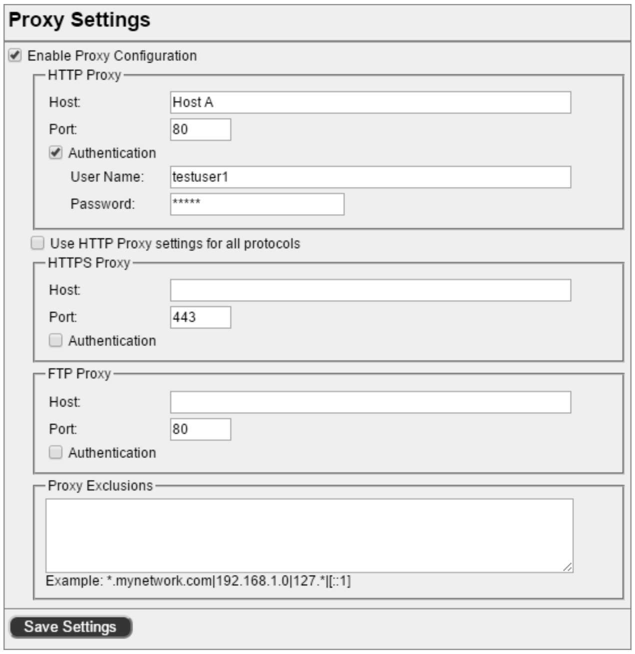
The data displays hosts that are currently online that have reported as untested or failed by BigFix.

These host reports only display online users. However, the action applied will affect all users who have a Persistent Agent and a BigFix Client installed simultaneously.

Proxy settings

Proxy Settings allows you to configure FortiNAC to direct web traffic to a proxy server in order to download OS updates and auto-definition updates.

Proxy communication is not supported for MDM Services.



Proxy Settings

☑ Enable Proxy Configuration

HTTP Proxy

Host: Host A

Port: 80

☑ Authentication

User Name: testuser1

Password: *****

□ Use HTTP Proxy settings for all protocols

HTTPS Proxy

Host:

Port: 443

□ Authentication

FTP Proxy

Host:

Port: 80

□ Authentication

Proxy Exclusions

Example: *.mynetwork.com|192.168.1.0|127.*|[::1]

1. Click **System > Settings**.
2. Expand the **System Communication** folder.
3. Select **Proxy Settings** from the tree.
4. Use the table below to enter the necessary settings.
5. Click **Save Settings**.

Settings

Field	Definition
Enable Proxy Configuration	If enabled, FortiNAC will use the Proxy Configuration to download OS updates and auto-definition updates.
Host	The hostname or address of the proxy server.
Port	Port used for communication with the proxy server. This must match the port setting on the proxy server itself.
Authentication	If enabled, you must enter the user name and password for the proxy server.
User Name	User Name for the email account used as the sender account.
Password	Password for the email account used as the sender account.
Use HTTP Proxy settings for all protocols	If enabled, the HTTP Proxy configuration will be used for both HTTPS and FTP Proxy communication.
Proxy Exclusions	Indicates the hosts that should be accessed without going through the proxy. The list of hosts are separated by the '|' character. The wildcard character '*' can be used for pattern matching (e.g., Dhttp.nonProxyHosts="*.foo.com|localhost" indicates that every host in the foo.com domain and the localhost should be access directly, even if a proxy server is specified).

SNMP

Use the SNMP Properties view to select the SNMP protocol for devices that query FortiNAC for information. If SNMP is enabled, FortiNAC responds to SNMP communication from other devices, such as a Network Management system that might include the FortiNAC server in its own database.

Go to **Settings > System Communication > SNMP**.

In addition, this view is also used to set the SNMP protocol to accept SNMPv3 traps that register hosts and users.

Both types of communication pass through port 161. Settings here are global. Therefore, if you choose to use SNMPv3 traps sent from other network devices to register hosts and users, then ALL other devices that query FortiNAC for information must also communicate using SNMPv3. You must modify the configuration of those external devices to use SNMPv3.

The SNMP protocols that are supported are SNMPv1/SNMPv2c and SNMPv3. SNMPv3 uses DES or AES encryption for the Privacy Password.

Privacy protocols supported are:

- DES
- Triple-DES
- AES-128

SNMP MIBs used to communicate with FortiNAC are in:

```
/bsc/campusMgr/ui/runTime/docs/mibs/
```

Settings

Field	Description
Enable SNMP Communication	If SNMP is enabled, FortiNAC responds to SNMP requests from other servers.
SNMP Protocol	Select the SNMP protocol FortiNAC will be responding to: SNMPv1/SNMPv2c SNMPv3-AuthPriv (SNMPv3 with Authentication and Privacy) SNMPv3 AuthNoPriv (SNMPv3 with Authentication but no Privacy.)
SNMPv1/SNMPv2c	
Security String	Enter the security string that FortiNAC will respond to when communicating with the server.
SNMPv3	
User Name	User Name for the SNMPv3 credentials.
Authentication Protocol	Specify the SNMPv3 Authentication Protocol. The available Authentication Protocols are MD5 SHA1

Field	Description
Authentication Password	Specify the Authentication Password required by FortiNAC when SNMPv3-AuthPriv or SNMPv3-AuthNoPriv queries are received.
Privacy Protocols	Specify the SNMPv3 Privacy Protocol. The available privacy protocols are: DES Triple-DES AES-128
Privacy Password	Specify the Privacy Password required by FortiNAC when SNMPv3-AuthPriv queries are received.
Management hosts	
IP addresses	List of IP addresses of the devices that have communicated with FortiNAC through SNMP.

Set up SNMP communication

1. Click **System > Settings**.
2. Expand the **System Communication** folder.
3. Select **SNMP** from the tree.
4. Click **Enable** and select an **SNMP protocol**.
5. Enter the parameters as required for the selected protocol. See the table above for additional information.
6. Click **Save Settings**.

Disable SNMP communication

1. Click **System > Settings**.
2. Expand the **System Communication** folder.
3. Select **SNMP** from the tree.
4. Click **Disable**.
5. Click **Save Settings**.

Register hosts and users with SNMPv3 traps

FortiNAC can use data sent in SNMPv3 traps from external devices to register hosts and users. This speeds up the process of adding hosts and users to your FortiNAC database by taking advantage of information that is readily available from another system. In addition, based on trap parameters hosts and users can be modified or removed from the database.

FortiNAC requirements

- FortiNAC must have an Integration Suite license. See Licenses on page 7.
- The Trap Sender must be modeled in the Topology View as a pingable device. See Add or modify a pingable device on page 725.
- You must enter SNMPv3 settings in System > Settings > System Communication > SNMP that match those of the device to which you are sending traps. Note that if you had previously entered SNMPv1/SNMPv2c settings for external devices querying FortiNAC for information, you must modify settings on those devices to use SNMPv3.
- If you are running FortiNAC in a FortiNAC Control Manager environment, the Trap Sender must be modeled on each FortiNAC Server or Control Server that should receive this information. Note that if you have enabled any of the Copy Registered Host options on the FortiNAC Control Manager it may not be necessary to receive traps on more than one managed server.
- When traps are received they can trigger the events listed below in the Event Log. These events can be mapped to Alarms. Make sure the events are enabled. See Event management on page 856. To map events to alarms see Add or modify alarm mapping on page 892.

Event	Definition
Add/Modify/Remove Host	Generated whenever a trap is received that adds, modifies or removes a host record in the database.
Add/Modify/Remove User	Generated when a trap is received that adds, modifies or removes a user record in the database.

Trap sender requirements

- Use the Management IP address (eth0) of the FortiNAC Server or Control Server as the destination for the trap.
- Send traps to port 161 on the FortiNAC Server or Control Server.
- If you are running FortiNAC in a High Availability environment, send traps to both the primary and the secondary FortiNAC Servers or Control Servers.
- You must have snmptrap.exe and libsnmp.dll on the device sending the traps. Download the latest binaries for the appropriate operating system from www.net-snmp.org/download.html.
- Configure the traps on the sending device. See the tables below for information on trap parameters.

Hosts

- If a trap is received for an existing host, the host's database record is updated with information from the trap.
- When a trap is received for a host that matches a rogue in FortiNAC, the rogue is converted to a registered host if the trap contains user data. It is converted to a registered device if there is no associated user.
- If a user is deleted based on a trap, associated hosts are not deleted and they become registered devices. To delete these hosts either send an additional trap that removes the host or you must go to the Host View and delete them manually. See Delete a host on page 809.
- If the same host is added twice but with different MAC addresses for separate adapters, it is treated as two separate records in the FortiNAC database. The two adapters are not linked to each other in any way and are not considered siblings in FortiNAC.
- Variables with spaces in the names should be in quotation marks, such as, "Windows Vista".
- Separators in MAC Addresses must be colons, such as, 90:21:55:EB:A3:87.

OID	Description	Definition
1.1.1.1	Host Name	Name of the host.
1.1.1.2	IP address	IP address of the host.
1.1.1.3	MAC Address	Physical Address of the host. Required.
1.1.1.4	Host Operating System	Name of the operating system on the host.
1.1.5	Role	Role assigned to the host. Roles are attributes of hosts used as filters in User/Host Profiles.
1.1.6	Action	Indicates whether this trap is adding or removing a host from the database. Adding an existing host will modify that host's record in the database. 1=Add 2=Remove
1.2.8	Element	Indicates that this trap is registering either a host or a host and its corresponding user.

Example traps

To add a host record for the PC with a hostname of *Gateway-notebook*, with an IP address of *160.87.100.117*, a MAC address of *00:26:9E:E2:DD:DB*, an OS of *Windows*, and a role of *Guest*:

```
snmptrap -v3 -u <user**> -l authNoPriv -a MD5 -A <Passphase**> 160.87.9.10:161 ''
1.3.6.1.4.1.16856.1.2.8 .1.3.6.1.4.1.16856.1.1.1.1 s Gateway-notebook
.1.3.6.1.4.1.16856.1.1.1.4 s Windows .1.3.6.1.4.1.16856.1.1.1.2 s 160.87.100.117
.1.3.6.1.4.1.16856.1.1.1.3 s 00:26:9E:E2:DD:DB .1.3.6.1.4.1.16856.1.1.5 s Guest
.1.3.6.1.4.1.16856.1.1.6 integer 1
```

To remove host record for the PC with a hostname of *Gateway-notebook*, with an IP address of *160.87.100.117*, a MAC address of *00:26:9E:E2:DD:DB*, an OS of *Windows*, and a role of *Guest*. Note that only MAC address is required to remove a host.

```
snmptrap -v3 -u <user**> -l authNoPriv -a MD5 -A <Passphase**> 160.87.9.10:161 ''
1.3.6.1.4.1.16856.1.2.8 .1.3.6.1.4.1.16856.1.1.1.1 s Gateway-notebook
.1.3.6.1.4.1.16856.1.1.1.4 s Windows .1.3.6.1.4.1.16856.1.1.1.2 s 160.87.100.117
.1.3.6.1.4.1.16856.1.1.1.3 s 00:26:9E:E2:DD:DB .1.3.6.1.4.1.16856.1.1.5 s Guest
.1.3.6.1.4.1.16856.1.1.6 integer 2
```

Users

- If an LDAP directory is modeled in the Topology View, FortiNAC checks the directory for information about the user included in the trap. If the user exists in the directory, additional fields are populated for that user in the FortiNAC database. If the user does not exist in the directory, a user record is created in FortiNAC with only the data received in the trap.
- If a trap is received for an existing user, the user's database record is updated with information from the trap.
- If a trap is received for an existing user and the trap contains host information, the host is registered to the user. If the host already has a rogue record, the rogue is converted to a registered host and associated with the user.
- If a user is deleted based on a trap, associated hosts are not deleted and they become registered devices. To delete these hosts you must go to the Host View and delete them manually. See Delete a host on page 809.

- When FortiNAC resynchronizes with the directory, user data may be overwritten by data from the directory depending on the directory attribute mappings.
- Variables with spaces in the names should be in quotation marks, such as, "Mary Ann".

Trap parameters

OID	Description	Definition
1.1.2.1	User Name	User Name stored in the directory. If the user is not in the directory, this record will still be added, modified or removed. Required.
1.1.2.2	User First Name	
1.1.2.3	User Last Name	
1.1.2.4	User Title	
1.1.2.5	Email	User's e-mail address.
1.1.5	Role	Role assigned to the User. If this trap is adding both a user and a host, both are set to the same role.
1.1.6	Action	Indicates whether this trap is adding or removing a user from the database. Adding an existing user will modify that user's record in the database. 1=Add 2=Remove
1.2.9	Element	Indicates that this trap is only registering a user.

Example traps

To add *testuser* to the database:

```
snmptrap -v3 -u <user**> -l authNoPriv -a MD5 -A <Passphase**> 160.87.9.10:161 ''
1.3.6.1.4.1.16856.1.2.9 .1.3.6.1.4.1.16856.1.1.2.1 s testuser
.1.3.6.1.4.1.16856.1.1.2.2 s John.1.3.6.1.4.1.16856.1.1.2.3 s Doe
.1.3.6.1.4.1.16856.1.1.2.4 s Mr .1.3.6.1.4.1.16856.1.1.2.5 s jdoe@megatech.com
.1.3.6.1.4.1.16856.1.1.5 s Guest .1.3.6.1.4.1.16856.1.1.6 integer 1
```

To delete user record for *testuser* from the database. Note that only User Name is required to remove a user.

*snmptrap -v3 -u <user**> -l authNoPriv -a MD5 -A <Passphase**> 160.87.9.10:161 '' 1.3.6.1.4.1.16856.1.2.9 .1.3.6.1.4.1.16856.1.1.2.1 s testuser .1.3.6.1.4.1.16856.1.1.2.2 s John.1.3.6.1.4.1.16856.1.1.2.3 s Doe .1.3.6.1.4.1.16856.1.1.2.4 s Mr .1.3.6.1.4.1.16856.1.1.2.5 s jdoe@megatech.com .1.3.6.1.4.1.16856.1.1.5 s Guest .1.3.6.1.4.1.16856.1.1.6 integer 2*

Syslog management

You can choose to send output from IPS/IDS devices to FortiNAC. Syslog Files that you create and store under Syslog Management are used by FortiNAC to parse the information received from these external devices and generate an event. The event can contain any or all of the fields contained in the syslog output.

Default Syslog Files

Default files include:

- FireEye
- FortiOS4
- FortiOS5
- Palo Alto Networks Firewall
- Sourcefire IPS
- StoneGate IPS
- TippingPoint SMS
- Top Layer IPS

Each of these files has corresponding events in the events list. You can add configurations for other Syslog files if they conform to either the CSV, CEF or TAG/VALUE formats.

Events and alarms

When those new Syslog configurations are added, corresponding events and alarms are created in the Events List. See Events and alarms list on page 868 for a complete list of events that can be tracked.

If a syslog message is received for a host that has more than one adapter, an event is generated for each adapter. Therefore a single host could generate multiple events and alarms.

Device model

You must model any device that sends Syslog information to FortiNAC in the Topology view. See Add or modify a pingable device on page 725 for detailed instructions.

Navigation

To access the Syslog Management View select **System > Settings > System Communication > Syslog Files**.

Settings

Field	Definition
Table configuration	
Enable Buttons	Enables or disables the selected Syslog file. If a file is disabled it is not used when processing inbound syslog messages.
Table columns	
Name	The name of the syslog file. This is a unique name for this syslog definition. This value is required.
Enabled	A green check mark indicates that the file is enabled. A red circle indicates that the file is disabled.
Label	The label for the Event or Alarm that will be generated. This value is required.

Field	Definition
Format	Message format for the Syslog file. Supported formats include: • **CSV** — Message is a series of data fields typically separated by commas. Comma separated value. Other characters can be used to separate data fields. • **TAG/VALUE** — Message is series of fields each with a tag and a value. For example, the message could contain the following : cip=192.168.10.182. cip is the tag indicating that this is the IP address of the user causing the problem. 192.168.10.182 is the value associated with that tag. • **CEF** — Message is a series of fields, some in a standard position, others with a tag and a value. For example the message could contain the following: `src=192.168.10.182.src` is the tag indicating that this is the IP address of the user causing the problem. `192.168.10.182` is the value associated with that tag.
Delimiter	Character used to separate the fields in the syslog message. Options include: space, comma (,) and pipe (|). This field is not available for the TAG/VALUE format. A space is used as the delimiter.
IP Tag/Column	Name of the field or number of the column containing the source IP address. This value is required.
Filter Tag/ Column	Name of the field or number of the column containing the filter. This value is required.
Filter Value	The value contained in the filter column or field. Only entries that contain matching data will be used. This value is required.
Severity Tag/Column	Name of the field or number of the column containing the severity. This value is required.
Low Severity Values	Entries containing one of these matching values in the severity field or column cause a Low Severity event to be generated. For CSV format, multiple values are entered separated by commas.
Medium Severity Values	Entries containing one of these matching values in the severity column will cause a Medium Severity event to be generated. For CSV format, multiple values are entered separated by commas.
High Severity Values	Entries containing one of these matching values in the severity field or column cause a High Severity event to be generated. For CSV format, multiple values are entered separated by commas.
Event Tag/ Column	Names of the fields or numbers of the columns used when populating items from the syslog entry into the Event Format.
Event Format	Message that is displayed when the event is generated. The text is generated from the items listed in the Event Tag field in the order they appear.
Right click options	
Add	Opens the Add Syslog Files dialog.

Field	Definition
Delete	Deletes the selected action.
Modify	Opens the Modify Security Action window for the selected action.
In Use	Shows if the Syslog File is in use or not
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.
Enable	Enables the syslog file.
Disable	Disables the syslog file.
Buttons	
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. Low, Medium and High severity levels are not included in the exported data. See Export data on page 710.

Inbound file formats

There are three supported syslog formats, CSV, TAG/VALUE and CEF. The CSV syslog output format is a comma-separated entry with seven items. Identify each item in the entry by its column number when you create the Event Message format. The TAG/VALUE syslog output format is a set of messages where the TAG indicates the name of the program or process that generated the message and the VALUE is the content of the message. The CEF syslog output format uses tags to mark the data so that it can be located by the device receiving the syslog file.

CSV Example:

```
Denied,10,192.168.1.1,00:10:8B:A7:EF:AA,IPS Sensor,214,P2P-TCP-BitTorrent-Network-Connect
```

Column Number	Description	Data From Example
1	Action taken by IPS/IDS	Denied
2	Alert Severity	10
3	Source IP address	192.168.1.1
4	Source MAC Address	00:10:8B:A7:EF:AA
5	Component ID	IPS Sensor
6	Rule ID	214
7	Situation	P2P-TCP-BitTorrent-Network-Connect

TAG/VALUE Example:

```
<38>Apr 14 09:48:55 192.168.5.199 IPS5500-1000: id=060001 pt=TLN-TM prot=TCP
cip=192.168.10.182 cprt=49161 sip=192.168.10.10 sprt=445 atck=tln-001017
disp=mitigate ckt=1 src=extern msg="NETWK: TCP Connection With Missed Setup"
```

Only the fields used by Syslog Management are defined in the table.

Values within the TAG/VALUE syslog must not contain spaces, unless the value is contained within double-quotes ("), such as msg="NETWK: TCP Connection With Missed Setup."

TAG Name	Description	VALUE From Example
cip	IP address of the host	192.168.10.182
prot	Protocol	TCP
atck	Filter - severity	tln-001017
TLN-	Filter	tln-
msg	Message	"NETWK: TCP Connection With Missed Setup"

CEF Example:

```
CEF:0|FireEye|MPS|5.1.0.55701|MC|malware-callback|9|src=195.2.252.157 spt=80
smac=00:0d:66:4d:fc:00 rt=May 08 2010 14:24:45 dst=128.12.95.64 dpt=0
dmac=00:18:74:1c:a1:80 cn1Label=vlan cn1=0 cn2Label=sid cn2=33331600 cs1Label=sname
cs1=Trojan.Piptea.2 msg= https://mil.fireeye.com/edp.php?sname\=Trojan.Piptea.2
cs4Label=link cs4= https://172.16.127.7/event_stream/events?event_id\=111
cs5Label=ccName cs5=195.2.252.157 cn3Label=ccPort cn3=80 proto=tcp shost=rescomp-
09-149735.Standard.EDU dvcHost=mslms dvc=172.16.127.7 externalId=111
```

The first part of the message has a common format and is not tagged. It follows the format shown below. Other fields are customized.

CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

This only an example and does not list all of the possible combinations of data that can be used to generate events and alarms.

TAG Name	Description	VALUE From Example
src	IP address of the host	195.2.252.157
Severity	Severity	9

TAG Name	Description	VALUE From Example
Name	Event Name	malware-callback
proto	Transport Protocol	tcp
cs1	Signature Name	Trojan Piptea 2

Add or modify a syslog file

Refer to for file format information.

The asterisk (*) wildcard can be used at the beginning and end of all values you enter.

1. Click **System > Settings**.
2. Select **Syslog Files** from the tree.
3. Click **Add** or select an existing Syslog File from the list and click **Modify**.
4. Check the **Processing Enabled** check box to enable this Syslog file.
5. Enter a **Name** for the Syslog File.
6. Use the table below to enter the file information.
7. Click **OK** to save the new Syslog file.
8. You need to add the IDS/IPS device if it is not already in the Topology view. See Add or modify a pingable device on page 725 for detailed instructions.

Settings

All possible fields are shown in the table. Fields on the Add or Modify dialog will vary depending on whether you chose CSV or TAG/VALUE format.

Field	Definition
Name	The name of the syslog file. This is a unique name for this syslog definition. This value is required.
Processing Enabled	Enables/disables processing of this type of inbound syslog messages.
Event Label	The label for the Event or Alarm that will be generated by FortiNAC. This value is required.

Field	Definition
Format	Supported message formats include: **CSV** — Message is a series of data fields typically separated by commas. Comma separated value. Other characters can be used to separate data fields. **TAG/VALUE** — Message is series of fields each with a tag and a value. For example, the message could contain the following : cip=192.168.10.182. cip is the tag indicating that this is the IP address of the user causing the problem. 192.168.10.1182 is the value associated with that tag. **CEF** — Message is a series of fields, some in a standard position, others with a tag and a value. For example the message could contain the following: src=192.168.10.182. src is the tag indicating that this is the IP address of the user causing the problem. 192.168.10.182 is the value associated with that tag.
IP Tag IP Column	Name of the field or number of the column containing the source IP address. This value is required.
Filter Tag Filter Column	Name of the field or number of the column containing the filter. This value is required. If left blank, there will be no matches and no syslog data is sent to FortiNAC.
Filter Values	The values contained in the filter column or field. Only entries that contain matching data will be used. This value is required. If left blank, everything is a match.
Severity Tag/Column	Name of the field or number of the column containing the severity. This value is required.
Severity Values	Entries containing one of these matching values in the severity field or column cause a Low, Medium or High Severity event to be generated. For CSV format, separate values with commas if entering more than one possible value.
Event Tag Event Column	The names of the fields or numbers of the columns used when populating items from the syslog entry into the Event Format.
Entire Syslog	Click this button to insert the entire raw syslog message in the event. The button inserts **%syslog%** as an event column in the location where you want the syslog message to appear in the event.
Event Format	Message that is displayed when the event is generated. The text is generated from the items listed in the Event Tag parameter in the order they appear.

Delete a syslog file

1. Click **System > Settings**.
2. Expand the **System Communication** folder.
3. Select **Syslog Files** from the tree.
4. Select the file to delete and click the **Delete** button.
5. The program asks if you are sure. Click **Yes** to continue.

Examples of syslog messages

Here are some examples of syslog messages that are returned from FortiNAC. In these examples, the Syslog server is configured as follows:

- Type: Syslog
- IP address: a.b.c.d
- Port: 514
- Facility: Authorization

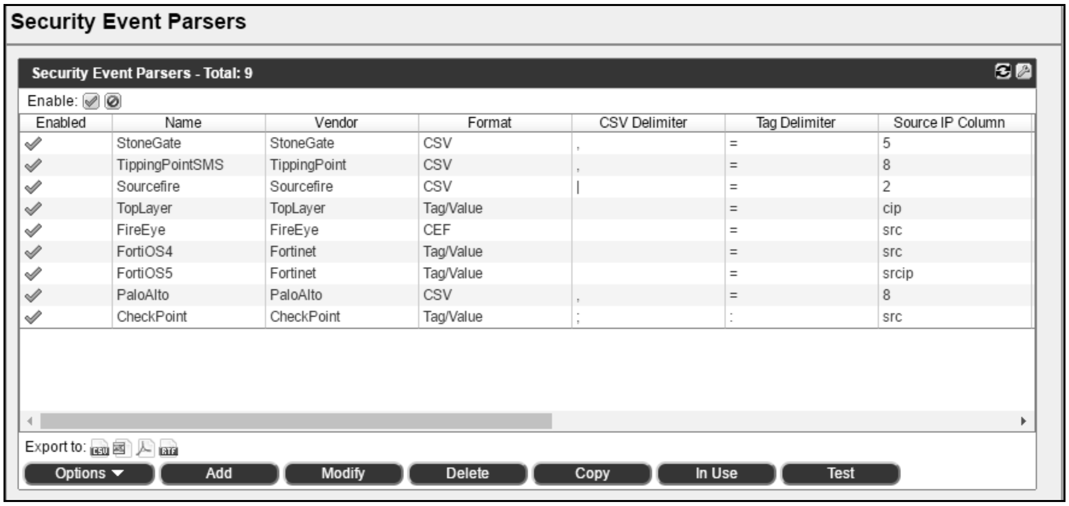
Event	Description	Syslog Message
Login Success	This is the event that is logged with a user logs into the Admin UI.	02-28-2014 08:16:04 Auth.Notice 192.168.34.31 Feb 27 22:16:14 : 2014/02/27 22:16:14 EST,1,545570,Login Success,0,12,,,,,User root logged in.
Map IP To MAC Failure	This is a legacy event logged when a scheduled task runs (these are no longer used for IP-MAC) and the ARP is not read.	--
Probe - Map IP To MAC Failure	This is the event when we fail to poll and L3 device for IP->MAC (reading Arp Cache) L3 Polling	02-28-2014 09:00:14 Auth.Notice 192.168.34.31 Feb 27 23:00:24 : 2014/02/27 23:00:24 EST,1,545702,Probe - MAP IP To MAC Failure,0,28,,Switch,192.168.34.1,,Failed to read IP address mappings from device Switch.
User Logged Out	This is the event that is logs when a user logs out of the Admin UI.	02-28-2014 08:48:55 Auth.Notice 192.168.34.31 Feb 27 22:49:04 : 2014/02/27 22:49:04 EST,1,545670,User Logged Out,0,12,,,,,User root Logged Out.
User Logged off Host	This event is logged when a user logs off a host	02-28-2014 08:44:25 Auth.Notice 192.168.34.31 Feb 27 22:44:34 : 2014/02/27 22:44:34 EST,1,545655,User Logged off Host,0,4155,,,,,"User Man, Bat logged off session 1 on host BRADSUPP7-LT

Event	Description	Syslog Message
User Logged onto Host	This event is logged when a user logs onto a host	02-28-2014 08:37:58 Auth.Notice 192.168.34.31 Feb 27 22:38:07 : 2014/02/27 22:38:07 EST,1,545633,User Logged onto Host,0,4155,,,,,"User Man, Bat logged onto session 1 on host BRADSUPP7-LT"
User Remotely Connected to Host	An event that is logged when a user remotely connected to a terminal session on a host using the PA	--
User Locked Session	This event is logged when a user locks his workstation	02-28-2014 08:49:53 Auth.Notice 192.168.34.31 Feb 27 22:50:03 : 2014/02/27 22:50:03 EST,1,545681,User Locked Session,0,4155,,,,,"User Man, Bat locked session 2 on host BRADSUPP7-LT"
User Unlocked Session	This event is logged when a user unlocks his workstation	02-28-2014 08:52:07 Auth.Notice 192.168.34.31 Feb 27 22:52:16 : 2014/02/27 22:52:16 EST,1,545691,User Unlocked Session,0,4155,,,,,"User Man, Bat unlocked session 2 on host BRADSUPP7-LT"

Security event parsers

The Security Event Parser allows you to customize parsing of syslog messages for generating security events. When a syslog message is received from a device, the message is parsed using the format specified in the security event parser. You can also define severity level mappings between the vendor and FortiNAC.

In Topology, you will see enabled security event parsers listed as options when configuring a pingable device to parse incoming security events. See Add or modify a pingable device on page 725.



Security Event Parsers

Security Event Parsers - Total: 9

Enable: ✓ ⊘

Enabled	Name	Vendor	Format	CSV Delimiter	Tag Delimiter	Source IP Column
✓	StoneGate	StoneGate	CSV	,	=	5
✓	TippingPointSMS	TippingPoint	CSV	,	=	8
✓	Sourcefire	Sourcefire	CSV	|	=	2
✓	TopLayer	TopLayer	Tag/Value		=	cip
✓	FireEye	FireEye	CEF		=	src
✓	FortiOS4	Fortinet	Tag/Value		=	src
✓	FortiOS5	Fortinet	Tag/Value		=	srcip
✓	PaloAlto	PaloAlto	CSV	,	=	8
✓	CheckPoint	CheckPoint	Tag/Value	;	:	src

To access the Security Event Parsers View, select **System > Settings > System Communication > Security Event Parsers**.

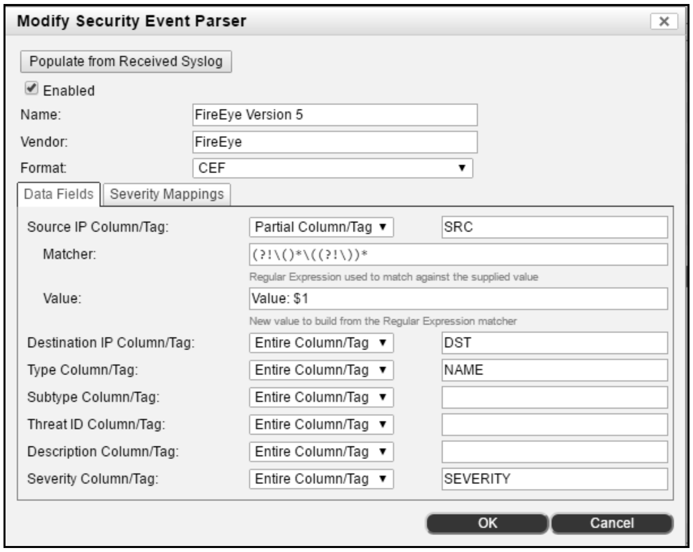
Settings

Field	Definition
Table columns	
Name	The name of the security event parser.
Enabled	A green check mark indicates that the security event parser is enabled. A red circle indicates that the security event parser is disabled. When enabled, the security event parser is available in Topology. When disabled, the security event parser is not available.
Vendor	The name of the vendor of the device that generated the event.
Format	Message format for the security event parser. Supported formats include: **CSV** — Message is a series of data fields typically separated by commas. Comma separated value. Other characters can be used to separate data fields. **TAG/VALUE** — Message is a series of fields each with a tag and a value. For example, the message could contain the following : cip=192.168.10.182. cip is the tag indicating that this is the IP address of the user causing the problem. 192.168.10.182 is the value associated with that tag. **CEF** — Message is a series of fields, some in a standard position, others with a tag and a value. For example the message could contain the following: src=192.168.10.182. src is the tag indicating that this is the IP address of the user causing the problem. 192.168.10.182 is the value associated with that tag.
CSV Delimiter	Character used to separate the fields in the security event parser. Most common options include: space, comma (,) and pipe (|). This field is not available for the TAG/VALUE format.
Tag Delimiter	Character used to separate field name and value in the security event parser. This field is not available for the CSV format. A space is used as the delimiter.
Source/IP Column	The name of the field or number of the column containing the source IP address.
Destination IP Column	The IP address of the host or device the source host was communicating with.
Type Column	The type of security event received.
Subtype Column	The subtype of the security event.
Threat ID Column	A unique identifying code supplied by the vendor for the specific type of threat or event that occurred.
Description Column	A description supplied by the security appliance of the event.
Severity Column	Name of the field or number of the column containing the severity.
Right click options	
Modify	Opens the Modify Security Event Parser window for the selected parser.
Delete	Deletes the selected security event parser.

Field	Definition
Copy	Click to copy information from the selected security parser to create a new security parser.
In Use	Shows which devices in Topology are currently using the security event parser.
Test	Allows you to test the security event parser by entering a syslog message received from a device.
Enable	Enables the security event parser.
Disable	Disables the security event parser.
Buttons	
Add	Opens the Add Security Event Parser window.
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. Low, Medium and High severity levels are not included in the exported data. See Export data on page 710.

Add or modify a security event parser

The Security Event Parser allows you to customize parsing of syslog messages for generating security events.



Modify Security Event Parser

☑ Enabled

Name: FireEye Version 5

Vendor: FireEye

Format: CEF

Source IP Column/Tag: Partial Column/Tag SRC

Matcher: (?!\()*\((?!\))*

Regular Expression used to match against the supplied value

Value: Value: $1

New value to build from the Regular Expression matcher

Destination IP Column/Tag: Entire Column/Tag DST

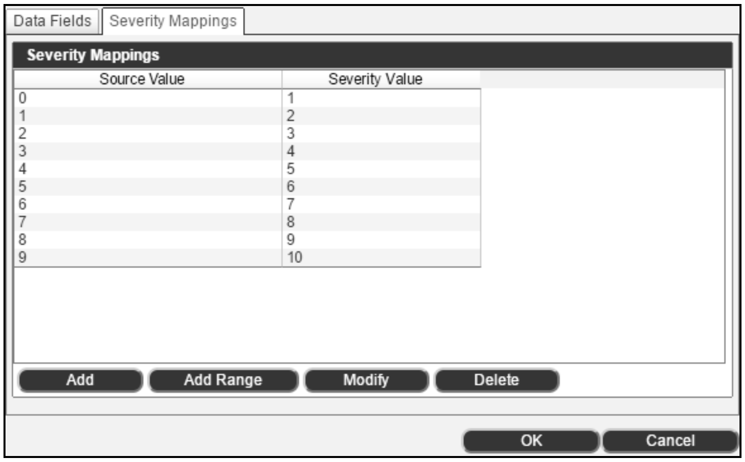
Type Column/Tag: Entire Column/Tag NAME

Subtype Column/Tag: Entire Column/Tag

Threat ID Column/Tag: Entire Column/Tag

Description Column/Tag: Entire Column/Tag

Severity Column/Tag: Entire Column/Tag SEVERITY



Source Value	Severity Value
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8
8	9
9	10

1. Click **System > Settings**.
2. In Flat View, select **Security Event Parsers** from the tree.
3. Select the **Enabled** check box to enable the security event parser.
4. Enter a **Name** for the security event parser.
5. (Optional) To build the security parser using a received syslog message, click **Populate from Received Syslog**.
6. Use the table below to enter the file information.

Settings

Field	Definition
Populate from Received Syslog	Allows you to select a current syslog message to build the security event parser. You must select the format of the selected syslog file from the Format drop-down list.
Enabled	Enables the security parser to be available as an option when configuring a pingable device to parse incoming security events
Name	Enter the name of the security event parser.
Vendor	Enter the name of the vendor of the device that will generated the event.
Format	Select the message format for the security event parser. Supported formats include: **CSV** — Message is a series of data fields typically separated by commas. Comma separated value. Other characters can be used to separate data fields. **TAG/VALUE** — Message is a series of fields each with a tag and a value. For example, the message could contain the following : cip=192.168.10.182. cip is the tag indicating that this is the IP address of the user causing the problem. 192.168.10.182 is the value associated with that tag. **CEF** — Message is a series of fields, some in a standard position, others with a tag and a value. For example the message could contain the following:

Field	Definition
	src=192.168.10.182. src is the tag indicating that this is the IP address of the user causing the problem. 192.168.10.182 is the value associated with that tag.
Data fields	
Entire Column/Tag	When you select Entire Column/Tag in the Data Fields drop-down list, enter the name of the field or number of the column containing the value. The entire value will be used to create the security event.
Partial Column/Tag	When you select Partial Column/Tag in the Data Fields drop-down list, you can build a regular expression that lets you to define which parts of the column to use when creating the security event. Refer to websites such as http://www.regular-expressions.info/ and https://www.debuggex.com/ for additional information about building regular expressions.
Source/IP Column	Enter the name of the field or number of the column containing the source IP address. The entire value will be used to create the security event.
Destination IP Column	Enter the IP address of the host or device the source host was communicating with.
Type Column	Enter the type of security event received.
Subtype Column	Enter the subtype of the security event.
Threat ID Column	Enter the unique identifying code supplied by the vendor for the specific type of threat or event that occurred.
Description Column	Enter the description supplied by the security appliance of the event.
Severity Column	Enter the name of the field or number of the column containing the severity.
Severity mappings	
Source Value	The severity value provided by the vendor.
Severity Value	The severity value in FortiNAC to be mapped to the source value.
Add	Click to add a severity level mapping.
Add Range	Click to map a single severity value in FortiNAC to a range of values provided by the source.
Modify	Click to modify a severity mapping.
Delete	Click to delete a severity mapping.

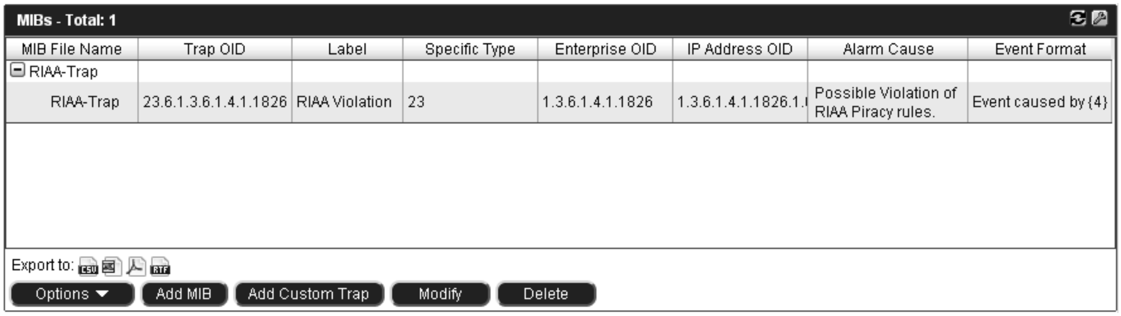
Trap MIB files

The Trap MIB Files view allows you to enter a configuration to interpret SNMP trap MIB information sent from a device and associate it with events and alarms in FortiNAC.

Requirements

- FortiNAC can only receive traps through SNMPv1 and SNMPv2 communications.
- To receive and interpret traps from devices or applications on your network, those devices or applications must be modeled in FortiNAC and have an associated IP address.
- The device or application must have traps configured to be sent to the IP address of the FortiNAC server or Control Server.
- Map events to Alarms. When a trap is received, FortiNAC compares the trap to the information listed in the Trap MIB Files and searches for a match. If a match is found, an event is generated. If corresponding alarms have been mapped to the event, alarms are also triggered.
- Multiple traps can be added to a single Trap MIB.

It is recommended that you generate and capture a trap from the sending device to make sure that you are entering the correct information when configuring the Trap MIB files.



MIBs - Total: 1

MIB File Name	Trap OID	Label	Specific Type	Enterprise OID	IP Address OID	Alarm Cause	Event Format
⊟ RIAA-Trap							
RIAA-Trap	23.6.1.3.6.1.4.1.1826	RIAA Violation	23	1.3.6.1.4.1.1826	1.3.6.1.4.1.1826.1.(	Possible Violation of RIAA Piracy rules.	Event caused by {4}

Settings

IP address OID, MAC Address OID and User ID OID are not all required. Any one OID can be used to identify the host or user that triggered the trap.

Field	Definition
MIB File Name	Name of the MIB file. FortiNAC creates the file when the Custom Trap data is entered. Any MIB file can have multiple custom traps.
Trap OID	The Trap OID compiled by FortiNAC based on the data entered in the Custom Trap section. More than one Custom Trap can be associated with a single Trap MIB file.
Label	Label used to identify the trap in the event and alarm configuration.
Specific Type	This a number that is specific to the sending device. For example, if you are looking for a trap from a Cisco device, you would enter a number that corresponds to Cisco specific traps.

Field	Definition
Enterprise OID	OID associated with the enterprise or manufacturer of the device sending the trap. For example, if FortiNAC were watching for traps from a Cisco device the enterprise OID would be 1.3.6.1.4.1.9.
IP address OID	OID associated with the trap varbinds that contain the IP address of the host that is triggering the trap.
MAC Address OID	OID associated with the trap varbinds that contain the Physical Address of the host that is triggering the trap.
User ID OID	OID associated with the trap varbinds that contain the User ID of the user logged onto the host that is triggering the trap.
Alarm Cause	Textual description of the probable cause of the alarm.
Event Format (Java Message API)	Textual description of the event which includes a variable for the varbind information to be displayed from the trap. For example, if you have entered "Event caused by {4}." Whatever data is contained in the fifth varbind in the trap, is included in the message. The number 4 represents the fifth varbind because the count begins with 0.
Buttons	
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.
Add MIB	Opens the Add MIB dialog and allows you to add both the MIB and the associated custom trap.
Add Custom Trap	Select a MIB in the Trap MIBs list and use this option to add another custom trap to the MIB. Opens the Add MIB dialog with the name of the selected MIB completed and blank custom trap fields.
Modify	If the MIB is selected, allows you to modify the name. If the custom trap is selected, allows you to modify the trap information.

Configure MIB files and custom traps

1. Click **System > Settings**.
2. Expand the **System Communication** folder.
3. Select Trap MIB Files from the tree.
4. Click **Add MIB** or select a MIB and click **Add Custom Trap**.
5. Enter the trap information using the settings shown in the table.
6. Click **OK** to save.

Vulnerability scanner

The Vulnerability Scanner integration enables FortiNAC to request and process scan results from a Vulnerability Scanner.

The Vulnerability Scanners view displays a list of scanners that are configured, allows you to add, modify, delete, and test a scanner connection, and configure polling for scanner results.

To access the Vulnerability Scanners View, go to System > Settings. From the folder view of the display, click the System Communications node, and then click Vulnerability Scanners.

Implementation

To integrate FortiNAC and a Vulnerability scanner, perform the following steps:

- Configure the scan(s) on your Vulnerability scanner.
- For Qualys integrations: Qualys Cloud Platform cannot scan hosts on an internal network, so you must configure an in-network scanner to scan hosts. Instructions for configuring the in-network scanner can be found on the Qualys website: https://www.qualys.com/docs/qualys-virtual-scanner-appliance-user-guide.pdf
- Set up and test the connection between FortiNAC and the Vulnerability scanner. Set the interval for FortiNAC to poll the scanner for new results. Select the Vulnerability scan(s) forFortiNAC to request and process information. Define each scan's threshold for triggering a scan failure.
- For visibility, add the Vulnerability Scan Status and Last Vulnerability Scan columns in the Host view by selecting them in the Settings dialog.
- For enforcement, configure the alarm actions and the Vulnerability Scanner portal page. To configure alarm actions, To customize the Vulnerability Scan information displayed on the Remediation Portal page, edit the content in the Global > Failure Information page in the Portal Content Editor.
- If specific hosts always require network access, regardless of scan results, you can add the hosts to the Vulnerability Scanner Exceptions group. Hosts in this group are allowed onto the network, even if they fail a Vulnerability Scan. See Add hosts to groups on page 811

Processing scan results

At each Vulnerability poll, FortiNAC retrieves and processes the results for each configured scan that has completed since the previous poll of the scanner. Multiple scans can target a host. If any host's scan result exceeds the scan's failure threshold configured in FortiNAC, the host will be identified as failing scan.

In the Host View, the Vulnerability Scan Status column indicates the host's current health status. The Last Vulnerability Scan column, which displays the most recent time/date when scan results were processed for the host, is also displayed. See Host view on page 793.

The Vulnerability Scan filters in the Custom Filters of the Host/Adapter Users views allow you to display hosts by Failed Scan, Passed Scan, or Not Scanned status. You can also display hosts that were scanned before, during, or after a specified time period. To configure the Vulnerability Scan filters for a host, see Settings on page 795.

The Show Events option of a host filters events from the Events Log for the selected host. When results exceed the failure threshold, a Vulnerability Scan Failed event is generated. When the host's scan results do not exceed the failure threshold, a Vulnerability Scan Passed event is generated. The date and time displayed in the message for a Vulnerability Scan Failed or Vulnerability Scan Passed event indicates when the Vulnerability scanner scanned the host. See Events view on page 867.

The following table lists the events that may be generated when the scan results are processed.

Events generated when FortiNAC processes scan results for hosts	
Vulnerability Scan Failed	The host failed the Vulnerability scan.

Vulnerability Scan Passed	The host passed the Vulnerability Scan.
Vulnerability Scan Started	The Vulnerability rescan has started.
Vulnerability Scan Finished	The Vulnerability rescan has finished.
Events generated for interaction between FortiNAC and the vulnerability scanner	
Vulnerability Scan Ignored	Scan results from the vendor include hosts that were added to the Vulnerability Exceptions Group, indicating which hosts were ignored. Hosts in this group are allowed onto the network, regardless of scan results.
Vulnerability Scan Incomplete	FortiNAC polls the vendor for scan results for a configured scan, but scan results are unavailable because the scan was not run by the vendor.
Vulnerability Scan Request Refused (Qualys Integration only)	The IP address targeted by a rescan is not included in the list of Qualysasset IPs.
Vulnerability Scan Removed	A Vulnerability scan that was added to FortiNAC was removed from the Vulnerability Scanner.
Vulnerability Scan Skipped	The Vulnerability scanner has not run the scan since FortiNAC previously polled it, so FortiNAC skipped the scan during processing.
Vulnerability Scanner Concurrent API Limit Exceeded (Qualys Integration only)	Exceeded the limit that is set for the number of requests that can be processed concurrently.
Vulnerability Scanner Connection Failure	The connection to the Vulnerability Scanner has failed.
Vulnerability Scanner Deleted	A Vulnerability Scanner was deleted from FortiNAC.
Vulnerability Scanner Periodic API Limit Exceeded (Qualys Integration only)	Qualys rejected an API request because the periodic API limit has been exceeded. The event message includes the number of seconds until the scanner will accept an API request.

These events can be enabled or disabled. For more information, see Enable and disable events on page 857.

Vulnerability scan results enforcement

In order to force hosts which have failed Vulnerability scans to remediate, use an Admin Scan mapped to the Vulnerability Scan Failed and the Vulnerability Scan Passed events, with Host Security actions of "At Risk" and "Safe", respectively. See Add a scan on page 481.

When the host fails the scan

In order to isolate hosts that have failed the Vulnerability Scan, configure an event to Alarm Mapping for the the "Vulnerability Scan Failed" event.

1. Create a Host Security Action, and add the **Mark Host At Risk** activity for the **Admin Scan**.
2. Map the Vulnerability Scan Failed event to the Security Action. Select **Host Security Action**, choose **At Risk**, and then select the **Admin Scan**. See Add or modify alarm mapping on page 892.
3. To customize the Vulnerability Scan information displayed on the Remediation Portal page, edit the content in the **Global > Failure Information** page in the Portal Content Editor.

When the host passes the scan

To move the host to production when the host passes the Vulnerability Scan, configure an Event to Alarm Mapping for the "Vulnerability Scan Passed" event, with a Host Security Action of "Safe" for the Admin Scan.

1. Create a Host Security Action, and add the **Mark Host Safe** activity for the **Admin Scan**.
2. Map the Vulnerability Scan Passed Event to the Security Action. Select **Host Security Action**, choose **Safe**, and then select the **Admin Scan**. See Add or modify alarm mapping on page 892.

Exceptions

Hosts that are added to the Vulnerability Scanner Exceptions Group are allowed onto the network even if the Vulnerability Scan fails. Failed Vulnerability Scans for hosts in this group will not be listed in the Remediation Portal page, and this page will not appear if a host in this group fails a Vulnerability Scan, but passes all other scans. For hosts in the Vulnerability Scanner Exceptions Group, the Vulnerability Scan Status column will always display "Passed" in the Host View.

Remediation

If the host fails a Vulnerability Scan, the Remediation Portal page will show details for the Vulnerability Scan that failed. Users can click the scan to see details of the failed scan provided by the Vulnerability Scanner, and solutions to fix the vulnerability. After remediation, users click the Rescan button to rescan the host. If a host fails for multiple Vulnerability Scans when FortiNAC performs a "Poll Now" of the Vulnerability Scanner, if you are enforcing access and using an Admin Scan with a Host Security Action to mark the host "at risk", each scan failure and rescan m be performed separately because each scan failure triggers an event/alarm that is unique to one scan.

Settings

Field	Definition
Name	The name of the scanner to be displayed in FortiNAC.
Request URL	The URL for retrieving scan results from the Vulnerability Scanner (typically in the format of https://<IP>:####).
User Name	The username for retrieving scan results from the Vulnerability Scanner.
Vendor	The vendor of the Vulnerability Scanner.
Poll Interval	The interval for how often FortiNAC retrieves scan results from the Vulnerability scanner.
Last Successful Poll	The last time FortiNAC successfully retrieved scan results from the Vulnerability scanner.
Last Modified By	The user who last modified the Occurs when a Vulnerability scanner was deleted from FortiNACVulnerability scanner configuration.
Last Modified Date	The date when the FortiNAC Vulnerability scanner configuration, as defined in FortiNAC, was last modified.
Right click options	

Field	Definition
Modify	Modifies the selected Vulnerability Scanner configuration.
Delete	Deletes the selected Vulnerability Scanner.
Test Connection	Tests the connection between FortiNAC and the Vulnerability Scanner.
Poll Now	Immediately polls selected Vulnerability Scanner for new scan results, instead of waiting for the poll interval.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.

Add or modify a vulnerability scanner

When you add or modify a vulnerability scanner, you are configuring the connection to the FortiNAC Vulnerability scanner.

1. Select **System > Settings**.
2. Expand the **System Communication** folder.
3. Select **Vulnerability Scanners**.
4. Click **Add** or select an existing scanner from the list and click **Modify**.
5. Use the table below to enter the Vulnerability Scanner information in the General Tab.

Field	Definition
Vendor	The vendor of the Vulnerability scanner.
Name	Enter a name for the scanner to be used in FortiNAC.
Request URL	The URL for retrieving scan results from the Vulnerability Scanner.
User Name	Enter the username for retrieving scan results.
Password	Enter the password for retrieving scan results.
Poll for Scan Results Every	Defines how often FortiNAC retrieves results from the Vulnerability Scanner.
Test Connection	Click to test the connection between FortiNAC and the Vulnerability Scanner.

6. Click the **Scans** tab.
7. Select the scan(s) in the Available Scans list and click the down arrow to add the scan(s) from the list of available scans on the Vulnerability Scanner to the selected scans list which FortiNAC will process. Click the double arrow to add all scans to the Selected Scans list. FortiNAC will only process results for scans in the Selected Scans list.
8. Select a scan in the Selected Scans list, and then click **Set Failure Thresholds**.
9. Select the check box next to each category where you wish to enter a threshold value.
10. Enter the minimum number of vulnerabilities for each category that may occur in the scan results before the host is

identified as failing the scan. For example, entering "5" in the "Medium" category means that if five or more Medium vulnerabilities are detected when the host is polled, the host will be marked as Failed for that scan.

Categories are vendor-specific.

11. Click **OK**.
12. To remove a scan from the Selected Scans list, click the scan and then click Delete. The scan is returned to the Available Scans list.

Qualys Scanner Integration

Qualys requires an in-network scanner host for scans. When Qualys is selected as the vendor, the Appliance tab appears where you must specify the host that will perform the scan.

Instructions for configuring the in-network scanner host can be found on the Qualys website: https://www.qualys.com/docs/qualys-virtual-scanner-appliance-user-guide.pdf

1. Select the Scanner Appliance.
2. Click **OK**.

Delete a vulnerability scanner

1. Select **System > Settings**.
2. Expand the **System Communication** folder.
3. Select **Vulnerability Scanners**.
4. Select the Vulnerability Scanner(s) you wish to delete, and click the **Delete** button.
5. A confirmation message is displayed. Click **Yes** to continue.

System management

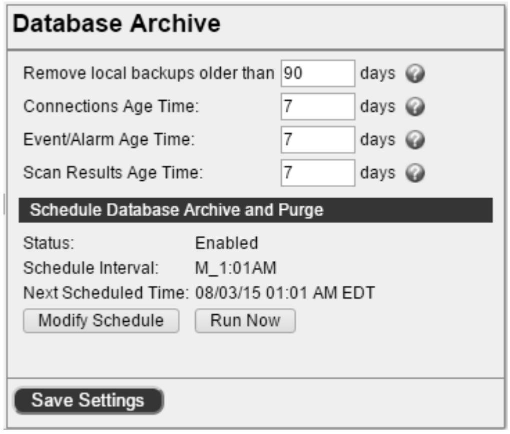
System Management groups together core server features such as data backup and restore, redundant servers, licensing and time zone settings. Options include:

Option	Definition
Database Archive	Set the age time for archived data files and configure the schedule for the Archive and Purge task. See Database archive on page 210.
Database Backup/Restore	Schedule database backups, configure how many days to store local backups, and restore a database backup. Note that this restores backups on the FortiNAC server, not backups on a remote server. See Backup/restore a database on page 213.

Option	Definition
High Availability	Configuration for Primary and Secondary appliances for High Availability. Saving changes to these settings restarts both the Primary and Secondary servers. See High availability on page 217.
License Management	View or modify the license key for this server or an associated Application server. See License management on page 215.
NTP and Time Zone	Reset the time zone and NTP server for your FortiNAC appliances. Typically the time zone and NTP server are configured using the Configuration Wizard during the initial appliance set up. Requires a server restart to take effect. See The NTP server is used to synchronize the clock on the FortiNAC appliance. FortiNAC contacts the NTP server periodically to synchronize its clock with the NTP servers. NTP server keeps time in UTC or Coordinated Universal Time, which corresponds roughly to Greenwich Mean time. on page 216.
Power Management	Reboot or power off the FortiNAC server. In the case of a FortiNAC Control Server / Application Server pair, reboot or power off each server individually. See Power management on page 219.
Remote Backup Configuration	Configure Scheduled Backups to use a remote server via FTP and/or SSH. See Backup to a remote server on page 220.
System Backups	Create a backup of all system files that are used to configure FortiNAC. See System backups on page 223.

Database archive

Use Database Archive to set age times for selected log files. Log files are archived and then purged from the FortiNAC database when the age time elapses. Archived data can be imported back into the database if necessary. Importing archived data does not overwrite existing data it adds the archived records back into the database. See Import archived data on page 696.



Database Archive

Remove local backups older than 90 days

Connections Age Time: 7 days

Event/Alarm Age Time: 7 days

Scan Results Age Time: 7 days

Schedule Database Archive and Purge

Status: Enabled

Schedule Interval: M_1:01AM

Next Scheduled Time: 08/03/15 01:01 AM EDT

Settings

Field	Definition
Remove local backups older than	Number of days for which you would like to keep backups. Anything older than the number of days entered, is removed the next time the scheduled task for backups runs. This setting removes backup files created on the FortiNAC server before they are copied to the remote server. Backups on the remote server are not removed. The timing of the scheduled backup task and the age of the files that are to be removed must be thought out carefully or you will remove all of your backups. For example, if the remove option is set to 5 days and your backup task runs every 15 days, you may inadvertently remove all of your backups. However, if the remove option is set to 15 days and the backup task runs every 5 days, then you would always have backup files.
Connections Age Time (days)	Number of days Connections data are maintained in the Connections log and viewable in the Connections view. Connections are archived and purged based on the scheduled task settings. Default setting = 7 days If the number of records exceeds 500,000 prior to the scheduled time, a portion of the records are archived and purged. The remaining records are archived and purged at the scheduled time.
Event/Alarms Age Time (days)	Number of days events or alarms are maintained in the Events or Alarms logs and viewable in the Events or Alarms View. Events and Alarms are archived and purged based on the scheduled task settings. Default setting = 7 days
Scan Results Age Time (days)	Number of days Scan results are maintained in the Scan results log and viewable in the Scan results view. Scan results are archived and purged based on the scheduled task settings. Default setting = 7 days

Edit archive age time

1. Click **System > Settings**.
2. Expand the **System Management** folder.
3. Select **Database Archive** from the tree.
4. Use the information in the table above to set **Age Time**.
5. Click **Save Settings**.

Schedule event archive and purge

1. Click **System > Settings**.
2. Expand the **System Management** folder.
3. Select **Database Archive** from the tree.
4. Click **Modify Schedule**.
5. Select the **Enabled** check box.
6. Enter a name for the task in the **Name** field.
7. The **Description** field is optional. Enter a description of the task.
8. Action type and Action are pre-configured based on the task and cannot be modified.
9. From the **Schedule Type** drop down list, select either **Fixed Day** or **Repetitive** and set the day and time that the task is to be performed.
10. A **Fixed Day Task** is one in which you schedule a task to run on a combination of days of the week and times of the day, such as Mondays at 1:00 pm and Fridays at 10:00 am. Select the day(s) and time to run the task.
    a. Click the box next to the day(s) to select the day.
    b. Click the down arrows and select the hour, minutes, and AM or PM from the drop-down list for each day.
    c. To enter days/times more quickly, use the **Set Multiple Days** button to set multiple days with the same time.
    d. To remove all settings click the **Clear All** button.
11. A **Repetitive Task** is one that you schedule to start on a given day, at a certain time, for the number of times you specify, such as every 10 days starting today. The repetition rate can be set to any number of minutes, hours, or days.
    a. Enter the **Repetition Rate** using whole numbers.

    A repetition rate of zero causes the task to run only once.

    b. Click the down arrow and select Minutes, Hours, or Days from the drop-down list.
    c. Enter the date and time for the task to run in the **Next Scheduled Time** field using the format MM/DD/YY hh:mm AM/PM Time Zone.

    The new Repetition Rate does not take effect immediately. It starts the next time the scheduled task runs. For the new Repetition Rate take effect immediately, click the **Update** button.

    d. Click **Update** to update the **Next Scheduled Time** field or change the **Repetition Rate**.
12. Click **OK**.

Schedule settings

Field	Definition
Remove local backups older than	Number of days for which you would like to keep backups. Anything older than the number of days entered, is removed the next time the scheduled task for backups runs. This setting removes backup files created on the FortiNAC server before they are copied to the remote server. Backups on the remote server are not removed. The timing of the scheduled backup task and the age of the files that are to be removed must be thought out carefully or you will remove all of your backups. For example, if the remove option is set to 5 days and your backup task runs every 15 days, you may inadvertently remove all of your backups. However, if the remove option is set to 15 days and the backup task runs every 5 days, then you would always have backup files.
Status	Indicates whether the task is Enabled or Disabled.
Schedule Interval	How often the scheduled task runs. Options are Minutes, Hours, or Days.
Next Scheduled Time	The next date and time the scheduled synchronization task will run. Entered in the format MM/DD/YY HH:MM AM/PM
Modify Schedule	Allows you to modify the scheduled activity.
Run Now	Runs the scheduled task immediately.

Backup/restore a database

A database backup creates a backup of the entire database. All database archives can be restored if the database becomes corrupted. To restrict the restoration to only alarms, connections, or events data, go to those specific views and select the Import option. See Alarms view on page 887, Connections view on page 927, and Events view on page 867 for more information.

Restoring a database archive causes the FortiNAC Server or Control Server to restart.

1. Click **System > Settings**.
2. Expand the **System Management** folder.
3. Select **Database Backup/Restore** from the tree.

Schedule a database backup

1. Under **Schedule Database Backup**, click **Modify Schedule**.
2. Select the **Enabled** check box.
3. Enter a name for the task in the **Name** field.
4. The **Description** field is optional. Enter a description of the task.
5. Action type and Action are pre-configured based on the task and cannot be modified.
6. From the **Schedule Type** drop down list, select either **Fixed Day** or **Repetitive** and set the day and time that the task is to be performed.

7. A **Fixed Day Task** is one in which you schedule a task to run on a combination of days of the week and times of the day, such as Mondays at 1:00 pm and Fridays at 10:00 am. Select the day(s) and time to run the task.
   - **a.** Click the box next to the day(s) to select the day.
   - **b.** Click the down arrows and select the hour, minutes, and AM or PM from the drop-down list for each day.
   - **c.** To enter days/times more quickly, use the **Set Multiple Days** button to set multiple days with the same time.
   - **d.** To remove all settings click the **Clear All** button.
8. A **Repetitive Task** is one that you schedule to start on a given day, at a certain time, for the number of times you specify, such as every 10 days starting today. The repetition rate can be set to any number of minutes, hours, or days.
   - **a.** Enter the **Repetition Rate** using whole numbers. A repetition rate of zero causes the task to run only once.
   - **b.** Click the down arrow and select Minutes, Hours, or Days from the drop-down list.
   - **c.** Enter the date and time for the task to run in the **Next Scheduled Time** field using the format MM/DD/YY hh:mm AM/PM Time Zone.
   - **d.** Click **Update** to update the **Next Scheduled Time** field or change the **Repetition Rate**.

     The new Repetition Rate does not take effect immediately. It starts the next time the scheduled task runs. For the new Repetition Rate take effect immediately, click the **Update** button.
9. Click **OK**.

Schedule settings

Field	Definition
Remove local backups older than	Number of days for which you would like to keep backups. Anything older than the number of days entered, is removed the next time the scheduled task for backups runs. This setting removes backup files created on the FortiNAC server before they are copied to the remote server. Backups on the remote server are not removed. The timing of the scheduled backup task and the age of the files that are to be removed must be thought out carefully or you will remove all of your backups. For example, if the remove option is set to 5 days and your backup task runs every 15 days, you may inadvertently remove all of your backups. However, if the remove option is set to 15 days and the backup task runs every 5 days, then you would always have backup files.
Status	Indicates whether the task is Enabled or Disabled.
Schedule Interval	How often the scheduled task runs. Options are Minutes, Hours, or Days.
Next Scheduled Time	The next date and time the scheduled synchronization task will run. Entered in the format MM/DD/YY HH:MM AM/PM
Modify Schedule	Allows you to modify the scheduled activity.
Run Now	Runs the scheduled task immediately.

Restore a database

1. Click on a backup to select it.
2. Click **Restore Database**.

License management

Manage license keys on the servers through this view. You can view and modify both the FortiNAC Control Server and FortiNAC Application Server licenses through this view. Servers that are part of a High Availability configuration appear in the drop-down list.

License information is displayed on the Dashboard. See Dashboard on page 37 for additional information.

The events related to license use help maintain proper appliance use per environment. Warning and critical events and alarms are generated based on a set of user defined thresholds. See Event thresholds on page 858 to set thresholds. See Map events to alarms on page 888 to set alarms based on threshold events.

View/modify license information

The license options will vary depending on whether pre-2016 (Secure Enterprise Standard, Secure Enterprise Advanced, or Secure Enterprise Mobility) or post-2016 (Secure Enterprise Advanced or Secure Enterprise Premier) license packages are installed on the server.

1. Click **System > Settings**.
2. Expand the **System Management** folder.
3. Select **License Management** from the tree.
4. From the drop-down list select the server containing the license key.
5. Click **Modify License Key**.
6. You can modify the license key in two ways:
   - To upload from a text file, click **Upload**, browse to the license key file, and click **Open**. This must be a text file not a zip file.
   - From another file, copy and paste the new license key text into the text box.
7. Click **OK** to apply the new license key. The existing key detail is displayed in a pop-up window along with the new key detail.
8. Click **OK** to apply the new license key. Click **Undo** if you want to revert to the existing license key.
9. To restart the server immediately, click **OK** on the dialog box.
10. To restart the server later, click Cancel on the dialog box. Another dialog box appears stating that the new key will not be applied until the server is restarted. New features or license counts contained in the new license cannot be accessed until the server is restarted. The new license is saved on the server, but is not read until the server is restarted.
11. Click **OK** to confirm.

Settings

Key	Definition
License Name	Indicates which license installed on the server.
Concurrent Licenses	Number of licenses configured for possible online connections to the network. Connections are counted for hosts and devices that are not switches or routers.
ATR Licenses	Indicates the number of licenses configured for ATR.
Evaluation Time	Indicates the number of days configured for an evaluation license. If you have purchased a full license for the product, this field does not display.
High Availability	Indicates whether or not High Availability has been enabled.
Device Profiler	Indicates whether or not the Device Profiler feature has been enabled.
Guest Manager	Indicates whether or not the Guest Manager feature has been enabled.
Endpoint Compliance	Indicates whether or not the Security Policy features have been enabled.
Integration Suite	Indicates whether or not access to third party information such as SNMP Traps and Syslogs has been enabled.
Wireless Only	Indicates whether or not a limited Wireless Only license has been enabled. Provided as a quick start solution for organizations that use only wireless devices on their network. This feature is not supported for all wireless devices. Currently only HP MSM and Ruckus controllers can be configured. For HP wireless devices, FortiNAC can write configuration changes to the device. For Ruckus controllers, FortiNAC cannot write configuration changes to the device only the device model in the database. Other wireless devices and up to five wired devices can be added using the Network Devices View or the Topology View. In addition, this license disables the Discovery feature. .

The NTP server is used to synchronize the clock on the FortiNAC appliance. FortiNAC contacts the NTP server periodically to synchronize its clock with the NTP servers. NTP server keeps time in UTC or Coordinated Universal Time, which corresponds roughly to Greenwich Mean time.

Settings

Field	Definition
FortiNAC Servers	Provides a list of servers for which you can change time settings. If you have a Control server and an Application server pair, both servers are displayed in the list. In an HA environment this would include up to four servers, two Control servers and two Application servers. Each server's time must be set individually. Settings apply only to the server displayed in this field.
NTP Server	External server used to synchronize or update the clock on the selected FortiNAC server. Defaults to pool.ntp.org.
Time Zone	Time zone where the selected FortiNAC server resides.

Modify time settings

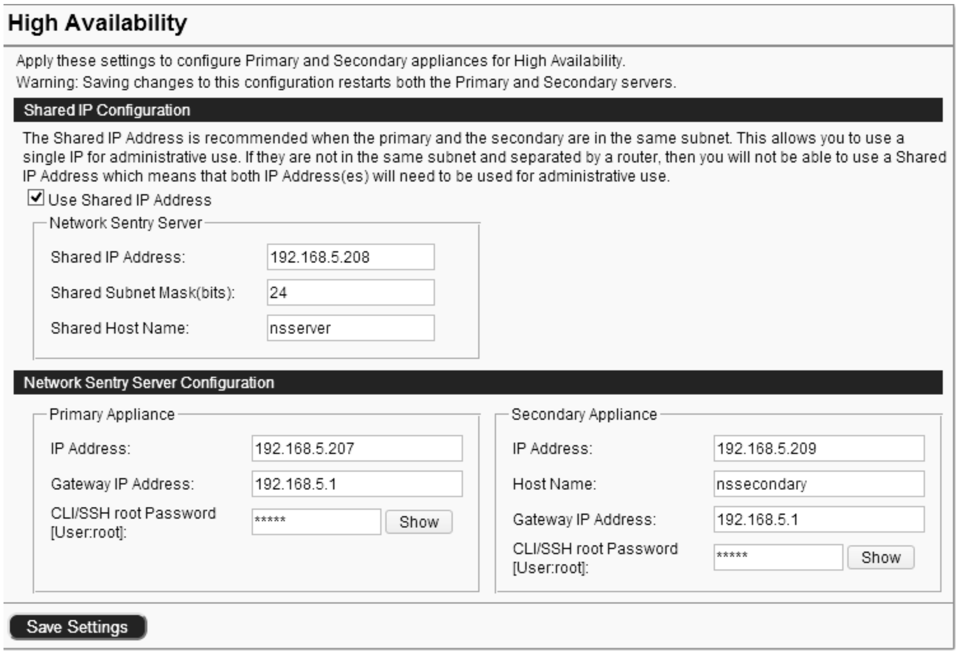
Changes to NTP or time zone require a server restart to take effect. Go to the Control Panel to restart the server now. See Power management on page 219.

1. Click **System > Settings**.
2. Expand the **System Management** folder.
3. Select **NTP And Time Zone** from the tree.
4. Click the **FortiNAC Servers** drop-down and choose the server to be modified.
5. Enter your preferred NTP Server in the **NTP Server** field.
6. Click the **Time Zone** drop-down and select the time zone for this server.
7. Click **Save Settings** to save settings for the selected server.
8. To modify another server, select it in the FortiNAC Servers drop-down and repeat steps 4 through 7.

High availability

Use the High Availability view to add to and update High Availability configuration information.

Use the Configuration Wizard to complete the initial configuration for each appliance. See the Appliance Installation Guide that came with the hardware for instructions on using the Configuration Wizard. See the for additional information on configuring appliances for a High Availability environment.



High Availability

Apply these settings to configure Primary and Secondary appliances for High Availability.
Warning: Saving changes to this configuration restarts both the Primary and Secondary servers.

Shared IP Configuration

The Shared IP Address is recommended when the primary and the secondary are in the same subnet. This allows you to use a single IP for administrative use. If they are not in the same subnet and separated by a router, then you will not be able to use a Shared IP Address which means that both IP Address(es) will need to be used for administrative use.

☑ Use Shared IP Address

Network Sentry Server

Shared IP Address:	192.168.5.208
Shared Subnet Mask(bits):	24
Shared Host Name:	nsserver

Network Sentry Server Configuration

Primary Appliance

IP Address:	192.168.5.207
Gateway IP Address:	192.168.5.1
CLI/SSH root Password [User:root]:	*****

Secondary Appliance

IP Address:	192.168.5.209
Host Name:	nssecondary
Gateway IP Address:	192.168.5.1
CLI/SSH root Password [User:root]:	*****

Configure high availability

1. Ensure that all appliances are keyed for High Availability. See View/modify license information on page 215 and check the High Availability field.

2. Click **System > Settings**.
3. Expand the **System Management** folder.
4. Select **High Availability** from the tree.
5. Use the table below to enter the required information.
6. Click **Save Settings** and wait for the success message.

When you click Save Settings on the Administration High Availability view, the primary server tries to communicate with the secondary to ensure that the database will be replicated. If the primary server cannot communicate with the secondary, it continues to try until communication is established.

If you are configuring High Availability in an environment where you have a FortiNAC Control Server and an Application Server, additional fields are displayed to configure the two Application Servers.

Settings

Field	Description
Shared IP configuration	
Use Shared IP address	Enables the use of a shared IP address in the High Availability configuration. If enabled, the administrator can manage whichever appliance that is in control with the shared IP address instead of the actual host IP address. If your primary and secondary servers are not in the same subnet, do not use a shared IP address.
Shared IP address	The shared IP address for the High Availability configuration. Added to the `/etc/hosts` file when the configuration is saved.
Shared Subnet Mask (bits)	The shared subnet mask in bits. For example, 255.255.255.0 = 24 bits.
Shared Host Name	Part of the entry in the `/etc/hosts` file for the shared IP address. Admin users can access the UI using either the Shared IP address or the shared host name.
Server configuration	
Primary Appliance	**IP address**—IP address assigned to eth0 for the primary. **Gateway IP address**—IP address pinged by the appliances to determine if network connectivity is still available. **CLI/SSH root Password [User:root]**—Root password on the appliance itself. Allows settings to be written to the appliance. **Retype root CLI/SSH Password [User:root]**—Retype the password entered in the CLI/SSH root Password field for confirmation.
Secondary Appliance	**IP address**—IP address assigned to eth0 for the secondary. **Host Name** — Name assigned to the secondary. **Gateway IP address**—IP address that is pinged by the appliances to determine if network connectivity is still available.

Field	Description
	CLI/SSH root Password [User:root]—Root password on the appliance itself. Allows settings to be written to the appliance. **Retype root CLI/SSH Password [User:root]**—Retype the password entered in the CLI/SSH root Password field for confirmation.

Unconfigure high availability

1. Click **System > Settings**.
2. Expand the **System Management** folder.
3. Select **High Availability** from the tree.
4. Clear the shared and secondary information, and leave the primary information filled in.
5. Click **Save Settings**.

Power management

The system can be rebooted or powered down through the FortiNAC interface, by any user whose Admin Profile allows access to the Settings view. In a High Availability environment or in the case where there is a FortiNAC Control Server/Application Server pair, servers must be rebooted or powered off individually.

In a HA environment, reboot or power off the secondary servers first.

Events associated with Power Management are as follows:

- **System Power Off**— Indicates that the server has been powered down and provides the user name of the user who initiated the action.
- **System Reboot**—Indicates that the system was rebooted and provides the user name of the user who initiated the action.

Reboot the server

1. Click **System > Settings**.
2. Select a server from the list.
3. Click the **Reboot** button. This process may take 2-3 minutes.

Power off the server

1. Click **System > Settings**.
2. Select a server from the list.
3. Click the **Power Off** button. This process may take 30 seconds.

Backup to a remote server

Backups of the database and other files occur automatically when the Backup Database and Purge Events scheduled tasks run. The backup files are stored on the local appliance.

The Administrator can additionally configure FortiNAC to place a copy of the database and other directories on an ftp and/or other remote server for safekeeping. The backup files are placed in time and date stamped files named DataBase_BackUp_YYYY-MM_DD_HH_mm_SS.gz.

Backup directory files

Appliance	Directories Included in Backup File	
FortiNAC Server	/etc	/bsc/VPN
	/home/cm	/bsc/WWW
	/root	/bsc/WEB-INF
	/var/spool/cron	/home/admin
	/bsc/Registration	/bsc/clientValidation
	/bsc/Remediation	/bsc/siteConfiguration
	/bsc/Hub	/bsc/services
	/bsc/Authentication	/bsc/campusMgr/master_loader/telnetMibs
	/bsc/DeadEnd	/bsc/campusMgr/master_loader/customTraps
	/bsc/CommonJspFiles	
FortiNAC Control Server	/etc	/bsc/siteConfiguration
	/root	/bsc/services
	/home/cm	/bsc/campusMgr/master_loader/telnetMibs
	/home/admin	/bsc/campusMgr/master_loader/customTraps
	/var/spool/cron	
	/bsc/clientValidation	
FortiNAC Application Server	/etc	/bsc/Authentication
	/home/cm	/bsc/DeadEnd
	/root	/bsc/CommonJspFiles
	/home/admin	/bsc/VPN
	/var/spool/cron	/bsc/www
	/bsc/Registration	/bsc/siteConfiguration
	/bsc/Remediation	/bsc/services
	/bsc/Hub	/bsc/WEB-INF

When configuring the backup for a pair of appliances (FortiNAC Control Server and FortiNAC Application Server) the remote back up is only configured on the FortiNAC Control Server appliance. The backup files from both servers will be placed in the directory specified. The host name of the appliance will be prefixed to the backup filename.

Configure the backup destination

Remote Backup Configuration defines the connection details used to copy files to a third party (remote) server when the Database Backup task is run in Scheduler. Transferring the backup files can be done using FTP and/or SSH protocols.

Remote server configuration using FTP

1. Create an account on the remote FTP server to be used by FortiNAC for backup file transfer.
2. Create a folder to which FortiNAC will copy the files.

For instructions on completing the above tasks, consult documentation specific to the FTP application used.

Remote server configuration using SSH

SSH communication must be established between the FortiNAC Control Server or FortiNAC Server and the remote backup server for the SSH remote backups to be successful. Ensure that the public key for the root user on the host being backed up has been appended to the authorized_keys file in the <root home dir>/.ssh directory of the remote server. In the case of High Availability, the SSH keys for both the primary and secondary must be appended to the authorized_keys file.

Copy the SSH key to the remote server account (Linux)

1. Access the CLI on the FortiNAC Control Server as `root`.
2. Navigate to the .ssh directory. Type: `cd /root/.ssh`.
3. Display and copy the key. Type: `cat id_rsa.pub`.
4. Access the remote server where the backups will be stored as `root`.
5. If the .ssh directory does not exist, create it. Type: `mkdir /home/backup_username/.ssh`.
6. Change the permissions. Type: `chmod 700 /home/backup_username/.ssh`.
7. Navigate to the .ssh directory, and then paste (append) the key you copied from the FortiNAC to the authorized_keys file. Type:
   ```
   cd /home/backup_username/.ssh
   vi authorized_keys
   ```

   The format of authorized_keys file is one entry per line.

8. Make sure the key you paste is identical to the key on the FortiNAC and does not include extra white space or characters.

Copy the SSH key to the remote server account (third party)

1. Access the CLI on the FortiNAC Control Server as `root`.
2. Navigate to the .ssh directory. Type: `cd /root/.ssh`.
3. Display and copy the key. Type: `cat id_rsa.pub`.
4. Associate the public key to the remote server where the backups will be stored.

This process will vary depending on the product. Refer to the SSH server product documentation for instructions.

Configure the remote backup target

1. Click **System > Settings**.

Settings

Field	Definition
Backup Timeout	Number of minutes for the backup to be created and copied to the remote server. If this time elapses before the backup is done, the process is interrupted. Be sure to select a time that is long enough for your system to complete its backup. The default is 20 minutes, however, large systems may require more time.
Enable FTP Remote Backup	Remote backups to this server are enabled when this is checked. Default = Unchecked
Display Public SSH Keys	Click to view the public SSH key from the FortiNAC Primary and Secondary Control Servers.
Server	IP address of the remote server.
User Name	User Name required for write access to the server.
Password	Password required for write access to the server.
Remote Path	The directory path where the remote backup files will be placed. This directory must exist on the server.
EnableSSH Remote Backup	Remote backups to this server are enabled when this is checked. The SSH keys must already be established for the SSH remote backups to be successful. Default = Unchecked
Server	The IP address of the remote server. Format is user@remote-server, such as asmith@192.168.1.1 .
Remote Path	The directory path where the remote backup files will be placed. This directory must exist on the server.
Test SSH Connection	Test the connection to the server using the SSH Server and SSH Remote Path settings to confirm the settings are valid. If the test fails, it means the Remote Backup task will not back up the files to the specified remote server.

Validate the connection and backup task

FTP

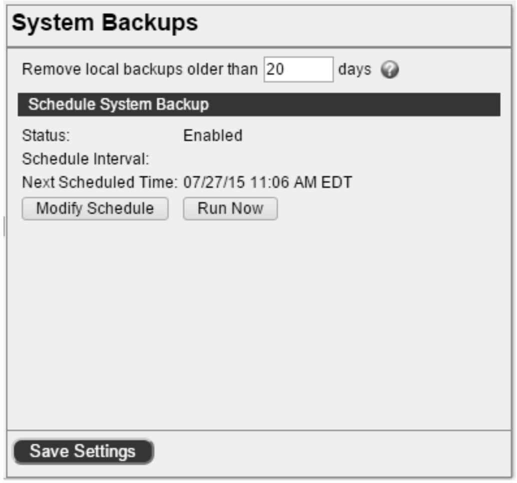
1. Navigate to **System > Scheduler**.
2. Add the **Database Backup** task (if not already present).
3. Highlight the **Database Backup** task and click **Run Now**.

SSH

1. Click the **Test SSH Connection** button to verify SSH communication with the remote server.
2. Once successfully tested, navigate to **System > Scheduler**.
3. Add the **Database Backup** task (if not already present).
4. Highlight the **Database Backup** task and click **Run Now**.

System backups

A system backup creates a backup of all system files that are used to configure FortiNAC, such as license key and web server configurations.


System Backups

Remove local backups older than 20 days

Schedule System Backup

Status: Enabled

Schedule Interval:

Next Scheduled Time: 07/27/15 11:06 AM EDT

1. Click **System > Settings**.
2. Expand the **System Management** folder.
3. Select **System Backups** from the tree.
4. In the **Remove local backups older than** field, enter the number of days for which you would like to keep backups.

The timing of the scheduled backup task and the age of the files that are to be removed must be thought out carefully or you will remove all of your backups. For example, if the remove option is set to 5 days and your backup task runs every 15 days, you may inadvertently remove all of your backups. However, if the remove option is set to 15 days and the backup task runs every 5 days, then you would always have backup files.

5. Click **Modify Schedule**.
6. Select the **Enabled** check box.

7. Enter a name for the task in the **Name** field.
8. The **Description** field is optional. Enter a description of the task.
9. **Action type** and **Action** are pre-configured based on the task and cannot be modified.
10. From the **Schedule Type** drop down list, select either **Fixed Day** or **Repetitive** and set the day and time that the task is to be performed.
11. A **Fixed Day Task** is one in which you schedule a task to run on a combination of days of the week and times of the day, such as Mondays at 1:00 pm and Fridays at 10:00 am. Select the day(s) and time to run the task.

    a. Click the box next to the day(s) to select the day.

    b. Click the down arrows and select the hour, minutes, and AM or PM from the drop-down list for each day.

    c. To enter days/times more quickly, use the **Set Multiple Days** button to set multiple days with the same time.

    d. To remove all settings click the **Clear All** button.
12. A **Repetitive Task** is one that you schedule to start on a given day, at a certain time, for the number of times you specify, such as every 10 days starting today. The repetition rate can be set to any number of minutes, hours, or days.

    a. Enter the **Repetition Rate** using whole numbers.

    A repetition rate of zero causes the task to run only once.

    b. Click the down arrow and select **Minutes**, **Hours**, or **Days** from the drop-down list.

    c. Enter the date and time for the task to run in the **Next Scheduled Time** field using the format MM/DD/YY hh:mm AM/PM Time Zone.

    The new Repetition Rate does not take effect immediately. It starts the next time the scheduled task runs. For the new Repetition Rate take effect immediately, click the **Update** button.

    d. Click Update to update the Next Scheduled Time field or change the Repetition Rate.
13. Click **OK**.
14. Click **Save Settings**.

Settings

Field	Definition
Remove local backups older than	Number of days for which you would like to keep backups. Anything older than the number of days entered, is removed the next time the scheduled task for backups runs. This setting removes backup files created on the FortiNAC server before they are copied to the remote server. Backups on the remote server are not removed. The timing of the scheduled backup task and the age of the files that are to be removed must be thought out carefully or you will remove all of your backups. For example, if the remove option is set to 5 days and your backup task runs every 15 days, you may inadvertently remove all of your backups. However, if the remove option is set to 15 days and the backup task runs every 5 days, then you would always have backup files.
Status	Indicates whether the task is Enabled or Disabled.
Schedule Interval	How often the scheduled task runs. Options are Minutes, Hours, or Days.
Next Scheduled Time	The next date and time the scheduled synchronization task will run. Entered in the format MM/DD/YY HH:MM AM/PM
Modify Schedule	Allows you to modify the scheduled activity.

Updates

Updates groups together options for updating FortiNAC servers with the latest software release and the latest Agent Packages.

Options

Option	Definition
Agent Packages	Displays a list of the Dissolvable, Persistent and Passive Agent versions available on your FortiNAC appliance. Download new agents and add them to FortiNAC as they become available from Fortinet using the Download button. Download an Administrative template for GPO configuration to your PC from the FortiNACappliance using the links at the top of the view. See Agent packages on page 226.
Operating System	Use Operating System Updates to download and install updates to the operating system on FortiNAC servers. See Updating CentOS on page 235.
System	Use System Updates to configure download settings, download updates from Fortinet, install updates and view the updates log. See System update on page 238.

Agent packages

The Agent Packages view displays a list of the Dissolvable, Persistent, Passive and Mobile Agent versions available on your FortiNAC appliance. This view allows you to download new agents and add them to FortiNAC as they become available from Fortinet.

Both the Dissolvable and Persistent Agents can be supplied to hosts automatically by FortiNAC through the captive portal when the host reaches the appropriate web page. The agent presented to the host is based on the configuration of the Endpoint Compliance Policy applied to that host. Supplying the Passive agent requires additional configuration. See Passive Agent on page 495.

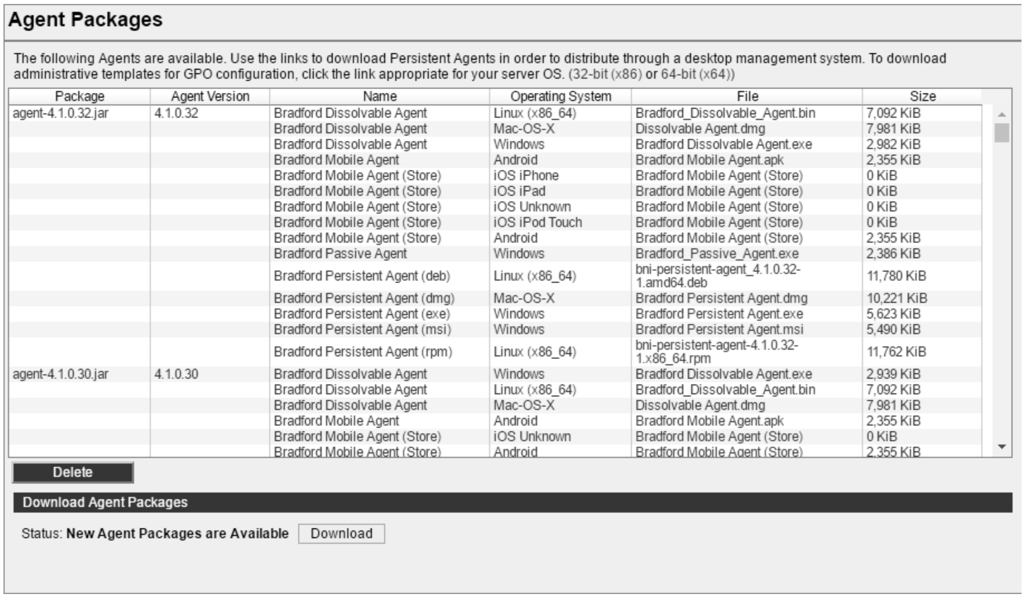
Hosts who already have a version of the Persistent Agent installed can be automatically updated to a newer version of the agent based on the settings you enter on the Agent Update tab. See Upgrade the Persistent Agent on page 518.

You also have the option to download a Persistent Agent from the list to your own computer to be distributed to hosts through your web site, using a login script or some other distribution method. Files are saved on your computer in the default download location. This location varies depending on the browser you are using.

The Windows Persistent Agent is available in two formats: .msi and .exe. The .msi file is recommended for use in a managed install by non-user-interactive means. The .exe file is recommended for user-interactive installation. The Linux Persistent Agent is also available in two formats: .deb or .rpm. The Mac OSX Persistent Agent is available in .dmg format.

If you choose to distribute the agent using Group Policy Objects, you must download and install administrative templates on your Windows server. Use the links at the top of the Agent Distribution view to download the templates.

Use the **Delete** button to remove old versions of the Agent from your server.



Agent Packages

The following Agents are available. Use the links to download Persistent Agents in order to distribute through a desktop management system. To download administrative templates for GPO configuration, click the link appropriate for your server OS. (32-bit (x86) or 64-bit (x64))

Package	Agent Version	Name	Operating System	File	Size
agent-4.1.0.32.jar	4.1.0.32	Bradford Dissolvable Agent	Linux (x86_64)	Bradford_Dissolvable_Agent.bin	7,092 KiB
		Bradford Dissolvable Agent	Mac-OS-X	Dissolvable Agent.dmg	7,981 KiB
		Bradford Dissolvable Agent	Windows	Bradford Dissolvable Agent.exe	2,982 KiB
		Bradford Mobile Agent	Android	Bradford Mobile Agent.apk	2,355 KiB
		Bradford Mobile Agent (Store)	iOS iPhone	Bradford Mobile Agent (Store)	0 KiB
		Bradford Mobile Agent (Store)	iOS iPad	Bradford Mobile Agent (Store)	0 KiB
		Bradford Mobile Agent (Store)	iOS Unknown	Bradford Mobile Agent (Store)	0 KiB
		Bradford Mobile Agent (Store)	iOS iPod Touch	Bradford Mobile Agent (Store)	0 KiB
		Bradford Mobile Agent (Store)	Android	Bradford Mobile Agent (Store)	2,355 KiB
		Bradford Passive Agent	Windows	Bradford_Passive_Agent.exe	2,386 KiB
		Bradford Persistent Agent (deb)	Linux (x86_64)	bni-persistent-agent_4.1.0.32-1.amd64.deb	11,780 KiB
		Bradford Persistent Agent (dmg)	Mac-OS-X	Bradford Persistent Agent.dmg	10,221 KiB
		Bradford Persistent Agent (exe)	Windows	Bradford Persistent Agent.exe	5,623 KiB
		Bradford Persistent Agent (msi)	Windows	Bradford Persistent Agent.msi	5,490 KiB
		Bradford Persistent Agent (rpm)	Linux (x86_64)	bni-persistent-agent-4.1.0.32-1.x86_64.rpm	11,762 KiB
agent-4.1.0.30.jar	4.1.0.30	Bradford Dissolvable Agent	Windows	Bradford Dissolvable Agent.exe	2,939 KiB
		Bradford Dissolvable Agent	Linux (x86_64)	Bradford_Dissolvable_Agent.bin	7,092 KiB
		Bradford Dissolvable Agent	Mac-OS-X	Dissolvable Agent.dmg	7,981 KiB
		Bradford Mobile Agent	Android	Bradford Mobile Agent.apk	2,355 KiB
		Bradford Mobile Agent (Store)	iOS Unknown	Bradford Mobile Agent (Store)	0 KiB
		Bradford Mobile Agent (Store)	Android	Bradford Mobile Agent (Store)	2,355 KiB

Download Agent Packages

Status: **New Agent Packages are Available**

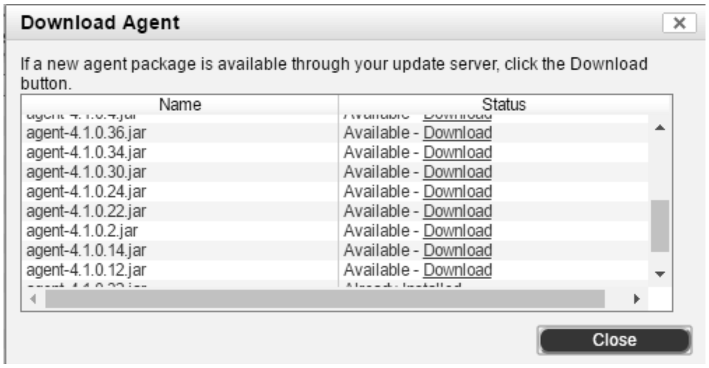
Settings

Field	Definition
Package	Name of the .jar file containing the agents and supporting files.

Field	Definition
Agent Version	Version number of the agent.
Name	Name of the type of agent. Agents include: • Mobile Agent • Dissolvable Agent • Persistent Agent • Passive Agent
Operating System	Operating system on which the agent can run.
File	File name and type, such as .exe or .bin.
Size	Download size of the agent file in KiB.
Delete	Allows you to delete old agent packages from the FortiNAC server.
Download agent packages	
Status	Indicates whether there are new agent packages available for download from Fortinet. Status messages include: • Up to Date • New Agent Packages Available
Download	Launches the Agent Download dialog allowing you to select new agent packages to be added to your FortiNAC server.

Download new agent packages

New Agent packages are placed on the Fortinet update server when they become available. Agent packages contain all of the available FortiNAC agents and agent related files. The Mobile Agent can be downloaded from the captive portal if the device allows downloads from unknown sources, otherwise it is distributed through Google Play. However, there are supporting files for Mobile Agents in the Agent package. For any agent update you must download and install the latest agent package.



Download Agent

If a new agent package is available through your update server, click the Download button.

Name	Status
agent-4.1.0.4.jar	Available - Download
agent-4.1.0.36.jar	Available - Download
agent-4.1.0.34.jar	Available - Download
agent-4.1.0.30.jar	Available - Download
agent-4.1.0.24.jar	Available - Download
agent-4.1.0.22.jar	Available - Download
agent-4.1.0.2.jar	Available - Download
agent-4.1.0.14.jar	Available - Download
agent-4.1.0.12.jar	Available - Download
[illegible]	Already Installed

Download settings must be configured correctly in order to download agent packages. See the Configure Settings section in System update on page 238.

1. Click **System > Settings**.
2. Expand the **Updates** folder.
3. Select **Agent Packages** from the tree.
4. Scroll to the bottom of the page. When new agents are available, the message **New Agent Packages Available** is displayed next to the **Download** button. Select the **Download** button to display a list of available agent packages.
5. Click the **Download** link next to an agent package to initiate the download. A progress page is displayed until the download is complete.
6. Click **Close** to return to the Agent Packages view.

Download the persistent agent for custom distribution

Follow the steps below to download a Persistent Agent from your FortiNAC appliance to your local computer.

1. Click **System > Settings**.
2. Expand the **Updates** folder.
3. Select **Agent Packages** from the tree.

The Dissolvable, Persistent and Passive Agent packages are included in the list, but only the Persistent and Passive Agent packages may be downloaded through this view. The links appear in blue.

4. Locate the agent you wish to download. Click on the name of the agent file in blue text in the **File** column of the table.
5. The file is typically saved to the default download location. This is controlled by your browser.
6. Distribute the file via the Desktop Management software of your choice. It is recommended that you visit our web site for additional information on deploying the Persistent Agent outside of FortiNAC.

Download and configure administrative templates for GPO

Administrative templates are used to configure registry settings on Windows endpoints through Group policy objects. For the Persistent Agent and the Passive Agent, there are templates to configure the Server URL of the FortiNAC Application Server with which the agent will communicate. There are also per-computer and per-user templates to enable or disable the System Tray Icon or Balloon Notifications of status changes. The Balloon Notification template does not affect the Server IP and is not required.

FortiNAC does not support an Administrative Template for deploying configuration changes to macOS computers or users through GPO. You can investigate 3rd party applications, such as Likewise Enterprise that support macOS computers using Group Policy Object editor. The modifications shown in the tables below can be made in the Preferences file on macOS hosts, using the tool of your choice.

The Persistent Agent running on a macOS computer can determine the server to which it should connect via DNS server records it does not require changes to Preferences.

If you are using Persistent Agent version 2.2.2 or higher your Windows login credentials are automatically passed to FortiNAC. You can modify the Administrative Template to hide the Persistent Agent Login dialog and use the Windows login credentials sent by the Persistent Agent by modifying the settings in the Administrative Template. See Using Windows domain logon credentials on page 516.

If you are using Agent package version 3.0 or higher, security is enabled by default. It is recommended that you update to the latest template files and configure the templates for the new security settings.

Requirements:

- Active Directory
- Group Policy Objects
- Template Files From Fortinet

Templates:

The templates listed below are provided by Fortinet. You must run the installation program for the templates on your Windows server . Be sure to select the appropriate MSI for your Windows server architecture.

- 32-bit (x86): Bradford Networks Administrative Templates.msi
- 64-bit (x86_64): Bradford Networks Administrative Templates-x64.msi

Install the templates for GPO

1. In FortiNAC select **System > Settings > Updates > Agent Packages**.
2. At the top of the Agent Distribution window click either the **32-bit (x86)** or the **64-bit (x86_64)** link to download the appropriate template file.
3. Copy the template file to the domain server.
4. On the domain server, double-click the msi file to start the installation wizard.
5. Click through the installation wizard. When installation has completed, the Microsoft Group Policy Management Console is required to complete the installation. Refer to the Windows Server documentation for details.
6. Navigate to the **Group Policy Object** you want to edit, right-click and select **Edit** to display the GPO Editor pane.
7. Right-click **Computer Configuration > Administrative Templates** and select **Add/Remove Templates**, shows the current templates pop-up.
8. Click **Add** and browse to **Program Files\Bradford Networks\Administrative Templates**.
   a. To use the Persistent Agent, select `Bradford Persistent Agent.adm` and click **Open**.
   b. To use the Passive Agent, select `Bradford Passive Agent.adm` and click **Open**.
9. Click **Close**, and the Administrative Templates will be imported into the GPO.

Install an updated template when balloon notifications are configured

If you have never configured Balloon Notifications, go to the section of this document labeled Install An Updated Template.

If you already have a Fortinet Administrative Template installed for the Persistent Agent and the Balloon Notifications were ever set to anything other than Not Configured (e.g. enabled or disabled), you must unconfigure the Balloon Notifications and push the settings to your clients. When your clients have all been updated, then the new template can be installed. These templates affect the registry settings on the client host. In the case of the Balloon Notifications, removing the previous configuration before installing the new one ensures that the keys will be set correctly.

Before updating a template, be sure to record the current template settings. Existing template settings are lost when the new template is installed.

1. In FortiNAC, navigate to **System > Settings > Persistent Agent Properties**.
2. Select **Security Management** and make sure that Display Notifications is disabled. When you have uploaded and configured the new template, come back to this view and restore the Display Notifications option to its original state.
3. Log into your Windows Server.
4. On your Windows server open the Group Policy Management Tool.
5. Navigate to the **Group Policy Object** you want to edit, right-click and select **Edit** to display the GPO Editor pane.
6. Select **Computer Configuration > Administrative Templates > Bradford Persistent Agent**.
7. In the pane on the right, right-click on the Balloon Notifications setting and select Properties.
8. On the **Setting** tab in the Properties window select **Not Configured** and click **OK**.
9. When all of your clients have received the updated settings, the new template can be installed.
10. Navigate to the **Group Policy Object** you want to edit, right-click and select **Edit** to display the GPO Editor pane.
11. Right-click **Computer Configuration > Administrative Templates** and select **Add/Remove Templates**, to show the current templates pop-up.
12. Select the old template and click **Remove**. Follow the instructions in the Install The Templates For GPO section shown above to install the new template.

Install an updated template

Occasionally new templates are made available to incorporate additional features. If you already have a Fortinet Administrative Template installed but it does not have Balloon Notifications enabled, follow the instructions below to update it. If you do have Balloon Notifications enabled, go to the previous section for instructions.

Before updating a template, be sure to record the current template settings. Existing template settings are lost when the new template is installed.

1. On your Windows server open the **Group Policy Management Tool**.
2. Navigate to the **Group Policy Object** you want to edit, right-click and select **Edit** to display the GPO Editor pane.
3. Right-click **Computer Configuration > Administrative Templates** and select **Add/Remove Templates**, to show the current templates pop-up.
4. Select the old template and click **Remove**. Follow the instructions in the Install The Templates For GPO section shown above to install the new template.

Modify settings

See the table below for settings which can be configured using the Administrative Templates provided.

Settings

Option	Definition
Persistent Agent template	
Host Name	Fully qualified host name of the FortiNAC Application Server or the FortiNAC Server if you are not using a pair. It is pushed out to the connecting host(s) to ensure that the Persistent Agent is communicating with the correct host in a distributed environment. This is an option for Persistent Agent Version 2.9.x and lower. Persistent Agent Versions 3.0 and higher do not use this setting.
Balloon Notifications	Enables or Disables Balloon Notifications on a per-host or per-user basis. This setting is not required for configuring Server IP information. Options include: • **Enabled** — Forces balloon notifications for host state changes to be enabled on the host. • **Disabled** — Forces balloon notifications for host state changes to be disabled on the host. • **Not Configured** — Use the non-policy setting (Enabled).
Login Dialog	Enables or Disables the login dialog on a per-host or per-user basis. This setting is not required for configuring Server IP information. See Using Windows domain logon credentials on page 516 for further instructions. Options include: • **Enabled** — The login dialog is enabled. This can be used per-user to override a per-host setting of Disabled. • **Disabled** — The login dialog is disabled. The agent will never prompt the user for credentials. This is useful in certain Single-sign-on configurations. • **Not Configured** — The login dialog is enabled, unless overridden by a per-user configuration.
System Tray Icon	Enables or Disables the System Tray Icon on a per-host or per-user basis. This setting is not required for configuring Server IP information. (Requires Persistent Agent 2.2.3 or higher). Options include: • **Enabled** — The System Tray Icon is enabled. This can be used per-user to override a per-host setting of Disabled. • **Disabled** — The System Tray Icon is disabled. Disabling the System Tray Icon also disables the following functionality: Status Notifications (Show Network Access Status, Login, Logout), Message Logs and the About dialog. • **Not Configured** — The System Tray Icon is enabled, unless overridden by a per-user configuration.
Max Connection Interval	The maximum number of seconds between attempts to connect to FortiNAC.
Persistent Agent security settings	
Security Mode	Indicates whether security is enabled or disabled.

Option	Definition
Home Server	Server with which the agent always attempts to communicate first. Protocol configuration change requests are honored only when they are received from this server. If this servers is not set, it is automatically discovered using Server Discovery. On upgrade, this is populated by the contents of ServerIP.
Limit Connections To Servers	• **Enabled** — Agent communicates only with its Home Server and servers listed under Allowed Servers list displayed. • **Disabled** — Agent searches for additional servers when the home server is unavailable. • **Allowed Servers List** — In large environments there may be more than one set of FortiNAC servers. If roaming between servers is limited, list the FQDNs of the FortiNAC Application Servers or FortiNAC Servers with which the agent can communicate.
Passive Agent template	
Passive Agent	**Server URL List**— Comma separated list of URLs (HTTP(s)://<server_name>/<context> formatted) for the FortiNAC servers that hosts running an agent should contact. Hosts must be able to reach all of the URLs in order to run properly. **Example:** http://qa228/registration NOTE: The context portion of the Server URL is the area of the captive portal the agents should contact, such as, registration, remediation, or authentication.

Registry keys

The template setup shown in the table above modifies the Windows host's registry settings. The table below shows the modifications made to the host's registry keys by the Group Policy Object using the administrative template. If you use a tool other than GPO, you must make sure to set the appropriate keys on each host.

Upon installation of the Persistent Agent, the following key is created by default (and can be viewed using the Windows registry editor on the endstation):

```
HKLM\Software\Bradford Networks\Client Security Agent
```

When registry settings are pushed to a host via software, one or both of the following keys are created (depending upon the values pushed):

```
HKEY_USERS\ … \Software\Policies\Bradford Networks\Persistent Agent
HKLM\Software\Policies\Bradford Networks\Persistent Agent
```

When the settings are pushed, the values for HKLM\Software\Bradford Networks\Client Security Agent will remain the same, but any settings altered via the software push will override those listed in the original key.

On 64-bit operating systems in RegEdit, these registry values will appear in the following key: `HKLM\Software\wow6432node`.

Key	Value	Data
Persistent Agent		
HKLM\Software\Policies\Bradford Networks\Persistent Agent	ServerIP	The fully-qualified hostname to which the agent should communicate. **Data Type:** String **Default:** Not Configured
HKLM\Software\Policies\Bradford Networks\Persistent Agent	ClientStateEnabled	**0** — Do not show balloon notifications on status changes. **1** — Show balloon notifications on status changes. Data Type: DWORD Default: Not Configured
HKEY_USERS\ … \Software\Policies\Bradford Networks\Persistent Agent	ClientStateEnabled	**0** — Do not show balloon notifications on status changes. **1** — Show balloon notifications on status changes. Data Type: DWORD **Default:** Not Configured
HKLM\Software\Policies\Bradford Networks\Persistent Agent	LoginDialogDisabled	**0** — Enable Login Dialog. **1** — Disable Login Dialog. **Data Type:** DWORD **Default:** Not Configured (Login Dialog displayed)
HKEY_USERS\ … \Software\Policies\Bradford Networks\Persistent Agent	LoginDialogDisabled	**0** — Enable Login Dialog. **1** — Disable Login Dialog. **Data Type:** DWORD **Default:** Not Configured (Login Dialog displayed)
HKEY_USERS\ … \Software\Policies\Bradford Networks\Persistent Agent	ShowIcon	**0** — Do not show the tray icon. **1** — Show the tray icon. **Data Type:** DWORD **Default:** Not Configured (Tray icon displayed)
HKLM\Software\Policies\Bradford Networks\Persistent Agent	ShowIcon	**0** — Do not show the tray icon. **1** — Show the tray icon. **Data Type:** DWORD **Default:** Not Configured (Tray icon displayed)

Key	Value	Data
HKEY_LOCAL_ MACHINE\SOFTWARE\Policies\ Bradford Networks\Persistent Agent	maxConnectInterval	The maximum number of seconds between attempts to connect to FortiNAC. **Data Type:** Integer **Default:** 960
HKEY_LOCAL_ MACHINE\SOFTWARE\Policies\ Bradford Networks\Persistent Agent	securityEnabled	**0** — Disable Agent Security. **1** — Enable Agent Security **Data Type:** Integer **Default:** 1
HKEY_LOCAL_ MACHINE\SOFTWARE\Policies\ Bradford Networks\Persistent Agent	homeServer	The fully-qualified hostname of the default server with which the agent should communicate. **Data Type:** String **Default:** Empty
HKEY_LOCAL_ MACHINE\SOFTWARE\Policies\ Bradford Networks\Persistent Agent	restrictRoaming	**0** — Do not restrict roaming. Allow agent to communicate with any server. **1** — Restrict roaming to the home server and the allowed servers list. **Data Type:** Integer **Default:** 0
HKEY_LOCAL_ MACHINE\SOFTWARE\Policies\ Bradford Networks\Persistent Agent	allowedServers	Comma-separated list of fully-qualified hostnames with which the agent can communicate. If restrict roaming is enabled, the agent is limited to this list. The home server does not need to be included in this list (for example, a.example.com, b.example.com, c.example.com). **Data Type:** String **Default:** Empty
Passive Agent		
HKEY_USERS\{SID}\Software\ Policies\Bradford Networks \PASSIVE	ServerURL	**Server URL List** — Comma separated list of URLs for the FortiNAC servers that an agent should contact. Example: http://qa228/registration NOTE: The context portion of the Server URL is the area of the captive portal the agents should contact, such as, registration, remediation, or authentication.

Key	Value	Data
HKLM\Software\Policies\Bradford Networks\PASSIVE	ServerURL	**Server URL List** — Comma separated list of URLs for the FortiNAC servers that an agent should contact. Example: http://qa228/registration NOTE: The context portion of the Server URL is the area of the captive portal the agents should contact, such as, registration, remediation, or authentication.

Deploy the Passive Agent

1. On your Windows server open the Group Policy Management Tool.
2. Navigate to the Group Policy Object you want to edit.
3. Right-click the Group Policy Object and select **Edit** to display the GPO Editor pane.
4. Click **User Configuration > Policies >Windows > Settings Scripts (Logon/Logoff)** to display the Logon and Logoff script configurations.
5. Double click **Logon** for Logon Properties.
6. Click **Add** and then browse to the location of `FortiNAC_Passive_Agent.exe`.
7. Select `FortiNAC_Passive_Agent.exe` to add it to the Script Name field.
8. Enter **-logon** in the Script Parameters field.
9. Click **OK**.

To ensure the user is logged off the host upon logging out, do the following:

1. Follow steps 1-4, and then double-click **Logoff**.
2. Add `FortiNAC_Passive_Agent.exe` to to the Script Name field, and then enter **-logoff** in the Script Parameter field.
3. Click **OK**.

Updating CentOS

This document describes the method for updating CentOS on FortiNAC appliances and virtual machines. It is recommended that the operating system be updated regularly to maintain the highest possible level of security on the server. Refer to Fortinet CentOS Update Policy for additional details.

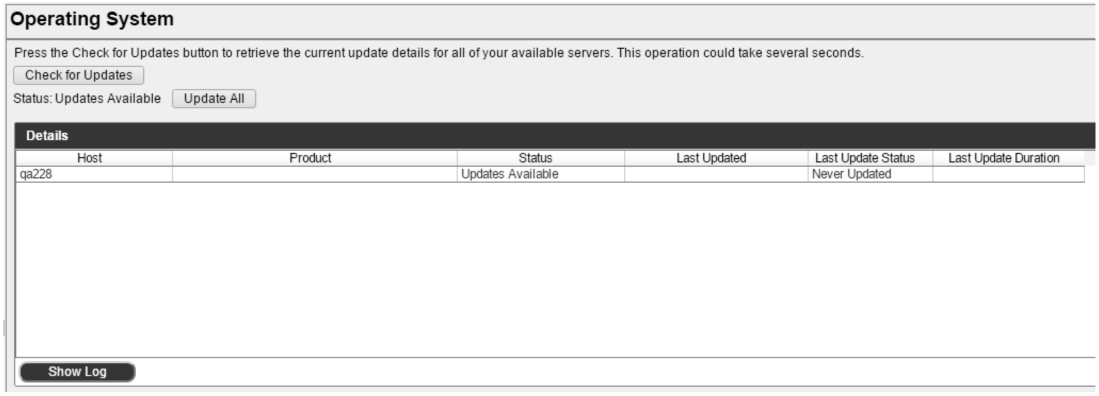
Operating system updates

In a High Availability (HA) environment with redundant servers or in the case of a FortiNAC Control Server/Application Server pair, all of the servers can be updated from the Operation System Updates panel. If a server cannot be reached an error message displays in the table along with the IP address of the server.

When the Operating System Updates panel is accessed, the table is empty. Clicking the Check for Updates button contacts the update repository and determines whether all of the available updates have been installed on each FortiNAC server. The status of each server is displayed in the table. Servers are updated by clicking the Update button.

Operating System updates are downloaded from Fortinet via FTP. When an update is initiated the following event is generated: Operating System Update Initiated.

The update process can take a long time and requires that the updated servers be rebooted.



Operating System

Press the Check for Updates button to retrieve the current update details for all of your available servers. This operation could take several seconds.

Status: Updates Available

Details

Host	Product	Status	Last Updated	Last Update Status	Last Update Duration
qa228		Updates Available		Never Updated	

Requirements

Update packages from both CentOS and Fortinet are signed and will not install if keys do not match those on the appliance or virtual machine.

- FortiNAC firmware versions 3.x and higher.
- FTP access to bradfordnetworks.com from each appliance or virtual machine.
- HTTP access to centos.org from each appliance or virtual machine.
- Maintenance window to reboot the appliance or virtual machine after installing the updates.
- If updating appliances, you must have Dell hardware with one of these SKUs:
  - SYS-G-BFN310-XXXX
  - SYS-G-BFN320-XXXX
  - SYS-G-BFN330-XXXX
  - SYS-G-BFN610-XXXX
  - SYS-G-BFN620-XXXX
  - SYS-G-BFN630-XXXX
- Outbound internet access is recommended for all servers that are being updated.
- If you are running FortiNAC in a virtual machine, take a snapshot of the VM before updating the Operating System.

Update the operating system

1. Click **System > Settings**.
2. Expand the **Updates** folder.
3. Select **Operating System** from the tree.

4. Click the **Check for Updates** button to check the FTP server for updates and assess whether the FortiNAC servers are up to date or not.
5. Click the **Update All** button to begin downloading and installing the Operating System updates.
6. A warning is displayed indicating that this is a long process and that you must reboot the server after the update. Click **Yes** to continue.
7. Use the **Show Log** button at the bottom of the table to view a log of the update process.
8. When the update is complete, select **System Management > Power Management** from the tree.
9. Select each server and click **Reboot** to reboot the FortiNAC Server. If you have a Control Server and an Application Server, they must both be rebooted.

Settings

Field	Definition
Check For Updates Button	Queries the Fortinet FTP site to determine if there are updates available and to check the update status of each FortiNAC server.
Update All Button	Displays only when there are updates available. The Status field indicates the status of the server selected in the table. It is the same as the Status column in the table.
Host	Name of the FortiNAC server.
Product	Type of FortiNAC server. Types include: • FortiNAC Server • FortiNAC Control Server • FortiNAC Application Server
Status	Indicates the overall update status of the FortiNAC Server or Control Server/Application server pair, including: **Updates Available** —Updates are available for one or more of the FortiNAC servers listed in the table. **Up To Date**—All servers are up to date. **Error** - Unable to establish an FTP session to downloads.bradfordnetworks.com **Error** - Unable to ping host **Error** - Unable to ssh to host
Last Updated	Date and time of the last update attempt.
Last Update Status	Indicates the state of the last update. States include: **Never Updated**—Server has never had an operating system update. **Success**—Server was updated successfully. **Failed**—Update attempt has failed.
Last Update Duration	Amount of time that it took to update the server on the most recent update attempt. If the last update was not successful, this number may be very low.
Show Log	Displays the update log.

System update

To update FortiNAC, download the most recent FortiNAC software distribution. Connection settings must be configured for access to the server where the download is hosted.

The database is automatically backed up during the update process.

Update in a high availability environment

To update your servers in a High Availability environment note the following:

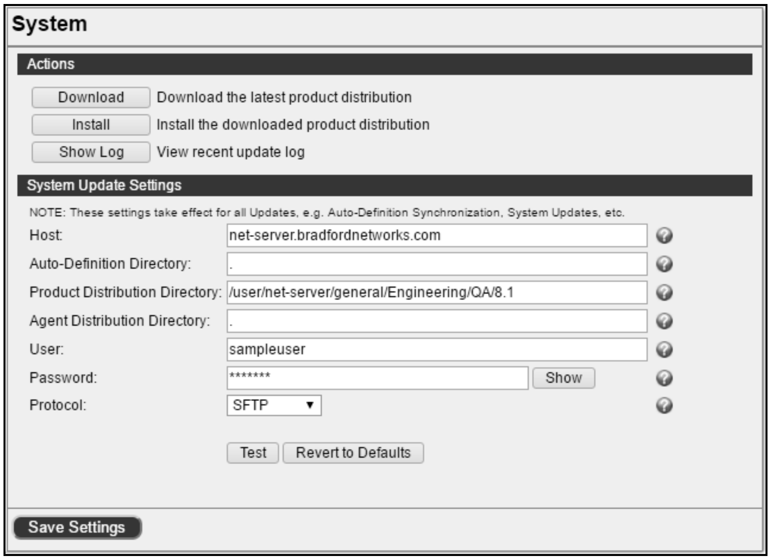
- The Primary server must be running and in control in order to update the system.
- The Secondary server(s) must be running.
- The Primary server must be able to communicate with the Secondary server(s).
- The Primary server automatically updates the Secondary server(s).
- If the Secondary server(s) is in control, FortiNAC prevents you from updating and displays a message with detailed instructions indicating that the Primary must be running and in control.

Update the Primary server following the instructions shown here for a regular update.

If you have a FortiNAC Control Manager that manages your FortiNAC servers, you can run the update from the FortiNAC Control Manager and select all managed servers to propagate the update throughout your environment.

Configure settings

Configure the connection settings for the download location so the Auto-Def Synchronizer, Agent Packages, and the Software Distribution Updates can be completed. You need to change the default settings if another server is used to host the auto-definition or updated distribution files.



Download the latest product distribution
Install the downloaded product distribution
View recent update log

NOTE: These settings take effect for all Updates, e.g. Auto-Definition Synchronization, System Updates, etc.

Host: net-server.bradfordnetworks.com
Auto-Definition Directory: .
Product Distribution Directory: /user/net-server/general/Engineering/QA/8.1
Agent Distribution Directory: .
User: sampleuser
Password: *******
Protocol: SFTP

1. Click **System > Settings**.

Settings

Field	Definition
Host	IP address, host name, or fully-qualified name of the server that is hosting the updates.
Auto-Definition Directory	The sub-directory where the weekly anti-virus and operating system updates are located. Default setting for this field is a period (.). If you are downloading these files from a server on your network, specify the directory containing the updates. If you prefer to download and install updates on a delayed schedule, you can choose system updates from one, two, three or four weeks ago by modifying this field with an additional sub-directory. For example, entering /week1 gives you an update that is one week old. Available directories are: **./week1** contains updates that are one week old. **./week2** contains updates that are two weeks old. **./week3** contains updates that are three weeks old. **./week4** contains updates that are four weeks old.
Product Distribution Directory	The sub-directory where the product software files are located. This field will vary depending on the version of the software being updated. A forward slash (/) may be required in the path configuration. Click the Test button to confirm the configuration. Refer to the System Update Settings section of the Release Notes on our web site for information about the distribution directory for the specific version package you wish to download and install.
Agent Distribution Directory	The sub-directory where the Agent update files are located. This field will vary depending on the version of the software being updated. A forward slash (/) may be required in the path configuration. Click the Test button to confirm the configuration. Refer to the System Update Settings section of the Release Notes on our web site for information about the distribution directory for the specific agent package you wish to download and install.
User	The user name for the connection.
Password	The password for the connection.
Protocol	**HTTP**—Hypertext Transfer Protocol. **HTTPS**—Secure communication over HTTP. **SFTP**—Secure FTP. This protocol provides a more secure connection. **FTP**—File Transfer Protocol. **PFTP**—Passive FTP. A more secure form of data transfer in which the flow of data is set up and initiated by the FTP client rather than by the FTP server program.
Buttons	
Test	Tests the connection between the FortiNAC program and the update server.
Revert To Defaults	Returns the window to the factory default settings.

Download

To update the software on the appliance, download the distribution files to the appliance.

1. Click **System > Settings**.
2. Click **Download**. FortiNAC automatically connects to the download server and retrieves a list of the files available for download. FortiNAC displays a warning message if no update files are found.
3. Scroll through the list of files available for download. Select the most recent distribution file and then click **Download**. Available distribution files are listed in order by version number with the most recent number at the top of the list.
4. Click **Download** to start the download process. This process runs in the background and closes automatically.

Install

Once the distribution files have been downloaded to the appliance, you must manually start the installation. Since the update process restarts the appliance, choose a time to install the update when it will have the least impact on services. The update takes several minutes.

1. Click **System > Settings**.
2. Click **Install**.
3. Select the distribution file from the drop-down list and click **Update**.
4. Verify that the update was successful by checking the version number for the currently installed version.

   From the Admin User Interface:

   - Click the Help Menu and select About.
   - Verify that the version number matches the update that was selected and installed.

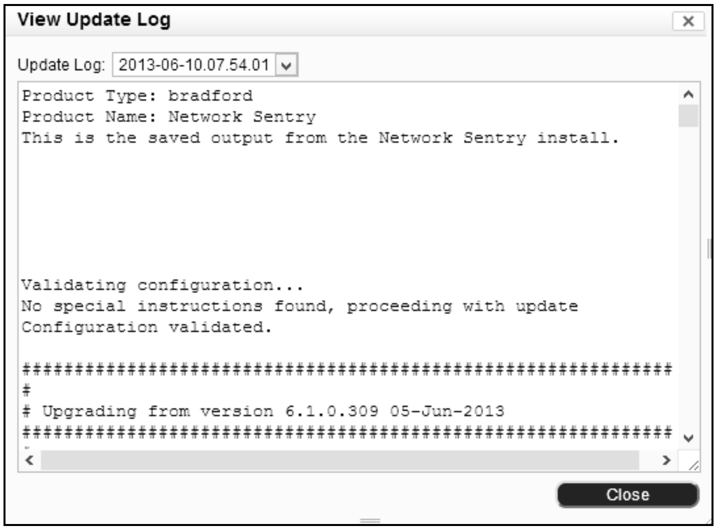
   From the CLI:

   - Enter the following at the FortiNAC command line prompt: `master; cat .version`.
   - Verify that the build date matches the update that was selected and installed.

Show log

A log of the updates is maintained during installation. To view the logs, after installation, click Show Log and select the date of the installation.

In a High Availability configuration, the Update Log files are located on the Primary appliance, since the Primary appliance must be in control during an update.



Update Log: 2013-06-10.07.54.01

```
Product Type: bradford
Product Name: Network Sentry
This is the saved output from the Network Sentry install.






Validating configuration...
No special instructions found, proceeding with update
Configuration validated.

##############################################################
#
# Upgrading from version 6.1.0.309 05-Jun-2013
##############################################################
```

1. Click **System > Settings**.
2. Click **Show Log**.
3. Select the **Date** from the list.
4. The log detail displays in the view.
5. Close the window.

User/host management

User/Host Management groups together global options for controlling user and host properties, such as aging or the number of hosts per user. Options include:

Option	Definition
Aging	Controls how long users and hosts remain in the database. See Aging on page 242.
Allowed Hosts	Controls the number of hosts that can be registered to an individual user in the database. See Allowed hosts on page 244.
Device Profiler	Enable or Disable creating rogues from DHCP packets heard on the network. See Device profiler on page 245.
MAC Address Exclusion	Lists the MAC addresses that can be ignored by FortiNAC when they connect to the network. These addresses will not be treated as rogues and will be allowed on the production network. See MAC address exclusion on page 245.

Aging

FortiNAC manages registered hosts, unregistered (rogue) hosts and users. The settings on the Aging view determine how long host and user records remain in the FortiNAC database.

Age times are used to calculate the Expiration Date and the Inactivity Date displayed on the Host Properties window. Age times for users are used to calculate the Expiration Date on the User Properties window for both network users and Administrative Users that are not set to Never Expire. Modifying age times on this window does not affect those hosts, users or Administrative Users whose Expiration and Inactivity date fields already contain data.

Once the specified time has elapsed for a record, it is removed from the database. These age times are global. Age times are applied to hosts and users as they are created and added to the database and to existing hosts, users with no aging values set. Age times are applied to Administrative Users with no aging values set that do not have the Never Expire option enabled.

Administrative Users that are assigned the Administrator profile cannot be aged out.

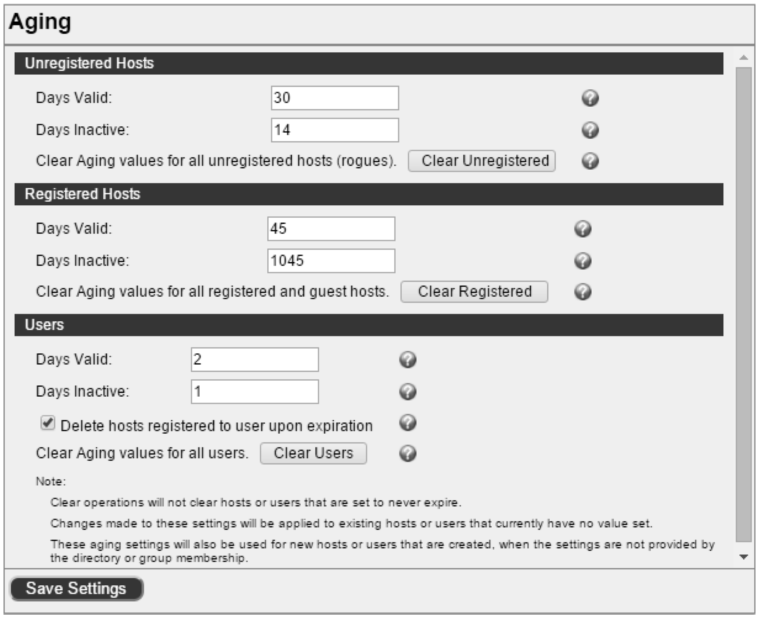
Adding age times to existing hosts or users with no age times can cause some hosts or users to be removed from the database immediately, depending on the creation date of the database record. If, for example, the host or user creation date is 01/01/2010, today's date is 02/02/2010 and Days Valid is set to 5, then the Expiration Date calculated is 01/06/2010. The record is deleted immediately because the calculated expiration date has already passed.

To reset dates on existing records, you must clear the dates using the appropriate Clear button. Then, enter new age times on this window and click Save Settings.

If users or hosts are set to Never Expire, clearing and resetting age times does not affect those records.

Age times can be overridden individually on the User or Host Properties window. The Set Expiration options on the Properties window allow you to set records to Never Expire. You can also use these settings to manage guests who will have access to the network for a limited time.

Aging a large number of hosts or users at the same time can cause processing delays with FortiNAC if users attempt to re-register within a short period of time of each other. It is recommended that you stagger the aging times to reduce the number of possible re-registrations at any given time.



Aging

Unregistered Hosts

Days Valid: 30

Days Inactive: 14

Clear Aging values for all unregistered hosts (rogues). Clear Unregistered

Registered Hosts

Days Valid: 45

Days Inactive: 1045

Clear Aging values for all registered and guest hosts. Clear Registered

Users

Days Valid: 2

Days Inactive: 1

☑ Delete hosts registered to user upon expiration

Clear Aging values for all users. Clear Users

Note:

Clear operations will not clear hosts or users that are set to never expire.

Changes made to these settings will be applied to existing hosts or users that currently have no value set.

These aging settings will also be used for new hosts or users that are created, when the settings are not provided by the directory or group membership.

Save Settings

1. Click **System > Settings**.
2. Expand the **User/Host Management** folder.
3. Select **Aging** from the tree.
4. Modify the settings shown in the table below.
5. Click **Save Settings**.

Settings

Field	Definition
Days Valid	Number of days a host record remains in the FortiNAC database before it is deleted. Host records are created when the host initially connects and is registered with the network.
Days Inactive	Number of days a host can be inactive before the host record is deleted from the database.
Clear Unregistered	Removes the Age Time Expiration Date and Inactivity Date that appears in the Host Properties for all unregistered hosts (i.e., a rogue).
Clear Registered	Removes the Age Time Expiration Date and Inactivity Date that appears in the Host Properties for all registered hosts, except those set to Never Expire. The Clear Registered button also removes the Age Time Expiration Date and Inactivity Date for registered hosts with age times set based on group membership or set individually. You must set individual and group based age times again after using the Clear Registered button.
Delete hosts registered to user upon expiration	If enabled, all hosts associated with a user are removed from the database when the user ages out of the database.

Field	Definition
Days Valid (Users)	Number of days a user record remains in the FortiNAC database before it is deleted. User records are created when the user registers a host.
Days Inactive (Users)	Number of days a user can be inactive before the user record is deleted from the database.
Clear Aging Values for All Users	Removes the Age Time Expiration Date that appears in the User Properties for all users, except those set to Never Expire.

The date on which the host record will be removed from the database is displayed in Properties on page 801. The date on which the user record will be removed from the database is displayed in User properties on page 649. The date on which an Administrative User will be removed from the database is displayed in Admin users on page 683.

Administrator Users never expire under any circumstances. These users must be removed manually from the Admin Users View.

If you leave these fields empty, global Aging is disabled. Setting the value to zero causes the record to be removed the next time the server polls the network.

See Aging out host or user records on page 823 for additional information on aging.

Allowed hosts

Use Allowed Hosts to configure the maximum hosts a single user can register.

Field	Definition
Allowed Host Records	Number of registered hosts a single user may have. For example, if a user has three (3) hosts and the limit is set to two (2), only two of the hosts can be registered on the network. This field can be modified for a single user on the User View. If Allowed Hosts is set under Add or Modify user, the default setting here is ignored. Default = 1000 See Add or modify a user on page 651.

1. Click **System > Settings**.
2. Expand the **User/Host Management** folder.
3. Select **Allowed Hosts** from the tree.
4. Enter the maximum number of hosts a user can register.
5. Click **Save Settings**.

Device profiler

Controls creation of rogue hosts from DHCP packets heard on the network.

Field	Definition
Create Rogues from DHCP packets	When enabled, rogues will be created from information learned from DHCP packets heard on the network. It helps to quickly learn about hosts communicating on the network, but in some network environments it can add a large number of rogues hosts from unmanaged areas of the network. Default = true
Perform Active (NMAP) profiling without ICMP ping	When enabled, Active NMAP scans will not perform a ICMP ping of the host prior to initiating the NMAP scan. This allows networks where ICMP is blocked to still do NMAP scanning. This is disabled by default as it could be a considerable performance drain scanning a large number of uncontactable hosts. Default = false

1. Click **System > Settings**.
2. Expand the **User/Host Management** folder.
3. Select **Device Profiler** from the tree.
4. Use the Create Rogues from DHCP packets check box to enable or disable creating rogues.
5. Click **Save Settings**.

MAC address exclusion

MAC Address Exclusion allows you to create a list of MAC addresses that will be ignored when they connect to the network. If a device or host with one of these MAC addresses connects to the network, FortiNAC ignores the connection and allows the host or device onto the production network.

An event, "Found Ignored MAC Address", is generated each time a host or device connects with a MAC address in this list. Configure an alarm for the event with email notification to alert Administrators. The event can also be disabled if notification is unnecessary.

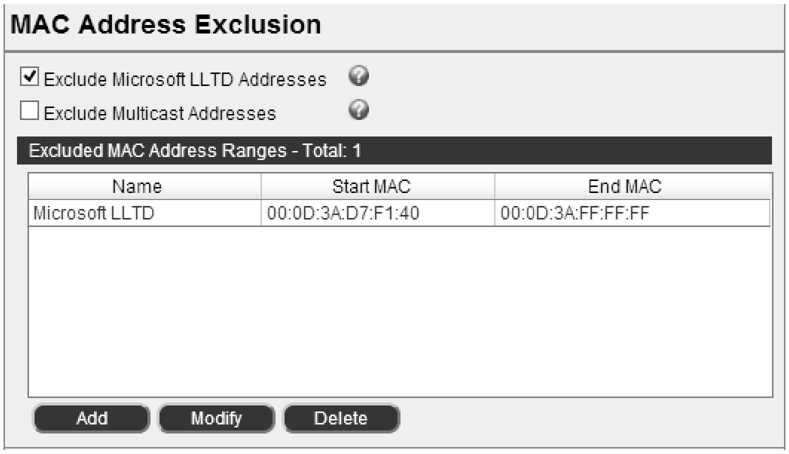
Default settings

This feature is set by default to ignore Microsoft LLTD and Multicast MAC addresses indefinitely. When any MAC address connects that falls within either the Microsoft LLTD or Multicast address range FortiNAC does the following:

- Creates a "Found Microsoft LLTD or Multicast Address" event and an alarm alerting the administrator that FortiNAC has seen a Microsoft LLTD or Multicast address on the network for the first time. This critical alarm warns administrators that if these addresses should continue to be ignored, they must configure the MAC Address Exclusions list or the MAC addresses will be treated as rogues.
- A timer is set that expires in 48 hours.
- While that timer is active, FortiNAC continues to ignore Microsoft LLTD and Multicast MAC addresses. Events and alarms continue to be created for each connection from one of these MAC addresses.

- If the administrator has not configured the MAC Address Exclusions, when the 48 hour timer expires FortiNAC no longer ignores Microsoft LLTD and Multicast MAC addresses. FortiNAC creates rogues for each MAC address that connects, just as it would any other MAC Address.

Administrators can configure MAC Address Exclusion at any time to include or exclude Microsoft LLTD and Multicast MAC addresses. As soon as settings have been modified, the default behavior described above stops and the new settings take effect.



MAC Address Exclusion

☑ Exclude Microsoft LLTD Addresses

□ Exclude Multicast Addresses

Excluded MAC Address Ranges - Total: 1

Name	Start MAC	End MAC
Microsoft LLTD	00:0D:3A:D7:F1:40	00:0D:3A:FF:FF:FF

Configure exclusion list

1. Click **System > Settings**.
2. Expand the **User/Host Management** folder.
3. Select **MAC Address Exclusion** from the tree.
4. Use the Exclude Microsoft LLTD Addresses and Exclude Multicast Addresses check boxes to add or remove those ranges from the Address Range table.
5. To Add Other Ranges, click **Add** and enter a name, starting MAC address and ending MAC address.
6. To Modify A Range, select it from the list and click **Modify**.
7. To Delete A Range, select it from the list and click **Delete**.
8. Changes are saved immediately.

Settings

Field	Definition
Exclude Microsoft LLTD Addresses	If enabled, adds the complete range of Microsoft LLTD MAC addresses to the Excluded MAC Address Ranges table ensuring that the correct range has been entered.
Exclude Multicast Addresses	If enabled, adds the complete range of Multicast MAC addresses to the Excluded MAC Address Ranges table ensuring that the correct range has been entered.
Name	User specified name of the MAC address range.
Start MAC	First MAC address in the range.

Field	Definition
End MAC	Last MAC address in the range.

Portal configuration

Portal Configuration is one in a series of initial setup windows designed to help you get your FortiNAC program up and running as quickly as possible. The Portal Configuration window is used to configure the content and layout of the portal pages that network users encounter when their devices or hosts are unregistered.

The embedded Content Editor allows you to modify selected properties of your portal pages from within the user interface. These changes affect the set of portal pages shipped with FortiNAC and will not modify any existing custom portal pages. If you want to continue to use legacy or custom portal pages, leave the check mark in the Use Portal Version 1 check box. If you would like to use the portal pages that can be modified with the Content Editor, first modify the pages and then, remove the check mark in the Use Portal Version 1 check box.

You may only see a sub-set of the options described in this document, based on the appliance being used. If an option is not displayed on your screen, continue with the next option described.

If you are running Firmware version 2.3.3.x or higher, you will not see references to Portal Version 1 on the Portal Configuration window.

If you choose to use your original Version 1 portal pages, refer to Portal configuration - version 1 settings on page 273 for additional information. If you choose to use the portal pages that can be edited with the Content Editor, refer to Portal content editor on page 250.

When working in Portal Configuration, FortiNAC displays a pop-up message warning you 45 seconds before your Admin login times out and automatically logs you out of the user interface. You can choose to extend your login time by clicking Yes on the confirmation dialog or allow the system to log you out at the end of the 45 seconds by clicking No. If you are logged out automatically before saving your changes, those changes are lost.

Portal Configuration can be accessed from **System** or from **System > Quick Start > Policy Configuration**, however configuration steps point you to System.

Splash page

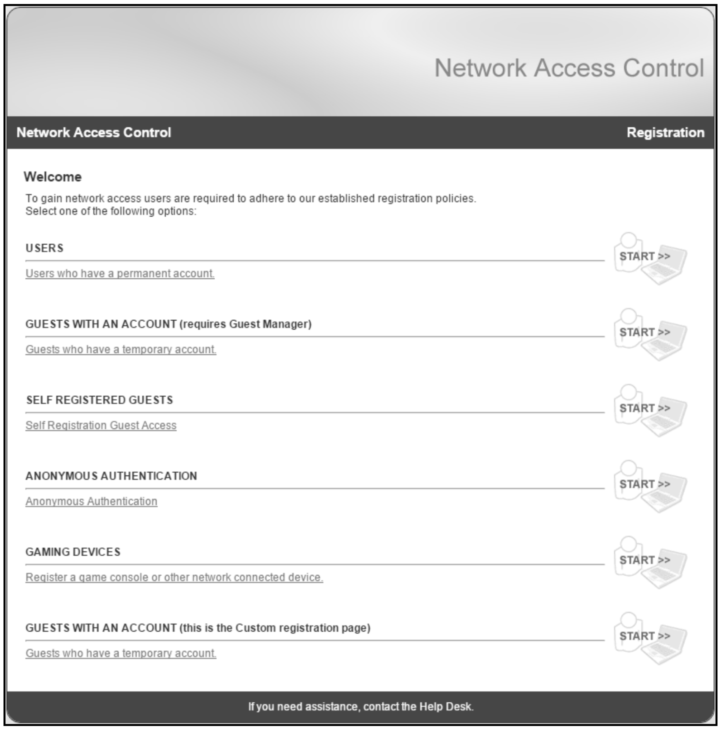
The Portal Splash Page is used in an environment where full guest management is not necessary. This feature allows you to set up a captive portal page to which guests are directed when they access the network. The page may contain an Acceptable Use Policy and guests must indicate that they agree before being granted access to the Production network. Using this option, guests do not register using credentials, they have no guest account, they are simply allowed to access the network on a specific SSID. Hosts are registered as devices, are displayed in Host view and are not associated with any user.

Using the Portal Splash Page or anonymous authentication eliminates the need to configure Guest Templates, Sponsors for guests and Guest Accounts, therefore those options are removed from the Quick Start wizard. However, you must still go through the Discovery process to locate FortiNAC arrays, the Portal Page step to configure the content displayed in the captive portal and the Network Devices step to configure your SSIDs.

Click Apply to save your changes or navigate to another step to abandon them. Navigating to this step refreshes the data with the latest information stored in the database.

Anonymous authentication is not supported with a portal configured with Host Inventory used as the success page type.

If you switch from Full Guest Management to Portal Splash Page existing settings for Full Guest Management will be lost, guests will not be asked for login credentials and guests may be asked to agree to your Acceptable Use Policy.



Network Access Control

Network Access Control — Registration

Welcome

To gain network access users are required to adhere to our established registration policies.
Select one of the following options:

USERS
Users who have a permanent account.

GUESTS WITH AN ACCOUNT (requires Guest Manager)
Guests who have a temporary account.

SELF REGISTERED GUESTS
Self Registration Guest Access

ANONYMOUS AUTHENTICATION
Anonymous Authentication

GAMING DEVICES
Register a game console or other network connected device.

GUESTS WITH AN ACCOUNT (this is the Custom registration page)
Guests who have a temporary account.

If you need assistance, contact the Help Desk.

Settings

Field	Definition
Portal Title	Title that displays across the top of all web pages in the captive portal.
Header Image	Image that displays as a banner across the top of each web page in the portal. Image size should be 80 pixels by 780 pixels.
Upload Image Button	Uploads new images to FortiNAC for use in the banner on web pages in the captive portal.

Field	Definition
Acceptable Use Policy	Controls the display of the Acceptable Use Policy in the portal during registration. Options include: • **None** — No policy is displayed. • **Show In Page** — Text entered in the Usage Policy field is displayed in its own section on the registration page in the portal. • **Show HTML Link** — Text entered in the Usage Policy field is added to a separate page in the portal and is accessed from the registration page via a link.
Acceptable Use Policy Checkbox Text	Text displayed next to the checkbox that allows the guest user to agree to or accept the policy.
URL For Acceptable Use Policy	If you would like to redirect the guest user to another web page to review the Acceptable Use Policy, enter the URL here.
Link Text For Acceptable Use Policy	If guest users will navigate to a different URL to review the Acceptable Use Policy, enter the text that will displayed as the link to that URL.
Text For Acceptable Use Policy	Type the text of your policy in this field to display it to network users when they are in the captive portal.
Style Editor Button	Opens a WYSIWYG style sheet editor.
Advanced Configuration	Opens the Advanced Portal Configuration view allowing you to modify the content of pages seen by users in the portal.
Change Portal Mode	Enables additional steps in the Quick Start wizard allowing you to set up Guest Management and Device Onboarding. Disables the Portal Splash Page. You must click Yes on the confirmation screen to complete this transition.

Portal content editor

The Content Editor tab on the Portal Configuration window allows you to edit the portal pages distributed with FortiNAC. If you have existing portal pages and you prefer not to use the ones distributed with FortiNAC, simply leave the Use Portal Version 1 option enabled on this window.

Use a separate browser to test Portal Pages. Testing pages in the same browser logs the Admin user out of the user interface.

In a High Availability environment, portal pages are copied every 10 minutes.

The Content Editor is navigated using the tree control on the left side. The top level of the hierarchy represents the scope, such as Registration or Remediation. The Global scope contains common items that apply to all portal pages including the Styles Editor. Within each scope are individual pages. When a page is selected the properties it contains are displayed on the right.

Each page contains properties that can be edited such as Window titles or login text. See Content fields on page 276 for instructions on using the Content Editor.

The Images tab displays the images used in Portal Pages, such as the banner. Images can also be uploaded from the Images tab.

Multiple portals can be created and managed from the Content Editor. Portals can be copied and then modified. For the Content Editor the information you display and modify pertains to the set of portal pages selected in the Portal drop-down at the bottom of the view. The images stored in and uploaded to the Images tab are global across all portals. See Multiple portals on page 269.

HTML can be used to format text that will display in the captive portal web pages. Some characters are reserved for HTML and must be entered using special character combinations, such as the & or ampersand symbol, which must be entered as &amp; to display correctly. If you enter one of these characters, a warning is displayed reminding you that it may cause issues when rendered on the web page shown to the user. For a complete list of reserved characters and charts for replacement options, see Using special characters on page 255.

You may see the same warnings when using a character in the course of formatting with HTML, such as <b>Bold</b>. This would trigger a warning because < and > are reserved characters.

Settings

Option	Definition
Use Portal Version 1	Indicates that the system should use the custom portal pages you created by hand. In addition, portal pages that can be modified with the Content Editor are provided with FortiNAC. This option can be enabled and disabled as needed. When enabled the original custom portal pages are used. When disabled the portal pages associated with the Content Editor are used. It is recommended that you configure the new pages first, then disable the Use Portal Version 1 option to begin using the new pages. If you disable the Use Portal Version 1 option before configuring your new pages, network users may not be able to access your network.
Adjust Width	Modifies the space available to display field titles. Slide to the right to expand the titles and contract the fields. Slide to the left to expand the fields and contract the titles.
Portal	Drop-down list of all of the existing portals. The portal selected in this field is the portal that is currently being edited. Use the **Create New Portal Configuration** option to add a new set of portal pages.
Copy	Copy the elements of one set of portal pages to another set. There are options to copy all elements or just the styles to create a new portal or to overwrite an existing portal. See Copy a portal on page 270.
Reset to Defaults	Resets all pages and page properties to their original factory defaults for the selected portal. This includes all user specified text.
Refresh	Refreshes the window and discards any unsaved changes.
Export	Allows you to export all portals with page properties, style sheets and images to a zip file that can be imported on another FortiNAC appliance or can be used as a backup of your portal page configuration. Each set of portal pages is stored as a single XML file within the Zip file. The Zip file can be edited to remove unwanted portals prior to importing on another appliance. See Export portal content on page 253.
Import	Allows you to select a previous export file for import. See Import portal content on page 253.

Option	Definition
Images Tab	Displays the images for the selected portal. Uploads new images to the appropriate location for use in the selected portal.See Upload images on page 254.

Edit style sheets

The Style Sheet Editor allows you to modify the look and feel of the portal pages seen by your network users. This editor only modifies portal pages distributed with FortiNAC in version 4.1.1 or higher. Legacy portal pages cannot be edited using this tool. See Portal content editor on page 250 for additional information.

When the Style Sheet Editor is accessed it displays a sample portal page. This gives you a way to preview your changes as you make them. There are two methods for editing your style sheets.

The first method is to click on an item in the sample page to pop-up a window of options that can be modified.

The second method allows you to enter custom rules for different items in the sample page. This option requires knowledge about cascading style sheets and elements within those style sheets.

Some mobile devices may automatically interpret any text resembling a phone number as a hyperlink. As a result, all rules relative to hyperlinks, including text color, are applied and may cause unexpected results. You may need to supply custom rules in the Style Editor to correct any unexpected issues.

Modifying styles using the sample portal page

1. Select **System > Portal Configuration**.
2. Click on the **Content Editor** tab.
3. If you have created more than one portal, select the portal to be edited from the drop-down list at the bottom of the view.
4. In the tree on the left, select **Global > Styles** to display the style editor.
5. As you pass the mouse over the page, a hand is displayed for items that can be edited.

   For example, if you pass the mouse over the word **Registration** on the right side of the window, a hand is displayed and you may see a blue block that reads "editable". Click on the word **Registration** to open a properties window. Options contained within the window will vary depending on the item selected.
6. Make changes as needed and click **Preview** to return to the Style Editor. Your changes display on the sample portal page.
7. When all of the necessary changes have been made,click the **Apply** button.

Modify styles using the custom rules definitions

In order to use custom rules, you must have a working knowledge of CSS.

1. Select **System > Portal Configuration**.
2. Click on the **Content Editor** tab.

3. If you have created more than one portal, select the portal to be edited from the drop-down list at the bottom of the view.
4. In the tree on the left, select **Global > Styles** to display the style editor.
5. Scroll to the **Custom Rules Definitions** section at the bottom of the window. Using the Custom Rules option you can add multiple rules and each rule can contain multiple properties.
6. To add a rule, click in the field and enter the selector and name of the element you wish to configure. The selector indicates the type of element being modified. For example a period (.) indicates that you are adding a property to a class in the style sheet. In the screen shot shown above, .pagetitle represents the banner at the top of the sample window.
7. Click in the **Property** field and enter the name of the property you wish to set. In the example above, the color property is being set.
8. Click in the **Value** field and enter the value of the property, such as blue for color or bold for font-weight.
9. To add another property to the rule, click the **Add Property** button and an addition set of fields is displayed.
10. To add another rule, click the **Add Rule** button and a new rule section is displayed.
11. The **Preview** button allows you to see your changes on the sample page.
12. The **Reset** button discards all changes and returns the sample page and the custom rules to the state they were in when the Style Editor was first opened.
13. To save, click **Apply** at the bottom of the Content Editor View. This saves changes both in the rules section and in the sample page section.

Export portal content

This option allows you to export the configuration of your portal pages done with the Portal Configuration Content Editor. Legacy page information configured outside the editor cannot be exported. Export to create a backup of your portal page configuration or to copy the configuration to another appliance using the import option. All portal page properties, style sheets and images are included in the export. The export process creates a single file named PortalContents.zip that contains an XML file with the contents of the portal.

If you have created multiple portals, each individual portal and its contents are stored as a separate XML file inside the PortalContents.zip. The original shipping portal is stored as portalContents.XML inside the PortalContents.zip. To import only selected portals, delete the XML files for the unwanted portals from the .zip file.

1. Select **System > Portal Configuration**.
2. Click on the **Content Editor** tab.
3. Click the **Export** button.
4. A message is displayed indicating that unsaved changes will not be exported. If you have saved all of your changes, click **Yes** to continue.
5. Depending on the browser you are using you may see slightly different options. Choose **Save**.

Import portal content

This option allows you to import portal page configuration information. The configuration must have been created using the Content Editor in the Portal Configuration window and exported from that window. Legacy page information configured outside the Content Editor cannot be imported.

When the Portal Page configuration is exported the export file contains portal page properties, style sheets and images combined into a single XML file. The XML file is then added to a zip file created by the export process called PortalContents.zip. Make sure this file is available before you begin the import process.

If you have created multiple portals, each individual portal and its contents are stored as a separate XML file inside the PortalContents.zip. The original shipping portal is stored as portalContents.XML inside the PortalContents.zip. To import only selected portals, delete the XML files for the unwanted portals from the .zip file.

1. Select **System > Portal Configuration**.
2. Click on the **Content Editor** tab.
3. Click the **Import** button.
4. On the Import window either type the path including the file name to the PortalContents.zip file or browse and select the file.
5. Click **OK** to being importing.
6. When the process is complete a message is displayed indicating that the import was successful. Click **OK**.

Upload images

Use the Images tab on the Portal Configuration view to upload and preview images for the portal configuration selected on the Content Editor tab.

1. Select **System > Portal Configuration**.
2. Click on the **Content Editor** tab.
3. If you have created more than one portal, select the portal to be edited from the drop-down list at the bottom of the view.
4. Click on the **Images** tab.
5. To view an image, select it from the list on the left. The image displays in the panel on the right.
6. To upload an image, click the **Upload Images** button.
7. Browse to the image you want to upload and click **Open**.
8. Scroll through the list on the left to make sure your image was uploaded.
9. Click **Apply** to save.

Sample portal page

The steps outlined in this example lead you through uploading an image, adding a banner to your web pages, including an image as the background for the banner and resizing the page.

Upload an image

First you must upload the image you wish to use as the background for your banner. Both the width of the banner and the width of the base page can be adjusted using the style editor. For this example, we will assume that the width needed is 780 pixels. The banner image uploaded would need to be 780 pixels.

1. Select **System > Portal Configuration**.
2. Click on the **Content Editor** tab.
3. If you have created more than one portal, select the portal to be edited from the drop-down list at the bottom of the view.

4. Click on the **Images** tab.
5. To view an image, select it from the list on the left. The image displays in the panel on the right.
6. To upload an image, click the **Upload Images** button.
7. Browse to the image you want to upload and click **Open**.
8. Scroll through the list on the left to make sure your image was uploaded.
9. Click **Apply** to save.

Create a banner with an image background

To create the Banner you will have to use the Custom Rules option at the bottom of the Style Sheet Editor to expand the banner from a height of 0 pixels to an appropriate size. In this example, we are setting the banner to 80 pixels by 780 pixels. We will also adjust the page width to 780 pixels.

To use Custom Rules you must have a working knowledge of CSS.

1. Select **System > Portal Configuration**.
2. Click on the **Content Editor** tab.
3. In the tree on the left, select **Global > Styles** to display the style editor.
4. Scroll to the **Custom Rules Definitions** section at the bottom of the window. Using the Custom Rules option you can add multiple rules and each rule can contain multiple properties.
5. Click **Add Rule**.
6. In the field containing **Enter Selector**, type *.branding*.
7. In the field containing **Enter Property**, type *height*.
8. In the field containing **Enter Value**, type the height of your image, such as *80px*.
9. Click **Add Property** to add the next property which is the width of the image.
10. In the **Property** field, enter ***width***.
11. In the **Value** field enter the width of the image, such as *780px*. Click **Add Property** to add the next property which is the background image.
12. In the Property field enter *background-image*.
13. In the Value field enter *url('../../img/imagename.jpg')* where imagename.jpg is the name of the image you uploaded earlier. If you would like to test this with a sample image, use *banner.jpg*.

    In order to display uploaded images, the path to the image directory must be included in the Value field as follows: `../../img/`
14. Click **Add Rule**.
15. In the field containing **Enter Selector** type *#custom-doc*.
16. In the **Property** field, enter *width*.
17. In the **Value** field, enter the width of the page, such as *780px*. Now the page and the banner will be the same width.
18. Click **Apply** to save.

Using special characters

In FortiNAC Portal Version 2, there are times when you may need to include special characters in your content that may not exist on your keyboard or may not display properly when copying and pasting. In those cases, you can use the following chart and replace those characters with the HTML entity name or the HTML entity number. See the examples below:

1. Entering the following in the Content Editor:

   ```
   L&#39;acc&egrave;s au pr&eacute;sent syst&egrave;me est r&eacute;serv&eacute;
   aux utilisateurs autoris&eacute;s de la Banque. Toute activit&eacute; dans ce
   syst&egrave;me peut &ecirc;tre enregistr&eacute;e et surveill&eacute;e.
   Conform&eacute;ment &agrave; la politique de la Banque, il est interdit aux
   utilisateurs de faire un usage inappropri&eacute; ou non autoris&eacute; du
   syst&egrave;me. Un tel acte peut &ecirc;tre passible de sanctions. En utilisant
   le syst&egrave;me, vous reconnaissez avoir lu et compris le pr&eacute;sent avis
   et acceptez de le respecter.
   ```

2. Will render the following in the Captive Portal:

   L'accès au présent système est réservé aux utilisateurs autorisés de la Banque. Toute activité dans ce système peut être enregistrée et surveillée. Conformément à la politique de la Banque, il est interdit aux utilisateurs de faire un usage inapproprié ou non autorisé du système. Un tel acte peut être passible de sanctions. En utilisant le système, vous reconnaissez avoir lu et compris le présent avis et acceptez de le respecter.

ISO-8859-1

- ISO-8859-1 is the default character set in most browsers.
- The first 128 characters of ISO-8859-1 is the original ASCII character-set (the numbers from 0-9, the uppercase and lowercase English alphabet, and some special characters).
- The higher part of ISO-8859-1 (codes from 160-255) contains the characters used in Western European countries and some commonly used special characters.
- Entities are used to implement reserved characters or to express characters that cannot easily be entered with the keyboard.

Reserved characters in HTML

Some characters are reserved in HTML and XHTML. For example, you cannot use the greater than or less than signs within your text because the browser could mistake them for markup.

Entity names are case sensitive.

HTML and XHTML processors must support the five special characters listed in the table below:

Character	Entity number	Entity name	Description
"	&#34;	&quot;	quotation mark
'	&#39;	&apos; (does not work in IE)	apostrophe
&	&#38;	&amp;	ampersand
<	&#60;	&lt;	less-than
>	&#62;	&gt;	greater-than

ISO 8859-1 symbols

Character	Entity number	Entity name	Description
	&#160;	&nbsp;	non-breaking space
¡	&#161;	&iexcl;	inverted exclamation mark
¢	&#162;	&cent;	cent
£	&#163;	&pound;	pound
¤	&#164;	&curren;	currency
¥	&#165;	&yen;	yen
¦	&#166;	&brvbar;	broken vertical bar
§	&#167;	&sect;	section
¨	&#168;	&uml;	spacing diaeresis
©	&#169;	&copy;	copyright
ª	&#170;	&ordf;	feminine ordinal indicator
«	&#171;	&laquo;	angle quotation mark (left)
¬	&#172;	&not;	negation
	&#173;	&shy;	soft hyphen
®	&#174;	&reg;	registered trademark
¯	&#175;	&macr;	spacing macron
°	&#176;	&deg;	degree
±	&#177;	&plusmn;	plus-or-minus
²	&#178;	&sup2;	superscript 2
³	&#179;	&sup3;	superscript 3
´	&#180;	&acute;	spacing acute
µ	&#181;	&micro;	micro
¶	&#182;	&para;	paragraph
·	&#183;	&middot;	middle dot
¸	&#184;	&cedil;	spacing cedilla
¹	&#185;	&sup1;	superscript 1
º	&#186;	&ordm;	masculine ordinal indicator
»	&#187;	&raquo;	angle quotation mark (right)
¼	&#188;	&frac14;	fraction 1/4

Character	Entity number	Entity name	Description
½	&#189;	&frac12;	fraction 1/2
¾	&#190;	&frac34;	fraction 3/4
¿	&#191;	&iquest;	inverted question mark
×	&#215;	&times;	multiplication
÷	&#247;	&divide;	division

ISO 8859-1 characters

Character	Entity number	Entity name	Description
À	&#192;	&Agrave;	capital a, grave accent
Á	&#193;	&Aacute;	capital a, acute accent
Â	&#194;	&Acirc;	capital a, circumflex accent
Ã	&#195;	&Atilde;	capital a, tilde
Ä	&#196;	&Auml;	capital a, umlaut mark
Å	&#197;	&Aring;	capital a, ring
Æ	&#198;	&AElig;	capital ae
Ç	&#199;	&Ccedil;	capital c, cedilla
È	&#200;	&Egrave;	capital e, grave accent
É	&#201;	&Eacute;	capital e, acute accent
Ê	&#202;	&Ecirc;	capital e, circumflex accent
Ë	&#203;	&Euml;	capital e, umlaut mark
Ì	&#204;	&Igrave;	capital i, grave accent
Í	&#205;	&Iacute;	capital i, acute accent
Î	&#206;	&Icirc;	capital i, circumflex accent
Ï	&#207;	&Iuml;	capital i, umlaut mark
Ð	&#208;	&ETH;	capital eth, Icelandic
Ñ	&#209;	&Ntilde;	capital n, tilde
Ò	&#210;	&Ograve;	capital o, grave accent
Ó	&#211;	&Oacute;	capital o, acute accent
Ô	&#212;	&Ocirc;	capital o, circumflex accent
Õ	&#213;	&Otilde;	capital o, tilde

Character	Entity number	Entity name	Description
Ö	&#214;	&Ouml;	capital o, umlaut mark
Ø	&#216;	&Oslash;	capital o, slash
Ù	&#217;	&Ugrave;	capital u, grave accent
Ú	&#218;	&Uacute;	capital u, acute accent
Û	&#219;	&Ucirc;	capital u, circumflex accent
Ü	&#220;	&Uuml;	capital u, umlaut mark
Ý	&#221;	&Yacute;	capital y, acute accent
Þ	&#222;	&THORN;	capital THORN, Icelandic
ß	&#223;	&szlig;	small sharp s, German
à	&#224;	&agrave;	small a, grave accent
á	&#225;	&aacute;	small a, acute accent
â	&#226;	&acirc;	small a, circumflex accent
ã	&#227;	&atilde;	small a, tilde
ä	&#228;	&auml;	small a, umlaut mark
å	&#229;	&aring;	small a, ring
æ	&#230;	&aelig;	small ae
ç	&#231;	&ccedil;	small c, cedilla
è	&#232;	&egrave;	small e, grave accent
é	&#233;	&eacute;	small e, acute accent
ê	&#234;	&ecirc;	small e, circumflex accent
ë	&#235;	&euml;	small e, umlaut mark
ì	&#236;	&igrave;	small i, grave accent
í	&#237;	&iacute;	small i, acute accent
î	&#238;	&icirc;	small i, circumflex accent
ï	&#239;	&iuml;	small i, umlaut mark
ð	&#240;	&eth;	small eth, Icelandic
ñ	&#241;	&ntilde;	small n, tilde
ò	&#242;	&ograve;	small o, grave accent
ó	&#243;	&oacute;	small o, acute accent
ô	&#244;	&ocirc;	small o, circumflex accent

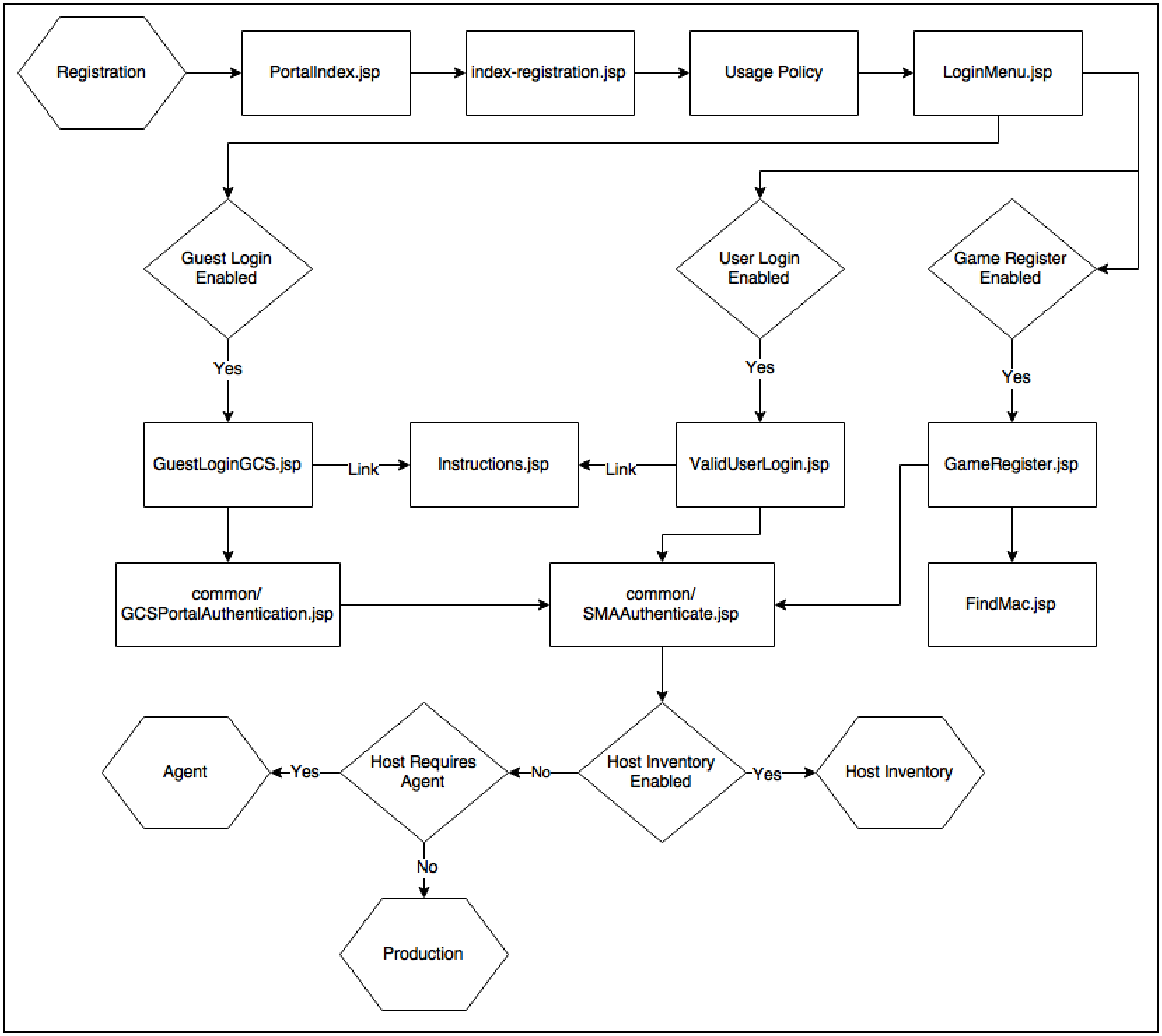
Character	Entity number	Entity name	Description
õ	&#245;	&otilde;	small o, tilde
ö	&#246;	&ouml;	small o, umlaut mark
ø	&#248;	&oslash;	small o, slash
ù	&#249;	&ugrave;	small u, grave accent
ú	&#250;	&uacute;	small u, acute accent
û	&#251;	&ucirc;	small u, circumflex accent
ü	&#252;	&uuml;	small u, umlaut mark
ý	&#253;	&yacute;	small y, acute accent
þ	&#254;	&thorn;	small thorn, Icelandic
ÿ	&#255;	&yuml;	small y, umlaut mark

Configuration

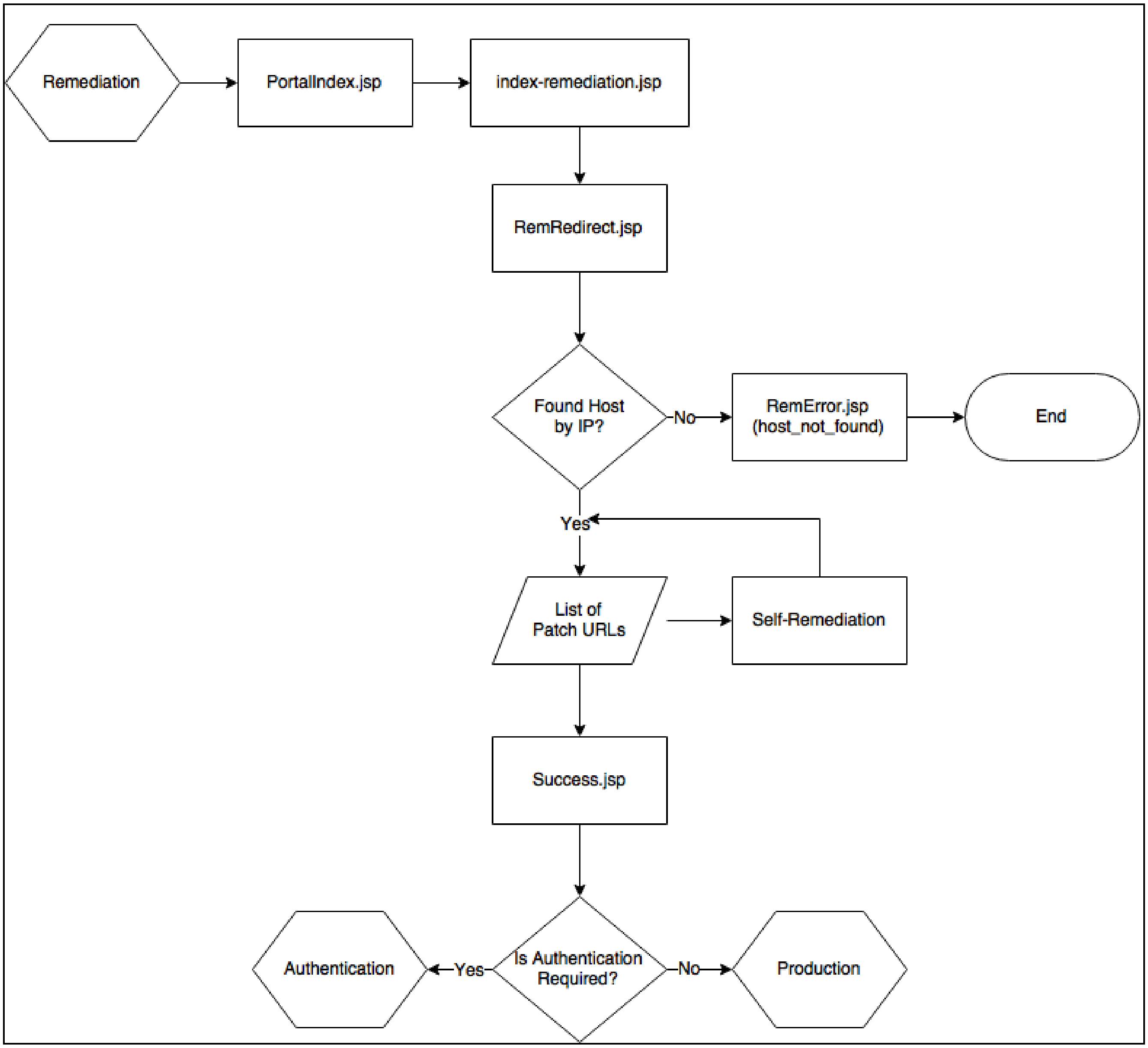
When a host connects to the network FortiNAC assesses the host state and determines where to send that host. Below are a series of diagrams that outline the portal pages used when processing a host request for access to the network. These diagrams and pages correspond roughly to the options in the tree on the Portal Configuration Content Editor when using Portal Version 2 web pages. Diagrams of the pages used include the following:

- Registration
- Remediation
- Authentication
- Dead end
- Hub
- VPN
- Agent
- Host inventory

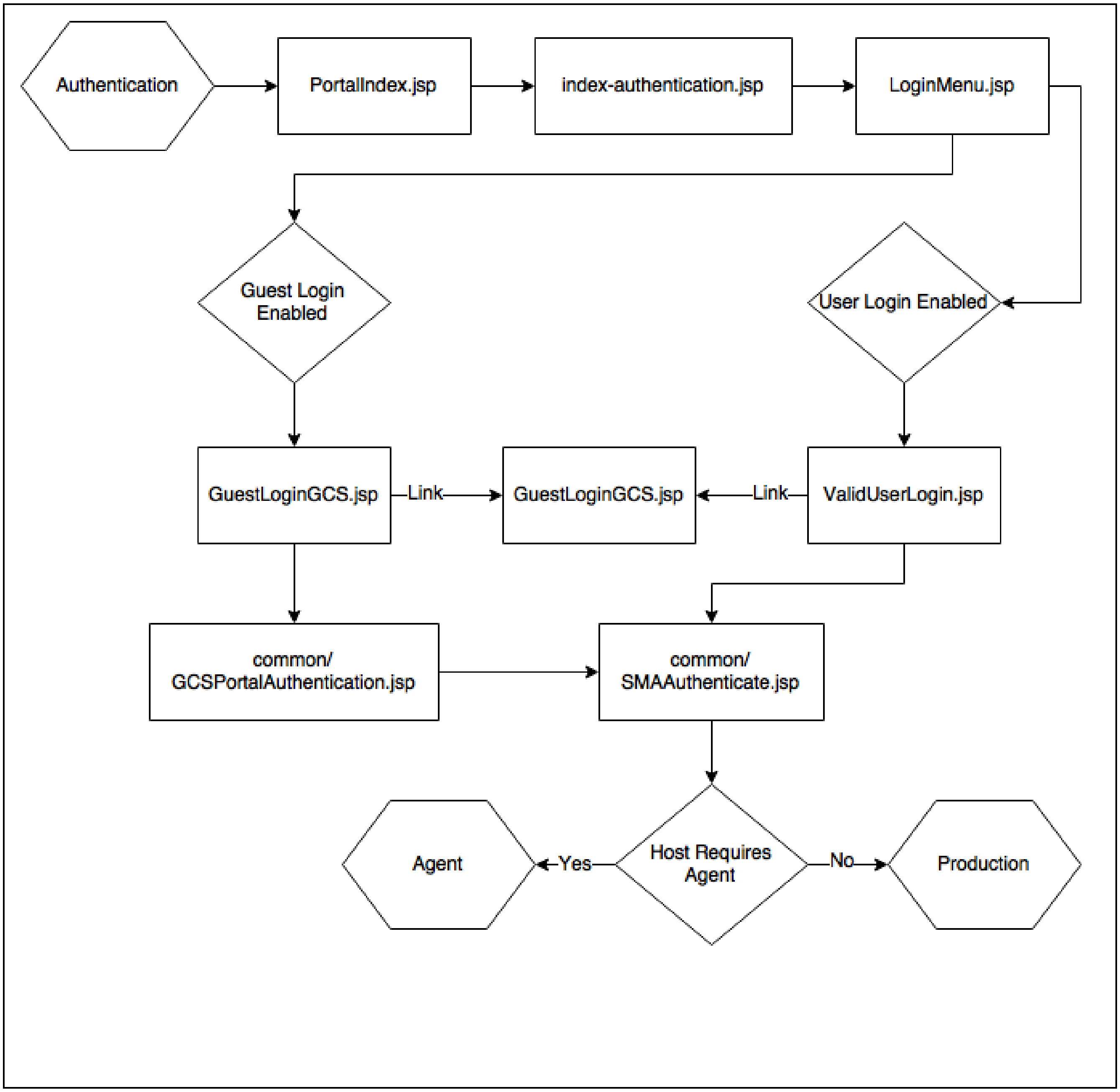
Registration



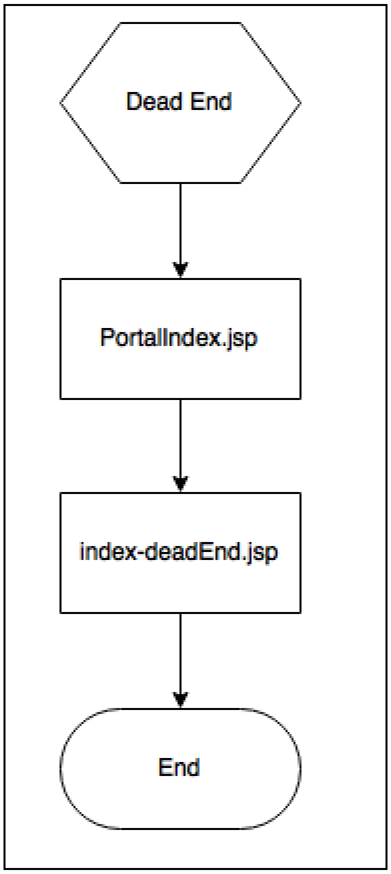
Remediation



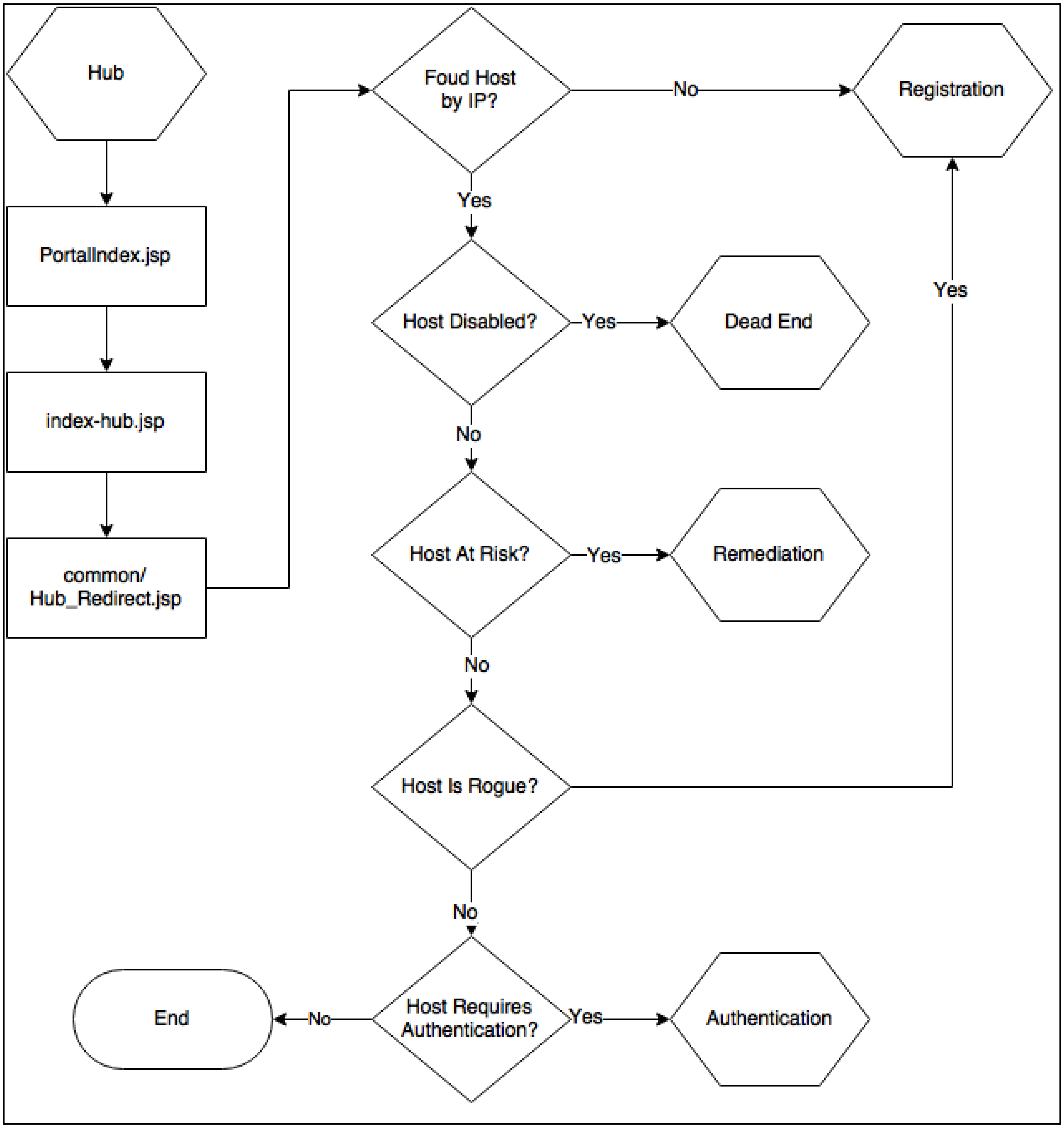
Authentication



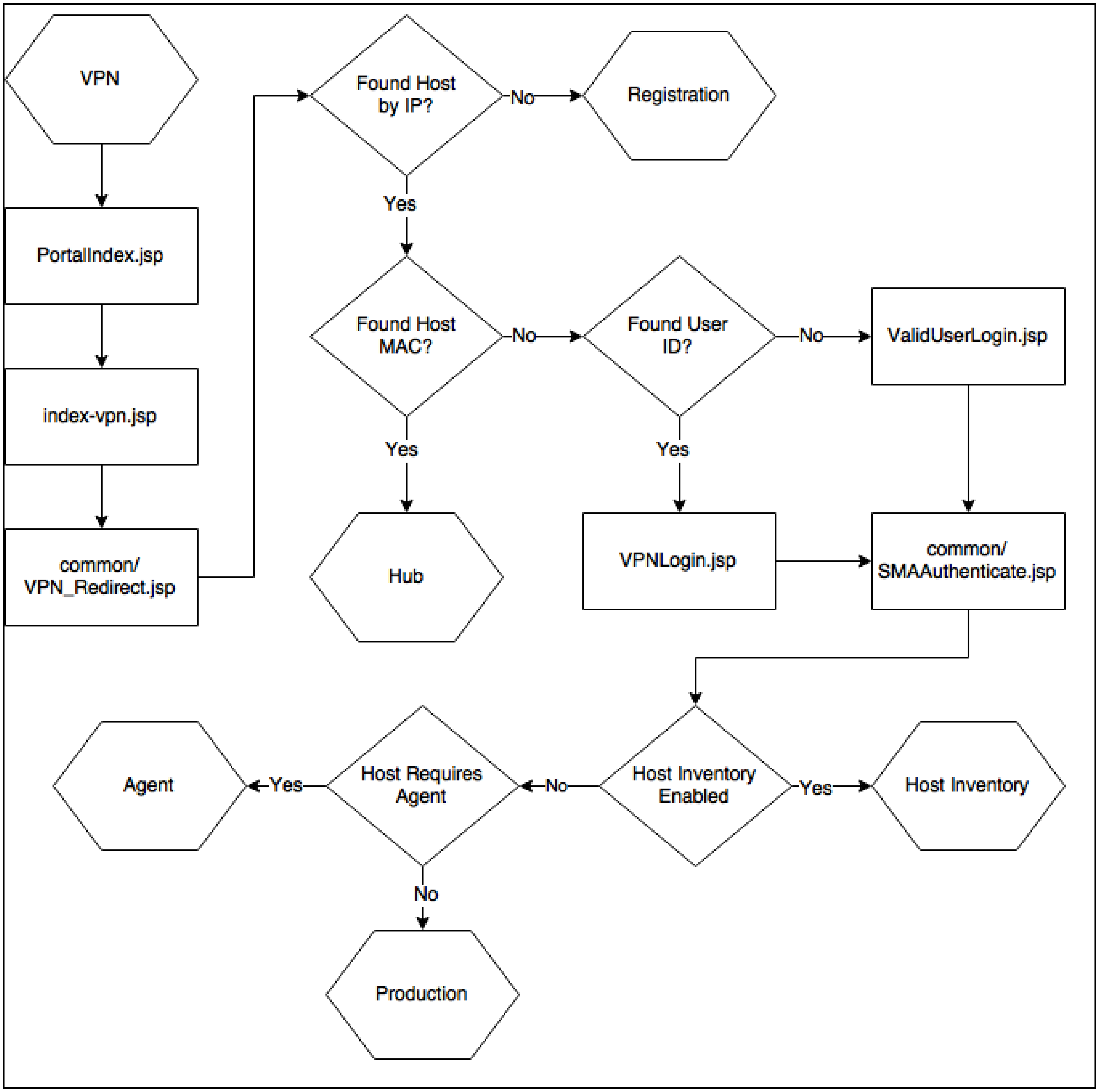
Dead end



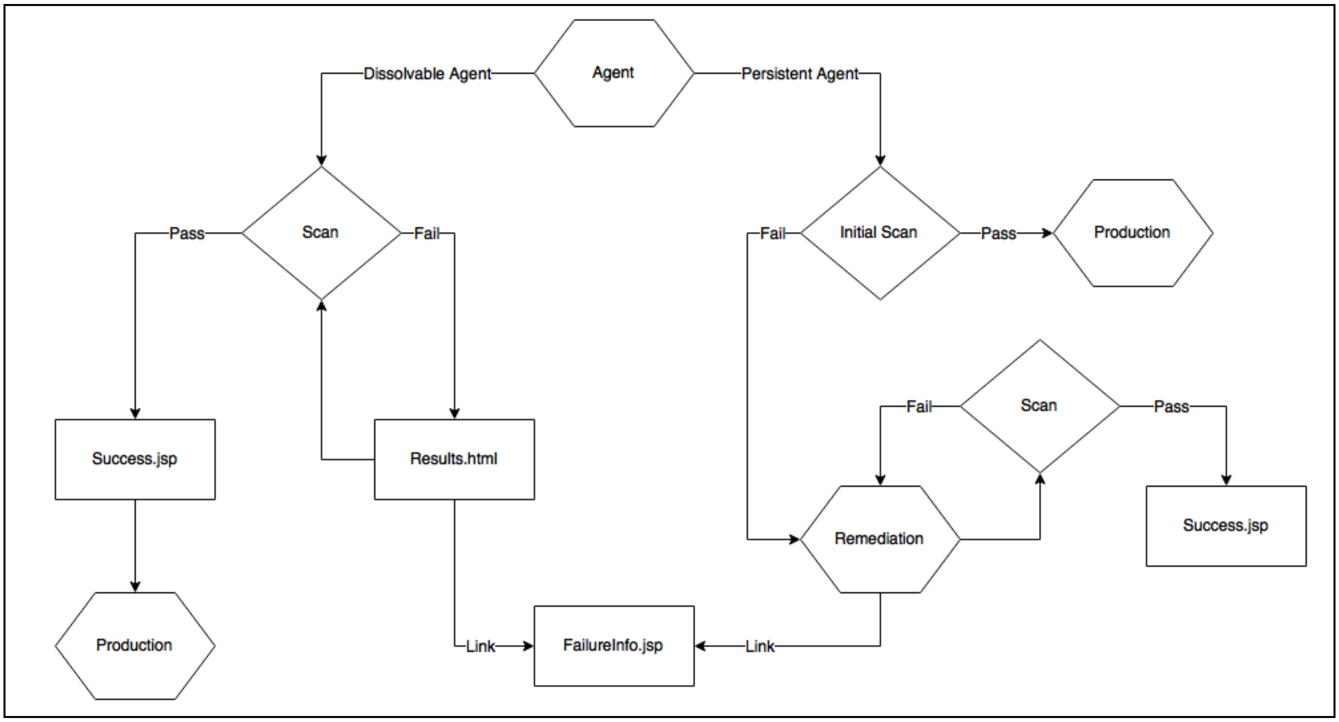
Hub


Hub
PortalIndex.jsp
index-hub.jsp
common/
Hub_Redirect.jsp
Foud Host
by IP?
No
Registration
Yes
Host Disabled?
Yes
Dead End
No
Host At Risk?
Yes
Remediation
No
Host Is Rogue?
Yes
No
End
No
Host Requires
Authentication?
Yes
Authentication

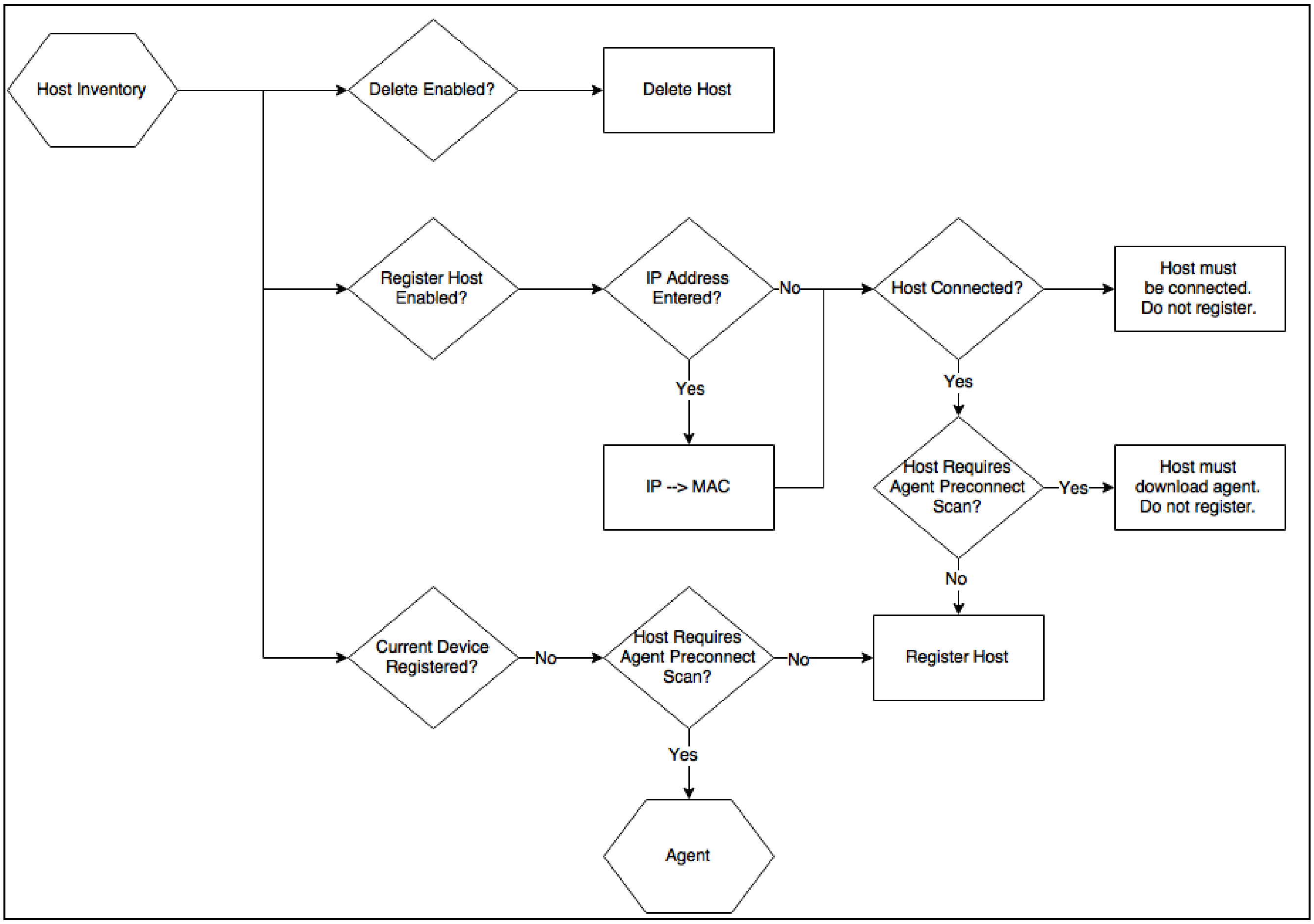
VPN


VPN
PortalIndex.jsp
index-vpn.jsp
common/ VPN_Redirect.jsp
Found Host by IP?
No
Registration
Yes
Found Host MAC?
No
Found User ID?
No
ValidUserLogin.jsp
Yes
Hub
Yes
VPNLogin.jsp
common/ SMAAuthenticate.jsp
Agent
Yes
Host Requires Agent
No
Host Inventory Enabled
Yes
Host Inventory
No
Production

Agent


Agent
Dissolvable Agent
Persistent Agent
Scan
Pass
Fail
Initial Scan
Fail
Pass
Production
Scan
Fail
Pass
Success.jsp
Results.html
Remediation
Success.jsp
Production
Link
FailureInfo.jsp
Link

Host inventory


Host Inventory
Delete Enabled?
Delete Host
Register Host Enabled?
IP Address Entered?
No
Yes
IP --> MAC
Host Connected?
Host must be connected. Do not register.
Yes
Host Requires Agent Preconnect Scan?
Yes
Host must download agent. Do not register.
No
Register Host
Current Device Registered?
No
Host Requires Agent Preconnect Scan?
No
Yes
Agent

Host inventory

Host inventory provides a way for end-users to manage which of their hosts are registered on the network without requiring assistance from an administrator. This is useful when there is a limit on the number of hosts that each user can have simultaneously registered.

The host inventory is an alternate success page. After authentication, if the user's device is already registered and doesn't require remediation they are brought to the host inventory.

Implementation

After the end user is registered and successfully authenticated, the portal advances to the host inventory page, where other hosts can be registered and/or existing registered hosts can be deleted.

The registration is conceptually similar to the gaming registration portal pages, but host inventory is not restricted to Vendor OUIs which are identified as gaming. Any host of any valid vendor OUI can be registered. There is also a control setting that even allows non-valid vendor OUIs to be registered.

In order to register a host using host inventory, the host must be online. This is to ensure that the host does not match an endpoint compliance policy that requires an agent. If the host matches an endpoint compliance policy, the host cannot be registered using the host inventory portal page.

If your policies are configured to bypass the agent, the hosts cannot register in host inventory. As long as FortiNAC supports an agent for the particular operating system, host inventory will identify the host as requiring an agent, independent of whether the host (and user) would match a policy that has the endpoint compliance policy set to **None-Bypass**.

Configuration

1. Click **System > Portal Configuration**.
2. Expand **Global** and click **Settings**.
3. Select **Host Inventory** from the **Success Page Type** drop-down list.

To configure the content that is displayed in the page and the messages that convey the status, use the options under the "Host Inventory" category in the Content Editor of the Portal Configuration. The controls for which capabilities to make available (Register Host, Delete Host, Require Valid Vendor OUI and Show Registration Counts) as well as other settings (for example, the Host Role to use) are also configured under "Host Inventory."

Accessing the host inventory portal page

To access the host inventory pages from a host that's already registered, navigate to this URL in a browser window:

https://<IP or hostname of FortiNAC appliance>/registration/DeviceInventory.jsp

Multiple portals

The Portal Content Editor has options to create separate portals for different sets of users. For example, if you are a conference center and you need to run conferences for three different businesses, each business will require guest access to your network to connect to the internet. Instead of having one generic portal experience, you can create multiple sets of portal pages, each tailored to one of the businesses using your facility. Using Portal Policies you can determine which portal should be presented to a user based on host attributes, such as connection location.

Any action that you perform on the Portal Content Editor only affects the portal selected in the bottom left corner of the view. Images are common to all portals.

Portal v1 pages cannot be used in a multiple portal environment. Disable Portal v1 under **System > Portal Configuration** and use portal v2 pages distributed with FortiNAC.

Implementation

- Using the Portal Content Editor, create a basic portal and configure the elements that are common to all of your portals. This one will serve as your template. See Portal content editor on page 250.
- In the Portal Content Editor under **Isolation > Common** there is an option to **Show Portal Selector Page**. Enable this option if you want to allow a user to select a Portal when the host is in Isolation and FortiNAC cannot determine the portal for that host.

- Use the **Copy** option in the Portal Content Editor to create a new set of portal pages based on the template set and edit those elements that make the new portal unique to a particular group of users. See Copy a portal on page 270.
- Select a default portal. If FortiNAC cannot determine the portal for a connecting host, the default portal is used. See Select a default portal on page 271.
- Create a User/Host Profile for each separate Portal. The User/Host Profile is used to match a host with a Portal Policy based on host attributes. Note that FortiNAC can only discover a small set of information about the host when it connects to the network. Therefore, the attributes that can be used in the User/Host profile are limited for determining the portal to be used. It is recommended that you use host connection location, IP address, MAC Address and/or Operating System. See User/host profiles on page 389.
- Create a Portal Policy for each separate Portal. The Portal Policy combined with the User/Host Profile determine which portal should be presented to a connecting host. See Portal policies on page 395.
- Specific portals can be associated with one or more SSIDs using the options under SSID Mappings. When a portal is assigned to an SSID a corresponding User/Host Profile and Portal Policy are created. The SSID to which the host connects will determine the portal presented to the user. See SSID mappings on page 989.

Create a portal

When you create a new portal configuration the content contains the factory default styles, images and text. New portals can also be created by copying an existing portal to a new name. See Copy a portal on page 270.

1. Select **System > Portal Configuration**.
2. Click on the **Content Editor** tab.
3. Click the drop-down list of portals at the bottom of the view.
4. Click the **Create New Portal Configuration** option at the top of the list.
5. Enter a unique name for the new portal.
6. Click **OK**.
7. The new portal name displays in the list of portals. Select the new portal to begin editing the contents.

Copy a portal

1. Select **System > Portal Configuration**.
2. Click on the **Content Editor** tab.
3. At the bottom of the view select the portal to be copied.
4. Click the **Copy** button.

5. Use the following table to select options:

Field	Definition
Copy Only Style Information	If enabled, copies only the Styles and Custom Rule Definitions configured under **Global > Styles**. If disabled, all elements are copied from the selected portal to the portal designated in the Portal Name field.
Copy Into An Existing Portal	If enabled, the **Portal Name** field becomes a drop-down list of existing portals. Elements from the portal selected on the Content Editor tab are copied to the portal selected in the drop-down list.
Portal Name	Name of the portal to which elements of another portal will be copied. If **Copy Into an Existing Portal** is disabled, a new portal is created. If **Copy Into an Existing Portal** is enabled, this field is a drop-down list of existing portals and the selected portal is updated.

6. Click **OK** to copy the portal.

Select a default portal

Select a default portal to be used if FortiNAC cannot determine the portal that should be presented to a user in an environment where there are multiple portals.

1. Select **System > Portal Configuration**.
2. Click on the **Content Editor** tab.
3. Click the drop-down list of portals at the bottom of the view.
4. Locate the portal that will be the default portal and click the **Edit** icon on the right.
5. In the Edit dialog, enable the **Set as Default Portal** option.
6. Click **OK**.
7. In the drop-down list of portals, the default portal is shown at the top of the list and it is separated from the rest of the portals by a gray bar.

Edit portal settings

Use this option to change the name of an existing portal or to set the selected portal as the default.

1. Select **System > Portal Configuration**.
2. Click on the **Content Editor** tab.
3. Click the drop-down list of portals at the bottom of the view.
4. Locate the correct portal and click the **Edit** icon on the right.
5. In the Edit dialog, modify the name of the portal.
6. If this will be the default portal, enable the **Set as Default Portal** option.
7. Click **OK**.

Delete a portal

If any portal policies use the portal configuration being deleted, those policies are also deleted.

1. Select **System > Portal Configuration**.
2. Click on the **Content Editor** tab.
3. Click the drop-down list of portals at the bottom of the view.
4. Locate the portal you want to remove and click the **Delete** icon on the right (red X).
5. A confirmation message is displayed. Click **Yes** to continue.

Configure authentication credentials

Authentication Credentials for Standard Users are configured in the Portal Configuration Content Editor tab under **Global > Settings > Standard User Authentication Type**. If Portal Version 1 is enabled, Authentication Credentials are configured on the Version 1 Settings tab. These options control how the system validates user credentials for the following login categories:

- **Standard Users**—Users that are assigned their own user names and passwords for logging onto the network on a regular basis. These users might include employees, students, and administrators.
- **Common Account**—Generic account that does not require guests to enter a user name and password, if enabled. Available for Portal Version 1 Only.

  The Common Account option is only available for appliances with firmware images 2.2.0.x through 2.3.2.x.

  The Version 1 Settings tab is only available if the Use Portal Version 1 option is enabled on the General tab of the Portal Configuration window.

Authenticate standard users

Valid users are allowed to access certain network areas on a regular basis. Authentication type is set differently depending on the configuration of your portal pages. Typically, authentication type is set through the Content Editor under **Global > Settings > Standard User Authentication Type**. If you have enabled the Use Portal Version 1 option on the Portal Page Configuration window, authentication is set on the Version 1 Settings tab of that window.

If you are using the Persistent Agent to scan hosts against security policies, the authentication method selected for the Persistent Agent must match the authentication method selected here. See Credential configuration on page 139.

Authentication types include:

- **Local** — Validates the user to a database on the local FortiNACappliance. Use this option if you plan to enter a list of registered users.
- **Local/Device** — Validates the user, but registers the host as the device with no owner.
- **LDAP** — Validates the user to a directory database. FortiNAC uses the LDAP protocol to communicate to an organization’s directory.
- **LDAP/Device** — Validates the user to a directory database, but registers the host as the device with no owner.
- **RADIUS** — Validates the user to a RADIUS server. PAP encryption must be set up on the RADIUS server for encryption/decryption of user names and passwords that are sent to and from FortiNAC, such as the user name and password for the Validation Account used for communication between FortiNAC and the RADIUS server.

- **RADIUS/LDAP** — Validates the user to a RADIUS server, but registers the user based on data contained in an LDAP server. If the user is successfully authenticated by the RADIUS server but does not exist in the LDAP database, FortiNAC will still create the user record in its own database.
- **RADIUS/Device** — Validates the user to a RADIUS server, but registers the host as a device with no owner.
- **HTTP User** — Delegates user validation to HTTP Authentication. Registers to, creating if necessary, a user in the local FortiNAC database.
- **HTTP User/LDAP** — Delegates the user validation to HTTP Authentication, but registers the user based on data contained in an LDAP server. If the user is successfully authenticated but does not exist in the LDAP database, FortiNAC will still create the user record in its own database.
- **HTTP User/Device** — Delegates user validation to HTTP Authentication, but registers the host as a device with no owner.
- **Google** — Requires Agent 3.3 and above. Enables the user to log in with a Google account.
- **Google/Device** — Requires Agent 3.3 and above. Enables the user to log in with a Google account, but registers the host as a device with no owner.
- **None/Device** — Requires Agent 3.3 and above. Allows user to register without a username and password. Registers the host as a device with no owner.

Assign an authentication type

1. Select **System > Portal Configuration**.
2. If Use Portal Version 1 is not enabled, click on the **Content Editor** tab.
3. If you have created more than one portal, select the portal to be edited from the drop-down list at the bottom of the view.
4. Click the **Global** option in the tree on the left to expand it. Under Global, select **Settings**. In the pane on the right locate the **Standard User Authentication** field and select **Local**, **LDAP**, **RADIUS**, **RADIUS/LDAP**, **HTTP User** or **HTTP User/LDAP** from the drop-down menu.
5. In the tree on the left select **Registration > Login Menu**. Make sure that **Standard User Login** is enabled.
6. Click **Apply**.

Portal configuration - version 1 settings

This option is only available for appliances with firmware images 2.2.0.x through 2.3.2.x.

The Version 1 Settings tab on the Portal Configuration window allows you to configure the how portal pages appear in the web browser if you are using legacy portal pages.

This tab is only available if the Use Portal Version 1 option is enabled on the Portal Configuration view. The **Use Portal Version 1** option is enabled by default. It controls which portal pages are used when network users log onto your network. Portal Version 1 represents existing portal pages created when you originally set up FortiNAC. Disabling the Portal Version 1 pages enables pages that are distributed with FortiNAC that can be edited using the Content Editor.

Properties Settings in this window include:

- **Labels** — Displays a text label below the portal page header.
- **Images** — Displays an image in the portal page header at the top of the page.
- **Links** — Specifies a web page that displays in the browser when the login credentials are successfully authenticated.

Settings

Field	Definition
Portal Settings	
Web Page Label	Banner that displays at the top of the portal page when a user attempts to connect to the network.
Web Page Footer	Text that displays across the bottom of the portal page when a user attempts to connect to the network.
Upload Image Button	Browse for and upload an image to display on the portal page.
Home Page URL for Successful Registration	URL to which the users are directed when they have successfully registered. Copy this URL into a browser to verify that the correct page is displayed.
Resolve URL button	Resolves the IP of the URL selected for the Home Page.
Standard User Authentication	
Authentication Type	Valid users are allowed to access certain network areas on a regular basis. Choose from three authentication types: **Local**—Validates the user to a database on the local FortiNAC appliance. **LDAP**—Validates the user to a directory database. FortiNAC uses the LDAP protocol to communicate to an organization's directory. See Directories on page 79 for configuration information. **RADIUS**—Validates the user to a RADIUS server. PAP encryption must be set up on the RADIUS server for encryption/decryption of user names and passwords that are sent to and from FortiNAC, such as the user name and password for the Validation Account used for communication between FortiNAC and the RADIUS server.

If you are not using Version 1 Portal Pages, authentication type is set in the Content Editor under **Global > Settings > Standard User Authentication Type**.

1. Select **System > Portal Configuration**.
2. Click the **Version 1 Settings** tab. This tab is only displayed if the Use Portal Version 1 option is enabled on the Portal Configuration view.
3. Under the Portal Settings section, enter a text label into the **Web Page Label** field. This label displays below the header image on your portal pages. Typically, this is the name of the company or organization.
4. Enter a text label into the **Web Page Footer** field. This label displays at the bottom of your portal pages, such as "For assistance, contact the help desk.".
5. To display an image on your portal page, click the **Upload Image** button. Navigate to the image file and select it.
6. To specify a web page for successful registration, enter a URL in the **Home Page URL for Successful Registration** field.

   Cut and paste the link into a browser to verify that the URL directs you to the correct page.

7. Click the **Resolve URL** button. The URL resolves to an IP. The IP address of the URL is entered into the field.
8. The Standard User Authentication section determines how users are authenticated.
9. Click **Apply**.

Enable the common account

The Common Account is only available if the **Use Portal Version 1** option is enabled on the Portal Configuration view. The Common Account can only be used with legacy portal pages.

Allows you to configure a generic or common account for visitors. If you check Enable in the Common Account section, visitors view a different login screen and do not enter a user name and password. The visitor enters only predefined information, such as first name, last name, telephone number, and so on. To be authenticated, the visitor uses the default user name and password that you specify in the Common Account section.

Configure the following parameters for Common accounts:

- **Enable** — Enables default user name and password for guest access.
- **User Name** — Specifies a default user name for the default guest account. You may choose a user name such as *defaultguest* to easily identify the statistics of all default guests.
- **Password** — Specifies a default password for the default guest accounts. The guest does not enter this password. FortiNAC uses this password internally to authenticate the guest to an existing user entry.

1. Select **System > Portal Configuration**.
2. Click on the **Version 1 Settings** tab.
3. In the Common Account section of the window select the **Enable** check box.
4. Enter a default user name into the **User Name** field.
5. Enter a default password into the **Password** field.
6. Click **Apply**.

Reserved portal page file names

If you choose to create your own pages for the portal, you must avoid using any of the following file names. Files with the names listed below are used by FortiNAC for the pages distributed with the program. These files should never be modified outside of the Portal Configuration Content Editor. Future upgrades could overwrite those changes.

- AgentDownload2.jsp
- CustomLogin.jsp
- Disagree.jsp
- Error.jsp
- ExternalLogOff.jsp
- Fail.jsp
- FailureInfo.jsp
- FindMac.jsp
- GameRegister.jsp
- GuestLoginGCS.jsp
- index-authentication.jsp
- index-deadEnd.jsp
- index-hub.jsp
- index-registration.jsp
- index-remediation.jsp
- index-vpn.jsp
- Instructions.jsp
- LoginMenu.jsp
- LogOff.jsp
- LogOffSuccess.jsp
- Policy.jsp
- PortalIndex.jsp
- RemoteScan.jsp
- RemoteSuccess.jsp
- RemRedirect.jsp
- Success.jsp
- ValidUserLogin.jsp
- VPNLogin.jsp

Anything starting with portalCommon should be avoided.

portalCommon/**

Content fields

The Content Editor allows you to modify the content of the portal pages seen by your network users. This editor only modifies portal pages distributed with FortiNAC in version 4.1.1 or higher. Legacy portal pages cannot be edited using this tool. See Portal content editor on page 250 for additional information.

If you are familiar with HTML, you can add formatting within the content fields for your pages. Test each page carefully because your formatting may conflict with something that is in the default settings for the page. Make sure to test portal pages in a separate browser of a different brand. If you test in the same browser you will be logged out of the Admin user interface. For example, if you are running the Admin user interface in Google Chrome, test the portal pages in Internet Explorer.

1. Select **System > Portal Configuration**.
2. Click on the **Content Editor** tab.
3. If you have created more than one portal, select the portal to be edited from the drop-down list at the bottom of the view.
4. Click a node in the left hand pane to expand it.
5. Click a page within the selected node. The properties for that page are displayed in the right pane.
6. Modify the properties as needed and click **Apply** to save your changes. When changes are made to the portal pages there is a delay before the changes are displayed.

Field types on each page include the following:

Type	Description
Boolean	Check box that enables or disables a feature or subsequent field.

Type	Description
Text	Text fields are available for you to enter custom text that is displayed on your Captive Portal Page. If you are familiar with HTML, you can include HTML in these fields. For example, to make something bold and italics, you would do the following: <b><i>Contact the Help Desk.</i></b> The message on the web page would display as: ***Contact the Help Desk.*** For users who are accessing your web pages you may also have text fields. These fields are set to type Input and typically only allow text.
Input	If you have set a data entry field to type input, you are indicating that the web page user should enter text. You can enter a default value to prompt the user but it can be overridden. For example, if you set Postal Code to your local postal code, most users would not have to modify this field and it would save them a step.
Password	If you have set a data entry field to type password, any data typed into the field by the user will display as dots or asterisks to mask the actual characters being entered.
Hidden	If you have set a data entry field to type hidden, the user does not see it on the web page, however, it does contain data that is passed to the server. You must enter the data in the Portal Content Editor. For example, if all users who register via the Registration page should be set to a particular Role, such as, Staff, you can enter Staff in the Role field for them and mark it as hidden.
Select	If you have set a data entry field to type select, the user is presented with a drop-down list of options on the web page. To construct the list of options you must enter list items as follows: (Value,Name : Value,Name) Example: Color1,Blue : Color2,Red : Color3,Green
Inline Help icon	Displays inline help containing a description and usage for the field.

Text fields in the Portal Contents Editor accept HTML. However, if you copy and paste HTML developed in another program you may corrupt the data stored for your web pages. Specifically, HTML containing curly or curved quotes instead of straight quotes will corrupt your web pages and they will become unusable.

The Content Editor is navigated using the tree control on the left side. The top level of the hierarchy represents the scope, such as Registration or Remediation. The Global scope contains common items that apply to all portal pages across all scopes. Within each scope are pages. When a page is selected the properties it contains are displayed on the right. Each page contains properties that can be edited such as Window titles or login text.

Global properties

Global properties are common to all portal pages. These properties are organized into property groups. Select a property group to view or modify property settings.

Settings

Setting	Definition
Network Label	Text label for the left side of the banner on each portal page.
Enable Mobile Enhancements	If enabled, uses an override stylesheet to optimize the portal for modern mobile browsers on mobile devices running Apple iOS, Android, Symbian, and others.
Show Left Column	Display a column to the left of the main content.
Show Usage Policy Before Registration	If enabled, displays the Usage Policy to the user before registration. Usage Policy text is entered in the Content Editor under Registration-Usage Policy-Usage Policy Content.
Standard User Login Type	Select the authentication method for users. This field must match the field selected in Persistent Agent Properties under the Credential Configuration Tab.
Custom Login Type	Select the authentication method for the Custom Login page.
Game Console Registration Login Type	Select the authentication method for the Game Console Registration page.
Authenticate Standard Users	If enabled, this option authenticates and registers users at the same time. Prevents users from needing to enter credentials on both the Registration and Authentication pages.
Show Passed Tests	Display criteria that were met during a host scan.
Use JavaScript UI Enhancements	If enabled, allows the system to use user interface enhancements such as the accordion view in all instructions pages. Features using JavaScript Enhancements can be disabled individually.
Use Configured MDM	If enabled, all browsers with mobile user agents will be redirected to the MDM Registration page.
Success Page Type	Select whether the host should be redirected to the default Success page or the Host Inventory Success page after logging in within the Registration or VPN context.

Common text

Setting	Definition
Username Label	Text label displayed on all generic Username fields.
Password	Text label displayed on all generic Password fields.
Footer Text	Text displayed at the bottom of each page in the footer section.
Physical Address	Text label displayed on fields where users enter the Physical Address or MAC Address of their host, gaming device or other network device.
IP address	Text label for the IP address field where users enter the IP address of their host.
Instructions	Text for all links to instructions, such as Persistent Agent installation instructions.

Setting	Definition
Result	Text label displayed above the result panel.
Passed Tests	Text label displayed above the list of criteria that was met during a host scan.
Passed Tests Help	Help information displayed above the list of criteria that was met during a host scan.
Warnings	Text label displayed above the list of criteria that generated warnings during a host scan. Warnings do not stop the user from accessing the network.
Warnings Help	Help information displayed above the list of criteria that generated warnings during a host scan.
Failed Tests	Text displayed above the list of criteria that was not met during a host scan.
Failed Tests Help	Help information displayed above the list of criteria that was not met during a host scan.
Default Select Option Text	Text label displayed above any selection boxes if they are enabled on a form.
Registration	Text label displayed on the banner for Registration.
Login Button Text	Text displayed on all Login buttons.
Logout	Text displayed on all Logout buttons.
Back	Text displayed on all Back buttons.
Register	Text displayed on all Register buttons. User clicks Register when registration information is complete.
Reset	Text displayed on all Reset buttons.
Agree	Button text for Agree
Disagree	Button text for Disagree
Failed Scan	Message displayed when a persistent agent client failed tests during a rescan.

Error messages

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Heading	Text label displayed on the banner when there is an error.
Left Column Content	Error message displayed when there is an error processing input in the left column of any page.
Unsupported OS	Error message displayed when a host has an unsupported operating system and the Security Policy used to scan that host has the unsupported operating system agent option set to "None-Deny Access".

Setting	Definition
Jailbroken Device Failure	Error message displayed when a host exceeds the threshold configured for potentially jailbroken devices.
Unauthorized Mobile Agent Failure	Error message displayed when an unauthorized host attempts to register using the Mobile Agent.
Host Already Registered	Error message displayed when the host is already registered.
User Account is invalid or disabled	Customizable message displayed when the user is not found. Defaults to "Authentication Failure".
Invalid Registration Key	Uncommon error message displayed when the system was unable to register the host with the supplied authentication key.
Other Registration Error	Error message displayed when any other Registration error occurs. Note: An additional error message is displayed after this text, which typically starts with "Registration Failed:".
Invalid OUI	Error message displayed when the Vendor OUI of the Physical Address entered is not configured as a gaming device OUI. To configure additional Vendor OUIs select Go- Manage - Vendor OUIs.
Gaming Device Not Connected	Error message displayed when the Gaming Device was not connected to the network before the registration attempt.
Host Not Found	Error message displayed when the software cannot locate the host attempting to use the portal.
Agent Version/Filename Does Not Exist	Error message displayed when a user tries to download an agent and that request references an agent that does not exist or has incomplete file information.
Isolation Redirect Error	Error message displayed when the host is still isolated because it could not be redirected. No action is required for the user. However, this does require network configuration changes.
No Scan Failures	Error message displayed when a host is in the remediation network but the host is not marked as failed for any scans.
Unable to Rescan	Error message displayed when a host is in the remediation network and tries to rescan, but the server was unable to scan via the agent.
General Error	Error message displayed for unknown or unspecified errors.

Failure information settings

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the Failure Information page.
Left Column Content	Text displayed in the left column of the page.

Setting	Definition
Rescan Button Text	Text displayed in a button on the Failure Information page to allow the user to re-run the failed Vulnerability Scan for their device.
Scan Pending Button Text	Text displayed in the Rescan Button while the scan is pending response. The button will be disabled while the scan is pending.
Vulnerability Scan Passed Test	Content displayed in Failure Information page when the vulnerability scan being viewed has no failures for the current device.
Poll for Vulnerability Rescan Results (minutes)	The frequency with which the Portal queries FortiNAC for updated scan results from the Vulnerability Scanner.

Styles

Setting	Definition
Portal Custom Styles	Contains the CSS text for the portal's custom styles.
Portal Custom Skin	Contains the CSS text for the portal's custom skin, created by the editor.

Registration

Configure the settings and behavior of your portal pages for registering hosts on your network.

Common text

Setting	Definition
Context Title	Text label to indicate the functional purpose of the context.

Login menu

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text for the title in the body of the login menu page. Displays above the text entered in the Text Content property.
Left Column Content	Text displayed in the left column of the login page.
Text Content	Text providing instructions or requirements for the use of the Login Menu. The Login Menu may contain multiple login options, such as Users or Guests.
Standard Login Enabled	If enabled, the Standard login option appears in the login menu for regular network users.

Setting	Definition
Standard Login Title	Text label above the link to the regular network user login.
Standard Login Link	Text displayed in the link to the regular network user login.
Standard Login Order	Integer value indicating the order this item should appear in on the page
Guest Login Enabled	If enabled, the Guest Login option appears in the login menu.
Guest Login Title	Text label above the link to the guest login.
Guest Login Link	Text displayed in the link to the guest login.
Guest Login Order	Integer value indicating the order this item should appear in on the page
Self Registration Guest Login Enabled	If enabled, the Self Registration Guest Login option appears in the login menu.
Self Registration Guest Login Title	Text label above the link to the self registration guest login.
Self Registration Guest Login Link	Text displayed in the link to the self registration guest login.
Self Registration Guest Login Order	Integer value indicating the order this item should appear in on the page.
Anonymous Authentication Enabled	If enabled, the Anonymous Authentication option appears in the login menu.
Anonymous Authentication Title	Text label above the link to the anonymous authentication.
Anonymous Authentication Link	Text displayed in the link to the anonymous authentication.
Anonymous Authentication Order	Integer value indicating the order this item should appear in on the page
Game Console Registration Enabled	If enabled, the Game Console Registration option appears in the login menu.
Game Console Title	Text label above the link to the Game Console Registration.
Game Console Link Text	Text displayed in the link for the Game Console Registration.
Game Console Order	Integer value indicating the order this item should appear in on the page
Custom Registration Enabled	If enabled, the Custom Registration Option appears in the login menu.
Custom Registration Title	Text label above the link to the custom registration.
Custom Registration Link Text	Text displayed in the link for a custom device registration, such as a mobile device.
Custom Registration Order	Integer value indicating the order this item should appear in on the page.

Standard user login

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the first paragraph in the login page. Displays above the text entered in the Introduction property.
Left Column Content	Text displayed in the left column of the page.
Introduction	Text displayed in the first paragraph of the regular network user login page.
Secondary Text	Text displayed in the second paragraph of the regular network user login page.
Instructions	Select whether instructions will be included in this page, as a link to Instructions, or not at all. Instruction are entered in the Content Editor under Registration-Instructions.

Standard user login form

Setting	Definition
Form Title	Text label displayed at the top of the login form.
Form Action	Redirects the user to the next page in the sequence. Changing the form action to an unsupported page may affect functionality.
Success Page (Relative)	Relative URL to the success message. Changing this may affect supported functionality.
Missing Fields Message	Message displayed to the user if all required fields on the form are not completed.
Host Expiration Period Enabled	If enabled, the amount of time that the host can access the network is limited to the time entered in the Host Expiration Period Value field. The Host Expiration Period Value field defaults to hidden. The time value provided by the Administrator and is submitted with the rest of the form data.
Host Expiration Period Unit	The Unit of measurement for the amount of time that the host will be registered before expiry.
Host Expiration Period Value	The amount of time that the host will be registered before expiry.
Username Field Enabled	If enabled, displays a Username field on the form.

Setting	Definition
Username Field Required	If enabled, the user is required to complete this field on the form.
Username Field Label	Text label for the Username field on the form.
Username Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Username Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Password Field Enabled	If enabled, displays a password field on the form.
Password Field Required	If enabled, the user is required to complete this field on the form.
Password Field Label	Text label for password field on the form.
Password Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Password Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
First Name Field Enabled	If enabled, displays a First Name field on the form.
First Name Field Required	If enabled, the user is required to complete this field on the form.
First Name Field Label	Text label for the First Name field on the form.
First Name Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
First Name Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Last Name Field Enabled	If enabled, displays a Last Name field on the form.
Last Name Field Required	If enabled, the user is required to complete this field on the form.
Last Name Field Label	Text label for the Last Name field on the form.

Setting	Definition
Last Name Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Last Name Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Security and Access Value (S&A) Field Enabled	If enabled, displays a field for the Security and Access Value on the form.
S&A Field Required	If enabled, the user is required to complete the Address field on the form.
S&A Field Label	Text label for the S&A field on the form.
S&A Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Role Field Enabled	If enabled, network access is limited based on the Role Name in the Role Field Value field and the roles created under Go - Manage - Roles. Roles provide location-based access control.
Role Field Required	If enabled, this field must be completed to submit the form.
Role Field Label	Text label for the Role field on the form.
Role Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Role Field Value	Data entry field used to submit data with the form. Requires a role name. Roles are used to control network access. Typically this field is set by the administrator with the field type set to hidden. Role names must match those in the database. You can also create a list of roles for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green.
Title Field Enabled	If enabled, displays a field for the user's title on the form.
Title Field Required	If enabled, the user is required to complete this field on the form.
Title Field Label	Text label for the title field on the form.
Title Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.

Setting	Definition
Title Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Address Field Enabled	If enabled, displays a field for the user's address on the form.
Address Field Required	If enabled, the user is required to complete the Address field on the form.
Address Field Label	Text label for the Address field on the form.
Address Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Address Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
City Field Enabled	If enabled, displays a field for the user's city on the form.
City Field Required	If enabled, the user is required to complete this field on the form.
City Field Label	Text label for the City field on the form.
City Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
City Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
State/Province Field Enabled	If enabled, displays a State/Province field on the form.
State/Province Field Required	If enabled, the user is required to complete this field on the form.
State/Province Field Label	Text label for the State/Province field on the form.
State/Province Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.

Setting	Definition
State/Province Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Postal Code Field Enabled	If enabled, displays a Postal Code field on the form.
Postal Code Field Required	If enabled, the user is required to complete this field on the form.
Postal Code Field Label	Text label for the Postal Code field on the form.
Postal Code Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Postal Code Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Email Field Enabled	If enabled, displays a field for the user's e-mail on the form.
Email Field Required	If enabled, the user is required to complete this field on the form.
Email Field Label	Text label for the e-mail field on the form.
Email Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Email Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Phone Field Enabled	If enabled, displays a telephone number field on the form.
Phone Field Required	If enabled, the user is required to complete this field on the form.
Phone Field Label	Text label for the telephone number field on the form.
Phone Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.

Setting	Definition
Phone Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Hardware Description Field Enabled	If enabled, displays a field for to describe the user's hardware on the form.
Hardware Description Field Required	If enabled, the user is required to complete this field on the form.
Hardware Description Field Label	Text label for the hardware description field on the form.
Hardware Description Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Hardware Description Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Serial Number Field Enabled	If enabled, displays a field for the serial number of the user's PC or other device on the form.
Serial Number Field Required	If enabled, the user is required to complete this field on the form.
Serial Number Field Label	Text label for the field containing the serial number of the user's PC or other device on the form.
Serial Number Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Serial Number Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Hostname Field Enabled	If enabled, displays a field for the name of the user's PC or hostname on the form.
Hostname Field Required	If enabled, the user is required to complete this field on the form.
Hostname Field Label	Text label for the field containing the name of the user's PC or hostname on the form.

Setting	Definition
Hostname Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Hostname Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.

Self registration login

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Left Column Content	Text displayed in the left column of the page.
Request Page Title	Text title for the first paragraph in the guest self registration request page.
Request Page Introduction	Text introduction on the guest self registration request page.
Request Page Form Title	Title of the self registration request guest form.
Request Access Button Text	Text displayed in the button to request guest access from the guest self registration page.
Pending Page Title	Text title for the first paragraph in the guest self registration request page.
Default Sponsor Email	Email of the sponsor(s) to send requests and/or notifications to. If this is not provided, the user will be required to enter this in. To enter multiple sponsors, separate emails by commas.
Sponsor Email Label	Label for the field to enter in the Sponsor's Email. This field only appears when there is no Default Sponsor Email.
Notify Sponsor of Guest Details	When enabled, sponsors will be notified of the Guests credentials through email and/or SMS.
Accept Notification	Text to notify the user that their guest request has been accepted.
Login Username Label	Label for the field to enter in the user name on the Guest Self Registration login page.
Login Password Label	Label for the field to enter in the password on the Guest Self Registration login page.
Require Sponsor Approval	When enabled, approval by a sponsor will be required before guest accounts will be created.
Guest Request Expiration (minutes)	Number of minutes that guest request will remain valid. After this time, a sponsor will no longer be able to approve this request.

Setting	Definition
Request Pending Message	Text to display in the Self Registration Request pending page.
Deny Notification	Text to notify the user that their guest request has been denied.
Expired Notification	Text to notify the user that their guest request has expired.
Cancel Request Button Text	Text displayed in the button to cancel a guest request.
Message from Sponsor Header	Header for the Message from the Sponsor.
Sponsor Email Intro Text	When sponsor approval is required, this text will appear before the html link in the email that is sent to the sponsor.
Sponsor Approval Link Requires Login	When enabled, the html link the sponsor receives in email will require them to login before approving or denying the request. If disabled, clicking on an approve or deny link will approve or deny the request without further interaction.
Use Secure Mode for Sponsor Approval Links	When enabled, secure html links will be used to approve or deny requests in the email the sponsor receives.
Sponsor Email Login Link Text	Text for the login link in the email sent to the sponsor. Only used when Sponsor Approval Link Requires Login is selected.
Sponsor Email Approve Link Text	Text for the approve link in the email sent to the sponsor. Only used when Sponsor Approval Link Requires Login is not selected.
Sponsor Email Deny Link Text	Text for the deny link in the email sent to the sponsor. Only used when Sponsor Approval Link Requires Login is not selected.
Notify User via Portal Page	When enabled, guest user will be notified of their credentials in the portal page.
Show Password in Portal Page Notification	When enabled and Notify User via Portal Page is enabled, the guest account password will be displayed in plain text in the login form.
Notify User via Email	When enabled, guest user will be notified of their credentials through email.
Notify User via SMS	When enabled, guest user will be notified of their credentials through a SMS Message.
Default Guest Template	Name of the Default Guest Template to use.
Acceptable Use Policy	Options for displaying or not displaying an Acceptable Use Policy.
Acceptable Use Policy Checkbox Text	Text label for the checkbox to agree to the Acceptable Use Policy.
URL for Acceptable Use Policy	Optional URL to an Acceptable Use Policy which the user must agree to before being allowed to log in.
Link text for Acceptable Use Policy URL	Optional URL to an Acceptable Use Policy which the user must agree to before being allowed to log in.
Text for Acceptable Use Policy	Optional Text for an Acceptable Use Policy which the user must agree to before being allowed to log in.

Setting	Definition
Instructions	Select whether instructions will be included in this page, as a link to Instructions, or not at all. Instruction are entered in the Content Editor under Registration-Instructions.

Primary guest login

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the first paragraph in the primary guest login page. Displays above the text entered in the Introduction property.
Left Column Content	Text displayed in the left column of the page.
Introduction	Text introduction to the primary login for Guests and Contractors.
Form Title	Title of the guest registration form.
Username Label	Label for the user name field.
Password Label	Label for the password field.
Missing Fields	Message displayed when required fields are missing.
Instructions	Select whether instructions will be included in this page, as a link to Instructions, or not at all. Instruction are entered in the Content Editor under Registration-Instructions.

Secondary guest login

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the first paragraph in the secondary guest login page. Displays above the text entered in the Introduction property.
Left Column Content	Text displayed in the left column of the page.
Main Content	Text content displayed above the login form.
Introductory Paragraph	Introduction text displayed above the Main Content property in the page.
Form Button Text	Text displayed in the form button.
Account Expiration Label	Label for displaying the account expiration information.
Login Availability Label	Label for displaying the assailable times to log in.

MDM registration

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the first paragraph in the login page. Displays above the text entered in the Introduction property.
Left Column Content	Text displayed in the left column of the page.
Header	Text displayed above the links to the MDM apps.
Content	The main body text for the MDM Providers. This text should include all links to the MDM apps for each operating system.

Anonymous authentication

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Left Column Content	Text displayed in the left column of the page.
Role	The role to apply to guests who authenticate anonymously.
Acceptable Use Policy	Options for displaying or not displaying an Acceptable Use Policy.
Acceptable Use Policy Checkbox Text	Text label for the checkbox to agree to the Acceptable Use Policy.
URL for Acceptable Use Policy	Optional URL to an Acceptable Use Policy which the user must agree to before being allowed to log in.
Link text for Acceptable Use Policy URL	Optional URL to an Acceptable Use Policy which the user must agree to before being allowed to log in.
Text for Acceptable Use Policy	Optional Text for an Acceptable Use Policy which the user must agree to before being allowed to log in.

Game device registration

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Form Title	Title of the game console registration form.
Left Column Content	Text displayed in the left column of the page.
Introduction	Text introducing the purpose of the game console registration page.

Setting	Definition
Description	Text describing the registration process for game consoles.
IP address Field Enabled	If enabled, shows a field where the user may enter the IP address of their gaming device.
IP address Label	Label of the IP address form field.
Device Type Field Enabled	If enabled, shows a select box to select the device type as defined in the Device Types field.
Device Type Label	The text label for the Device Type form field.
Device Types (Value,Name : Value, Name)	Example: "Wii,Nintendo Wii : XBox 360 : Microsoft XBox 360
Device Type Error	The error displayed when a device type has not been selected.
MAC Address Example	Example MAC Address
IP address Example	Example IP address.
Role Field Enabled	If enabled, network access is limited based on the Role Name in the Role Field Value field and the roles created under Go - Manage - Roles. Roles provide location-based access control.
Role Field Label	Text label for the Role field on the form.
Role Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Role Field Value	Data entry field used to submit data with the form. Requires a role name. Roles are used to control network access. Typically this field is set by the administrator with the field type set to hidden. Role names must match those in the database. You can also create a list of roles for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green.
Validate Gaming Device OUI	When enabled, a valid gaming device OUI is required for registration using the Game Device Registration portal. When not enabled, a gaming device OUI is not required, meaning that any host can be registered using the Game Device Registration portal. This allows a host without access to a web browser, such as a printer, to be registered through the Game Device Registration portal.
Invalid MAC Address Error	Error message displayed to the user when the MAC address entered was invalid.
Invalid IP address Error	Error message displayed to the user when the IP address entered was invalid.

Game device help

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.

Setting	Definition
Title	Text title for the help page for gaming devices. Displays above the text entered in the Content property.
Left Column Content	Text displayed in the left column of the page.
Content	Instructional text on how to find the MAC addresses of specific game consoles.

Custom login

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the first paragraph in the custom login page. Displays above the text entered in the Introduction property.
Left Column Content	Text displayed in the left column of the page.
Introduction	Text introduction for the custom login page.
Secondary Text	Additional text which displays below the text entered in the Introduction property.
Instructions	Select whether instructions will be included in this page, as a link to Instructions, or not at all. Instruction are entered in the Content Editor under Registration-Instructions.

Custom login form

Setting	Definition
Form Title	Title of the form field set.
Form Action	Redirects the user to the next page in the sequence. Changing the form action to an unsupported page may affect functionality.
Success Page (Relative)	Relative URL to the success message. Changing this may affect supported functionality.
Missing Fields Message	Message displayed to the user if all required fields on the form are not completed.

Setting	Definition
Host Expiration Period Enabled	If enabled, the amount of time that the host can access the network is limited to the time entered in the Host Expiration Period Value field. The Host Expiration Period Value field defaults to hidden. The time value provided by the Administrator and is submitted with the rest of the form data.
Host Expiration Period Unit	The Unit of measurement for the amount of time that the host will be registered before expiry
Host Expiration Period Value	The amount of time that the host will be registered before expiry
Username Field Enabled	If enabled, displays a Username field on the form.
Username Field Required	If enabled, the user is required to complete this field on the form.
Username Field Label	Text label for the Username field on the form.
Username Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Username Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Password Field Enabled	If enabled, displays a password field on the form.
Password Field Required	If enabled, the user is required to complete this field on the form.
Password Field Label	Text label for password field on the form.
Password Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Password Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
First Name Field Enabled	If enabled, displays a First Name field on the form.
First Name Field Required	If enabled, the user is required to complete this field on the form.
First Name Field Label	Text label for the First Name field on the form.
First Name Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.

Setting	Definition
First Name Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Last Name Field Enabled	If enabled, displays a Last Name field on the form.
Last Name Field Required	If enabled, the user is required to complete this field on the form.
Last Name Field Label	Text label for the Last Name field on the form.
Last Name Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Last Name Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Security and Access Value (S&A) Field Enabled	If enabled, displays a field for the Security and Access Value on the form.
S&A Field Required	If enabled, the user is required to complete the Address field on the form.
S&A Field Label	Text label for the S&A field on the form.
S&A Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
S&A Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Role Field Enabled	If enabled, network access is limited based on the Role Name in the Role Field Value field and the roles created under Go - Manage - Roles. Roles provide location-based access control.
Role Field Required	If enabled, the user is required to complete this field on the form.
Role Field Label	Text label for the Role field on the form.
Role Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.

Setting	Definition
Role Field Value	Data entry field used to submit data with the form. Requires a role name. Roles are used to control network access. Typically this field is set by the administrator with the field type set to hidden. Role names must match those in the database. You can also create a list of roles for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green.
Title Field Enabled	If enabled, displays a field for the user's title on the form.
Title Field Required	If enabled, the user is required to complete this field on the form.
Title Field Label	Text label for the title field on the form.
Title Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Title Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Address Field Enabled	If enabled, displays a field for the user's address on the form.
Address Field Required	If enabled, the user is required to complete the Address field on the form.
Address Field Label	Text label for the Address field on the form.
Address Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Address Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
City Field Enabled	If enabled, displays a field for the user's city on the form.
City Field Required	If enabled, the user is required to complete this field on the form.
City Field Label	Text label for the City field on the form.
City Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.

Setting	Definition
City Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
State/Province Field Enabled	If enabled, displays a State/Province field on the form.
State/Province Field Required	If enabled, the user is required to complete this field on the form.
State/Province Field Label	Text label for the State/Province field on the form.
State/Province Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
State/Province Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Postal Code Field Enabled	If enabled, displays a Postal Code field on the form.
Postal Code Field Required	If enabled, the user is required to complete this field on the form.
Postal Code Field Label	Text label for the Postal Code field on the form.
Postal Code Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Postal Code Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Email Field Enabled	If enabled, displays a field for the user's e-mail on the form.
Email Field Required	If enabled, the user is required to complete this field on the form.
Email Field Label	Text label for the e-mail field on the form.
Email Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.

Setting	Definition
Email Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Phone Field Enabled	If enabled, displays a telephone number field on the form.
Phone Field Required	If enabled, the user is required to complete this field on the form.
Phone Field Label	Text label for the telephone number field on the form.
Phone Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Phone Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Hardware Description Field Enabled	If enabled, displays a field for to describe the user's hardware on the form.
Hardware Description Field Required	If enabled, the user is required to complete this field on the form.
Hardware Description Field Label	Text label for the hardware description field on the form.
Hardware Description Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Hardware Description Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Serial Number Field Enabled	If enabled, displays a field for the serial number of the user's PC or other device on the form.
Serial Number Field Required	If enabled, the user is required to complete this field on the form.
Serial Number Field Label	Text label for the field containing the serial number of the user's PC or other device on the form.

Setting	Definition
Serial Number Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Serial Number Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Hostname Field Enabled	If enabled, displays a field for the host name of the user's PC or other device on the form.
Hostname Field Required	If enabled, the user is required to complete this field on the form.
Hostname Field Label	Text label for the field containing the name of the user's PC or hostname on the form.
Hostname Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Hostname Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.

Profile configuration download

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Left Column Content	Text displayed in the left column of the page.
Introduction	Introductory text explaining what steps need to be taken.
Download Link Prefix	Text displayed before the download link.
Download Link	Text displayed as a link.
Download Link Suffix	Text displayed after the download link.
Button Text	Text displayed on the button on the profile download page.

Mobile Agent download

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Left Column Content	Text displayed in the left column of the page.
Profile Introduction	Introductory text explaining what steps need to be taken with respect to configuration profile installation.
Profile Download Link Prefix	Text displayed before the profile download link.
Profile Download Link	Text displayed as a link.
Profile Download Link Suffix	Text displayed after the profile download link.
Introduction	Introductory text explaining what steps need to be taken.
Download Link Prefix	Text displayed before the download link.
Download Link	Text displayed as a link.
Download Link Suffix	Text displayed after the download link.

Instructions

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the instructions page. Displays above the text entered in the Introduction property.
Left Column Content	Text displayed in the left column of the page.
Introduction	Text introduction to the instructions page.
Show Windows Instructions	If enabled, display instructions for computers running Windows.
Windows Instructions	Instructional text for computers running Windows.
Show macOS Instructions	If enabled, display instructions for computers running macOS.
macOS Instructions	Instructional text for computers running macOS.
Show Linux Instructions	If enabled, display instructions for computers running Linux.
Linux Instructions	Instructional text for computers running Linux.
Show Other Instructions	If enabled, display instructions for other computers.
Other Instructions Title	Text displayed as the title for the instructions for other computers.
Other Instructions	Instructional text for other computers.
Display as Accordion View	Use JavaScript to display the instructions as an accordion. Requires the global "Use JavaScript UI Enhancements" property to be enabled.

Usage policy

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the usage policy. Displays above the text entered in the Usage Policy Contents property.
Left Column Content	Text displayed in the left column of the page.
Usage Policy Contents	Contents of the Usage Policy.

Usage policy disagreement

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the first paragraph in Acceptable Use Policy Disagreement page. Displays above the text entered in the Disagree Instructions property.
Left Column Content	Text displayed in the left column of the page.
Disagree Instructions	Instructional text for users who disagree with the usage policy.
Start Again Instructions	Instructions for getting back to the usage policy.

Client certificate download

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the Client Certificate Download page. Displays above the text entered in the Introduction property.
Left Column Content	Text displayed in the left column of the page.
Introduction	Text introduction to the instructions page.
Secondary Text	Text displayed in the second paragraph of the certificate download page. This is an HTML fieldand HTML may be freely entered in this field.
Session Expired Message	Text displayed when the server is unable to find an existing session to determine the user who is currently logged into the portal. This field contains contents which are output as strings in JavaScript. Certain special characters may be escaped or removed.

Setting	Definition
Missing Certificate Message	Text displayed when no existing certificate could be found for the user. This is a mixed text field. HTML may be included, but may not always be rendered.
Download Link Prefix	Text displayed before the download link. This is a mixed text field. HTML may be included, but may not always be rendered.
Download Link	Text displayed as a link. This is a mixed text field. HTML may be included, but may not always be rendered.
Download Link Suffix	Text displayed after the download link. This is a mixed text field. HTML may be included, but may not always be rendered.
Resubmit Request Link Prefix	Text displayed before the download link. This is a mixed text field. HTML may be included, but may not always be rendered.
Resubmit Request Link	Text displayed as a link. This is a mixed text field. HTML may be included, but may not always be rendered.
Resubmit Request Link Suffix	Text displayed after the download link. This is a mixed text field. HTML may be included, but may not always be rendered.
Continue Link Prefix	Text displayed before the download link. This is a mixed text field. HTML may be included, but may not always be rendered.
Continue Link	Text displayed as a link. This is a mixed text field. HTML may be included, but may not always be rendered.
Continue Link Suffix	Text displayed after the download link. This is a mixed text field. HTML may be included, but may not always be rendered.

Success

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the success page. Indicates that the user has successfully registered. Displays at the top of the content section.
Left Column Content	Text displayed in the left column of the page.
Progress Bar Enabled	If checked, display a progress bar and display the Finished Message.
Progress Bar Title	Title displayed above all text in the contents pane.
Please Wait Message	Message displayed to the user while the progress bar moves. To change the amount of time the message and progress bar are displayed, modify the default 45 second countdown number.
Success Message	Message displayed to indicate successful completion of the process.
Finished Message	Appears after the progress bar has finished.

Authentication

Configure the settings and behavior of your portal pages for authenticating hosts on your network. This includes settings for remote scanning.

Common

Setting	Definition
Context Title	Text label to indicate the functional purpose of the context.

Login menu

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the first paragraph in the guest login page. Displays above the text entered in the Introduction property.
Left Column Content	Text displayed in the left column of the login page.
Text Content	Text introducing the login menu for Authentication.
Standard Login Enabled	When enabled, the Standard login option appears in the login menu.
Standard Login Title	Short text to indicate who should use the standard login.
Standard Login Link	Text displayed below the link for the Standard login.
Standard Login Order	Integer value indicating the order this item should appear in on the page.
Guest Login Enabled	When enabled, the Guest Login option appears in the login menu.
Guest Login Title	Short text to indicate who should use the standard login.
Guest Login Link	Text displayed as a link to the Guest Access page.
Guest Login Order	Integer value indicating the order this item should appear in on the page.
Custom Registration Enabled	If enabled, the Custom Registration Option appears in the login menu.
Custom Registration Title	Text label above the link to the custom registration.
Custom Registration Link Text	Text displayed in the link for a custom device registration, such as a mobile device.
Custom Registration Order	Integer value indicating the order this item should appear in on the page.

Standard user login

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Title displayed above the contents of the Introduction property.
Left Column Content	Text displayed in the left column of the login page.
Introduction	Text introduction to the Standard Login page.
Secondary Text	Text displayed above the login form.
Instructions	Select whether instructions will be included in this page, as a link to Instructions, or not at all. Instruction are entered in the Content Editor under Authentication-Instructions.
Scan Registered Hosts	If enabled, scan the host using Dissolvable or Persistent Agent, if a Security Policy is applicable.
Scan Rogue Hosts	If enabled, scan a rogue host using Dissolvable or Persistent Agent, if a Security Policy is applicable.
Register Rogue Hosts	If enabled, register a rogue host.

Standard user login form

Setting	Definition
Form Title	Text title of the login form field set.
Form Action	Redirects the user to the next page in the sequence. Changing the form action to an unsupported page may affect functionality.
Success Page (Relative)	Relative URL to the success message. Changing this may affect supported functionality.
Missing Fields Message	Message displayed to the user if all required fields on the form are not completed.
Host Expiration Period Enabled	If enabled, the amount of time that the host can access the network is limited to the time entered in the Host Expiration Period Value field. The Host Expiration Period Value field defaults to hidden. The time value provided by the Administrator and is submitted with the rest of the form data.

Setting	Definition
Host Expiration Period Unit	The Unit of measurement for the amount of time that the host will be registered before expiry.
Host Expiration Period Value	The amount of time that the host will be registered before expiry.
Username Field Enabled	If enabled, displays a Username field on the form.
Username Field Required	If enabled, the user is required to complete this field on the form.
Username Field Label	Text label for the Username field on the form.
Username Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Username Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Password Field Enabled	If enabled, displays a password field on the form.
Password Field Required	If enabled, the user is required to complete this field on the form.
Password Field Label	Text label for password field on the form.
Password Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Password Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
First Name Field Enabled	If enabled, displays a First Name field on the form.
First Name Field Required	If enabled, the user is required to complete this field on the form.
First Name Field Label	Text label for the First Name field on the form.
First Name Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.

Setting	Definition
First Name Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Last Name Field Enabled	If enabled, displays a Last Name field on the form.
Last Name Field Required	If enabled, the user is required to complete this field on the form.
Last Name Field Label	Text label for the Last Name field on the form.
Last Name Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Last Name Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Security and Access Value (S&A) Field Enabled	If enabled, displays a field for the Security and Access Value on the form.
S&A Field Required	If enabled, the user is required to complete the Address field on the form.
S&A Field Label	Text label for the S&A field on the form.
S&A Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
S&A Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Role Field Enabled	If enabled, network access is limited based on the Role Name in the Role Field Value field and the roles created under Go - Manage - Roles. Roles provide location-based access control.
Role Field Required	If enabled, the user is required to complete this field on the form.
Role Field Label	Text label for the Role field on the form.
Role Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.

Setting	Definition
Role Field Value	Data entry field used to submit data with the form. Requires a role name. Roles are used to control network access. Typically this field is set by the administrator with the field type set to hidden. Role names must match those in the database. You can also create a list of roles for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green.
Title Field Enabled	If enabled, displays a field for the user's title on the form.
Title Field Required	If enabled, the user is required to complete this field on the form.
Title Field Label	Text label for the title field on the form.
Title Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Title Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Address Field Enabled	If enabled, displays a field for the user's address on the form.
Address Field Required	If enabled, the user is required to complete the Address field on the form.
Address Field Label	Text label for the Address field on the form.
Address Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Address Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
City Field Enabled	If enabled, displays a field for the user's city on the form.
City Field Required	If enabled, the user is required to complete this field on the form.
City Field Label	Text label for the City field on the form.
City Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.

Setting	Definition
City Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
State/Province Field Enabled	If enabled, displays a State/Province field on the form.
State/Province Field Required	If enabled, the user is required to complete this field on the form.
State/Province Field Label	Text label for the State/Province field on the form.
State/Province Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
State/Province Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Postal Code Field Enabled	If enabled, displays a Postal Code field on the form.
Postal Code Field Required	If enabled, the user is required to complete this field on the form.
Postal Code Field Label	Text label for the Postal Code field on the form.
Postal Code Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Postal Code Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Email Field Enabled	If enabled, displays a field for the user's e-mail on the form.
Email Field Required	If enabled, the user is required to complete this field on the form.
Email Field Label	Text label for the e-mail field on the form.
Email Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.

Setting	Definition
Email Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Phone Field Enabled	If enabled, displays a telephone number field on the form.
Phone Field Required	If enabled, the user is required to complete this field on the form.
Phone Field Label	Text label for the telephone number field on the form.
Phone Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Phone Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Organization Field Enabled	If enabled, displays a organization field on the form.
Organization Field Required	If enabled, the user is required to complete this field on the form.
Organization Field Label	Text label for the organization field on the form.
Organization Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Organization Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Hardware Description Field Enabled	If enabled, displays a field for to describe the user's hardware on the form.
Hardware Description Field Required	If enabled, the user is required to complete this field on the form.
Hardware Description Field Label	Text label for the hardware description field on the form.
Hardware Description Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.

Setting	Definition
Hardware Description Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Serial Number Field Enabled	If enabled, displays a field for the serial number of the user's PC or other device on the form.
Serial Number Field Required	If enabled, the user is required to complete this field on the form.
Serial Number Field Label	Text label for the field containing the serial number of the user's PC or other device on the form.
Serial Number Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Serial Number Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Hostname Field Enabled	If enabled, displays a field for the name of the user's PC or hostname on the form.
Hostname Field Required	If enabled, the user is required to complete this field on the form.
Hostname Field Label	Text label for the field containing the name of the user's PC or hostname on the form.
Hostname Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Hostname Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.

Primary guest login

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for guest login and authentication page. Displays at the top of the

Setting	Definition
	content section of the page above the Introduction property.
Left Column Content	Text displayed in the left column of the page.
Introduction	Introductory text to describe the Guest process.
Form Title	Title of the guest authentication form.
Username Label	Label for the user name field.
Password Label	Label for the password field.
Missing Fields	Message displayed when required fields are missing.
Instructions	Select whether instructions will be included in this page, as a link to Instructions, or not at all. Instruction are entered in the Content Editor under Authentication-Instructions.

Secondary guest login

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the first paragraph in the secondary guest login page. Displays above the text entered in the Introduction property.
Left Column Content	Text displayed in the left column of the page.
Main Content	Text content displayed above the login form.
Introductory Paragraph	Introduction text displayed above the Main Content property in the page.
Form Button Text	Text displayed in the form button.
Account Expiration Label	Label for displaying the account expiration information.
Login Availability Label	Label for displaying the available times to log in.

Custom login

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the first paragraph in the custom login page. Displays above the text entered in the Introduction property.

Setting	Definition
Left Column Content	Text displayed in the left column of the page.
Introduction	Text introduction for the custom login page.
Secondary Text	Additional text which displays below the text entered in the Introduction property.
Instructions	Select whether instructions will be included in this page, as a link to Instructions, or not at all. Instruction are entered in the Content Editor under Authentication-Instructions.
Scan Registered Hosts	If enabled, scan the host using Dissolvable or Persistent Agent, if a Security Policy is applicable.
Scan Rogue Hosts	If enabled, scan a rogue host using Dissolvable or Persistent Agent, if a Security Policy is applicable.
Register Rogue Hosts	If enabled, register a rogue host.

Custom login form

Setting	Definition
Form Title	Title of the form field set.
Form Action	Redirects the user to the next page in the sequence. Changing the form action to an unsupported page may affect functionality.
Success Page (Relative)	Relative URL to the success message. Changing this may affect supported functionality.
Missing Fields Message	Message displayed to the user if all required fields on the form are not completed.
Host Expiration Period Enabled	If enabled, the amount of time that the host can access the network is limited to the time entered in the Host Expiration Period Value field. The Host Expiration Period Value field defaults to hidden. The time value provided by the Administrator and is submitted with the rest of the form data.
Host Expiration Period Unit	The Unit of measurement for the amount of time that the host will be registered before expiry
Host Expiration Period Value	The amount of time that the host will be registered before expiry.
Username Field Enabled	If enabled, displays a Username field on the form.
Username Field Required	If enabled, the user is required to complete this field on the form.

Setting	Definition
Username Field Label	Text label for the Username field on the form.
Username Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Username Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Password Field Enabled	If enabled, displays a password field on the form.
Password Field Required	If enabled, the user is required to complete this field on the form.
Password Field Label	Text label for password field on the form.
Password Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Password Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
First Name Field Enabled	If enabled, displays a First Name field on the form.
First Name Field Required	If enabled, the user is required to complete this field on the form.
First Name Field Label	Text label for the First Name field on the form.
First Name Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
First Name Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Last Name Field Enabled	If enabled, displays a Last Name field on the form.
Last Name Field Required	If enabled, the user is required to complete this field on the form.
Last Name Field Label	Text label for the Last Name field on the form.

Setting	Definition
Last Name Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Last Name Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Security and Access Value (S&A) Field Enabled	If enabled, displays a field for the Security and Access Value on the form.
S&A Field Required	If enabled, the user is required to complete the Address field on the form.
S&A Field Label	Text label for the S&A field on the form.
S&A Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
S&A Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Role Field Enabled	If enabled, network access is limited based on the Role Name in the Role Field Value field and the roles created under Go - Manage - Roles. Roles provide location-based access control.
Role Field Required	If enabled, the user is required to complete this field on the form.
Role Field Label	Text label for the Role field on the form.
Role Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Role Field Value	Data entry field used to submit data with the form. Requires a role name. Roles are used to control network access. Typically this field is set by the administrator with the field type set to hidden. Role names must match those in the database. You can also create a list of roles for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green.
Title Field Enabled	If enabled, displays a field for the user's title on the form.
Title Field Required	If enabled, the user is required to complete this field on the form.
Title Field Label	Text label for the title field on the form.

Setting	Definition
Title Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Title Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Address Field Enabled	If enabled, displays a field for the user's address on the form.
Address Field Required	If enabled, the user is required to complete the Address field on the form.
Address Field Label	Text label for the Address field on the form.
Address Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Address Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
City Field Enabled	If enabled, displays a field for the user's city on the form.
City Field Required	If enabled, the user is required to complete this field on the form.
City Field Label	Text label for the City field on the form.
City Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
City Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
State/Province Field Enabled	If enabled, displays a State/Province field on the form.
State/Province Field Required	If enabled, the user is required to complete this field on the form.
State/Province Field Label	Text label for the State/Province field on the form.

Setting	Definition
State/Province Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
State/Province Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Postal Code Field Enabled	If enabled, displays a Postal Code field on the form.
Postal Code Field Required	If enabled, the user is required to complete this field on the form.
Postal Code Field Label	Text label for the Postal Code field on the form.
Postal Code Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Postal Code Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Email Field Enabled	If enabled, displays a field for the user's e-mail on the form.
Email Field Required	If enabled, the user is required to complete this field on the form.
Email Field Label	Text label for the e-mail field on the form.
Email Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Email Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Phone Field Enabled	If enabled, displays a telephone number field on the form.
Phone Field Required	If enabled, the user is required to complete this field on the form.
Phone Field Label	Text label for the telephone number field on the form.

Setting	Definition
Phone Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Phone Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Organization Field Enabled	If enabled, displays a organization field on the form.
Organization Field Required	If enabled, the user is required to complete this field on the form.
Organization Field Label	Text label for the organization field on the form.
Organization Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Organization Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Hardware Description Field Enabled	If enabled, displays a field for to describe the user's hardware on the form.
Hardware Description Field Required	If enabled, the user is required to complete this field on the form.
Hardware Description Field Label	Text label for the hardware description field on the form.
Hardware Description Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Hardware Description Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Serial Number Field Enabled	If enabled, displays a field for the serial number of the user's PC or other device on the form.
Serial Number Field Required	If enabled, the user is required to complete this field on the form.

Setting	Definition
Serial Number Field Label	Text label for the field containing the serial number of the user's PC or other device on the form.
Serial Number Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Serial Number Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Hostname Field Enabled	If enabled, displays a field for the host name of the user's PC or other device on the form.
Hostname Field Required	If enabled, the user is required to complete this field on the form.
Hostname Field Label	Text label for the field containing the name of the user's PC or hostname on the form.
Hostname Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Hostname Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.

Authentication failure

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for authentication failure page. Displays at the top of the content section of the page.
Left Column Content	Text displayed in the left column of the page.
Description	Failure Text displayed when the user failed to authenticate.

Remote scan index

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being

Setting	Definition
	used, the title also displays on the appropriate tab.
Title	Text title for remote scan index page. Displays at the top of the content section of the page.
Left Column Content	Text displayed in the left column of the page.
Scan Name	Name of the security policy to scan remote computers against.
Description	Brief description and instructional text for the Remote Scan process.

Remote scan success

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for remote scan success page. Displays at the top of the content section of the page.
Left Column Content	Text displayed in the left column of the page.
Success Message	Message displayed to the user after the remote scanning process completed successfully.

Log off form

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the log off form. Displays above the logout fields.
Left Column Content	Text displayed in the left column of the page.
Description	Text displayed above the Logout button.

Log off success

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title displayed above the Success Message.
Left Column Content	Text displayed in the left column of the page.
Success Message	Message displayed upon successful log off.

Profile configuration download

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Left Column Content	Text displayed in the left column of the page.
Introduction	Introductory text explaining what steps need to be taken.
Download Link Prefix	Text displayed before the download link.
Download Link	Text displayed as a link.
Download Link Suffix	Text displayed after the download link.
Button Text	Text displayed on the button on the profile download page.

Mobile Agent download

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Left Column Content	Text displayed in the left column of the page.
Introduction	Introductory text explaining what steps need to be taken.
Download Link Prefix	Text displayed before the download link.
Download Link	Text displayed as a link.
Download Link Suffix	Text displayed after the download link.

Instructions

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the instructions page. Displays at the top of the content section of the page above the Introduction property.
Left Column Content	Text displayed in the left column of the page.
Introduction	Introductory text explaining what steps need to be taken.
Show Windows Instructions	If enabled, displays instructions for computers running Windows.
Windows Instructions	Instructions for computers running Windows.
Show macOS Instructions	If enabled, displays instructions for computers running macOS.

Setting	Definition
macOS Instructions	Instructions for computers running macOS.
Show Linux Instructions	If enabled, shows instructions for computers running Linux.
Linux Instructions	Instructions for computers running Linux.
Show Other Instructions	If enabled, show instructions for other computers.
Other Instructions Title	Text title of the instructions for other computers.
Other Instructions	Instructions for other computers.
Display as Accordion View	Use JavaScript to display the instructions as an accordion.

Success

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title displayed above the Success Message contents.
Left Column Content	Text displayed in the left column of the page.
Progress Bar Enabled	If checked, display a progress bar and display the finished message.
Progress Bar Title	Text title for the progress bar.
Please Wait Message	Message displayed to the user while the progress bar moves. To change the amount of time the message and progress bar are displayed, modify the default 45 second countdown number.
Success Message	Message displayed to the user upon successful authentication.
Finished Message	Appears after the progress bar has finished.

Remediation

Configure the settings and behavior of your portal pages for hosts in remediation.

Common

Setting	Definition
Context Title	Text label to indicate the functional purpose of the context.

Index (redirect)

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Title displayed above the Description property contents.
Left Column Content	Text displayed in the left column of the login page.
Description	Text describing what is happening.

Dissolvable Agent rescan (login)

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Title displayed above the Description property contents.
Form Title	Text label displayed at the top of the login form.
Left Column Content	Text displayed in the left column of the login page.
Instructions	Instructional text displayed above the login form.
Username Field Label	Text label for the Username field on the form.
Password Field Label	Text label for the Password field on the form.
Authenticate Users	If enabled, authenticate users upon successful scanning.
Missing Fields Message	Message displayed to the user if all required fields on the form are not completed.

Dissolvable Agent rescan (no login)

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Title displayed above the Instructions property contents.
Left Column Content	Text displayed in the left column of the login page.
Instructions	Instructional text displayed above the download form.

Agent download

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Left Column Content	Text displayed in the left column of the login page.
Introduction	Introductory text explaining what steps need to be taken.
Download Link Prefix	Text displayed before the download link.
Download Link	Text displayed as a link.
Download Link Suffix	Text displayed after the download link.

Profile configuration download

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Left Column Content	Text displayed in the left column of the login page.
Introduction	Introductory text explaining what steps need to be taken.
Download Link Prefix	Text displayed before the download link.
Download Link	Text displayed as a link.
Download Link Suffix	Text displayed after the download link.
Button Text	Text displayed on the button on the profile download page.

Mobile Agent download

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Left Column Content	Text displayed in the left column of the login page.
Introduction	Introductory text explaining what steps need to be taken.
Download Link Prefix	Text displayed before the download link.
Download Link	Text displayed as a link.
Download Link Suffix	Text displayed after the download link.

Instructions

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Title displayed above the Introduction property contents.
Left Column Content	Text displayed in the left column of the login page.
Introduction	Introductory text explaining what steps need to be taken.
Show Windows Instructions	If enabled, display instructions for computers running Windows.
Windows Instructions	Instructional text for computers running Windows.
Show macOS Instructions	If enabled, display instructions for computers running macOS.
macOS Instructions	Instructional text for computers running macOS.
Show Linux Instructions	If enabled, display instructions for computers running Linux.
Linux Instructions	Instructional text for computers running Linux.
Show Other Instructions	If enabled, display instructions for other computers.
Other Instructions Title	Title of the instructions for other computers.
Other Instructions	Instructional text for other computers.
Display as Accordion View	Use JavaScript to display the instructions as an accordion.

Failure index

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Title displayed above the lists of failures.
Contents	Expanded text contents displayed below the title.
Left Column Content	Text displayed in the left column of the page.

Success

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Title displayed above the Remediation Successful property contents.
Left Column Content	Text displayed in the left column of the page.

Setting	Definition
Please Wait Message	Message displayed to the user while the progress bar moves. To change the amount of time the message and progress bar are displayed, modify the default 45 second countdown number.
Progress Bar Enabled	If checked, display a progress bar and display the finished message.
Progress Bar Title	Title for the progress bar.
Finished Message	Message displayed when the progress bar finishes.
Remediation Successful	Text displayed when the remediation process is completed successfully.
Proactive Scan Successful	Text displayed when the Proactive Scan is completed successfully.

VPN portal

Configure the settings and behavior of your portal pages specifically for VPN access.

Common

Setting	Definition
Context Title	Text label to indicate the functional purpose of the context.

Index (redirect)

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Title displayed above the Description property contents.
Left Column Content	Text displayed in the left column of the login page.
Description	Text describing the redirect.

Download page

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the first paragraph in the download page. Displays above the text entered in the Introduction property.
Left Column Content	Text displayed in the left column of the login page.
Introduction	Text displayed in the first paragraph of the regular network user login page.
Secondary Text	Text displayed in the second paragraph of the regular network user login page.

Setting	Definition
Instructions	Select whether instructions will be included in this page, as a link to Instructions, or not at all. Instruction are entered in the content editor under VPN instructions.

Download page form

Setting	Definition
Form Title	Text label displayed at the top of the login form.
Form Action	Redirects the user to the next page in the sequence. 💡 Changing the form action to an unsupported page may affect functionality.
Success Page (Relative)	Relative URL to the success message. 💡 Changing this may affect supported functionality.
Missing Fields Message	Message displayed to the user if all required fields on the form are not completed.
Host Expiration Period Enabled	If enabled, the amount of time that the host can access the network is limited to the time entered in the Host Expiration Period Value field. The Host Expiration Period Value field defaults to hidden. The time value provided by the Administrator and is submitted with the rest of the form data.
Host Expiration Period Unit	The Unit of measurement for the amount of time that the host will be registered before expiry.
Host Expiration Period Value	The amount of time that the host will be registered before expiry.
Username Field Enabled	If enabled, displays a Username field on the form.
Username Field Required	If enabled, the user is required to complete this field on the form.
Username Field Label	Text label for the Username field on the form.
Username Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Username Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.

Setting	Definition
Password Field Enabled	If enabled, displays a password field on the form.
Password Field Required	If enabled, the user is required to complete this field on the form.
Password Field Label	Text label for password field on the form.
Password Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Password Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
First Name Field Enabled	If enabled, displays a First Name field on the form.
First Name Field Required	If enabled, the user is required to complete this field on the form.
First Name Field Label	Text label for the First Name field on the form.
First Name Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
First Name Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Last Name Field Enabled	If enabled, displays a Last Name field on the form.
Last Name Field Required	If enabled, the user is required to complete this field on the form.
Last Name Field Label	Text label for the Last Name field on the form.
Last Name Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Last Name Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Security and Access Value (S&A) Field Enabled	If enabled, displays a field for the Security and Access Value on the form.

Setting	Definition
S&A Field Required	If enabled, the user is required to complete the Address field on the form.
S&A Field Label	Text label for the S&A field on the form.
S&A Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
S&A Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Role Field Enabled	If enabled, network access is limited based on the Role Name in the Role Field Value field and the roles created under Go - Manage - Roles. Roles provide location-based access control.
Role Field Required	If enabled, this field must be completed to submit the form.
Role Field Label	Text label for the Role field on the form.
Role Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Role Field Value	Data entry field used to submit data with the form. Requires a role name. Roles are used to control network access. Typically this field is set by the administrator with the field type set to hidden. Role names must match those in the database. You can also create a list of roles for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green.
Title Field Enabled	If enabled, displays a field for the user's title on the form.
Title Field Required	If enabled, the user is required to complete this field on the form.
Title Field Label	Text label for the title field on the form.
Title Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Title Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Address Field Enabled	If enabled, displays a field for the user's address on the form.

Setting	Definition
Address Field Required	If enabled, the user is required to complete the Address field on the form.
Address Field Label	Text label for the Address field on the form.
Address Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Address Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
City Field Enabled	If enabled, displays a field for the user's city on the form.
City Field Required	If enabled, the user is required to complete this field on the form.
City Field Label	Text label for the City field on the form.
City Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
City Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
State/Province Field Enabled	If enabled, displays a State/Province field on the form.
State/Province Field Required	If enabled, the user is required to complete this field on the form.
State/Province Field Label	Text label for the State/Province field on the form.
State/Province Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
State/Province Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Postal Code Field Enabled	If enabled, displays a Postal Code field on the form.
Postal Code Field Required	If enabled, the user is required to complete this field on the form.
Postal Code Field Label	Text label for the Postal Code field on the form.

Setting	Definition
Postal Code Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Postal Code Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Email Field Enabled	If enabled, displays a field for the user's e-mail on the form.
Email Field Required	If enabled, the user is required to complete this field on the form.
Email Field Label	Text label for the e-mail field on the form.
Email Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Email Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Phone Field Enabled	If enabled, displays a telephone number field on the form.
Phone Field Required	If enabled, the user is required to complete this field on the form.
Phone Field Label	Text label for the telephone number field on the form.
Phone Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Phone Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Hardware Description Field Enabled	If enabled, displays a field for to describe the user's hardware on the form.
Hardware Description Field Required	If enabled, the user is required to complete this field on the form.
Hardware Description Field Label	Text label for the hardware description field on the form.

Setting	Definition
Hardware Description Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Hardware Description Field Value	Data entry field provided for user. You have the option to enter a default value for the field that can be overridden by the user or a list of items for selection. If the field type is set to hidden, you can submit a hidden value with the form.
Serial Number Field Enabled	If enabled, displays a field for the serial number of the user's PC or other device on the form.
Serial Number Field Required	If enabled, the user is required to complete this field on the form.
Serial Number Field Label	Text label for the field containing the serial number of the user's PC or other device on the form.
Serial Number Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Serial Number Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Hostname Field Enabled	If enabled, displays a field for the name of the user's PC or hostname on the form.
Hostname Field Required	If enabled, the user is required to complete this field on the form.
Hostname Field Label	Text label for the field containing the name of the user's PC or hostname on the form.
Hostname Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Hostname Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.

Profile configuration download

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being

Setting	Definition
	used, the title also displays on the appropriate tab.
Left Column Content	Text displayed in the left column of the page.
Introduction	Introductory text explaining what steps need to be taken.
Download Link Prefix	Text displayed before the download link.
Download Link	Text displayed as a link.
Download Link Suffix	Text displayed after the download link.
Button Text	Text displayed on the button on the profile download page.

Mobile Agent download

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Left Column Content	Text displayed in the left column of the page.
Introduction	Introductory text explaining what steps need to be taken.
Download Link Prefix	Text displayed before the download link.
Download Link	Text displayed as a link.
Download Link Suffix	Text displayed after the download link.

Instructions

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Title displayed above the Introduction property contents.
Left Column Content	Text displayed in the left column of the page.
Introduction	Text introduction to the instructions page.
Show Windows Instructions	If enabled, display instructions for computers running Windows.
Windows Instructions	Instructional text for computers running Windows.
Show macOS Instructions	If enabled, display instructions for computers running macOS.
macOS Instructions	Instructional text for computers running macOS.
Show Linux Instructions	If enabled, display instructions for computers running Linux.
Linux Instructions	Instructional text for computers running Linux.

Setting	Definition
Show Other Instructions	If enabled, display instructions for other computers.
Other Instructions Title	Title of the instructions for other computers.
Other Instructions	Instructional text for other computers.
Display as Accordion View	Use JavaScript to display the instructions as an accordion.

User login (in-line only)

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the first paragraph in the login page. Displays above the text entered in the Introduction property.
Left Column Content	Text displayed in the left column of the page.
Introduction	Text displayed in the first paragraph of the regular network user login page.
Secondary Text	Text displayed in the second paragraph of the regular network user login page.
Instructions	Select whether instructions will be included in this page, as a link to Instructions, or not at all. Instruction are entered in the Content Editor under VPN-Instructions.

User login form (in-line only)

Setting	Definition
Form Title	Text label displayed at the top of the login form.
Form Action	Redirects the user to the next page in the sequence. 💡 Changing the form action to an unsupported page may affect functionality.
Success Page (Relative)	Relative URL to the success message. 💡 Changing this may affect supported functionality.
Missing Fields Message	Message displayed to the user if all required fields on the form are not completed.
Host Expiration Period Enabled	If enabled, the amount of time that the host can access the network is limited to the time entered in the Host Expiration Period Value field. The Host Expiration Period Value field defaults to hidden. The time value provided by the

Setting	Definition
	Administrator and is submitted with the rest of the form data.
Host Expiration Period Unit	The Unit of measurement for the amount of time that the host will be registered before expiry.
Host Expiration Period Value	The amount of time that the host will be registered before expiry.
Username Field Enabled	If enabled, displays a Username field on the form.
Username Field Required	If enabled, the user is required to complete this field on the form.
Username Field Label	Text label for the Username field on the form.
Username Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Username Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Password Field Enabled	If enabled, displays a password field on the form.
Password Field Required	If enabled, the user is required to complete this field on the form.
Password Field Label	Text label for password field on the form.
Password Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Password Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
First Name Field Enabled	If enabled, displays a First Name field on the form.
First Name Field Required	If enabled, the user is required to complete this field on the form.
First Name Field Label	Text label for the First Name field on the form.
First Name Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.

Setting	Definition
First Name Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Last Name Field Enabled	If enabled, displays a Last Name field on the form.
Last Name Field Required	If enabled, the user is required to complete this field on the form.
Last Name Field Label	Text label for the Last Name field on the form.
Last Name Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Last Name Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Security and Access Value (S&A) Field Enabled	If enabled, displays a field for the Security and Access Value on the form.
S&A Field Required	If enabled, the user is required to complete the Address field on the form.
S&A Field Label	Text label for the S&A field on the form.
S&A Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
S&A Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Role Field Enabled	If enabled, network access is limited based on the Role Name in the Role Field Value field and the roles created under Go - Manage - Roles. Roles provide location-based access control.
Role Field Required	If enabled, this field must be completed to submit the form.
Role Field Label	Text label for the Role field on the form.
Role Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.

Setting	Definition
Role Field Value	Data entry field used to submit data with the form. Requires a role name. Roles are used to control network access. Typically this field is set by the administrator with the field type set to hidden. Role names must match those in the database. You can also create a list of roles for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green.
Title Field Enabled	If enabled, displays a field for the user's title on the form.
Title Field Required	If enabled, the user is required to complete this field on the form.
Title Field Label	Text label for the title field on the form.
Title Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Title Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Address Field Enabled	If enabled, displays a field for the user's address on the form.
Address Field Required	If enabled, the user is required to complete the Address field on the form.
Address Field Label	Text label for the Address field on the form.
Address Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Address Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
City Field Enabled	If enabled, displays a field for the user's city on the form.
City Field Required	If enabled, the user is required to complete this field on the form.
City Field Label	Text label for the City field on the form.
City Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.

Setting	Definition
City Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
State/Province Field Enabled	If enabled, displays a State/Province field on the form.
State/Province Field Required	If enabled, the user is required to complete this field on the form.
State/Province Field Label	Text label for the State/Province field on the form.
State/Province Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
State/Province Field Value	Data entry field provided for the user. You have the option to enter a default value for the field that can be overridden by the user or a list of items for selection. If the field type is set to hidden, you can submit a hidden value with the form.
Postal Code Field Enabled	If enabled, displays a Postal Code field on the form.
Postal Code Field Required	If enabled, the user is required to complete this field on the form.
Postal Code Field Label	Text label for the Postal Code field on the form.
Postal Code Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Postal Code Field Value	Data entry field provided for the user. You have the option to enter a default value for the field that can be overridden by the user or a list of items for selection. If the field type is set to hidden, you can submit a hidden value with the form.
Email Field Enabled	If enabled, displays a field for the user's e-mail on the form.
Email Field Required	If enabled, the user is required to complete this field on the form.
Email Field Label	Text label for the e-mail field on the form.
Email Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Email Field Value	Data entry field provided for user. You have the option to enter a default value for the field that can be overridden by the user or a list of items for selection. If the field type is set to hidden, you can submit a hidden value with the form.
Phone Field Enabled	If enabled, displays a telephone number field on the form.
Phone Field Required	If enabled, the user is required to complete this field on the form.

Setting	Definition
Phone Field Label	Text label for the telephone number field on the form.
Phone Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Phone Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Hardware Description Field Enabled	If enabled, displays a field for to describe the user's hardware on the form.
Hardware Description Field Required	If enabled, the user is required to complete this field on the form.
Hardware Description Field Label	Text label for the hardware description field on the form.
Hardware Description Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Hardware Description Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Serial Number Field Enabled	If enabled, displays a field for the serial number of the user's PC or other device on the form.
Serial Number Field Required	If enabled, the user is required to complete this field on the form.
Serial Number Field Label	Text label for the field containing the serial number of the user's PC or other device on the form.
Serial Number Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Serial Number Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.

Setting	Definition
Hostname Field Enabled	If enabled, displays a field for the name of the user's PC or hostname on the form.
Hostname Field Required	If enabled, the user is required to complete this field on the form.
Hostname Field Label	Text label for the field containing the name of the user's PC or hostname on the form.
Hostname Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Hostname Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.

Success

Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title displayed above the Success Message contents.
Left Column Content	Text displayed in the left column of the page.
Please Wait Message	Message displayed to the user while the progress bar moves. To change the amount of time the message and progress bar are displayed, modify the default 45 second countdown number.
Progress Bar Enabled	If checked, display a progress bar and display the finished message.
Progress Bar Title	Text title displayed above the progress bar.
Finished Message	Message displayed to the user when the progress bar has finished.
Success Message	Message displayed upon successful connection.

Isolation portal

Configure the settings and behavior of your portal pages for hosts in isolation.

Common

Setting	Definition
Context Title	Text label to indicate the functional purpose of the context.
Show Portal Selector Page	Displays a portal selection page immediately following isolation. Users can pick a portal from the list to continue the portal process.

Index (redirect)

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title displayed above the content property contents.
Left Column Content	Text displayed in the left column of the page.
Content	Text describing the redirect.

Portal selector

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title displayed above the content property contents.
Left Column Content	Text displayed in the left column of the page.
Show Continue Link	If enabled, a continue link is shown that allows the user to proceed with the current portal.
Continue Text	Text for the button to proceed with the current portal selection.
Header Content	Text describing the portal options the user can select. This is displayed below the option to continue with the current portal.
Portal Options	A selection of the portals shown in the list of available options
Footer Content	Text to display below the portal selections

Dead end portal

Configure the settings and behavior of your portal pages for hosts in dead end.

Common

Setting	Definition
Context Title	Text label to indicate the functional purpose of the context.

Index

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Title displayed above the content property contents.
Left Column Content	Text displayed in the left column of the page.
Content	Text content displayed to the user.
Show Disabling Security Alarm	Select to display information in the portal to the user about why the user is in dead end.
Security Alarm Title	Text label for the title of the column displaying the security alarm.
Security Alarm Description	Text displayed for the security alarm description.
Show Alarm Rule Text	Select to display alarm rule text.
Show All Event Types	Select to display all event types.
Alert Type Header	Text displayed for the alert type column header.
Show All Event Subtypes	Select to display all event subtypes.
Subtype Header	Text displayed for the event subtype column header.
Show All Event Severities	Select to display severities for all events.
Severity Header	Text displayed for the severity column header.
Show All Event Thread IDs	Select to display threat IDs for all events.
Threat ID Header	Text displayed for the threat ID column header.
Show All Event Descriptions	Select to display descriptions for all events.
Event Description Header	Text displayed for the event description column header.
Custom Columns (Header, Column:Header, Column)	Text displayed for custom column headers.

Policy failure portal

Specify the Default Instructions to show when the host fails their Policy. Navigate to **Policy > Policy Configuration > Endpoint Compliance > Scans**, select a scan, and then select a category (Operating System, Anti-Virus). Click an operating system or anti-virus package to see the Web Address parameter that is being used.

Default instructions

Setting	Definition
Windows Operating System	Displayed when clicking on the link for the Operating System.

Setting	Definition
Windows Operating System Updates	Displayed when clicking on the link for the Windows Service Pack or Updates.
macOS Operating System and Updates	Displayed when clicking on the link for the Operating System or Updates for macOS systems.
Anti-Virus Installed	Displayed when clicking on the link for the antivirus products.
Anti-Virus Definitions	Displayed when clicking on the link for the antivirus Definitions products.

Agent portal

Configure the settings and behavior of agents.

Mobile

Setting	Definition
Message	Text displayed in the middle of the screen.
Username Hint	Text displayed as a hint in the user name field.
Password Hint	Text displayed as a hint in the password field.
Button Text	Text displayed in the registration button.
Authenticate Mobile Hosts	If enabled, authenticate registered hosts.

Dissolvable

Setting	Definition
Skip Message Screen	When enabled, automatically starts the Dissolvable agent without displaying the initial message screen. Requires Agent version 4.0.5 and higher.
Message	Text displayed in the middle of the screen.
Username Hint	Text displayed as a hint in the user name field.
Password Hint	Text displayed as a hint in the password field.
Button Text	Text displayed in the registration button.
Results Text	Text displayed above the results list.
Rescan Button Text	Text displayed in the rescan button.
Cancel Button Text	Text displayed in the Cancel button.
Finish Button Text	Text displayed in the Finish button.
Login Type Label	Text displayed as the first option in the login type box.

Setting	Definition
EasyConnect Login Dialog Title	Text displayed as the title for the Dissolvable Agent Login dialog. Requires agent version 3.3 or higher.
EasyConnect Login Dialog Message	Text displayed when the Dissolvable Agent prompts for credentials. Requires agent version 3.3 or higher.
Success Text	Text displayed after a successful registration.
Skip Success Screen	When enabled, closes the agent without displaying the success screen. Requires Agent version 4.0.5 and higher.
Launch Success Page	Select to launch the success page after the user clicks Finish.
Connection test URL	A publicly accessible URL that is otherwise blocked from an isolation VLAN. When the agent receives a 200 response while attempting to connect to the URL, the success message appears.

EasyConnect portal

Provides a button to run EasyConnect through the Persistent Agent, allowing the EasyConnect process to run again if the secure wireless configuration on a device has changed.

Requires agent version 3.3 or higher.

Run EasyConnect

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title displayed above the Success Message contents.
Left Column Content	Text displayed in the left column of the page.
Content	Text displayed in the web page.
Button Text	Text displayed on the button to re-run EasyConnect.
Retry Text	Text displayed on the Retry button.
Validating Persistent Agent Message	Text displayed while system communicates with Persistent Agent.
Validating EasyConnect Policy Message	Text displayed while system searches for EasyConnect policy.
Policy Matched Message	Text displayed when the EasyConnect policy is found.

Success

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title displayed above the Success Message contents.
Left Column Content	Text displayed in the left column of the page.
Progress Bar Enabled	If checked, display a progress bar and display the finished message.
Please Wait Message	Message displayed to the user while the progress bar moves. To change the amount of time the message and progress bar are displayed, modify the default 45 second countdown number.
Progress Bar Title	Text title displayed above the progress bar.
Success Message	Message displayed upon successful connection.
Finished Message	Message displayed to the user when the progress bar has finished.

Host inventory portal

Common

Setting	Definition
Nameless Host Label	Text label for any hosts that do not have a name.
Text Content	Text providing instructions and information about how to use the Host Inventory.
Status Section Title	Text label for the status messages for each host.
Adapters Section Title	Text label for the adapters for each host.
Show Operating System	When enabled, the operating system field is displayed for each host.
Show Notes	When selected, the notes field is displayed for each host in the host list.

Controls

Setting	Definition
Log Out Text	The text displayed on the log out button.
Log out URL	The URL for the landing page where the user will be redirected when the user logs out or when the session times out.
Register This Host	The text of the banner where the user my register their current host.
Show Registration Counts	When enabled, the user can view the current vs. maximum number of registrations available.

Setting	Definition
Host Count Text	The text displayed after the ratio of hosts and maximum number of registrations that are allowed.
Register Enabled	When enabled, the user can register new hosts from the host inventory. In an NCM environment, to add new hosts to a user's Host Inventory the user must access the Host Inventory portal from the FortiNAC Server containing a rogue record for the host being added. Once the host is added, the NCM will enable access for the new registered host on any FortiNAC Server.
Remote Host Role	The role to apply to guest who register third party hosts through the portal. It does not apply when the host being registered is currently using the portal.
Require Valid Vendor OUI	When enabled, the vender OUI of the MAC address is checked against the known OUIs.
Register Host Text	The text displayed on the register button.
Register Dialog Title	The text displayed as the title of the register dialog.
Physical Address Label	The label text displayed for the physical address.
Physical Address Example	The example value displayed for the physical address.
IP address Label	The label text displayed for the IP address.
IP address Example	Example value displayed for the IP address.
Delete Enabled	When enabled, users can delete their host from the FortiNAC. Deleting a host locally cannot be done in an NCM enviroment.
Delete Text	The text displayed on the Delete button.
Delete Confirmation	The message that is displayed to confirm if the host should be deleted.

Status messages

Setting	Definition
Disconnected	Status message displayed when the host is disconnected and has no other status messages.
Connected	Status message displayed when the host is successfully connected.
Disabled	Status message displayed when the host has been disabled.
Marked as Security Risk	Status message displayed when the host is marked as a security risk.
Passed the Security Scan	Status message displayed when the host has passed the security scan.

Setting	Definition
Invalid MAC Address	Status message displayed when the host has an invalid MAC address.
User is Logged On	Status message displayed when a user is logged onto the host.
Directory Authenication Disabled	Status message displayed when the directory authentication is disabled.
Not Authenticated	Status message displayed when the host is not authenticated.
Has a Static IP address	Status message displayed when the host has a static IP address.
Has Persistent Agent	Status message displayed when the host has the Persistent Agent.
Connected Through VPN	Status message displayed when the host connected through VPN.
Connected Through Dialup	Status message displayed when the host connected through dial up.
Will Be Scanned On Connect	Status message displayed when the host will be scanned on connect.
Is Being Scanned	Status message displayed when the host is being scanned.
Persistent Agent Connected	Status message displayed when the host has the Persistent Agent and the agent is actively communicating.

Device profiler

Device profiler is a mechanism to automatically categorize and control unknown or rogue devices that connect to your network and receive an IP address. This process runs continuously. It scans the host database for rogues with IP addresses and assigns them a device type based on profiles or rules set up in FortiNAC. Device profile rules use information such as operating system and vendor OUI to determine what the connecting device might be.
Device profiler is installed with some default rules which can be refined and new rules can be added. You can evaluate uncategorized rogues manually as new rules are added or existing rules are modified.

During an initial installation of FortiNAC this feature increases the speed with which devices are identified. After installation, device profiler provides easy management of new devices as they come online. Devices that are typically identified by device profiler include items such as IP phones, gaming devices, or mobile devices.

After a device has been categorized, the rule used to profile the device is associated with that device. If the device disconnects from the network and later reconnects, device profiler confirms that the device still matches the rule. If the device does not match its associated rule, device profiler can disable the device or notify the administrator by using events and alarms. Rule confirmation is an optional setting. This setting can be applied globally on the rule itself or individually on a profiled device.

To manage device profiler, you have the option of creating administrative users known as device managers with an admin profile that limits their permissions within FortiNAC. Creating additional users with limited permissions to manage new devices frees your regular IT staff to perform other tasks.

Process

As new, unknown devices connect to the network, Device Profiler categorizes them and places the devices within FortiNAC based on its Device Profiling Rules. The process is as follows:

1. A device or host connects to the network.
2. FortiNAC learns that something has connected.
3. The Device Identity feature checks for a MAC address. If the MAC address is available, Device Identity compares it to known MAC addresses.
4. If the MAC address is unknown, the device is placed in the host database as a rogue with any additional information available, such as, IP address or operating system. The time interval that Device Profiler waits to resolve a MAC address to an IP address is 30 minutes, thus allowing time for normal IP to MAC polling to occur.
5. If the device has an IP address, Device Profiler begins to compare the available device information to its Device Profiling Rules. It starts with the rule that is ranked number one and works its way through the list of rules in order by rank until it finds a match to one of the rule's criteria or matching methods. Disabled rules are ignored.
6. A match is determined by a combination of the device type selected on the General Tab for the rule and one or more methods selected on the Methods Tab. For example, if the device type selected is Mobile Device and the Method selected is DHCP fingerprinting, then a hand held device running Windows CE would match this rule. DHCP fingerprinting would determine that the device is using Windows CE which is an operating system that corresponds to a Mobile Device.

   However, if the device type selected is Gaming Device and the Method selected is DHCP fingerprinting, then a hand held device running Windows CE would not match this rule because Gaming Devices do not use Windows

CE.

Identification methods based on fingerprinting use the FortiNAC fingerprint database which cannot be modified by the user.

The exception to this is the Vendor OUI method. This method ignores the device type selected on the General Tab and uses the information selected within the method, such as the OUI, Vendor name, Vendor Alias or Device Type. Multiple entries are allowed, but the device only has to match one item to match the rule.

7. If Notify Sponsor is enabled, an email is sent by the FortiNAC server or Control server to all Device managers who have permission for devices associated with this rule. Permissions are based on the configuration of the Admin Profile attached to the administrative user. The email indicates that a new device has been processed.
8. The device is assigned the device type contained within the rule. Unless it is the Catch All rule which has no type. The type assigned by Device Profiler takes precedence over any type associated with the device's Vendor in the FortiNAC database. See Vendor OUIs on page 127.
9. The device is assigned the role contained within the rule. If no role is selected, the device is assigned the NAC Default role. The role assigned by Device Profiler takes precedence over any role associated with the device's Vendor OUI in the FortiNAC database. See Vendor OUIs on page 127.
10. Devices can be registered automatically or manually. If the rule is set to register manually, you must go to the Profiled Devices window to register the device.
11. If **Register As** is enabled in the matching rule, the device can be placed in the Host View or the Topology View or both.
12. If a Host View option was chosen the device can be added to a specific group as it is added to the Host View.
13. If a Topology View option was chosen in the rule, the device is added to a user-specified Container.
14. If the Access Availability option has been set to Specify Time, network access for devices placed in the Host View is limited to the configured times. To prevent devices from accessing the network outside the configured timeframe, they are marked "At Risk" for the Guest No Access admin scan.
15. When the device has been through the entire process and has been registered either automatically or manually, it will no longer display as a rogue. Depending on the options you chose in the rule it is displayed in the Host View, the Topology View or both.
16. If the device does not match any rule, it is associated with the default Catch All rule. Depending on the settings configured within this rule, the device can be associated with the rule but still remain a rogue.
17. Devices that are registered and associated with a user are placed in the Host View and removed from the Profiled Devices window. Devices that are placed in Topology only are removed from Profiled Devices. All other devices processed by Device Profiler remain in the Profiled Devices window and in the Host View.

Implementation

The initial implementation of Device Profiler is performed by a FortiNAC administrator. Day-to-day management of Device Profiler can be done by an administrative user with an Admin Profile, referred to here as a Device manager profile. This section of the documentation outlines the implementation process in the order in which it should be done.

Administrator

Administrators have full rights to all parts of the FortiNAC system and can fully implement Device Profiler without needing a Device manager user to manage devices. However, in most organizations these responsibilities are divided up. To begin implementing Device Profiler, you must do the following:

- Create or modify device profile rules that help identify new devices. See Rules on page 350.
- If you plan to have a Device manager manage new devices you must create a Device manager Admin Profile that can be attached to an administrative user and provide the appropriate permissions. Keep in mind that an Admin Profile can be created so that the same administrative user can also be responsible for Guest Manager. Guest Manager permissions are provided via an Admin Profile. See Administrative user profiles for device managers on page 363.
- Once the Device manager Admin Profile has been created with the appropriate permissions, you must attach that profile to an administrative user. Administrative users can only have one profile attached. See Add an administrative user for device profiler on page 364.
- If you decide to use the role-based access features of FortiNAC for hosts managed in Topology View you must go to Role Management and configure settings for the device roles. You can create and use additional roles also. In this case, the devices that are managed by Device Profiler are considered hosts. Roles are assigned to devices as they are added to FortiNAC. Every device and host must have a role. If no role is selected, devices and hosts are added to the NAC Default role. See Role management on page 553 for additional information.
- For hosts managed in the Hosts View role is an attribute of the host and can be used as a filter in User/Host Profiles. Those profiles determine which Network Access Policy, Endpoint Compliance Policy, Supplicant EasyConnect Policy and Portal Policy is applied. See Policies on page 377.
- Device Profiler processes can generate events and alarms that you may want to monitor. See Device profiler events and alarms on page 366.
- Device Profiling rules allow you to limit access to the network based on time of day or day of week. During the time that the device is not allowed to access the network it is marked "At Risk" for the Guest No Access admin scan. If you choose to implement this feature for any rule, the following requirements must be met:
  - You must have a quarantine or remediation VLAN on your network.
  - Ports through which a device would connect must be in the Forced Remediation Group (applies only to wired ports). See Groups view on page 838.
  - The Access Time feature can only be enabled for rules that register a device in the Host View.
  - The Model Configuration for all switches to which devices connect must have an entry for the Quarantine VLAN. This applies to both wired and wireless switches and access points. See Model configuration on page 767.
  - The Access Time feature can only be enabled for rules that register a device in the Host View or both Host and Topology View.

Device manager

Device managers have the following responsibilities. Administrators can perform these functions also.

Device managers can manage devices or end-stations that have been categorized by Device Profiler. Management options include registering, deleting and enabling/disabling devices. In addition, the Device manager can add notes to a device record and export a list of records in multiple formats. See Profiled devices on page 367 for more information.

Rules

Device Profiling Rules are used by the Device Profiler feature to categorize rogue hosts that connect to the network. As a rogue connects to the network and receives an IP address its information is compared to all methods within each enabled rule in turn until a match is found. The rogue device can be managed in a variety of ways depending on the configuration of the rule.

Any of the following scenarios could result from a match.

- The rogue matches a rule and is placed in the Topology View as a device. It cannot be seen in the Profiled Devices window and cannot be managed by a Device manager. Future rules cannot be run against this device unless it is deleted from the system and becomes a rogue again when it connects to the network.
- The rogue matches a rule and is registered. It is displayed in the Host View as a registered host and can be seen in the Profiled Devices window. It remains associated with the matching rule and can be managed by a Device manager. Future rules cannot be run against this device unless it is deleted from the system and becomes a rogue again when it connects to the network.
- The rogue matches a rule and is registered. It is displayed in the Host View as a registered host and is associated with a specific user, thus creating an identity for that device. It is removed from the Profiled Devices window and cannot be managed by a Device manager. Future rules cannot be run against this device unless it is deleted from the system and becomes a rogue again when it connects to the network.
- The rogue matches a rule, but the rule is not configured to place the device in Topology View or Host View. The device remains a rogue, but is associated with the rule. Future rules can be run against this device as long as it remains unregistered. The device can be seen in the Profiled Devices window. If Notify Sponsor is enabled, the Device manager receives an e-mail that there was a match. The device can be managed by the Device manager. The Device manager can register the device which places it in the Host View or can delete the device. An administrative user can access the device in the Host View and change it to a device if it needs to be in Topology.

  Device Profiler does not see devices that are no longer rogues and cannot match those devices with new or modified rules.

In summary, Devices placed in the Topology View only cannot be seen in the Profiled Devices window. Devices placed in the Host View display in the Profiled Devices window until the device is associated with a user. Devices placed in both Host and Topology View display in the Profiled Devices window until the device is associated with a user.

Host view vs. topology view

Device Profiling Rules can be used to place rogue devices in the Host View, the Topology View or both. There are certain advantages to each option that should be kept in mind when determining where to place a device.

Devices that are kept in the Host View have a connection history and can be associated with a user. Devices that are placed in the Topology View can be polled for their connection status. Devices that are not connected display in red on the Topology View. If the connection to the device fails, events and alarms can be configured to notify you that the device is no longer communicating.

Manage rules

The Device Profiling Rules window displays the default set of rules provided. Use this window to modify the default rules or to create your own set of rules. Default rules vary depending on the version of the software and the firmware installed. Upgrading to a newer version of the software does not add or modify default rules.

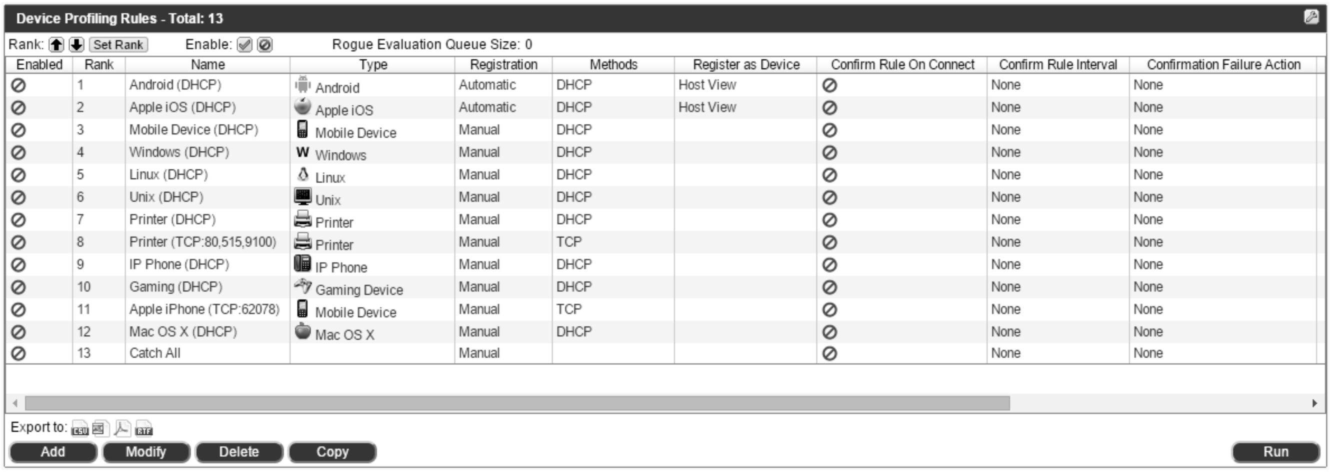
Disabled rules are ignored when processing rogues. Device Profiling rules are disabled by default and are set not to register devices. When you are ready to begin profiling, enable the rule or rules you wish to use.

Enabling certain rules could result in all unregistered PCs on your network being displayed in the Profiled Devices window. Review each rule carefully before enabling it.

The **Catch All** rule is always at the end of the list and its rank cannot be changed. As new rules are added they are inserted into the list immediately above the Catch All rule. This guarantees that all rogues profiled by Device Profiler are associated with a rule and can be managed by an administrative user with the appropriate Admin Profile, a Device manager. Device managers cannot manage devices that are not associated with a rule. This rule has no identification methods and no device type.

Device Profiling Rules created on the FortiNAC server will be ranked above global Device Profiling Rules created on the NCM. The rank of a local Device Profiling Rule can be adjusted above or below another local Device Profiling Rule, but cannot be ranked below a global Device Profiling Rule. The rank for a global Device Profiling Rule cannot be modified from the FortiNAC server.

Device Profiling Rules can be accessed from **Hosts > Device Profiling Rules** or from **System > Quick Start > Policy Configuration**, however configuration steps point you to Hosts / Device Profiling Rules.



Device Profiling Rules - Total: 13

Rank: ⬆ ⬇ Set Rank Enable: ✓ ⊘ Rogue Evaluation Queue Size: 0

Enabled	Rank	Name	Type	Registration	Methods	Register as Device	Confirm Rule On Connect	Confirm Rule Interval	Confirmation Failure Action
⊘	1	Android (DHCP)	Android	Automatic	DHCP	Host View	⊘	None	None
⊘	2	Apple iOS (DHCP)	Apple iOS	Automatic	DHCP	Host View	⊘	None	None
⊘	3	Mobile Device (DHCP)	Mobile Device	Manual	DHCP		⊘	None	None
⊘	4	Windows (DHCP)	Windows	Manual	DHCP		⊘	None	None
⊘	5	Linux (DHCP)	Linux	Manual	DHCP		⊘	None	None
⊘	6	Unix (DHCP)	Unix	Manual	DHCP		⊘	None	None
⊘	7	Printer (DHCP)	Printer	Manual	DHCP		⊘	None	None
⊘	8	Printer (TCP:80,515,9100)	Printer	Manual	TCP		⊘	None	None
⊘	9	IP Phone (DHCP)	IP Phone	Manual	DHCP		⊘	None	None
⊘	10	Gaming (DHCP)	Gaming Device	Manual	DHCP		⊘	None	None
⊘	11	Apple iPhone (TCP:62078)	Mobile Device	Manual	TCP		⊘	None	None
⊘	12	Mac OS X (DHCP)	Mac OS X	Manual	DHCP		⊘	None	None
⊘	13	Catch All		Manual			⊘	None	None

Export to:

Settings

An empty field in a column indicates that the option has not been set.

Field	Definition
Table configuration	
Rank Buttons	Moves the selected rule up or down in the list. Devices are compared to rules in order by rank.
Set Rank Button	Allows you to type a different rank number for a rule and immediately move the rule to that position. In an environment with a large number of rules this process is faster than using the up and down Rank buttons. Rank can only be set on local policies, rank changes for global policies must be done at the NCM.
Enable Buttons	Enables or disables the selected rule. If a rule is disabled it is not used when processing a rogue host.
Table columns	

Field	Definition
Rogue Evaluation Queue Size	Indicates the number of Rogues waiting to be processed by the Device Profiling Rules. The queue is filled by Rogues as they connect to the network. If the Run button at the bottom of the window is clicked, any rogues that were not previously categorized are added to the queue immediately. This number moves up and down as the system processes rogues.
Enabled	A green check mark indicates that the rule is enabled. A red circle indicates that the rule is disabled.
Rank	Rule's rank in the list of rules. Rank controls the order in which devices are compared to rules.
Name	User defined name for the rule.
Type	Device type that is assigned when the rule is a match for a rogue host.
Registration	Indicates whether devices matching this rule are registered automatically or manually.
Methods	The method or methods used to identify a device. Methods include: IP Range, DHCP fingerprinting, Location, TCP, NMAP, Passive Fingerprinting, Vendor OUI and UDP.
Register As Device	When a device is registered it can be placed in the Host View, the Topology View or both. This column indicates where the device is placed when it is registered. If the column is blank, then the registration option has not been set for this rule.
Notify	A green check mark indicates that Notify is enabled. When a new device is detected and it matches this rule, an email is sent to all Device managers that have this rule associated with their Admin Profile. A red circle indicates that the Notify option is disabled.
Role	Role assigned to devices matching this rule.
Access Availability	Times that devices matching this rule are permitted to access the network. Devices matching this rule are marked "At Risk" for the **Guest No Access** admin scan during the times they are not permitted to access the network.
Add To Group	Devices matching this rule are added to the group displayed. Add to Group is only available for devices that are added to the Host View.
Container	Devices matching this rule are added to the Container displayed. Devices can only be placed in a Container if they are being added to the Topology View.
Confirm Rule On Connect	If enabled, Device Profiler confirms that previously profiled devices associated with this rule still match this rule the next time they connect to the network. A green check mark indicates that the option is enabled. A red circle indicates that the option is disabled.
Confirm Rule Interval	If enabled, Device Profiler confirms at set intervals that previously profiled devices associated with this rule still match this rule.
Confirmation Failure Action	If enabled, Device Profiler disables previously profiled devices that no longer match their associated rule.
Last Modified By	User name of the last user to modify the rule.
Last Modified Date	Date and time of the last modification to this rule.

Field	Definition
Right click options	
Copy	Copy the selected Rule to create a new record.
Delete	Deletes the selected Rule(s). Removes the association between that rule and the devices it matched. Devices associated with deleted rules will no longer display on the Profiled Devices window.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847 You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671
Modify	Opens the Modify Device Profiling Rule window for the selected rule.
Buttons	
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.
Run Button	Used to re-run the Device Profiler process when rules have been modified or added. Devices that have already been categorized are not affected. Only rogues that remain in the Host View are processed. If rules are set to notify Device managers via e-mail when rogues connect, processing existing rogues triggers those e-mails again. Rogues that are no longer connected are ignored.

Best practices

The configuration of Device Profiling rules should be considered carefully to optimize performance. The list below outlines concepts that should be taken into account when configuring rules.

1. When a device or host connects to the network, the Device Profiling Rules are checked in order starting with the rule ranked number 1. The order of the rules is important. For the best performance, it is recommended that you rank rules based on the Methods used to categorize devices and hosts as follows: OUI rules first, DHCP rules next and Active, TCP/UDP port, IP Range, Location rules last.

   In an environment where static IP addresses are used, DHCP rules should be at the end of the list. Devices with static IP addresses do not send out DHCP broadcast packets. Therefore, FortiNAC will never receive a DHCP fingerprint for those devices and the profiling process will not continue past the DHCP rules.

   It is recommended that you set up IP Helper addresses for DHCP on your routers when using DHCP fingerprinting. Use the IP address of eth0 on the FortiNAC Server or the Application Server. Do not use the IP address of the FortiNAC Control Server.
2. The device information necessary to compare against a rule, must be available for Device Profiler to successfully move from one rule to the next. If the information required for a rule to be matched is unavailable, the evaluation of that device ends. For example, if the IP address of the device cannot be determined, Device Profiler cannot move past any rule that uses IP address as match criteria. The reason that the Device Profiler does not skip the rule and continue with the next one is that combinations of rules would not work. In the example below, if the Device Profiler skips the first rule because the TCP port cannot be found, the Apple iPhone will be miscategorized. If the Device

Profiler does not skip the rule, Apple iPhone remains uncategorized and the user can either manually determine what the device is or can adjust the rules to catch it.

Example:

This example outlines how two rules can be used together to provide greater accuracy when profiling devices. Apple iPhone and MAC OS fingerprints tend to be almost identical, but the iPhone can be distinguished by a TCP port which can be used in a rule to identify that device. In this case, you can create two rules: the first to identify iPhones by scanning for the iPhone TCP port and the second to scan for MAC OS in general. The iPhone rule is more granular and will catch the phone before it is categorized by the MAC OS rule.

3. OUI only rules are the quickest to process because no outside data is necessary.
4. Rules that require an IP address take longer to process because the FortiNAC server may need to read the DHCP leases file or layer 3 tables from the routers.
5. Device Profiler uses the latest IP address from the IP-to-MAC cache, if the IP address exists. It does not rely on the IP address seen in the Adapter View because it may be stale. If the IP address does not exist in the cache, FortiNAC starts an IP –to-MAC lookup on all L3 devices. FortiNAC stops the lookup as soon as the address is found, therefore, in most cases every L3 device will not be polled. If the FortiNAC server is not properly configured to read layer 3 from the routers, it may cause Device Profiling rules that require an IP address to fail.

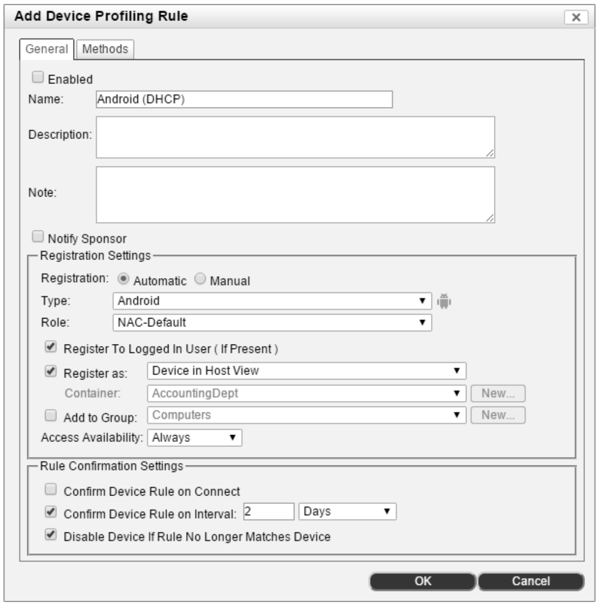
Add or modify rules

1. Click **Hosts > Device Profiling Rules**.
2. Click the **Add** button or select a rule and click **Modify**.
3. Refer to the tables below for information on each option on this window.
4. On the **Methods** tab you can select one or more methods for identification.

The device must meet criteria established for all of the methods selected.

5. Select a single method of identification. If you find that too many devices match the rule, add a second method to refine the profiling process and reduce the number of false matches.
6. Click **OK** to save.

General tab



□ Enabled

Name: Android (DHCP)

Description:

Note:

□ Notify Sponsor

Registration Settings

Registration: ● Automatic ○ Manual

Type: Android

Role: NAC-Default

☑ Register To Logged In User (If Present)

☑ Register as: Device in Host View

Container: AccountingDept New...

□ Add to Group: Computers New...

Access Availability: Always

Rule Confirmation Settings

□ Confirm Device Rule on Connect

☑ Confirm Device Rule on Interval: 2 Days

☑ Disable Device If Rule No Longer Matches Device

Settings

Field	Definition
Enabled	Mark with a check mark to enable this rule. Disabled rules are skipped when comparing devices to rules.
Name	User specified name for this rule. Required.
Description	Description of the rule.
Note	User specified note that can be viewed by administrators and users with the appropriate Admin profile who manage devices that match this rule.
Notify Sponsor	If enabled, users whose Admin Profile gives them permission to manage devices associated with this rule are notified whenever a device has been matched to this rule. This includes rogues that have been processed again by clicking the Run button on the Device Profiling Rules window. An e-mail is sent by the FortiNAC server or Control server indicating that a device matched this rule. The message would read as follows: A new rogue (00:12:3F:19:1A:F4), matching rule Windows, was found. Requires that the Device Profile Rule Match event be enabled. It is enabled by default and should not be disabled.
Registration settings	
Registration	Indicates whether device registration is automatic or manual. **Automatic:** The device is registered immediately if the Register As option is enabled.

Field	Definition
	Manual: The device is registered manually from the Profiled Devices window. The **Register As** option on this window must be enabled in order to manually register the device.
Type	Device category in which a device matching this rule should be placed. This controls the icon associated with the device in the Host or Topology Views.
Tags	Mapping values to be applied to the firewall via the 550 Agent. Tags will take precedence over the userID
Role	Roles are attributes of users and hosts and are used as filters in User/Host Profiles. Those profiles are used to determine which Network Access Policy, Endpoint Compliance Policy or Supplicant Easy Connect Policy to apply. If you are using Role-based access for hosts/devices managed in Topology View, select the role that controls access to the network for this device. If you are not using Role-based access, select NAC-Default.
Register To Logged In User (If Present)	If a user logs into the device being profiled, the user becomes the owner of that device in the FortiNAC database. This applies only to users that log in with an 802.1x supplicant configured to send the User ID. If the device is registered to the logged in user, then any options selected under **Register As** are ignored even if **Register As** is enabled.
Register As	If **Register To Logged In User** is enabled, and a user is logged in, this option is ignored even if it is enabled. If **Register To Logged** In User is disabled, this option is used to determine where to place the connecting device. Click the check box to enable this option. Indicates where the registered device will be placed. Options include: • Device in Host View • Device in Topology View • Device in Host And Topology View If the device is an Access Point and you register it in Host View, it is removed from the Host View and moved to Topology View after the first poll. It is also removed from the Concurrent License count once it is recognized as an Access Point.
Container	Select or create a container for this type of device. Click the **New** button to create a new Container. Containers are a mechanism used to group items in Topology. This field remains disabled unless one of the Topology View options is selected in the Register As field.
Add to Group	Place devices in an existing group or create a new group for them. Grouping devices to manage them as a group instead of individually. See Groups view on page 838. This field remains disabled unless one of the Host View options is selected in the Register As field.

Field	Definition
Access Availability	Allows you to control when devices that match this rule can access the network. Options include: Always or Specify Time. This option is only enabled for devices that are managed in the Host View or both the Host View and the Topology View. If you set times for Access Availability, devices that match this rule are marked "At Risk" for the **Guest No Access** admin scan during the time that they are not permitted to access the network.
Rule confirmation settings	
Confirm Device Rule On Connect	If enabled, Device Profiler confirms that previously profiled devices associated with this rule still match this rule the next time they connect to the network.
Confirm Device Rule On Interval	If enabled, Device Profiler confirms at set intervals that previously profiled devices associated with this rule still match this rule. Interval options include Minutes, Hours, or Days.
Disable Device If Rule No Longer Matches Device	If enabled, Device Profiler disables previously profiled devices that no longer match their associated rule.

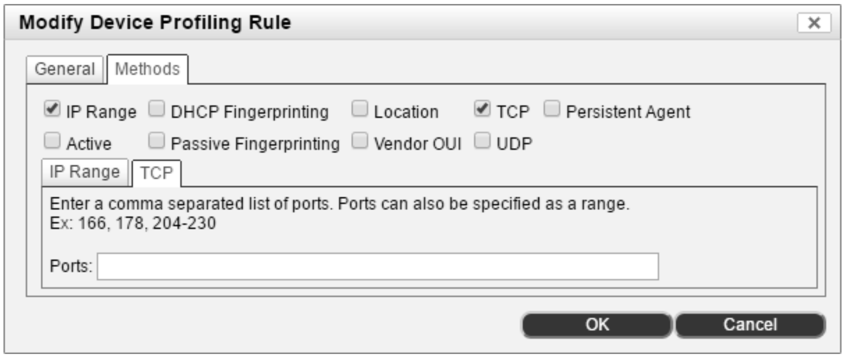
Specify access availability time

This option allows you to limit network access for a device based on the time of day and the day of the week. Any device associated with a rule, can only access the network as specified in the Access Availability field for the rule. This option is only enabled for devices that are managed in the Host View or both the Host View and the Topology View.

If you set times for Access Availability, FortiNAC periodically checks the access time for each device associated with the rule. When the device is not allowed to access the network it is marked "At Risk" for the **Guest No Access** admin scan. When the time is reached that the device is allowed to access the network, the "At Risk" state is removed. These changes in state occur on the device record whether the device is connected to the network or not. If the device has a browser and connects to the network outside its allowed timeframe, a web page is displayed with the following message: "Your Network Access has been disabled. You are outside of your allowed time window. To regain network access call the help desk.".

1. Click **Hosts > Device Profiling Rules**.
2. Click select a rule and click **Modify**.
3. In the **Access Availability** field select **Specify Time**.
4. In the **Time Range** section enter the From and To times for the time of day that devices should be able to access the network.
5. In the **Days of the Week** section select the days during which these devices should be allowed to access the network.
6. Click **OK**.

Methods tab



Modify Device Profiling Rule

General | Methods

☑ IP Range ☐ DHCP Fingerprinting ☐ Location ☑ TCP ☐ Persistent Agent

☐ Active ☐ Passive Fingerprinting ☐ Vendor OUI ☐ UDP

IP Range | TCP

Enter a comma separated list of ports. Ports can also be specified as a range.
Ex: 166, 178, 204-230

Ports:

Settings

Method	Definition
IP Range	Matches if the IP address of a device falls within one of the ranges specified. You must specify at least one IP range.
DHCP Fingerprinting	Matches by device type or with a custom set of attributes. **Match type** Matches if the device type selected on the General tab corresponds to the Operating System of the device being profiled. The DHCP fingerprint is used to determine the Operating System of the device using FortiNAC's fingerprint database. For example, if the Operating System is Windows CE and the device type on the General Tab is Mobile Device, then the device matches this rule. If the Operating System is Windows CE and the device type on the General Tab is Gaming Device, then the device does not match this rule. **Match custom attributes** Matches if a set of custom attributes correspond to a DHCP packet from the device. Fields left blank will be ignored. The custom attributes supported are: DHCP message type, option list, vendor class (DHCP option 60), host name (DHCP option 12), parameter list (DHCP option 55) and operating system. DHCP fingerprinting is more accurate than passive fingerprinting. It is recommended that you set up IP Helper addresses for DHCP on your routers when using DHCP fingerprinting.
Location	Matches if the device connects to the selected location on your network. Options are: anything within a Container in the Topology View, anything in a Port Group or anything in a Device Group.

Method	Definition
HTTP/HTTPS	Matches if the device successfully responds to a HTTP request with optional fields for authentication parameters and response text. If multiple response values are entered, it will attempt to match any of them.
SNMP	Matches if the device successfully responds to a SNMP GET request for the OID specified. SNMP security credentials are required. If there are multiple security credentials, each set of credentials will be attempted to find a potential match. There is an optional field to match the response string value. If multiple string values are entered, it will attempt to match any of them.
SSH	Matches if the device successfully responds to a SSH client session request. User name and password credentials are required. If there are multiple credentials, each set of credentials will be attempted to find a potential match. The commands are used to automate interaction with the device. The possible commands are "expect" and "send". "expect" is a regular expression string that matches the response from the device. "send" will send a string to the device. "send" has two keywords %USERNAME% and %PASSWORD% for the username and password. There is an optional field to match the response string value. If multiple string values are entered, it will attempt to match any of them.
Telnet	Matches if the device successfully responds to a telnet client session request. User name and password credentials are not required. If there are multiple credentials, each set of credentials will be attempted to find a potential match. The commands are used to automate interaction with the device. The possible commands are "expect" and "send". "expect" is a regular expression string that matches the response from the device. "send" will send a string to the device. "send" has two keywords %USERNAME% and %PASSWORD% for the username and password. There is an optional field to match the response string value. If multiple string values are entered, it will attempt to match any of them.
TCP	Matches if the device provides a service on all of the ports specified. You must specify at least one port, but all specified ports must match. Multiple ports can be entered separated by commas, such as, 162, 175, 188. A range of ports can be entered using a hyphen, such as 204-215.
Active	Match Type Matches if the device type selected on the General tab is the same as that determined by NMAP for the connecting device. Match Custom Matches if the response from the device contains the specified value. Either an exact string match or regular expression can be used.

Method	Definition
Persistent Agent	Matches if the device type selected on the General tab corresponds to the Operating System of the device being profiled, and if the device has an Agent installed on the host, such as, the Persistent Agent or one of the Mobile Agent. The Agent is used to determine the Operating System of the device. To register hosts running the Persistent Agent using this method, you must disable registration under Persistent Agent Properties. If you do not, the Persistent Agent may register the host before the Device Profiler has the opportunity to register it. See Credential configuration on page 139.
Passive Fingerprinting	Matches if the device type selected on the General tab corresponds to the Operating System of the device being profiled. The DHCP fingerprint is used to determine the Operating System of the device. Based on FortiNAC's fingerprint database.
Vendor OUI	Matches if the Vendor OUI for the device corresponds to the OUI information selected for this method. You must specify at least one Vendor option. If there are multiple entries, the device only has to match one to match this rule. Options include: **Vendor Code** — A specific Vendor OUI selected from the list in the FortiNAC database. To select the OUI begin typing the first few characters. A list of matching OUIs is displayed in a drop-down list. **Vendor Name** — A single Vendor Name selected from the list in the FortiNAC database. To select the name, begin typing the first few characters. A list of matching Vendors is displayed in a drop-down list. The asterisk (*) wildcard can be used at the beginning and end to capture all variations of the Vendor Name (e.g., Avaya*). **Vendor Alias** — Enter a Vendor alias that exists in the FortiNAC vendor database. Must be an exact match. The asterisk (*) wildcard can be used at the beginning and end to capture all variations of the Vendor Alias. **Device Type** — Select a device type from the drop-down list provided. Includes items such as Alarm System or Card Reader. If this option is selected the device type associated with the Vendor OUI of the connecting device must match the device type for the Vendor in the FortiNAC vendor database.
UDP	Matches if the device provides a service on all of the ports specified. You must specify at least one port, but all specified ports must match. Multiple ports can be entered separated by commas, such as, 162, 175, 188. A range of ports can be entered using a hyphen, such as 204-215.

Method	Definition
WinRM	Matches if the device successfully responds to a WinRM client session request. User name and password credentials are required. If there are multiple credentials, each set of credentials will be attempted to find a potential match. The commands are used to automate interaction with the device. Each command is run via Powershell. There is an optional field to match the response string value. If multiple string values are entered, it will attempt to match any of them.
WMI Profile	Matches if the device successfully responds to a WinRM or SSH client session request and successfully creates a profile through various Powershell commands primarily querying WMI. User name (user principal name format, such as winrmadmin@example.com) and password credentials are required. If there are multiple credentials, each set of credentials will be attempted to find a potential match. Additional options allow you to match specific versions of Microsoft Windows, installed applications, Windows Service statuses, running processes, serial number, and asset tag (with wildcard matching). Requires Windows Management Framework 3.0.

Delete a rule

When a Device Profiling Rule is deleted the association between that rule and the devices it matched is removed. Devices associated with that rule will no longer display on the Profiled Devices window. They will continue to display in the Host View.

The Catch All rule is a default system rule that cannot be removed. Other default rules can be removed.

1. Click **Hosts > Device Profiling Rules**.
2. Click select a rule and click **Delete**.
3. A message displays asking if you are sure. Click **Yes** to continue.

Copy a rule

1. Click **Hosts > Device Profiling Rules**.
2. Click select a rule and click **Copy**.
3. The Add Device Profiling Rule window displays with the information from the selected rule.
4. You must, at minimum, modify the name of the rule. Modify other fields as needed and click **OK** to save.
5. For Settings, see Add or modify rules on page 355.

Evaluate rogue hosts

Over time you may have hosts that remain rogues because they do not match any of the rules enabled in the Device Profiling Rules window. You may also have hosts that have been categorized incorrectly. At any time you can modify the rules or create additional rules and then re-evaluate hosts. Only those hosts that remain unregistered can be re-evaluated.

If a host has been categorized incorrectly and has been registered, you have two options. Either manually modify the host or delete the host and when it connects to the network again, it will be evaluated by the rules.

Rogues that are no longer connected or are offline are ignored.

1. Click **Hosts > Device Profiling Rules**.
2. Click **Run**.
3. A message displays asking if you would like to evaluate rogues. Click **Yes** to continue.
4. A new message displays indicating that x number of rogues are being evaluated.
5. Device Profiler compares any rogue hosts to the list of enabled Device Profiling Rules and processes them accordingly. See Process on page 348 for additional information.
6. When the process is complete, click **OK** to close the message box.

Administrative user profiles for device managers

In FortiNAC, you can create an administrative user and give that user an Admin Profile that contains permissions for the Device Profiler feature set. These privileges are designed to restrict this user to certain parts of the program.

For Device Profiler, the Admin Profile, referred to as a Device manager in documentation, requires permission for Profiled Devices. This allows the user to manage new devices and categorize them.

Additional permissions can be given to Device Managers based on the parameters of their responsibilities. Create one or more Admin Profiles for these types of users. See Admin profiles and permissions on page 657.

Add a device manager admin profile

This procedure describes how to create an Admin Profile for an administrative user with permissions for Device Profiler. This user can access the Profiled Devices tab and use that window to register, delete, enable or disable hosts and enter notes about a host. The Profiled Devices window displays devices that are treated as hosts and are also displayed in the Host View.

You can have an Admin Profile that allows an administrative user to perform additional tasks by adding more permission sets. These step-by-step instructions assume that the Admin Profile will provide permissions only for Device Profiler. Details on other settings and permissions sets see Add an admin profile on page 671.

To create a Device manager Admin Profile you must first be logged into your Administrator account.

1. Click **Users > Admin Profiles**.
2. Click **Add**. The **Add Admin Profile** screen appears with the **General** tab highlighted.
3. On the **General** tab, enter a name for the profile, such as Device Manager.
4. Under **Manage Hosts and Ports**, select **All**.
5. Leave the defaults for the remaining fields and click on the **Permissions** tab.
6. On the Permissions tab note that some permissions are dependent on each other. Refer to the Permissions list on page 666 for additional information.
7. The minimum that this Device Manager must have is the **Profiled Devices** permission set. Select all of the check boxes for this set including the **Custom** check box.
8. When you select the Profiled Devices permission set, the Landing Page field defaults to Profiled Devices.
9. The Profile Devices tab is enabled when Custom is selected for the Profiled Devices permission set. Click on the **Profiled Devices** tab.

10. Use the table below to configure the Profile Devices specific fields.
11. Click **OK** to save.

Settings

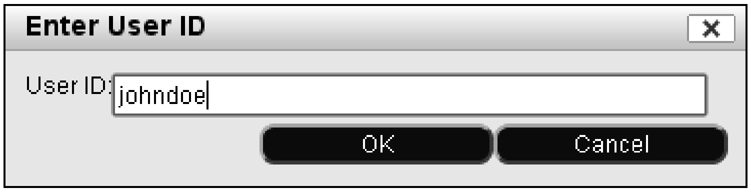
Field	Definition
Register, Delete, and Disable Profiled Devices	If enabled, the user can register, delete and disable devices that have been profiled by Device Profiler.
Modify Device Rule Confirmation Settings	If enabled, the user can change rule confirmation settings on devices that have been profiled by Device Profiler. Rule confirmation settings control whether or not Device Profiler checks a previously profiled device to determine if it still meets the criteria of the rule that categorized the device.
Manage Profiled Devices Using These Rules	• **All Rules**—includes current rules and any rules created in the future. • **Specify Rules**—you must choose the rules from the Available Rules field and manually move them to the Specify Rules field.
Available Rules	Shows the existing rules you can select for this profile. Select the rule and click the right arrow to move it to the Selected Rules pane.
Selected Rules	Shows the rules you selected from the Available Rules section. The user can only access the devices associated with the rules in this list.
Add Icon	Click this button to create a new Device Profiling Rule. For information on rules, see Add or modify rules on page 355.
Modify Icon	Click this button to modify the selected Device Profiling Rule. For information on rules, see Add or modify rules on page 355.

Add an administrative user for device profiler

If you are creating Admin Users to manage guests or devices, you must create an Administrative User who has the appropriate Admin User Profile associated. See Admin profiles and permissions on page 657.

1. Select **Users > Admin Users**.
2. Click the **Add** button.
3. In the User ID window displayed, enter an alphanumeric **User ID** for the new Admin user and click **OK**. As you enter the User ID, the network user database is checked to see if there is a current user with the same ID and a drop-down list of matching users is displayed. If you enter an ID that already exists as a regular network user, the network user and the Admin user become the same person with a single account.

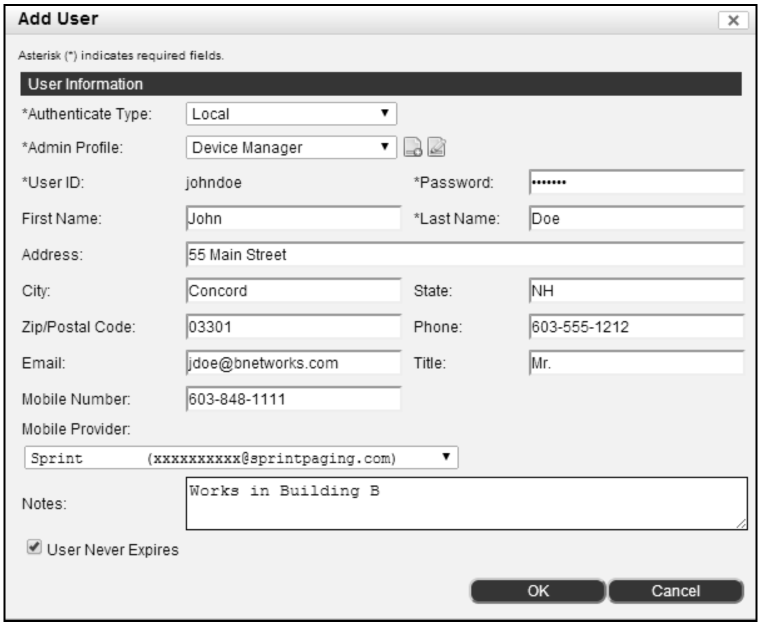
   This allows you to give a network user administrator privileges to help with some administrative tasks.



Enter User ID

User ID: johndoe

4. Use the table of Settings below to complete the information in the Add User dialog.
5. Click **OK** to save the new user.



Asterisk (*) indicates required fields.

User Information

*Authenticate Type:	Local ▼		
*Admin Profile:	Device Manager ▼		
*User ID:	johndoe	*Password:	•••••••
First Name:	John	*Last Name:	Doe
Address:	55 Main Street		
City:	Concord	State:	NH
Zip/Postal Code:	03301	Phone:	603-555-1212
Email:	jdoe@bnetworks.com	Title:	Mr.
Mobile Number:	603-848-1111		
Mobile Provider:			

Sprint (xxxxxxxxxx@sprintpaging.com) ▼

Notes: Works in Building B

☑ User Never Expires

Settings

Field	Definition
Authentication Type	Authentication method used for this Admin user. Types include: • **Local** — Validates the user to a database on the local FortiNAC appliance. • **LDAP** — Validates the user to a directory database. FortiNAC uses the LDAP protocol to communicate to an organization's directory. • **RADIUS** — Validates the user to a RADIUS server.
Admin Profile	Profiles control permissions for administrative users. See Admin profiles and permissions on page 657. • **Add** — Opens the Admin Profiles window allowing you to create a new profile without exiting the Add User window. • **Modify** — Allows you to modify the selected Admin Profile. Note that modifications to the profile affect all Administrative Users that have been assigned that profile.
User ID	Unique alphanumeric ID for this user.
Password	Password used for local authentication. If you authenticate users through LDAP or RADIUS, the password field is disabled and the user must log in with his LDAP or RADIUS password.
First Name	User's first name.
Last Name	User's last name.

Field	Definition
Address	Optional demographic information.
City	
State	
Zip/Postal Code	
Phone	
E-mail	E-mail address used to send system notifications associated with features such as alarms or profiled devices. Also used to send Guest Self-Registration Requests from guests requesting an account. For multiple e-mail addresses, enter addresses separated by commas or semi-colons. Messages are sent to all e-mail addresses provided.
Title	User's title, such as Mr. or Ms.
Mobile Number	Mobile Phone number used for sending SMS messages to administrators.
Mobile Provider	Mobile provider for the mobile phone number entered in the previous field. Used to send SMS messages to administrators. This field also displays the format of the SMS address that will be used to send the message. For example, if the provider is US Cellular, the format is xxxxxxxxxx@email.uscc.net, where the x's represent the user's mobile phone number. The number is followed by the email domain of the provider's message server.
Notes	Free form notes field for additional information.
User Never Expires	If enabled, Admin users are never aged out of the database. The default is enabled. Admin Users assigned the Administrator Profile cannot be aged out.
Propagate Hosts	The Propagate Hosts setting controls whether or not the record for the host owned by the user is copied to all managed FortiNAC appliances. This field is only displayed if the FortiNAC server is managed by a FortiNAC Control Manager.

Device profiler events and alarms

Certain actions within Device Profiler generate events that appear in the Event Log. Examples of Device Profiler events are listed in the following table.

Event	Definition
Device Profile	Generated whenever device profiling updates a rogue.

Event	Definition
Device Profile Rule Match	A rogue host has matched a Device Profiling rule allowing it to be assigned a device type and registered.
Device Profiling Automatic Registration	A rogue host has been registered by device profiling based on a device profiling rule.
Device Profiling Rule Missing Data	Indicates that Device Profiler cannot compare a rogue against a rule because FortiNAC does not have enough information about the rogue, such as a DHCP fingerprint. If Device Profiler cannot compare a rogue against a rule it does not continue processing that rogue, and moves on to the next rogue.
Device Rule Confirmation Success Device Rule Confirmation Failure	Devices identified by a Device Profiling rule maintain their association with that rule. If enabled, the associated rule and the device are checked periodically to see if the rule is still valid for the device. These event messages indicate whether or not the device matched the associated rule.

Events can be mapped to alarms. Alarms can be set to notify an administrator when they are triggered. Alarms can also be viewed on the Alarms Panel on the Dashboard. For more information on events and alarms, e-mail notifications, and how to map events to alarms see Map events to alarms on page 888.

Profiled devices

The Profiled Devices view displays a list of devices that have been profiled using the Device Profiling Rules. Based on how closely each device matched a rule it was given a device type and placed either in the Topology View, the Host View or both. Devices placed in the Topology View do not display on the Profiled Devices tab. Devices placed in the Host View are shown on the Profiled Devices tab. When a device is registered and it has an associated user, it is removed from the Profiled Devices tab and displays only in the Host View.

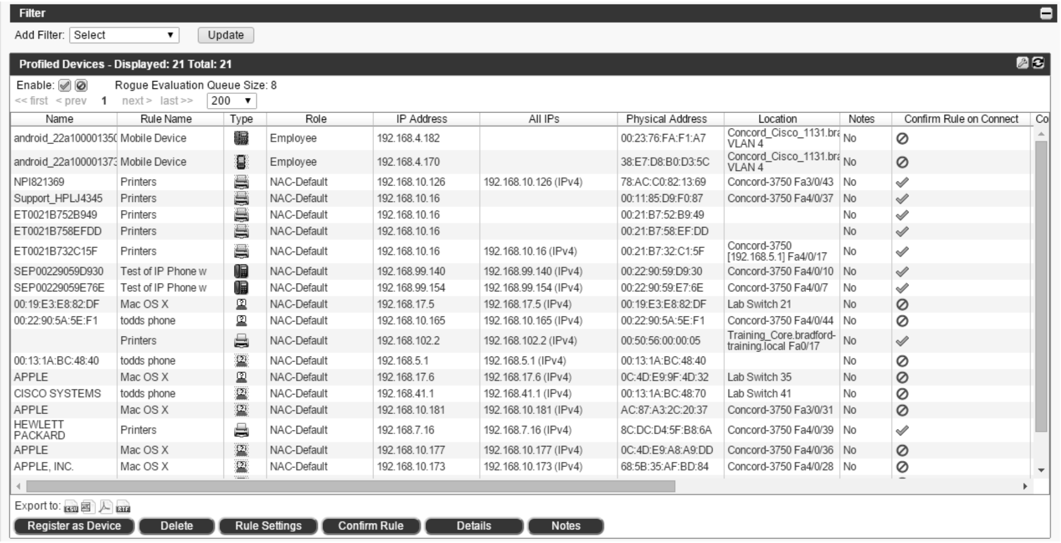
Administrators and administrative users with a Device manager Admin Profile can access this list of devices. Device managers can only see those devices that match rules listed in the Device manager's profile.

Only Administrative Users with additional permissions have access to the Views column, the Rule Settings, Confirm Rule and Details buttons on the Profiled Devices View. See Permissions list on page 666 for additional information.

Entries in this window are devices that require network services. Typically they include things such as mobile devices, gaming devices or PCs. They are considered hosts on the network. Only those devices associated with a Device Profiling Rule are displayed.

New devices are not displayed in Profiled Devices unless you click the Refresh button or close and reopen the tab.

Devices identified by a Device Profiling rule maintain their association with that rule. If rule confirmation is enabled, the associated rule and the device are checked periodically to see if the rule is still valid for the device. Rule confirmation can be enabled for a rule, which affects all devices associated with the rule, or it can be enabled for individual devices.



Filter

Add Filter: Select ▾ Update

Profiled Devices - Displayed: 21 Total: 21

Enable: ✓ ⊘ Rogue Evaluation Queue Size: 8

<< first < prev 1 next > last >> 200 ▾

Name	Rule Name	Type	Role	IP Address	All IPs	Physical Address	Location	Notes	Confirm Rule on Connect	Co
android_22a10000135(	Mobile Device	📱	Employee	192.168.4.182		00:23:76:FA:F1:A7	Concord_Cisco_1131.bra VLAN 4	No	⊘	
android_22a10000137:	Mobile Device	📱	Employee	192.168.4.170		38:E7:D8:B0:D3:5C	Concord_Cisco_1131.bra VLAN 4	No	⊘	
NPI821369	Printers	🖶	NAC-Default	192.168.10.126	192.168.10.126 (IPv4)	78:AC:C0:82:13:69	Concord-3750 Fa3/0/43	No	✓	
Support_HPLJ4345	Printers	🖶	NAC-Default	192.168.10.16		00:11:85:D9:F0:87	Concord-3750 Fa4/0/37	No	✓	
ET0021B752B949	Printers	🖶	NAC-Default	192.168.10.16		00:21:B7:52:B9:49		No	✓	
ET0021B758EFDD	Printers	🖶	NAC-Default	192.168.10.16		00:21:B7:58:EF:DD		No	✓	
ET0021B732C15F	Printers	🖶	NAC-Default	192.168.10.16	192.168.10.16 (IPv4)	00:21:B7:32:C1:5F	Concord-3750 [192.168.5.1] Fa4/0/17	No	✓	
SEP00229059D930	Test of IP Phone w	☎	NAC-Default	192.168.99.140	192.168.99.140 (IPv4)	00:22:90:59:D9:30	Concord-3750 Fa4/0/10	No	✓	
SEP00229059E76E	Test of IP Phone w	☎	NAC-Default	192.168.99.154	192.168.99.154 (IPv4)	00:22:90:59:E7:6E	Concord-3750 Fa4/0/7	No	✓	
00:19:E3:E8:82:DF	Mac OS X	?	NAC-Default	192.168.17.5	192.168.17.5 (IPv4)	00:19:E3:E8:82:DF	Lab Switch 21	No	⊘	
00:22:90:5A:5E:F1	todds phone	?	NAC-Default	192.168.10.165	192.168.10.165 (IPv4)	00:22:90:5A:5E:F1	Concord-3750 Fa4/0/44	No	⊘	
	Printers	🖶	NAC-Default	192.168.102.2	192.168.102.2 (IPv4)	00:50:56:00:00:05	Training_Core.bradford-training.local Fa0/17	No	✓	
00:13:1A:BC:48:40	todds phone	?	NAC-Default	192.168.5.1	192.168.5.1 (IPv4)	00:13:1A:BC:48:40		No	⊘	
APPLE	Mac OS X	?	NAC-Default	192.168.17.6	192.168.17.6 (IPv4)	0C:4D:E9:9F:4D:32	Lab Switch 35	No	⊘	
CISCO SYSTEMS	todds phone	?	NAC-Default	192.168.41.1	192.168.41.1 (IPv4)	00:13:1A:BC:48:70	Lab Switch 41	No	⊘	
APPLE	Mac OS X	?	NAC-Default	192.168.10.181	192.168.10.181 (IPv4)	AC:87:A3:2C:20:37	Concord-3750 Fa3/0/31	No	⊘	
HEWLETT PACKARD	Printers	🖶	NAC-Default	192.168.7.16	192.168.7.16 (IPv4)	8C:DC:D4:5F:B8:6A	Concord-3750 Fa4/0/39	No	✓	
APPLE	Mac OS X	?	NAC-Default	192.168.10.177	192.168.10.177 (IPv4)	0C:4D:E9:A8:A9:DD	Concord-3750 Fa4/0/36	No	⊘	
APPLE, INC.	Mac OS X	?	NAC-Default	192.168.10.173	192.168.10.173 (IPv4)	68:5B:35:AF:BD:84	Concord-3750 Fa4/0/28	No	⊘	

Export to: CSV RTF

Settings

Field	Definition
Rogue Evaluation Queue Size	Indicates the number of Rogues waiting to be processed by the Device Profiling Rules. The queue is filled by Rogues as they connect to the network. If the Run button on the Device Profiling Rules window is clicked, any rogues that were not previously categorized are added to the queue immediately. This number will move up and down as the system processes rogues.
Name	Name of the user associated with this device or the name of the manufacturer. For example, if a PC connects and has no associated user, you may see DELL, INC. in the name field. If the device is registered, but has no associated user the name field may be blank. Devices that are registered and have an associated user display in the Host View but are removed from the Profiled Devices tab.
Rule Name	Name of the Device Profiling Rule that was a match for this device.
Type	Icon that represents the type of host, such as Mobile Device or Gaming System. This field is populated by the Device Profiling Rule. Device type can also be assigned by Vendor OUI, however, the type in the Device Profiling Rule takes precedence. If this host is associated with a user, a host status icon is displayed. See Icons on page 30
Role	Role assigned to this host by the Device Profiling Rule. Roles can also be assigned by Vendor OUI, however, the role in the Device Profiling rule takes precedence.
IP address	IP address of the device.
Physical Address	MAC address of the device.
Location	Location where the device connected to the network.
Notes	Indicates whether or not there are notes for this device.

Field	Definition
Registered	Indicates whether or not the device is registered.
Views	Displays icons for the FortiNAC views that can be accessed for this device. Click an icon to go to the view. Possible views include: Adapter, Group Membership, Port Properties and Device Properties.
Confirm Rule On Connect	If enabled, Device Profiler confirms that previously profiled devices still match their associated rule the next time they connect to the network. A green check mark indicates that the option is enabled. A red circle indicates that the option is disabled.
Confirm Rule Interval	If enabled, displays the interval used to confirm device rules, such as, 2 Days. Indicates that Device Profiler will confirm that the associated rule matches the device every two days.
Last Confirmation Time	If Rule Confirmation is enabled, this column displays the last time this device had its associated rule confirmed.
Confirmation Failure Action	If Rule Confirmation is enabled, this column indicates the action to be taken if a device no longer matches its associated rule. Options are Disable Device or None.
Export	Exports data to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.
Right click options	
Register As Device	Registers selected devices. If the device is not associated with a user, the name is blank or displays as ROGUE, ROGUE. If the device is associated with a user, it is removed from the Profiled Devices tab and displays in the Host View.
Delete	Deletes selected devices from the database. This deletes the hosts from both the Profiled Devices window and the Host View.
Rule Settings	Changes rule confirmation settings for the selected device.
Confirm Rule	Runs the rule confirmation process for the selected device. If the device does not match the rule an event is generated. See Device profiler events and alarms on page 366. The device must be online in order to confirm the associated rule.
Details	Allows you to modify the role of a single device. Only available for Administrators users.
Notes	Opens the Notes window for the selected device. Allows you to add a note and view previous notes. Notes include the date and time they were created.
Enable	Enables the selected device.
Disable	Disables the selected device.

Export profiled devices

This option on the Profiled Devices tab allows you to export the device data displayed in the tab.

1. Click **Hosts > Profiled Devices**.
2. A list of devices is displayed.

3. At the bottom of the window in the **Export to:** section select the file format for the export file.
4. Either save or open the file created.

Monitor devices

FortiNAC provides a window into your network. It allows you to register known devices, isolate unknown devices and see where devices are connected to the network. Devices can be managed or controlled based on device roles.

There are a variety of ways to implement monitoring depending on how you choose to control your network. The implementation process outlined below touches on features within FortiNAC that can be used to control devices. These features are distributed throughout the product, therefore links to relevant sections of the documentation have been provided.

View and register known devices

Provisioning FortiNAC with known devices can be accomplished in several ways. However, you should start with switches, routers and controllers, since those devices control the network and provide FortiNAC with information about other devices connected to the network. Switches, routers and controllers can be imported into FortiNAC from .csv files or can be automatically discovered by FortiNAC. Other devices can be imported or detected as they connect to the network.

Import devices

If you already have spreadsheets or .csv files containing device information, you may be able to leverage them to import devices into FortiNAC. Each device type must be in a separate file. Both SNMP devices and Non-SNMP or pingable devices can be imported. See CLI import tool on page 706.

Discover devices

Discovery is an automated process started by the FortiNAC administrator. FortiNAC searches ranges of IP addresses for devices that can be managed using SNMP. A model of each device is created in FortiNAC as it is discovered and can be viewed in the Network Devices View. After Discovery each device must be configured to ensure that FortiNAC has the correct CLI passwords and VLAN configurations. See Network devices on page 833, Model configuration on page 767, Network access/VLANs on page 745, and Device properties on page 753 for additional information.

Register non-SNMP devices

Most networks also have a series of devices that cannot be managed using SNMP, such as printers, security cameras or alarm systems. This type of device is referred to as a pingable device. Non-SNMP devices can be imported into the database as noted above, can be registered manually or can be automatically registered by Device Profiler.

For manual registration, you must connect the device to the network. When FortiNAC detects that a device has connected, that device is displayed as a rogue in the Host View. From the Host View you can select one or more rogues and register them as devices. Devices registered from the Host View can be configured to display in the Host View, the Topology View or both. See Register a host as a device on page 812 and Learning about hosts on the network on page 372.

If you have implemented Device Profiler, devices can be categorized and automatically registered based on Profiling Rules. See Device profiler on page 348.

Register PCs

Registering PC's as devices can be done manually by connecting the PC to the network. When FortiNAC detects the connection, the PC is displayed in the Host View as a rogue. From the Host View you can select one or more rogues and register them as devices as noted above. See Register a host as a device on page 812 and Learning about hosts on the network on page 372.

Registering PCs can be automated to a certain extent. You can configure the Persistent Agent to register PCs by hostname using . Then serve the Persistent Agent to users PCs either at login or by asking the user to download and install the agent. The agent connects to the FortiNAC server, registers the PC by hostname and sends information such as IP address and MAC address back to the database. Because the agent is only being used as a mechanism to register PCs, no security policy is required. See Agent overview on page 491 and Credential configuration on page 139.

Login scripts can be used to automatically register PCs as network users log onto the network. The script must be modified slightly to indicate that PCs should be registered by hostname. See Passive registration on page 96.

View devices

There are many options for viewing devices that have been added to FortiNAC.

- **Network Devices View** — Displays lists of devices in a table. Links in the Views column allow you to display additional device information and configuration views. See Network devices on page 833.
- **Topology View** — Displays lists of devices on the left side. When a device is selected, the right pane displays known information about that device with a graphic representation of device ports and connections. See Topology view on page 712.
- **Host View** — Displays rogues or unknown devices and any devices that were manually registered and configured to display in Host View. See Host view on page 793.
- **Dashboard** — Host Summary and Device Summary panels provide totals for each device type broken down by status. See Host summary on page 41 and Network device summary on page 42.

Learning about hosts on the network

When a host is on the network, FortiNAC needs to know that the host has connected or disconnected and what that host's IP address and MAC address are. FortiNAC can learn this information in several ways including, link up/link down traps sent by the switch, MAC learned traps sent by the switch with the MAC address or by polling network devices.

Link up and link down traps

If a device on the network supports link up and link down traps, you should enable this feature and configure the device to send traps to the IP address of the FortiNAC Server or Control Server. As soon as the device is modeled in FortiNAC, FortiNAC listens for traps from that device. When FortiNAC receives a Linkup trap, it polls the switch to read the available host information. If FortiNAC does not receive information from the device after the first poll, it retries up to seven times.

Polling triggered by traps is configured from **System > Settings > Network Device**. The Minimum Trap Period (Sec) field controls the number of seconds FortiNAC waits after receiving a linkup trap before reading the forwarding table from the switch associated with the trap. The default is 10 seconds. The Max Number of Trap Periods field controls the number of periods FortiNAC waits before reading the forwarding table on the switch. The default setting for this field is 4. The number of retries is not configurable. See Network device on page 130.

If you use link up traps, the process for learning that the host is connected and its MAC address and IP address is as follows:

1. A host connects to a switch.
2. The switch sends a link up trap to FortiNAC.
3. Assuming that the Minimum Trap Period is set to 10 seconds and the Max Number of Periods is set to 4, then FortiNAC waits 40 seconds to read the forwarding table on the switch.
4. If the host's MAC Address is not returned, FortiNAC waits another 40 seconds and reads the forwarding table on the switch again. FortiNAC repeats this process up to seven times until it retrieves the host data.
5. If after seven retries the host data is not retrieved, FortiNAC does not try any more until the next scheduled poll for the device.

It is possible for a trap to be sent from the device and not be received by FortiNAC. Therefore, in addition to traps it is important to configure polling intervals in FortiNAC for each of your devices. Configuring polling is particularly important for wireless devices because it is the method used to determine that a host has disconnected from the wireless device. See L2 polling (resync hosts) on page 748 and L3 polling (IP address to MAC address) on page 750.

MAC notification traps

MAC Learned or MAC Notification Traps are traps that send host information when the host connects or disconnects alleviating the need for FortiNAC to poll. These traps are only supported on some devices, such as Cisco switches. If MAC Notification traps are available and supported by FortiNAC for the device, it is beneficial to enable them and reduce network traffic created by frequent polling. To use MAC Notification Traps they must be enabled on the device and configured to be sent to the IP address of the FortiNAC Server or Control Server and the device must be modeled in FortiNAC.

If you enable MAC Notification or MAC Learned traps on a device, you should disable Link Up and Link Down traps. They are redundant, cause additional traffic and prevent the MAC Learned event messages from being generated on FortiNAC.

If MAC Notification traps configured on Cisco devices are not being processed, verify the following:The SNMP user credentials entered in FortiNAC are for a User who is a member of a SNMP Group on the device. That the SNMP Group is configured with the contexts the group needs to access. Below is an example from a running configuration on a Cisco device:

```
snmp-server group testv3 v3 auth write view2
snmp-server group testv3 v3 auth context vlan-35
snmp-server group testv3 v3 auth context vlan-85
```

Polling

FortiNAC has a built in polling mechanism that compensates for missed traps or devices that are not configured to send traps by reading tables on network devices and retrieving host information. Polling information is stored for each device individually including: Enable/Disable Polling, Polling Interval, Last Successful Poll Time and Last Attempted Poll Time. For L3 devices Polling Priority is also stored.

Using the polling interval and the Last Successful Poll information stored for the device, FortiNAC polls devices individually. For example if device A has a polling interval of 15 minutes and a Last Successful Poll time of 10:15, then the next poll happens at 10:30 regardless of when other devices are being polled. The Last Successful Poll Time is updated any time the device is read, including using the Poll Now option or when a trap triggers FortiNAC to read the device. Updating Last Successful Poll Time for each contact with the device prevents unnecessary polling.

The Polling interval on devices is set initially based on device media type (wired or wireless). When network devices are discovered, they are analyzed and placed in groups. L2 devices are automatically placed in either the L2 Wired Devices or L2 Wireless groups. The default polling interval is 10 minutes for wireless devices and one hour for wired devices. Polling on wireless devices is more frequent because it is the only method for determining that a host has disconnected from the wireless device.

A default L3 (IP --> MAC) group is created by FortiNAC. During discovery this group is not automatically populated. You must add your L3 devices to this group.

Traps and SNMP support

The following table lists the traps and SNMP version that FortiNAC supports.

Vendor	Trap Name	OID	SNMP Version
MIB 2	linkUp	0.3	1
	linkDown	0.2	1
	linkUp	1.3.6.1.6.3.1.1.5.4	2
	linkDown	1.3.6.1.6.3.1.1.5.3	2
HP	MACNotification	1.3.6.1.4.1.11.2.14.11.5.1.66.1.7	1
Aerohive	LinkTrap	1.3.6.1.4.1.26928.1.1.1.1.1	1
	LinkTrap	1.3.6.1.4.1.26928.1.1.1.1.1.3	2
Extreme	linkUp	1.3.6.1.4.1.1916.2.131.50.0.16.0.1	2
	linkDown	1.3.6.1.4.1.1916.2.131.50.0.16.0.2	2
	MACNotification	1.3.6.1.4.1.1916.1.16.6.1	1
	MacAdded	1.3.6.1.4.1.1916.1.16.6.0.1	2
	MacDeleted	1.3.6.1.4.1.1916.1.16.6.0.2	2
	MacMoved	1.3.6.1.4.1.1916.1.16.6.0.3	2
Cisco	MacNotification	1.3.6.1.4.1.9.9.215.1.1.8.1.2	1

Vendor	Trap Name	OID	SNMP Version
H3C	MacNotification	1.3.6.1.4.1.25506.2.87.1.3.0.1	2
	MacNotification2	1.6.1.3.6.1.4.1.25506.2.87.1.4	2
	MacNotification3	1.3.6.1.4.1.25506.2.87.1.4	2
Juniper	MacNotification	1.3.6.1.4.1.2636.3.40.1.7.2.0.1	2
	MacNotification	1.3.6.1.4.1.2636.3.40.1.7.1.1.1.8.1.2	1
Brocade	Trap	1.3.6.1.4.1.1991	1, 2

Isolate unknown devices

When any device connects to the network FortiNAC checks to see if it is registered or not. Registered devices are allowed to access the production network. Unregistered or unknown devices are placed in an isolation VLAN. There is some configuration required to isolate unknown devices.

VLANs

Make sure that you have at least one isolation VLAN where unknown devices can be placed until they are registered. Typically this is called the Registration VLAN. The condition for being placed in the Registration VLAN is that the device be unknown.

VLANs should also be configured on each switch or controller. VLANs should be read from the switches and included in the model configuration for each switch. See Network access/VLANs on page 745 and Model configuration on page 767.

Forced registration group

Ports that will be used to access your network should be placed in the Forced Registration Group. Placing ports in the Forced Registration Group, indicates to FortiNAC that unregistered devices connecting on those ports must be placed in the Registration VLAN to be isolated until the device is registered. For instructions on placing ports in this group

Control access based on device types

Depending on the demands of your organization you may need to limit device access to the network by time of day or by the type of Device. You may need to alter device parameters, such as baud rate or setting up traps, based on the type of device and where it is connecting.

Disable devices with scheduled tasks

To disable ports or adapters based on time of day use the Scheduler to create Scheduled Tasks that act on groups of ports or devices. The Scheduler associates tasks with groups. Therefore, either the affected ports must be placed in a port group or the affected devices must be placed in a host group. Only those devices that have been registered and configured to display in the Host View can be included in a host group. Since disabling ports blocks all network access, it is recommended that you disable the adapters of the devices that should be denied access to the network. For additional information see Add groups on page 839 and Add a task on page 850.

Modify device settings

FortiNAC has the ability to store and use sets of CLI commands called CLI configurations. These command sets can be very powerful when managing devices and have several implementation options. CLI configurations can be implemented:

- By using the Scheduler to complete a task, such as setting up Link up/ Link down traps on a series of switches.
- By the role assigned to the device and the port on which it connects. For example, you could alter the baud rate of a medical device when it connects to the network.
- Through the model configuration of the switch to control VLANS or to implement ACLs that control connecting devices.

See CLI configuration on page 928 for additional information.

Role based access

Every device in FortiNAC is assigned a role of NAC Default as it registers. Additional roles can be created and assigned to devices that require network services, such as printers. Only those devices that have been registered and configured to be managed in Topology View can use role-based access. Ports or switches must be placed in Port or Device groups. For example, if you have a role called Accounting, you can map that role to devices in with role X. Then indicate that when a device in with role X connects to the network through a switch or port in group Y, that device can only access VLAN 10. See Role management on page 553 for detailed instructions.

View logs and reports

As devices register, and connect and disconnect from the network data is collected for all of those transactions. In addition events and alarms are generated depending on the activities of the device. Logs and reports that display device activity include the following:

- **Events View** — Displays a chronological list of events generated by device activity on the network. Each event contains data pertaining to the device that triggered the event, such as IP address or MAC address. See Events view on page 867.
- **Connections View** — Displays the connection log of users and hosts that have connected to the network. See Connections view on page 927.
- **Reports View** — Provides access to standard reports and allows you to create custom reports based on the information in the database. The report data may be output to HTML, CSV, EXCEL, XML, RTF, and PDF formats.

Policies

Policies are assigned to hosts based on the User/Host Profile associated with each policy. User/Host Profiles allow you to select one or more pieces of user or host data to match with users and hosts and determine which policy is applied to that host. Policies are ranked in priority starting with number 1. When a host requires a particular service, such as Network Access, the host and user data are compared to the User/Host Profile in each policy starting with the first policy in the list. If the host and user do not match criteria in the first policy, the next one is checked until a match is found.

Types of data used to determine whether or not the host/user is a match include the following:

Data	Definition
Where (Location)	One or more port or device groups. A User/Host Profile can include more than one port or device group, however the connection location only needs to be contained in one of the selected groups. If the Location field is empty it is set to Any, indicating that location is not being used as criteria for the match, therefore any host connection location would be a match. .
Who/What by Group	One or more user or host groups. If the host or user is in at least one of the groups listed, then the host is considered a match. If this field is empty, it is set to Any, indicating that the Groups field is not used as criteria for the match, therefore any host is a match.
Who/What by Attribute	Allows you to create matches based on Adapter, Host or User data. A single filter can contain checks for multiple pieces of data, however the host, user and adapter must be an exact match to all of that data. If more than one filter is used, the host, user and adapter need only match the contents of one filter to be a match for the policy. See Filter example on page 393 for additional information on filters.
When	Allows you to create matches based on the current time. If Always is selected, then time of day is not used. If Specify Time is selected, then the current time must be within the days and times included in the list to be a match for the host.

The host/user must match at least one item in each field that contains criteria other than Any. If the host/user does not match something in all fields, the policy is not selected and the next policy is checked.

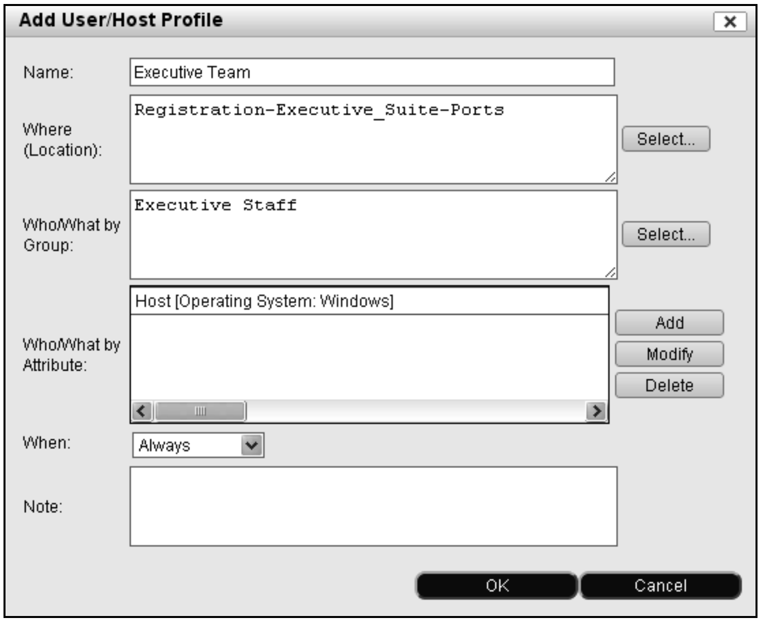
A host that has had a policy applied based on time of day, may be moved to a different policy when the window of time in the current policy has passed. For example, the host may be moved to another VLAN or disconnected from the network when the window of time in the applied Endpoint Compliance Policy has passed. Hosts are re-evaluated frequently, such as, when the device where they are connected is polled or when the Persistent Agent contacts the server. If another Policy exists that applies to this host, the host will be provided with configuration parameters from that new policy.

There may be more than one Policy that is match for this host/user, however, the first match found is the one that is used.

Policy assignments are not permanent. Each time a host is re-evaluated by FortiNAC, the User/Host Profile data is re-evaluated and a Policy is selected.

Policy assignment

Policies are applied to hosts by comparing user and host data to the User/Host Profile contained in the each policy until a match is found. The example below demonstrates this process.



Name: Executive Team

Where (Location): Registration-Executive_Suite-Ports

Who/What by Group: Executive Staff

Who/What by Attribute: Host [Operating System: Windows]

When: Always

Note:

Policy types

Policy Type	Location	Groups	Attributes	Time	Host Notes
Location Based	One or more Port or Device Groups	Any	None	Always	Host connects to a port or device in one of the selected groups and is assigned this policy.
Role Based	Any	Any	User Role = (Role Name)	Always	Host connects to the network. If the logged in user has the selected role, the host is assigned this policy.
Role Based	Any	Any	Host Role = (Role Name)	Always	Host connects to the network. If the host has the selected role, it is assigned this policy.
Security and Access Attribute Value	Any	Any	User SaaV = (Attribute Value)	Always	Host connects to the network. If the logged in user has the selected Security and Access Value, the host is assigned this policy.

Policy Type	Location	Groups	Attributes	Time	Host Notes
Group Based	Any	User Group1 User Group2	None	Always	Host connects to the network. If the logged in user is a member of either one of the selected groups, the host is assigned this policy.
Group Based	Any	Host Group1 Host Group2	None	Always	Host connects to the network. If the host is a member of either one of the selected groups, it is assigned this policy.
Guest	Any	Any	Guest Role = Role Name	Always	Host connects to the network. If the Guest has the selected role, the host is assigned this policy.
Registration	Any	Any	Host = Rogue	Always	Host connects to the network. If the host is a rogue, it is assigned this policy.
Remediation	Any	Any	Host State = At Risk	Always	Host connects to the network. If the host state is At Risk, it is assigned this policy.
VPN	Any	Any	Host = VPN Client	Always	Host connects to the network. If the host is a VPN Client, it is assigned this policy.
Time of Day	Any	Any	None	Monday - Friday 9 am to 5 pm	Host connects to the network. If the connection time is on any day Monday through Friday and between 9 am and 5 pm, it is assigned this policy.
Default or Catch All	Any	Any	None	None	This policy will match ALL hosts and users. Host connects to the network. If the host does not match any other policy, it is assigned this policy. When this policy is reached, no other policies after it will be considered.

Example endpoint compliance policy

The example below outlines how FortiNAC would choose an Endpoint Compliance Policy for a specific host.

Assume the Host has the following characteristics:

- Connects on a port that is contained within the Library Ports group.
- Host is a member of the Accounting Group and the Finance Group.
- Host is running a Persistent Agent.

- Logged in user has a Role called Management.
- Logged in user has a Security and Access Attribute value of Accounting.

Rank	Policy	Location	Groups	Attributes	Process
1	Policy A	Port Group = Lobby Ports	Accounting	Filter1=User Role "Staff"	**Location** - Not a match **Group** - Matches **Attribute1** - Not a Match Go to the next policy.
2	Policy B	Port Group = Library Ports	Accounting	Filter1=User Role "Management" and User Security and Access Value "Human Resources" Filter2=User Role "Staff"	**Location** - Matches **Group** - Matches **Filter1** - Does not match both pieces of data. **Filter2** - Does not match. Go to the next policy.
3	Policy C	Port Group1 = Lobby Ports Port Group2 = Second Floor Ports	Finance Admin	Filter1=User Role "Staff" and User Security and Access Value "Accounting" Filter2=User Role "Management" and Host has Persistent Agent	**Location** - Not a match for either location. **Group** - Matches Finance group **Filter1** - Does not match both pieces of data. **Filter2** - Matches all data. In this case, the fact that the neither location matches prevents the host from getting this policy.In the Group field, the host or user need only match one group. In the filter field, the host or user need only match one filter as long as it matches all parts of the filter. Go to the next policy.
4	Policy D	Any	Finance Admin	Filter1=User Role "Management" and Host has Persistent Agent Filter2=User Role "Executives" and Host has Persistent Agent	**Location** - No location selected so this field is not used. **Group** - Matches Finance group **Filter1**=Matches all data **Filter2**=Does not match both pieces of data This policy is selected for the host because Location is irrelevant, one group matches and one filter matches.

Rank	Policy	Location	Groups	Attributes	Process
5	Policy E	Port Group1 = Library Ports Port Group2 = Second Floor Ports	Finance Admin	Filter1=User Role "Management" and Host has Persistent Agent Filter2=User Role "Executives" and Host has Persistent Agent	**Location** - Matches Port Group1 **Group** - Matches Finance group **Filter1**=Matches all data **Filter2**=Does not match both pieces of data This policy is not selected because policies are checked in order by rank. The policy in rank 4 has already been selected even though this policy matches on more points. You must be careful about the order of the policies to ensure that the correct policy is applied to a host.

Policy details

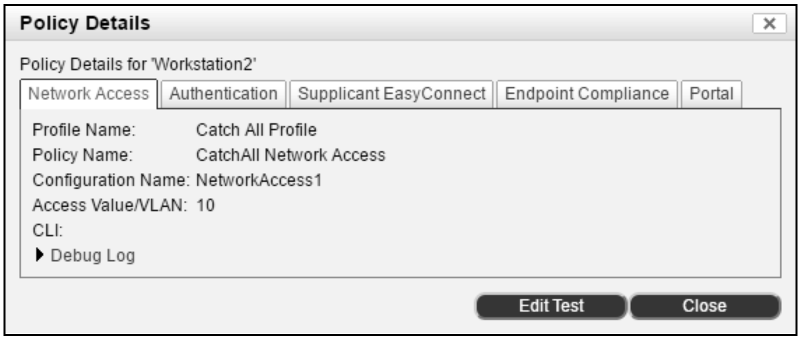
Policy Details assesses the selected host or user and displays the specific profile and policies that apply to the host at the moment the dialog was opened. User/host profiles have a time component and hosts may be connected at different locations. Therefore, the profile and policy displayed in Policy Details now, may be different than the profile and policies that display tomorrow. Policies displayed in this view include: Network Access Policies, Endpoint Compliance Policies, Supplicant Policies and Portal Policies. Each type of policy is displayed in a separate tab that also contains a Debug Log. This log can be sent to Customer Support for analysis.

To access Policy Details from Host View:

1. Select **Hosts > Host View**.
2. Search for the appropriate host.
3. Select the host and either right-click or click the **Options** button.
4. From the menu, select **Policy Details**.

To access Policy Details from User View

1. Select **Users > User View**.
2. Search for the appropriate user.
3. Select the user and either right-click or click the **Options** button.
4. From the menu, select **Policy Details**.

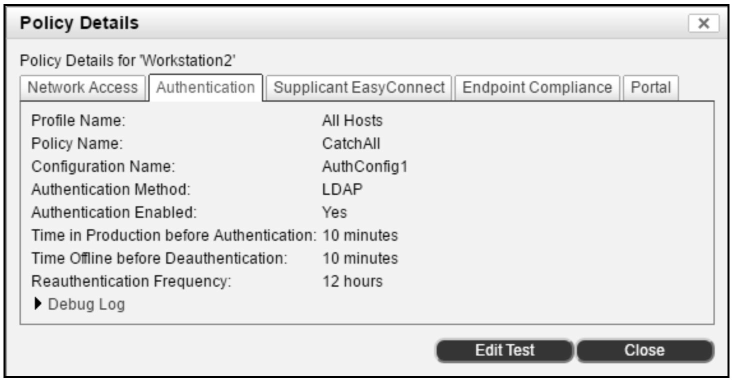


Policy Details for 'Workstation2'

Profile Name: Catch All Profile
Policy Name: CatchAll Network Access
Configuration Name: NetworkAccess1
Access Value/VLAN: 10
CLI:

Network access settings

Field	Definition
Profile Name	Name of the User/Host profile that matched the selected host or user when it was assessed by Policy Details. This profile contains the required criteria for a connecting host, such as connection location, host or user group membership, host or user attributes or time of day. Host connections that match the criteria within the User/Host Profile are assigned the associated Network Access Policy and Network Access Configuration. See User/host profiles on page 389.
Policy Name	Name of the Network Access Policy that currently applies to the host. See Network access policies on page 407.
Configuration Name	Name of the configuration that currently applies to the host. This is the configuration for the VLAN, CLI Configuration or VPN Group Policy for the host. See Network access configurations on page 412.
Access Value/VLAN	The specific network access that would be provided to the host, such as a VLAN ID or Name.
CLI	Name of the CLI Configuration that currently applies to this host or the connection port. This field may be blank.
Debug Log	Click this link to display a log of the policy assessment process. Text within the log can be copied and pasted into a text file for analysis by Customer Support.
Edit Test	Opens the Test Policy dialog where you can simulate host, adapter, and user combinations to create test scenarios for policies and profiles. See Policy simulator on page 386.



Policy Details

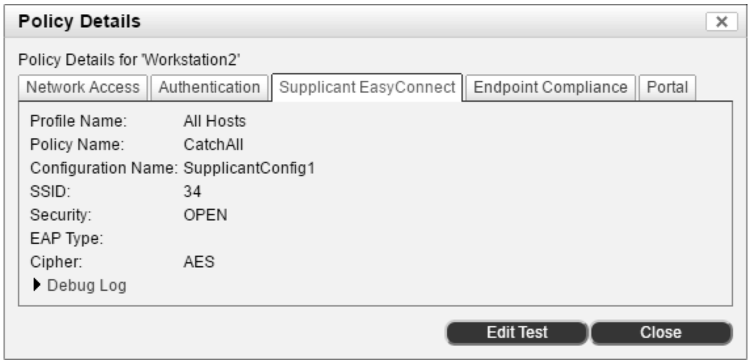
Policy Details for 'Workstation2'

Profile Name: All Hosts
Policy Name: CatchAll
Configuration Name: AuthConfig1
Authentication Method: LDAP
Authentication Enabled: Yes
Time in Production before Authentication: 10 minutes
Time Offline before Deauthentication: 10 minutes
Reauthentication Frequency: 12 hours

Authentication tab settings

Field	Definition
Profile Name	Name of the User/Host profile that matched the selected host or user when it was assessed by Policy Details. This profile contains the required criteria for a connecting host, such as connection location, host or user group membership, host or user attributes or time of day. Host connections that match the criteria within the User/Host Profile are assigned the associated Network Access Policy and Network Access Configuration. See User/host profiles on page 389.

Field	Definition
Policy Name	Name of the Network Access Policy that currently applies to the host. See Network access policies on page 407.
Configuration Name	Name of the configuration that currently applies to the host. This is the configuration for the VLAN, CLI Configuration or VPN Group Policy for the host. See Network access configurations on page 412.
Authentication Method	When enabled, the selected authentication method will override all other authentication methods configured in the portal, guest/contractor template, and Persistent Agent Credential configuration.
Authentication Enabled	Indicates whether Authentication is enabled. When enabled, the user is authenticated against a directory, the FortiNAC database, or a RADIUS server when logging on to access the network.
Time in Production before Authentication	When a user is waiting to authenticate, the host remains in the production VLAN until this time expires. If the user fails to authenticate within the time specified, the host is moved to the Authentication VLAN.
Time Offline before Deauthentication	Once the host is offline, the user remains authenticated for this period of time. If the host comes back online before the time period ends the user does not have to reauthenticate. If the host comes back online after the time period ends, the user is required to re-authenticate.
Reauthentication Frequency	When set, this forces users to re-authenticate after the amount of time defined in this field passes since the last authentication regardless of the host's state. The host is moved to the authentication VLAN.
Debug Log	Click this link to display a log of the policy assessment process. Text within the log can be copied and pasted into a text file for analysis by Customer Support.

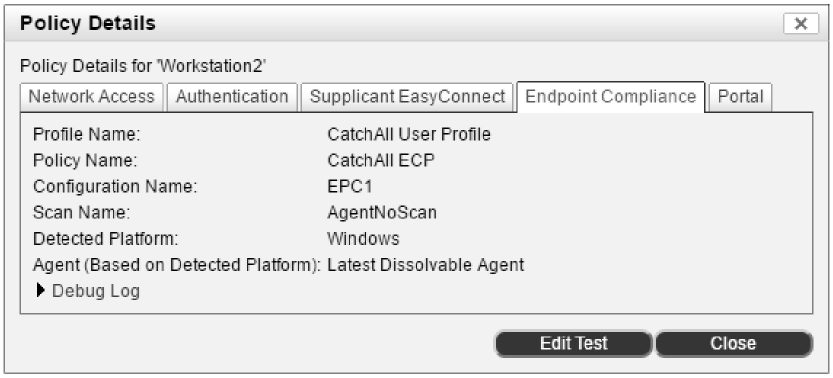


Policy Details for 'Workstation2'

Profile Name: All Hosts
Policy Name: CatchAll
Configuration Name: SupplicantConfig1
SSID: 34
Security: OPEN
EAP Type:
Cipher: AES
▸ Debug Log

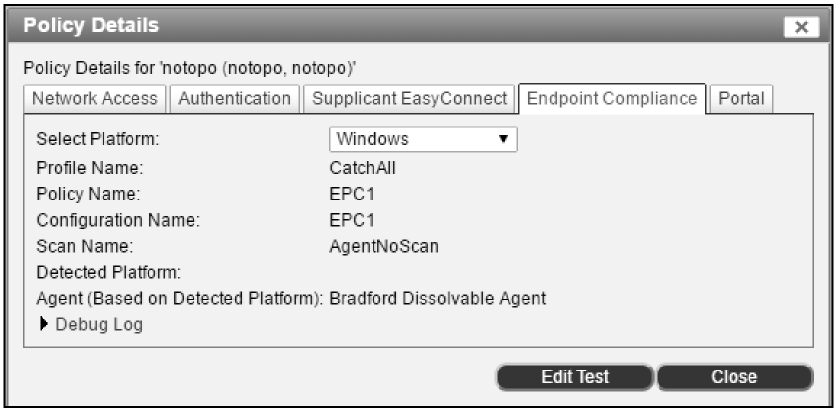
Supplicant EasyConnect tab settings

Field	Definition
Profile Name	Name of the User/Host profile that matched the selected host or user when it was assessed by Policy Details. This profile contains the required criteria for a connecting host, such as connection location, host or user group membership, host or user attributes or time of day. Host connections that match the criteria within the User/Host Profile are assigned the associated Supplicant Policy and Supplicant Configuration. See User/host profiles on page 389.
Policy Name	Name of the most recent Supplicant Policy that currently applies to the selected host. See Supplicant EasyConnect policies on page 471.
Configuration Name	Name of the configuration that applies to the selected host. This is the configuration for the supplicant on the host to allow access on a particular SSID. See Supplicant configurations on page 476.
SSID	Name of the SSID for which the supplicant is being configured.
Security	Type of encryption that used for connections to this SSID, such as WEP or WPA.
EAP Type	Currently only PEAP is supported. Not always required. This field may be blank.
Cipher	Encryption/decryption method used in conjunction with the information in the Security field to secure this connection.
Debug Log	Click this link to display a log of the policy assessment process. Text within the log can be copied and pasted into a text file for analysis by Customer Support.


Policy Details

Policy Details for 'Workstation2'

Profile Name: CatchAll User Profile
Policy Name: CatchAll ECP
Configuration Name: EPC1
Scan Name: AgentNoScan
Detected Platform: Windows
Agent (Based on Detected Platform): Latest Dissolvable Agent

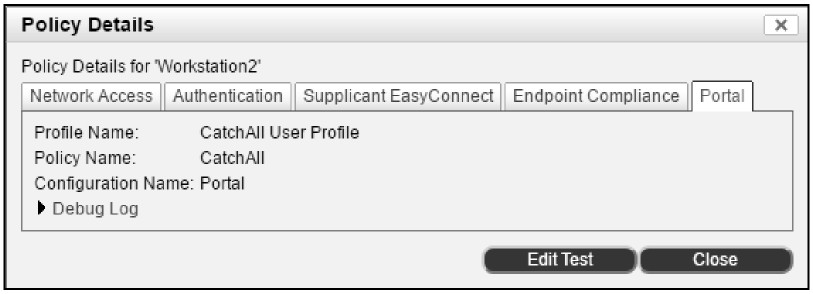

Policy Details

Policy Details for 'notopo (notopo, notopo)'

Select Platform: Windows
Profile Name: CatchAll
Policy Name: EPC1
Configuration Name: EPC1
Scan Name: AgentNoScan
Detected Platform:
Agent (Based on Detected Platform): Bradford Dissolvable Agent

Endpoint compliance tab settings

Field	Definition
Select Platform	When the Policy Details option is selected from the User View, you must select the Platform of the device that the user anticipates connecting to the network. The platform is used to determine the agent that would be assigned to the host. Not all platforms are displayed here. Only the platforms that support the Persistent or Mobile Agent.
Profile Name	Name of the User/Host profile that matched the selected host. This profile contains the required criteria for a connecting host, such as connection location, host or user group membership, host or user attributes or time of day. Host connections that match the criteria within the User/Host Profile are assigned the associated Endpoint Compliance Policy and Endpoint Compliance Configuration. See User/host profiles on page 389.
Policy Name	Name of the Endpoint Compliance Policy currently applies to the selected host. See Endpoint compliance policies on page 415.
Configuration Name	Name of the configuration that currently applies to the selected host. This is the configuration for the Scan and Agent for the host. See Endpoint compliance configurations on page 420.
Scan Name	Name of the scan that would be used to evaluate this host. See Scans on page 426.
Detected Platform	The device type, such as iPhone or Android, that FortiNAC thinks the host is, based on the information currently available in the system.
Agent	Agent setting that would be applied to the host. Determines whether or not an agent is used and which agent is required. Agent settings are selected in the Endpoint Compliance Configuration.
Debug Log	Click this link to display a log of the policy assessment process. Text within the log can be copied and pasted into a text file for analysis by Customer Support.



Policy Details for 'Workstation2'

Profile Name: CatchAll User Profile
Policy Name: CatchAll
Configuration Name: Portal
▸ Debug Log

Portal tab settings

Field	Definition
Profile Name	Name of the User/Host profile that matched the selected host or user when it was assessed by Policy Details. This profile contains the required criteria for a connecting host, such as connection location. Host connections that match the criteria within the User/Host Profile are assigned the associated Portal Configuration. See User/host profiles on page 389.

Field	Definition
Policy Name	Name of the Portal Policy that was applied to the host. See Portal policies on page 395.
Configuration Name	Name of the Portal Configuration that applied to the host. SeePortal content editor on page 250.
Debug Log	Click this link to display a log of the policy assessment process. Text within the log can be copied and pasted into a text file for analysis by Customer Support.

Policy simulator

The policy simulator allows users to customize information and create scenarios to be used to virtually test policies. Instead of connecting a physical device to the network at a specific time and location in order to test a policy, the Policy Simulator allows users to test policies by virtually simulating multiple host, adapter, and user combinations. The ability to reproduce complicated scenarios without being limited to the information currently available in the system provides more accurate test results for policies, such as Authentication or Portal.

You can test policies from the Host View and User View.

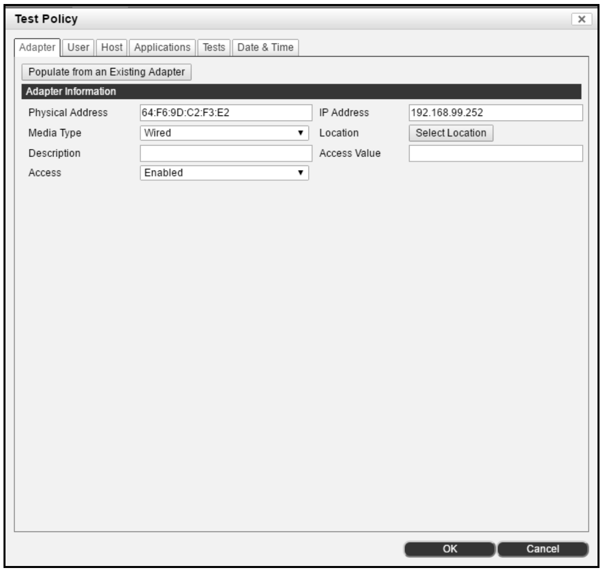
Host view

1. Select **Hosts > Host View**.
2. Search for the appropriate host.
3. Select the host and either right-click or click the **Options** button.
4. From the menu select **Policy Details**.
5. Select the tab for the policy you want to test.
6. Click **Edit Test**.
7. In the **Test Policy** dialog, click the tabs to enter the information for each scenario you want to test.
8. Click **OK** to see the matching policy and profile to verify that the policy and profiles are correctly configured.

User view

1. Select **Users > User View**.
2. Search for the appropriate user.
3. Select the user and either right-click or click the **Options** button.
4. From the menu select **Policy Details**.
5. Select the tab for the policy you want to test.
6. Click **Edit Test**.
7. In the **Test Policy** dialog, click the tabs to enter the information for each scenario you want to test.
8. Click **OK** to see the matching policy and profile to verify that the policy and profiles are correctly configured.

Adapter tab

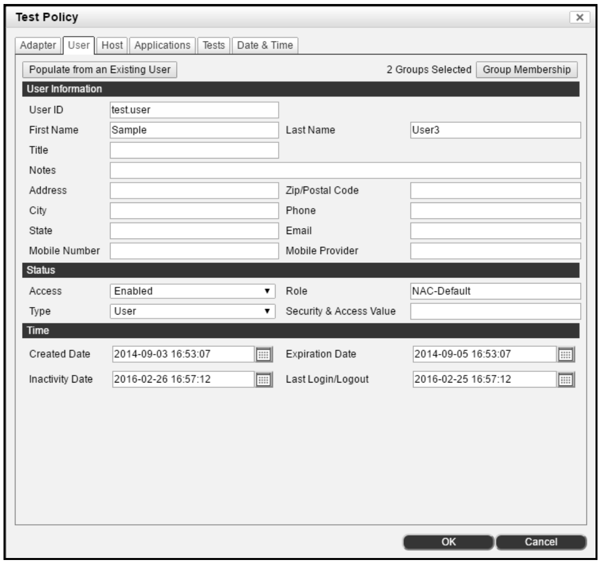


Adapter Information

Physical Address: 64:F6:9D:C2:F3:E2
IP Address: 192.168.99.252
Media Type: Wired
Location:
Description:
Access Value:
Access: Enabled

Enter information for the adapter you want to use to test the policy, or click Populate from an Existing Adapter to enter an existing adapter's information. See View and search settings on page 820.

User tab



User Information

User ID: test.user
First Name: Sample
Last Name: User3
Title:
Notes:
Address:
Zip/Postal Code:
City:
Phone:
State:
Email:
Mobile Number:
Mobile Provider:

Status

Access: Enabled
Role: NAC-Default
Type: User
Security & Access Value:

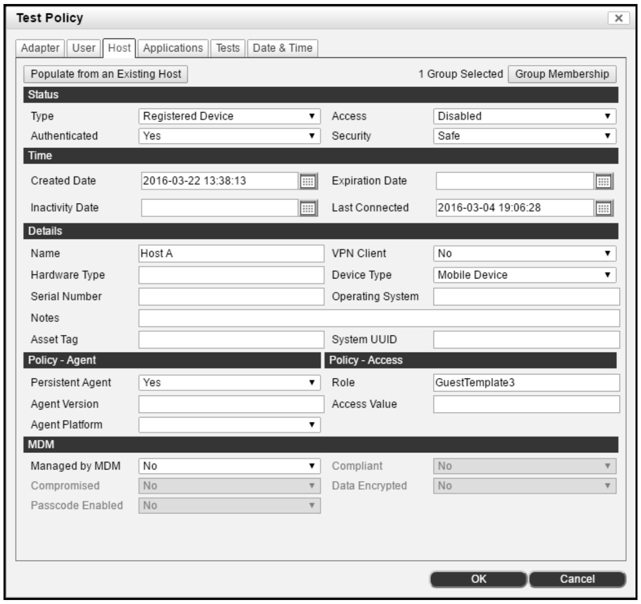
Time

Created Date: 2014-09-03 16:53:07
Expiration Date: 2014-09-05 16:53:07
Inactivity Date: 2016-02-26 16:57:12
Last Login/Logout: 2016-02-25 16:57:12

Enter information for the user you want to use to test the policy, or click Populate from an Existing User to enter an existing user's information. See Search settings on page 646.

To add or change User or Administrator Groups, click **Group Membership**.

Host tab



1 Group Selected

Status

Type	Registered Device	Access	Disabled
Authenticated	Yes	Security	Safe

Time

Created Date	2016-03-22 13:38:13	Expiration Date	
Inactivity Date		Last Connected	2016-03-04 19:06:28

Details

Name	Host A	VPN Client	No
Hardware Type		Device Type	Mobile Device
Serial Number		Operating System	
Notes			
Asset Tag		System UUID	

Policy - Agent		Policy - Access	
Persistent Agent	Yes	Role	GuestTemplate3
Agent Version		Access Value	
Agent Platform			

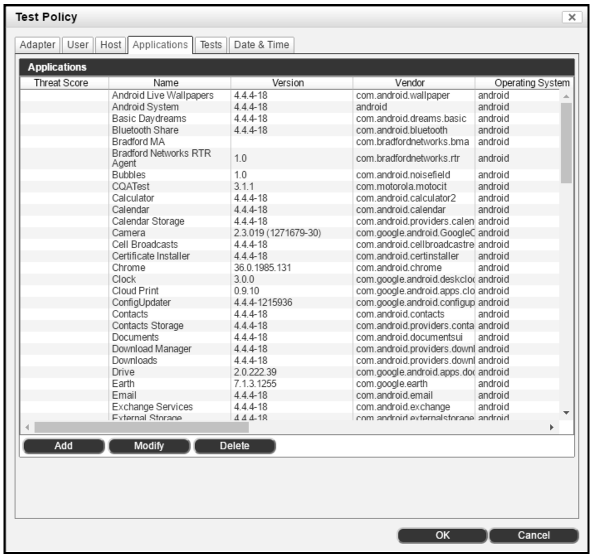
MDM

Managed by MDM	No	Compliant	No
Compromised	No	Data Encrypted	No
Passcode Enabled	No		

Enter information for the host you want to use to test policy, or click Populate from an Existing Host to enter an existing host's information. See Settings on page 795.

To add or change Host Groups, click **Group Membership**.

Applications tab



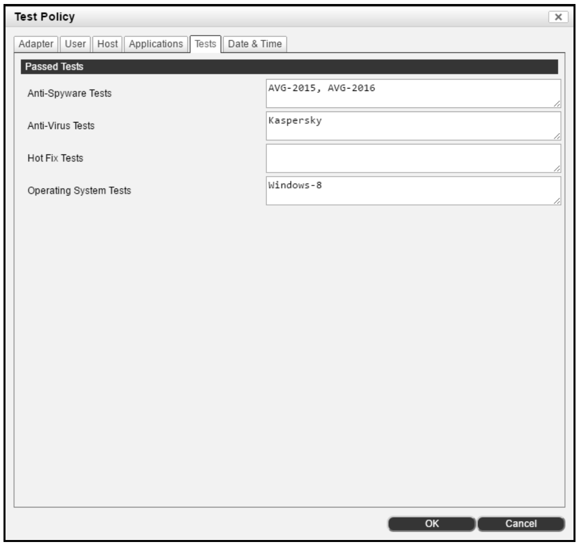
Applications

Threat Score	Name	Version	Vendor	Operating System
	Android Live Wallpapers	4.4.4-18	com.android.wallpaper	android
	Android System	4.4.4-18	android	android
	Basic Daydreams	4.4.4-18	com.android.dreams.basic	android
	Bluetooth Share	4.4.4-18	com.android.bluetooth	android
	Bradford MA		com.bradfordnetworks.bma	android
	Bradford Networks RTR Agent	1.0	com.bradfordnetworks.rtr	android
	Bubbles	1.0	com.android.noisefield	android
	CQATest	3.1.1	com.motorola.motocit	android
	Calculator	4.4.4-18	com.android.calculator2	android
	Calendar	4.4.4-18	com.android.calendar	android
	Calendar Storage	4.4.4-18	com.android.providers.calen	android
	Camera	2.3.019 (1271679-30)	com.google.android.GoogleC	android
	Cell Broadcasts	4.4.4-18	com.android.cellbroadcastre	android
	Certificate Installer	4.4.4-18	com.android.certinstaller	android
	Chrome	36.0.1985.131	com.android.chrome	android
	Clock	3.0.0	com.google.android.deskcloc	android
	Cloud Print	0.9.10	com.google.android.apps.clo	android
	ConfigUpdater	4.4.4-1215936	com.google.android.configup	android
	Contacts	4.4.4-18	com.android.contacts	android
	Contacts Storage	4.4.4-18	com.android.providers.conta	android
	Documents	4.4.4-18	com.android.documentsui	android
	Download Manager	4.4.4-18	com.android.providers.downl	android
	Downloads	4.4.4-18	com.android.providers.downl	android
	Drive	2.0.222.39	com.google.android.apps.doc	android
	Earth	7.1.3.1255	com.google.earth	android
	Email	4.4.4-18	com.android.email	android
	Exchange Services	4.4.4-18	com.android.exchange	android
	External Storage	4.4.4-18	com.android.externalstorage	android

Add, modify, or delete application(s) you want to use to test the policy. See Application view on page 825 for information about the fields in the Applications tab.

All changes are for testing purposes only, and do not affect applications in the system.

Tests tab



Passed Tests

Anti-Spyware Tests: AVG-2015, AVG-2016

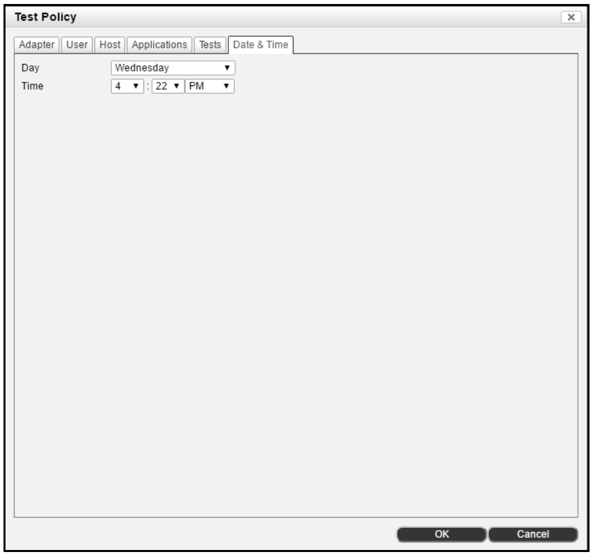
Anti-Virus Tests: Kaspersky

Hot Fix Tests:

Operating System Tests: Windows-8

Enter the required anti-virus software, hot fixes, and permitted operating systems to use to test the policy. Multiple entries for each category must be comma-separated.

Date & time tab



Day: Wednesday

Time: 4 : 22 PM

Select the day and time criteria to be used to test the policy.

User/host profiles

User/Host Profiles are used to map sets of hosts and users to Network Access Policies, Endpoint Compliance Policies, Supplicant EasyConnect Policies, Portal Policies, or Security Rules (ATR must be enabled). User/Host Profiles can be reused across many different policies.

For example, Network Access Policies are used to assign the VLAN in which a host is placed. Each Network Access Policy has a specific User/Host profile and a Network Access Configuration containing a VLAN, CLI Configuration or VPN Group. When a host requires network access, FortiNAC looks at the Network Access Policies starting with the first policy in the list and checks that the User/Host profile is a match. If it is not, the next Network Access Policy is checked until a match is found.

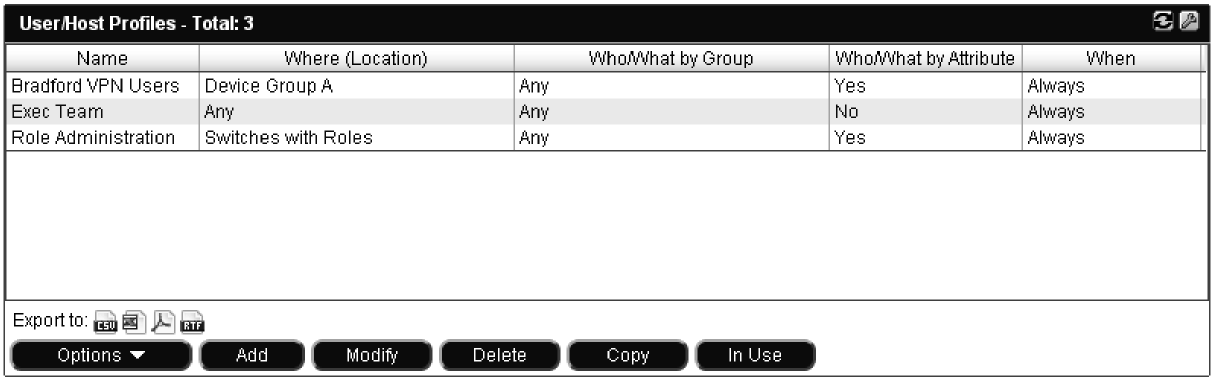
User/Host Profiles are combinations of User/Host data. A host's or user's profile is not fixed but can change based on the user/host being moved to a different group, having a new attribute applied, connecting to the network in a different place or the current time of day. Users/hosts are only classified at the time that they need a service, such as a Network Access Policy. When FortiNAC evaluates a host connection, the data for the user and host are prioritized as follows:

- Logged in User and Host
- Registered User and Host
- Registered Host

If you create a User/Host Profile with fields Where (Location) set to Any, Who/What by Group set to Any, Who/What by Attribute left blank and When set to always, it matches ALL users and hosts. This is essentially a Catch All profile. If this User/Host Profile is used in a policy, all policies below that policy are ignored when assigning a policy to a user or a host. To highlight this, policies below the policy with the catch all profile are grayed out and have a line through the data.

The best way to use a Catch All profile is to create a general policy with that profile and place it last in the list of policies.

User/Host Profiles can be accessed from **Policy > Policy Configuration > User/Host Profiles** or from **System > Quick Start > Policy Configuration**, however configuration steps point you to **Policy > Policy Configuration > User/Host Profiles**. See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.



User/Host Profiles - Total: 3

Name	Where (Location)	Who/What by Group	Who/What by Attribute	When
Bradford VPN Users	Device Group A	Any	Yes	Always
Exec Team	Any	Any	No	Always
Role Administration	Switches with Roles	Any	Yes	Always

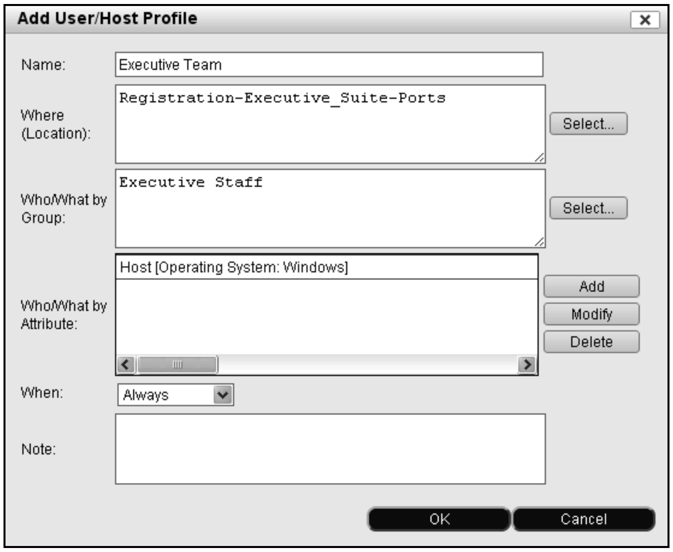
Settings

Field	Definition
Name	Each profile must have a unique name.

Field	Definition
Where (Location)	Location on the network where the host is connected. This field lists groups of ports, SSIDs or devices. Hosts are checked to determine whether they have connected to the network via one of the selected devices, ports or SSIDs. Host must connect on one of the items contained within one of the selected groups to match this profile. When set to Any, this field is a match for all hosts or users.
Who/What By Group	Host or User groups where the host or user must be a member to match this profile. Host or user must be in at least one of the groups listed. When set to Any, this field is a match for all hosts or users.
Who/What By Attribute	Indicates whether or not attribute filters have been created for this Profile. Filters are based on Adapter, Host and User data. A host or user must meet all parameters within a single filter, but is only required to match one filter in the list. See Filter example on page 393.
When	If the host is on the network during the specified time frame, it matches this profile. Time options include Always or a specific set of days of the week and times of the day.
Note	User specified note field. This field may contain notes regarding the data conversion from a previous version of FortiNAC.
Last Modified By	User name of the last user to modify the profile.
Last Modified Date	Date and time of the last modification to this profile.
Right click options	
Copy	Copy the selected Profile to create a new record.
Delete	Deletes the selected Profile. Profiles that are currently in use cannot be deleted.
In Use	Indicates whether or not the selected Profile is currently being used by any other FortiNAC element. See Profiles in use on page 395.
Modify	Opens the Modify Profile window for the selected Profile.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.
Buttons	
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.

Add or modify a profile

You are not required to complete all of the fields when creating a User/Host Profile. If you leave a field blank, it is set to Any or is left blank. When set to Any or blank, the field is a match for all hosts or users. You can create a profile with only location, only a group, only an attribute filter, only a time range or any combination of those options.



Add User/Host Profile

Name: Executive Team

Where (Location): Registration-Executive_Suite-Ports

Who/What by Group: Executive Staff

Who/What by Attribute: Host [Operating System: Windows]

When: Always

Note:

1. Select **Policy > Policy Configuration**.
2. In the menu on the left, **User/Host Profiles** should be selected.
3. Click the **Add** button or select an existing Profile and click **Modify**.
4. Click in the **Name** field and enter a name for this Profile.
5. Click the **Select** button next to the **Where (Location)** field. This opens the Select Location window.

   Choose one or more device, port or SSID groups by clicking on the names in the All Groups column and clicking the right arrow to move them to the Selected Groups column.

   In the Select Location window, you can click **Add Group** to create a group, or click **Modify Group** to modify the selected group.

   Click **OK** to continue.
6. Click the **Select** button next to the **Who/What by Group** field. This opens the Select Groups window.

   Choose one or more Host, User, or Administrator groups by clicking on the names in the All Groups column and clicking the right arrow to move them to the Selected Groups column.

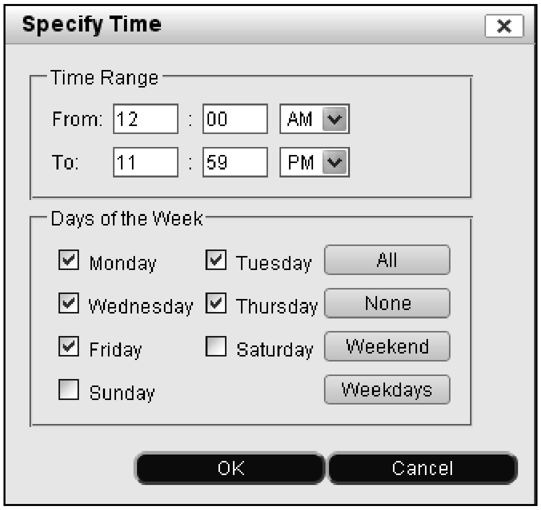
   In the Select Groups window, you can click **Add Group** to create a group, or click **Modify Group** to modify the selected group.

   Click **OK** to continue.
7. To add a filter, click the **Add** button next to the **Who/What by Attribute** field. These filters narrow the number of hosts to which this Profile applies.

   The Adapter, Host, User, Application Filter window displays allowing you to select one or more pieces of data to use as a filter. See Settings on page 795, View and search settings on page 820, Search settings on page 646, and Application view on page 825for detailed descriptions of the fields on the Filter window.
8. Click in the drop-down menu next to the **When** field. Select either **Always** or select **Specify Time**. **Always** indicates that there is no time criteria to match this Profile. **Specify Time** allows you to choose days and times to

be used as criteria for connecting hosts. Hosts must connect to the network during the selected times to match this profile.

9. To specify a time, select Specify Time in the drop-down to display the Specify Time dialog.



Specify Time

Time Range

From: 12 : 00 AM

To: 11 : 59 PM

Days of the Week

☑ Monday ☑ Tuesday

☑ Wednesday ☑ Thursday

☑ Friday □ Saturday

□ Sunday

In the **Time Range** section enter the **From** and **To** times for the time of day that devices should be able to access the network.

In the **Days of the Week** section select the days during which these devices should be allowed to access the network.

Click **OK**.

10. Click OK to save your data.

Filter example

User/Host Profiles contain filters to narrow the group of hosts or users that match a particular profile. This allows you to create special profiles for certain hosts or users and filter by host, adapter or user criteria. For example, if you had hosts that were running on different operating systems, you might want to have a special profile for each operating system. By filtering for the operating system, you could provide different treatment for each type of host without having to create and maintain special host groups.

Filter examples

Filters are based on Host, Adapter or User attributes and can be applied such that the host or user must meet all criteria or only some criteria. Within the Who/What by Attribute filter, the user/host must match all of the data specified. If there are multiple Who/What by Attribute filters, the user/host must match all of the data specified in only one of the filters.

Assume that you want to create User/Host Profile A to handle rogue hosts by Operating System. In this case, the host must meet the following criteria to match User/Host Profile A:

- **Location** = Connected to a device in Device Group A
- **Host Filter** = Running a Windows operating system and is a Rogue (not registered).

In the second example, the User/Host Profile contains two options under Who/What by Attribute. The first filter requires that the host state be Safe and Authenticated. The second filter requires that the host be a VPN client. In this case the host must meet the following criteria to match the User/Host Profile:

- **Location** = Connected to a device in Device Group A
- **Host Filter** = One of the following sets of options from the filters:
  - Host must be Safe and Authenticated
  - Host must be a VPN Client

Profile example

Assume that you are running a network at a University. You have Students and Faculty that must be allowed on the network. Due to the volume of traffic you determine that you will have four VLANs. This division of network users requires a mechanism for matching them to the appropriate VLANs. To accomplish this task you must do the following:

- Determine how you are going to divide your network users into four groups. In this case you decide that you will break up users as follows:
  - Students that connect to devices in Dorm A
  - Students that connect to devices in Dorm B
  - Faculty running Windows
  - Faculty running macOS
  - Make sure that Students are in a group labeled Students and Faculty are in a group labeled Faculty.
- Make sure that you have two device groups, one for devices in Dorm A and another for devices in Dorm B.
- Based on the divisions you have selected, you must create four User/Host Profiles. You need one Profile for each combination of data that defines a set of users, such as Students that connect to devices in Dorm A.
- Create four Network Access Configurations to configure the VLANs for your four groups of users.
- Create four Network Access Policies to map the four User/Host Profiles to the appropriate VLANs.

User/host profiles

Create four User/Host Profiles that have the following settings:

Name	Where (Location)	Who/What by Group	Who/What by Attribute	Time
Students Dorm A	Device Group = Dorm A Devices	User Group = Students	None	Always
Students Dorm B	Device Group = Dorm B Devices	User Group = Students	None	Always
Faculty Windows	Any	User Group = Faculty	Host OS = Windows	Always
Faculty macOS	Any	User Group = Faculty	Host OS = macOS	Always

Network access configurations

Create a Network Access Configuration for each of the four VLANs that you wish to assign. For this example we will create configurations for VLANS 10, 20, 30 and 40.

Name	Access Value
Students Dorm A VLAN	10
Students Dorm B VLAN	20
Faculty Windows VLAN	30
Faculty macOS VLAN	40

Network access policies

Now you must map the User/Host Profiles to the Network Access Configurations you created. That will tie the different types of users to the appropriate VLAN. Create four Network Access Policies that contain the following data:

Name	User/Host Profile	Network Access Configuration
Students Connecting in Dorm A	Students Dorm A	Students Dorm A VLAN
Students Connecting in Dorm B	Students Dorm B	Students Dorm B VLAN
Faculty running Windows	Faculty Windows	Faculty Windows VLAN
Faculty running macOS	Faculty macOS	Faculty macOS VLAN

Profiles in use

To find the list of FortiNAC features that reference a specific User/Host Profile, select the Profile from the User/Host Profiles View and click the In Use button. A message is displayed indicating whether or not the Profile is associated with any other features. If the Profile is referenced elsewhere, a list of each feature that references the Profile is displayed.

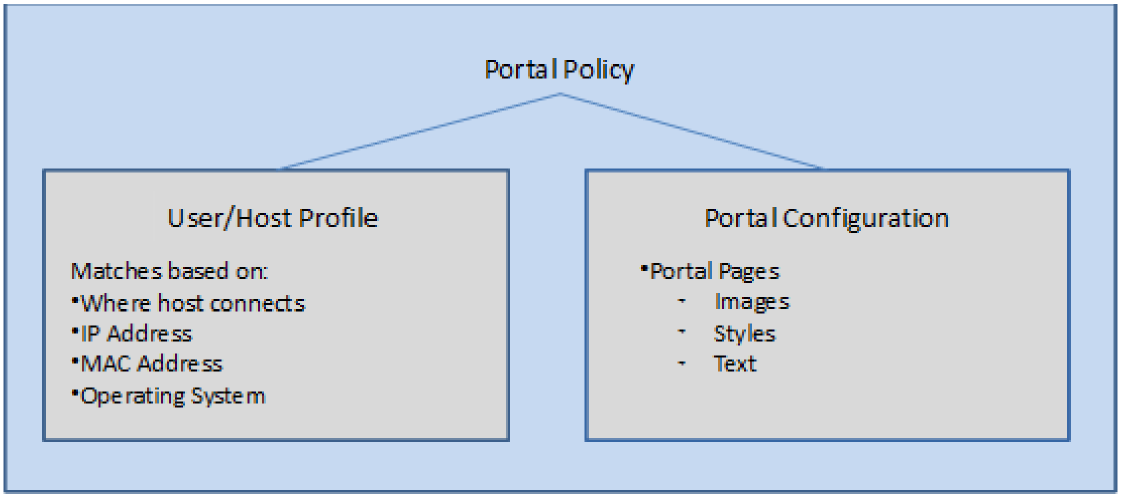
Delete a profile

If a profile is in use by another configuration or feature in FortiNAC, it cannot be deleted. A dialog displays with a list of the configurations in which the profile is used. Remove the association between the profile and other configurations before deleting the profile.

1. Click **Policy > Policy Configuration**.
2. In the menu on the left, **User/Host Profiles** should be selected.
3. Select the profile to be removed.
4. Click **Delete**.
5. Click **OK** to confirm that you wish to remove the profile.

Portal policies

A Portal Policy consists of one User/Host Profile and one Portal Configuration. The User/Host Profile is used to determine the hosts to which this policy might apply. The Portal Configuration controls the look and feel of the portal pages displayed to those users and hosts when they connect to the network and register. Portal Policies determine the portal assigned to a connecting host in an environment where there are multiple portals.



Portal Policies rely on a limited set of host information to match a Portal Configuration with a User/Host Profile. When an unregistered host connects to the network, there are only a few pieces of data that are known about the host and no data is known about the user. Therefore, the User/Host profile used in a Portal Policy can only use the connection location, the host IP address, the host MAC Address or the Operating System to match a connecting host.

Portal Policies are ranked with 1 being the highest rank. When a host connects to the network, the policies are evaluated from the highest rank down until a matching policy is found. That policy is assigned to the host and the portal within the policy is displayed.

There may be more than one Portal Policy that is a match for this host/user, however, the first match found is the one that is used.

If you create a User/Host Profile with fields Where (Location) set to Any, Who/What by Group set to Any, Who/What by Attribute left blank and When set to always, it matches ALL users and hosts. This is essentially a Catch All profile. If this User/Host Profile is used in a policy, all policies below that policy are ignored when assigning a policy to a user or a host. To highlight this, policies below the policy with the catch all profile are grayed out and have a line through the data.

The best way to use a Catch All profile is to create a general policy with that profile and place it last in the list of policies.

If a host does not match any of the policies listed, FortiNAC connects the host to the user-specified default portal. See Select a default portal on page 271.

Implementation

- Create a separate Portal Configuration for each group of users that requires different treatment. See Multiple portals on page 269.

- Create a User/Host Profile for each type of user, but base the profile on Host attributes that can be discovered when the host connects to the network, such as, connection location, IP address, MAC Address or Operating System. See User/host profiles on page 389.
- Create a Portal Policy for each group of users that requires different treatment. See Manage policies on page 397.

Manage policies

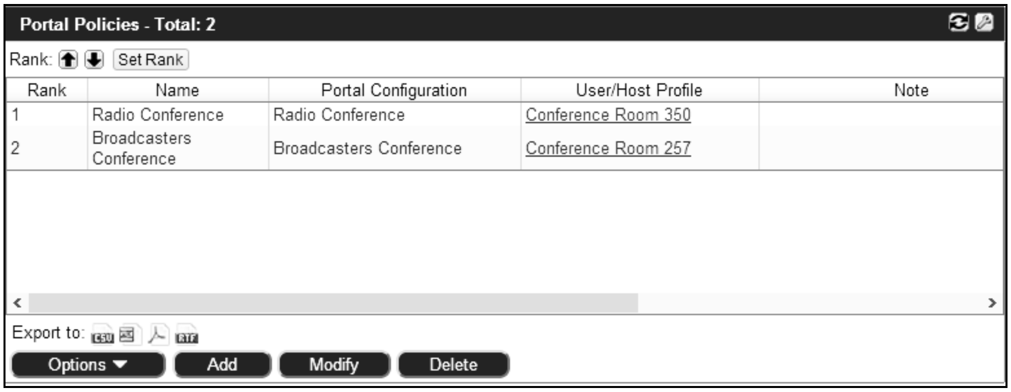
Create Portal Policies to assign a portal when an unregistered host connects to the network. Policies are selected for a connecting host by matching host attributes to the criteria defined in the associated User/Host Profile. The first policy that matches the host data is assigned.

If the host does not match any policy, it is assigned the default Portal. See Select a default portal on page 271.

If you create a User/Host Profile with fields Where (Location) set to Any, Who/What by Group set to Any, Who/What by Attribute left blank and When set to always, it matches ALL users and hosts. This is essentially a Catch All profile. If this User/Host Profile is used in a policy, all policies below that policy are ignored when assigning a policy to a user or a host. To highlight this, policies below the policy with the catch all profile are grayed out and have a line through the data.

The best way to use a Catch All profile is to create a general policy with that profile and place it last in the list of policies.

See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.



Portal Policies - Total: 2

Rank	Name	Portal Configuration	User/Host Profile	Note
1	Radio Conference	Radio Conference	Conference Room 350	
2	Broadcasters Conference	Broadcasters Conference	Conference Room 257	

Settings

An empty field in a column indicates that the option has not been set.

Field	Definition
Rank Buttons	Moves the selected policy up or down in the list. Host connections are compared to Policies in order by rank.

Field	Definition
Set Rank Button	Allows you to type a different rank number for a selected policy and immediately move the policy to that position. In an environment with a large number of policies this process is faster than using the up and down Rank buttons.
Table columns	
Rank	Policy's rank in the list of policies. Rank controls the order in which host connections are compared to Policies.
Name	User defined name for the policy.
Network Access Configuration	Contains the configuration for the portal that will be assigned if this Portal Policy matches the connecting host. See Portal content editor on page 250.
User/Host Profile	Contains the required criteria for a connecting host, such as connection location. Host connections that match the criteria within the User/Host Profile are assigned the associated Portal Configuration. See User/host profiles on page 389.
Where (Location)	The connection location specified in the User/Host Profile. The host must connect to the network on a device, port or SSID contained within one of the groups shown here to be a match. When set to Any, this field is a match for all hosts or users.
Who/What by Group	User or Host group or groups specified in the User/Host Profile. These groups must contain the connecting user or host for the connection to be a match for this policy. When set to Any, this field is a match for all hosts or users. It is not recommended that you use groups in User/Host Profiles for Portal assignment because an unregistered host will not be contained in any host groups and user data is unknown until after the portal is assigned.
Who/What by Attribute	User or Host attributes specified in the selected User/Host Profile. The connecting host or user must have the attributes to be a match. See Filter example on page 393. Do not select user attributes in User/Host Profiles used to assign a portal. FortiNAC does not have access to any user attributes when an unregistered host connects to the network. Only the following host attributes are known at the time of connection: connection location, IP address, MAC Address and Operating System.
When	The time frame specified in the selected User/Host Profile. The host must be on the network within this time frame to be a match. When set to Always this field is a match for all hosts or users.
Note	User specified note field. This field may contain notes regarding the data conversion from a previous version of FortiNAC.
Last Modified By	User name of the last user to modify the policy.
Last Modified Date	Date and time of the last modification to this policy.
Right click options	
Delete	Deletes the selected Portal Policy.
Modify	Opens the Modify Portal Policy window for the selected policy.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item.

Field	Definition
	For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.
Buttons	
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.

Add or modify a policy

1. Select **Policy > Policy Configuration**.
2. In the menu on the left select **Portal**.
3. Click the **Add** button or select an existing policy and click **Modify**.
4. Click in the **Name** field and enter a name for this policy.
5. Select a **User/Host Profile** from the drop-down menu. You can use the icons next to the User/Host Profile field to add a new profile or modify the profile shown in the drop-down menu. Note that if you modify this profile, it is modified for all features that make use of the profile. Connecting hosts must match this User/Host Profile to be assigned the Portal Configuration specified in the next step.

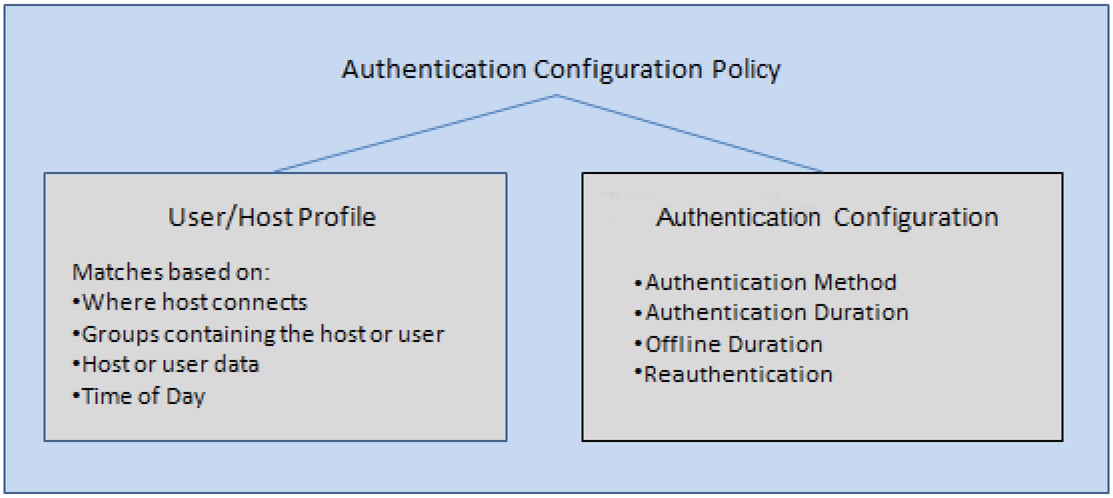
   User/Host Profiles for Portal Policies should contain some combination of connection location, host IP address, host MAC Address or Operating System as criteria for matching the connecting host. FortiNAC has no other information available at the time the host connects to the network and a portal must be assigned.
6. Select a **Portal Configuration** from the drop-down menu. If the Portal Configuration you need is not shown, you must go to the Portal Content Editor and create it before adding the Portal Policy. See Multiple portals on page 269.
7. The **Note** field is optional.
8. Click **OK** to save your Policy.

Delete a policy

1. Select **Policy > Policy Configuration**.
2. In the menu on the left select **Portal**.
3. Select a Policy and click **Delete**.
4. A confirmation message is displayed. Click **Yes** to continue.

Authentication policies

An Authentication Policy consists of one User/Host Profile and one Authentication Configuration. The User/Host Profile is used to determine the users and hosts to which this policy might apply. The Authentication Configuration assigns the treatment those users and hosts receive when they connect to the network.



The Authentication Configuration specifies the Time in Production before Authentication, Time Offline before Deauthentication, Reauthentication Frequency, and Authentication Method Policy that apply to a host that requires network access.

When Authentication Method is enabled, the selected authentication is used instead of the default authentication method. This authentication method will override the authentication methods selected for the portal login, guest/contractor template, and the Persistent Agent Credential Configuration. For example, if the Portal Configuration for the user's portal had a Standard User Login Type of LDAP, but the user matched an Authentication Policy with the Authentication Configuration set to Local, Local will be used instead. If the Authentication Method is not enabled, the default authentication method is used.

Policies are assigned based on matching data when a host requires network access. The host/user and the connection location are compared to each Authentication Policy starting with the first policy in the list. When a policy is found where the host and user data and the connection location match the selected User/Host Profile, that policy is assigned. Policy assignments are not permanent. Hosts are re-evaluated frequently, such as when a switch is polled or the Persistent Agent contacts the server. When host and user data are re-evaluated a different Authentication Policy may be selected.

There may be more than one Authentication Policy that is a match for this host/user, however, the first match found is the one that is used.

If you create a User/Host Profile with fields Where (Location) set to Any, Who/What by Group set to Any, Who/What by Attribute left blank and When set to always, it matches ALL users and hosts. This is essentially a Catch All profile. If this User/Host Profile is used in a policy, all policies below that policy are ignored when assigning a policy to a user or a host. To highlight this, policies below the policy with the catch all profile are grayed out and have a line through the data.

The best way to use a Catch All profile is to create a general policy with that profile and place it last in the list of policies.

Manage policies

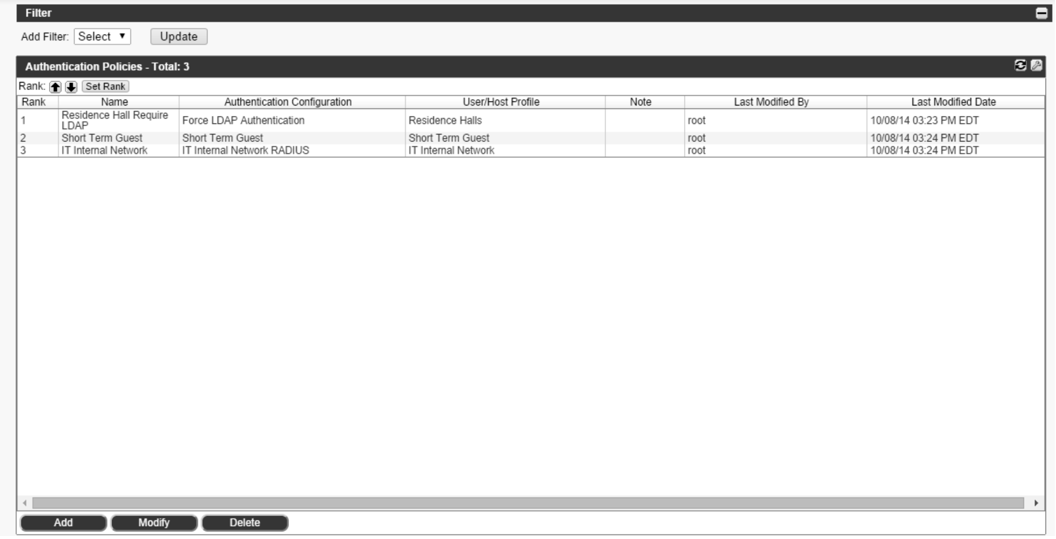
Create Authentication Policies to assign an Authentication Configuration when a host requires network access. Policies are selected for a connecting host by matching host and user data to the criteria defined in the associated User/Host Profile. The first policy that matches the host and user data is assigned.

If the host does not match any policy, it is assigned the default authentication method configured in the Portal, Guest Template, or Persistent Agent Credential Configuration.

If you create a User/Host Profile with fields Where (Location) set to Any, Who/What by Group set to Any, Who/What by Attribute left blank and When set to always, it matches ALL users and hosts. This is essentially a Catch All profile. If this User/Host Profile is used in a policy, all policies below that policy are ignored when assigning a policy to a user or a host. To highlight this, policies below the policy with the catch all profile are grayed out and have a line through the data.

The best way to use a Catch All profile is to create a general policy with that profile and place it last in the list of policies.

Authentication Policies can be accessed from **Policy > Policy Configuration > Authentication Policy**.



Authentication Policies - Total: 3

Rank	Name	Authentication Configuration	User/Host Profile	Note	Last Modified By	Last Modified Date
1	Residence Hall Require LDAP	Force LDAP Authentication	Residence Halls		root	10/08/14 03:23 PM EDT
2	Short Term Guest	Short Term Guest	Short Term Guest		root	10/08/14 03:24 PM EDT
3	IT Internal Network	IT Internal Network RADIUS	IT Internal Network		root	10/08/14 03:24 PM EDT

Settings

An empty field in a column indicates that the option has not been set.

Field	Definition
Rank Buttons	Moves the selected policy up or down in the list. Host connections are compared to Policies in order by rank.

Field	Definition
Set Rank Button	Allows you to type a different rank number for a selected policy and immediately move the policy to that position. In an environment with a large number of policies this process is faster than using the up and down Rank buttons.
Table columns	
Rank	Policy's rank in the list of policies. Rank controls the order in which host connections are compared to Policies.
Name	User defined name for the policy.
Authentication Configuration	Contains the configuration for the Authentication Policy that will be assigned if this Authentication Policy matches the connecting host. See Authentication configurations on page 404
User/Host Profile	Contains the required criteria for a connecting host, such as connection location, host or user group membership, host or user attributes or time of day. Host connections that match the criteria within the User/Host Profile are assigned the associated Authentication Configuration. See User/host profiles on page 389.
Note	User specified note field.
Last Modified By	User name of the last user to modify the policy.
Last Modified Date	Date and time of the last modification to this policy.
Right click options	
Delete	Deletes the selected Authentication Policy.
Modify	Opens the Modify Authentication Policy window for the selected policy.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.

Add or modify a policy

1. Select **Policy > Policy Configuration**.
2. In the menu on the left select **Authentication Policy**.
3. Click the **Add** button or select an existing policy and click **Modify**.
4. Click in the **Name** field and enter a name for this policy.
5. Select a **User/Host Profile** from the drop-down menu. You can use the icons next to the User/Host Profile field to add a new profile or modify the profile shown in the drop-down menu. Note that if you modify this profile, it is modified for all features that make use of the profile. Connecting hosts must match this User/Host Profile to be assigned the Authentication Configuration specified in the next step.
6. Select an **Authentication Configuration** from the drop-down menu. You can use the icons next to the Authentication Configuration field to add a new configuration or modify the configuration shown in the drop-down

menu. Note that if you modify this configuration, it is modified for all features that make use of it. See Add or modify a configuration on page 414.

7. The **Note** field is optional.
8. Click **OK** to save your policy.

Delete a policy

If a configuration is in use by another feature in FortiNAC, it cannot be deleted. A dialog displays with a list of the features in which the configuration is used. Remove the association between the configuration and other features before deleting the configuration.

1. Click **Policy > Policy Configuration**.
2. In the menu on the left select **Authentication Policy**.
3. Select the policy to be removed.
4. Click **Delete**.
5. Click **OK** to confirm that you wish to remove the policy.

When no profile or policy exists

The following describes authentication scenarios when no authentication profile or policy exists. In these cases, authentication was done via LDAP using the configuration in **System > Settings > Authentication > LDAP**.

Without an authentication policy, no host is marked with a red "A" to indicate the need to authenticate or to force authentication.

Wired connection and wireless MAC auth (authentication set to enforce)

You must have a Passive Agent Configuration set up in order to obtain logged on users via the Passive Agent.

When the Passive Agent Configuration is set to Register Host by User and a directory user logs into the host/domain where the rogue is registered, a logged on user is displayed. The logged on user is the user who is logged onto the domain. When the user logs off the domain, the logged on user in FortiNAC is removed.

If the passive agent configuration is not set to register the host, the host must register by another method. Once registered whenever the host is logged onto a domain, the logged on user will be set to the domain user.

If an online host with a logged on user disconnects before logging off the user, the logged on user is removed from the host after 10 minutes. A red "A" is displayed with the offline host, indicating a need to authenticate. If the host connects with or without user information from the Passive Agent, the red "A" is no longer displayed.

802.1X with the Passive Agent (authentication set to enforce)

This scenario is similar to the Wired Connection and Wired MAC Auth (Authentication Set to Enforce) scenario, except the logged on user is initially set to the 802.1x user, and is then switched to the user logged onto the domain.

802.1X without Passive Agent (authentication set toenforce)

When registered via the Portal, the logged on user is displayed as the 802.1x user.

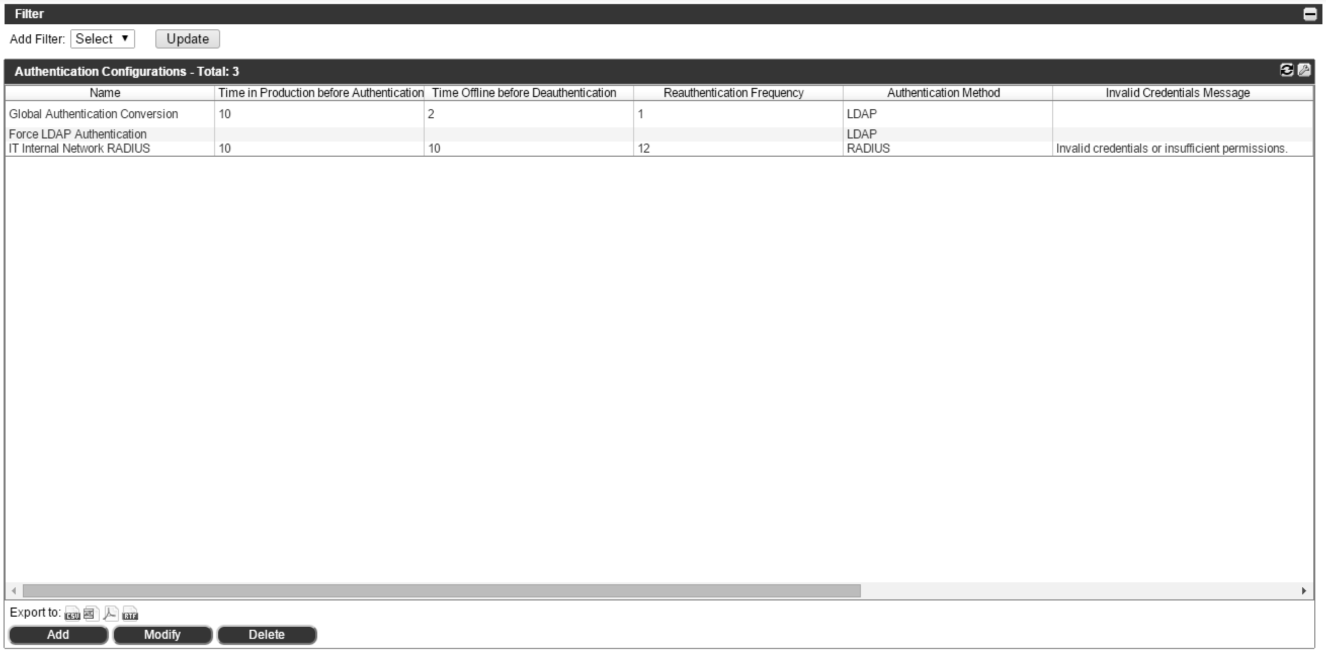
Wired connection registering via the pop up dialog provide by the PA

The rogue is connected to a Port that is not in Forced Authentication. After entering directory credentials the host is registered to that user, and there is no logged on user.

Authentication configurations

Authentication Configurations define authentication methods for connecting hosts and users. Users can enable hosts to authenticate using a specific authentication method, define authentication duration, and require reauthentication after a defined time period. The Authentication Configuration that is assigned to a particular host is determined by the pairing of a Authentication Configuration and a User/Host Profile within an Authentication Policy.

Enabling authentication allows the Administrator to determine whether or not hosts connecting to the network will be forced to authenticate. Hosts can be forced to reauthenticate after a specified period of time.



Authentication Configurations - Total: 3

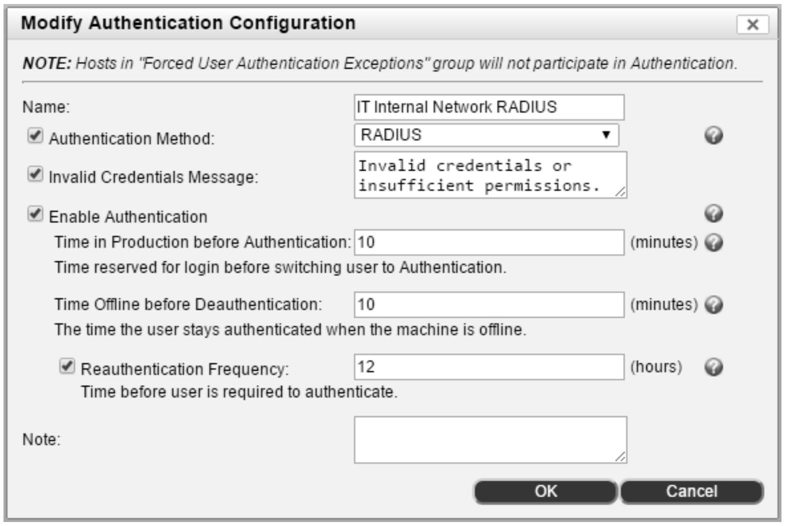
Name	Time in Production before Authentication	Time Offline before Deauthentication	Reauthentication Frequency	Authentication Method	Invalid Credentials Message
Global Authentication Conversion	10	2	1	LDAP	
Force LDAP Authentication				LDAP	
IT Internal Network RADIUS	10	10	12	RADIUS	Invalid credentials or insufficient permissions.

Settings

Field	Definition
Add Filter drop-down list	Allows you to select a field from the current view to filter information. Select the field from the drop-down list, and then enter the information you wish to filter.
Update Button	Displays the filtered data in the table.
Table columns	
Name	The name of the authentication configuration.

Field	Definition
Time in Production before Authentication	When a user is waiting to authenticate, the host remains in the production VLAN until this time expires. If the user fails to authenticate within the time specified, the host is moved to the Authentication VLAN.
Time Offline before Deauthentication	Once the host is offline, the user will remain authenticated for this period of time. If the host comes back online before the time period ends, the user will not need to re-authenticate. If the host comes back online after the time period ends, the user will be required to re-authenticate. Hosts which don't match a User/Host profile that is associated with an Authentication Policy Configuration will be deauthenticated after the system default time of 10 minutes. To ensure that all hosts get an Authentication Policy, create a "Catch All" User/Host profile and associate it to an Authentication Configuration.
Reauthentication Frequency	When set, this forces users to re-authenticate after the amount of timedefined in this field passes since the last authentication regardless of the host's state. The host is moved to the authentication VLAN.
Authentication Method	When enabled, the selected authentication method will override all other authentication methods configured in the portal, guest/contractor template, and Persistent Agent Credential configuration.
Invalid Credentials Method	Enables you to modify the error message displayed in the Portal and Persistent Agent when a user fails to successfully authenticate.
Note	User-defined information about the policy configuration.
Last Modified By	User name of the last user to modify the policy configuration.
Last Modified Date	Date and time of the last modification to this policy.
Right click options	
Delete	Deletes the selected Authentication Configuration.
Modify	Opens the Modify Authentication Configuration window for the selected configuration. See Add or modify a policy on page 406
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671
Buttons	
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.

Add or modify a policy



Modify Authentication Configuration

NOTE: Hosts in "Forced User Authentication Exceptions" group will not participate in Authentication.

Name: IT Internal Network RADIUS

☑ Authentication Method: RADIUS

☑ Invalid Credentials Message: Invalid credentials or insufficient permissions.

☑ Enable Authentication

Time in Production before Authentication: 10 (minutes)

Time reserved for login before switching user to Authentication.

Time Offline before Deauthentication: 10 (minutes)

The time the user stays authenticated when the machine is offline.

☑ Reauthentication Frequency: 12 (hours)

Time before user is required to authenticate.

Note:

1. Select **Policy > Policy Configuration**.
2. In the menu on the left select **Authentication**.
3. Click the **Add** button or select an existing policy and click **Modify**.
4. Enter a name for the policy.
5. Use the settings below to configure the new authentication policy.
6. Click **OK** to save your policy.

Settings

Field	Definition
Name	Enter a name that describes the policy configuration.
Authentication Method	When enabled, the selected authentication method will override all other authentication methods configured in the portal, guest/contractor template, and Persistent Agent Credential configuration.
Invalid Credentials Message	Enables you to modify the error message displayed in the Portal and Persistent Agent when a user fails to successfully authenticate.
Enable Authentication	When enabled, the user is authenticated against a directory, the FortiNAC database, or a RADIUS server when logging on to access the network.
Time in Production before Authentication	When a user is waiting to authenticate, the host remains in the production VLAN until this time expires. If the user fails to authenticate within the time specified, the host is moved to the Authentication VLAN.

Field	Definition
Time Offline before Deauthentication	Once the host is offline, the user will remain authenticated for this period of time. If the host comes back online before the time period ends, the user will not need to re-authenticate. If the host comes back online after the time period ends, the user will be required to re-authenticate. Hosts which don't match a User/Host profile that is associated with an Authentication Policy configuration will be deauthenticated after the system default time of 10 minutes. To ensure that all hosts get an Authentication Policy, create a "Catch All" User/Host profile and associate it to an Authentication Configuration.
Reauthentication Frequency	When set, this forces users to re-authenticate after the amount of time defined in this field passes since the last authentication regardless of the host's state. The host is moved to the authentication VLAN.
Note	Allows users to enter additional information about the policy.

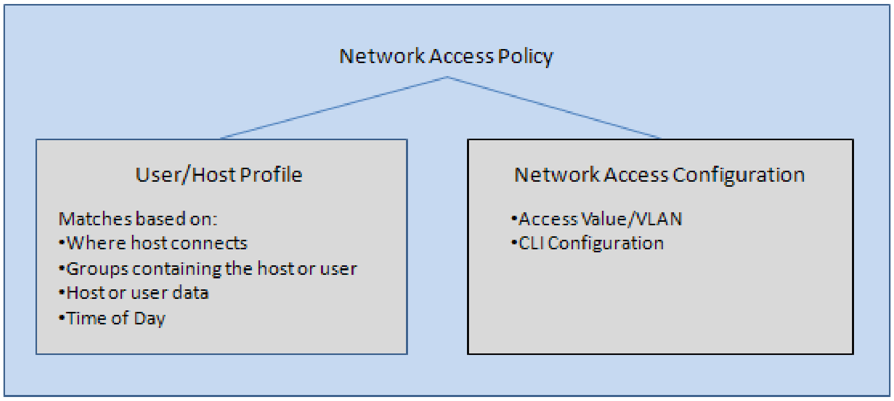
Delete a configuration

1. Click **Policy > Policy Configuration**.
2. In the menu on the left select **Authentication Policy**.
3. Select **Configuration** from the menu on the left.
4. Select the authentication configuration to be removed.
5. Click **Delete**.
6. Click **OK** to confirm that you wish to remove the configuration.

Network access policies

A Network Access Policy consists of one User/Host Profile and one Network Access Configuration. The User/Host Profile is used to determine the users and hosts to which this policy might apply. The Network Access Configuration assigns the treatment those users and hosts receive when they connect to the network.

Network Access Policies are used for registered hosts only.



The Network Access Configuration specifies the VLAN, CLI Configuration or VPN Group Policy that apply to a host that requires network access. If the user or host matches the selected User/Host Profile they are given the network access defined in the configuration.

Network Access Policies follow a pattern, such as, when anyone in group X of people connects to a device in group Y of devices only put those users on VLAN 10. Devices that are end-stations, such as a gaming device, a printer or a medical device can be treated as if they were people. For example, if a gaming device that matches the specified User/Host Profile is connected to a switch that also matches the User/Host Profile it can be moved to a special VLAN for gaming devices defined in the Network Access Configuration.

Network Access Policies are very flexible and can be used in more complex situations. For example, Network Access Policies can be created for medical devices that are end stations. When a medical device is connected to any port in the hospital, FortiNAC can use a Network Access Policy that contains a CLI configuration to reduce the rate of data transfer on those ports.

Network Access Policies can also be used to pass a group policy to a user connecting through a VPN concentrator. When a user connects through a VPN you do not want to disconnect the user in order to move the user from one VLAN to another. However, when the user is authenticated and the authentication is returned to the VPN concentrator, FortiNAC can also send a group policy for that user. The policy can then restrict the user's network access to certain areas. Group policies are configured on the VPN concentrator. When the name of the Group policy is entered into the Access Value/VLAN field on the Network Access Configuration window, that VPN group policy is then enforced for the connecting user.

Policies are assigned based on matching data when a host requires network access. The host/user and the connection location are compared to each Network Access Policy starting with the first policy in the list. When a policy is found where the host and user data and the connection location match the selected User/Host Profile, that policy is assigned. Policy assignments are not permanent. Hosts are re-evaluated frequently, such as when a switch is polled or the Persistent Agent contacts the server. When host and user data are re-evaluated a different Network Access Policy may be selected.

There may be more than one Network Access Policy that is a match for this host/user, however, the first match found is the one that is used.

If you create a User/Host Profile with fields Where (Location) set to Any, Who/What by Group set to Any, Who/What by Attribute left blank and When set to always, it matches ALL users and hosts. This is essentially a Catch All profile. If this User/Host Profile is used in a policy, all policies below that policy are ignored when assigning a policy to a user or a host. To highlight this, policies below the policy with the catch all profile are grayed out and have a line through the data.

The best way to use a Catch All profile is to create a general policy with that profile and place it last in the list of policies.

Implementation

- Determine which device(s) will be used to support a specific Network Access Policy.
- Configure the device(s) with the VLAN or Interface ID information for the Network Access Policy.
- Create a device group and add the device(s) for each set of devices that will be used for Network Access Policies. For example, you might have a group of devices that provide network access in Building A. That group of devices will provide different types of access than the devices in Building B, therefore you would create two separate device groups. See Groups view on page 838 for information on groups.
- If only some ports on a device or devices will be used for Network Access Policies, you can place just the required ports in a Port group specifically for use in Network Access Policies. First, determine which ports will participate in Network Access Policies and place those ports in the Role Based Access Group. Ports that are not in this group cannot apply policies. Once ports are in the Role Based Access group, place them in groups that will be associated with specific User/Host Profiles and Network Access Policies. See Groups view on page 838 for information on groups.

  Ports that are designated as connection locations for Network Access Policies are typically included in the Role Based Access Group. If a port is used in a policy but is not included in the Role Based Access Group, devices connecting to that port are placed in the default VLAN entered on the Model Configuration window for that device. They are not placed on the VLAN defined for the Network Access Policy.
- Determine which hosts or users will receive which network access. Create User/Host Profiles that would match each set of Users or Hosts that require different treatment. For example, if you want your Executives on VLAN 10 and you Admin Staff on VLAN 20 you must create a User/Host Profile for each set of users. See User/host profiles on page 389.
- Create a Network Access Configuration for each VLAN, CLI Configuration or VPN Group Policy that you wish to assign to connecting hosts. See Network access configurations on page 412.
- Create your Network Access Policies by mapping a User/Host Profile to a Network Access Configuration. See Network access policies on page 407.

Manage policies

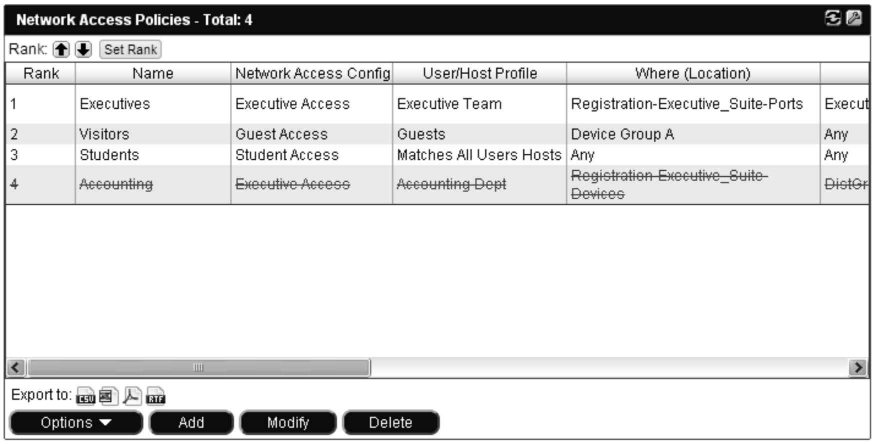
Create Network Access Policies to assign a VLAN, implement a CLI Configuration or assign a VPN Group Policy when a host requires network access. Policies are selected for a connecting host by matching host and user data to the criteria defined in the associated User/Host Profile. The first policy that matches the host and user data is assigned.

If the host does not match any policy, it is assigned the default VLAN configured on the switch.

If you create a User/Host Profile with fields Where (Location) set to Any, Who/What by Group set to Any, Who/What by Attribute left blank and When set to always, it matches ALL users and hosts. This is essentially a Catch All profile. If this User/Host Profile is used in a policy, all policies below that policy are ignored when assigning a policy to a user or a host. To highlight this, policies below the policy with the catch all profile are grayed out and have a line through the data.

The best way to use a Catch All profile is to create a general policy with that profile and place it last in the list of policies.

Network Access Policies can be accessed from **Policy > Policy Configuration > Network Access** or from **System > Quick Start > Policy Configuration**, however configuration steps point you to **Policy > Policy Configuration > Network Access**.



Network Access Policies - Total: 4

Rank: Set Rank

Rank	Name	Network Access Config	User/Host Profile	Where (Location)	
1	Executives	Executive Access	Executive Team	Registration-Executive_Suite-Ports	Execut
2	Visitors	Guest Access	Guests	Device Group A	Any
3	Students	Student Access	Matches All Users Hosts	Any	Any
~~4~~	~~Accounting~~	~~Executive Access~~	~~Accounting Dept~~	~~Registration-Executive_Suite-Devices~~	~~DistGr~~

Settings

An empty field in a column indicates that the option has not been set.

Field	Definition
Rank Buttons	Moves the selected policy up or down in the list. Host connections are compared to Policies in order by rank.
Set Rank Button	Allows you to type a different rank number for a selected policy and immediately move the policy to that position. In an environment with a large number of policies this process is faster than using the up and down Rank buttons.
Table columns	
Rank	Policy's rank in the list of policies. Rank controls the order in which host connections are compared to Policies.
Name	User defined name for the policy.
Network Access Configuration	Contains the configuration for the VLAN, CLI Configuration or VPN Group Policy that will be assigned if this Access Policy matches the connecting host. See Network access configurations on page 412.

Field	Definition
User/Host Profile	Contains the required criteria for a connecting host, such as connection location, host or user group membership, host or user attributes or time of day. Host connections that match the criteria within the User/Host Profile are assigned the associated Network Access Configuration. See User/host profiles on page 389.
Where (Location)	The connection location specified in the User/Host Profile. The host must connect to the network on a device, port or SSID contained within one of the groups shown here to be a match. When set to Any, this field is a match for all hosts or users.
Who/What by Group	User or Host group or groups specified in the User/Host Profile. These groups must contain the connecting user or host for the connection to be a match for this policy. When set to Any, this field is a match for all hosts or users.
Who/What by Attribute	User or Host attributes specified in the selected User/Host Profile. The connecting host or user must have the attributes to be a match. See Filter example on page 393.
When	The time frame specified in the selected User/Host Profile. The host must be on the network within this time frame to be a match. When set to Always this field is a match for all hosts or users.
Note	User specified note field. This field may contain notes regarding the data conversion from a previous version of FortiNAC.
Last Modified By	User name of the last user to modify the policy.
Last Modified Date	Date and time of the last modification to this policy.
Right click options	
Delete	Deletes the selected Network Access Policy.
Modify	Opens the Modify Network Access Policy window for the selected policy.
Buttons	
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.

Add or modify a policy

1. Select **Policy > Policy Configuration**.
2. In the menu on the left select **Network Access**.
3. Click the **Add** button or select an existing Policy and click **Modify**.
4. Click in the **Name** field and enter a name for this Policy.
5. Select a **User/Host Profile** from the drop-down menu. You can use the icons next to the User/Host Profile field to add a new profile or modify the profile shown in the drop-down menu. Note that if you modify this profile, it is modified for all features that make use of the profile. Connecting hosts must match this User/Host Profile to be assigned the Network Access Configuration specified in the next step.
6. Select a **Network Access Configuration** from the drop-down menu. You can use the icons next to the Network Access Configuration field to add a new configuration or modify the configuration shown in the drop-down menu. Note that if you modify this configuration, it is modified for all features that make use of it. See Add or modify a configuration on page 414.

7. The **Note** field is optional.
8. Click **OK** to save your policy.

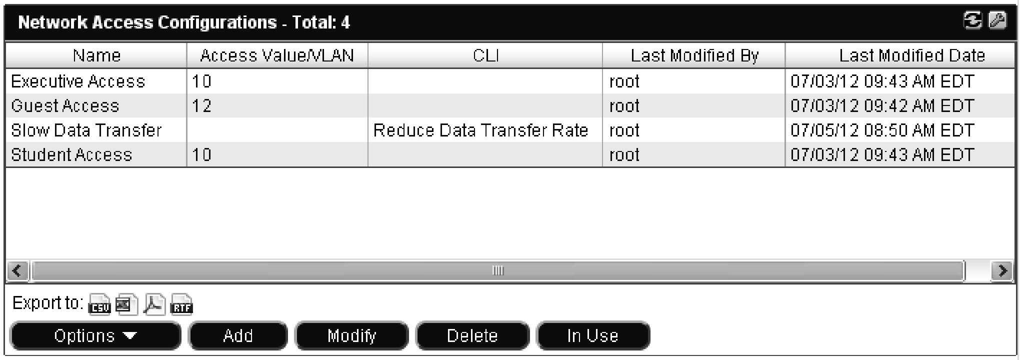
Delete a policy

1. Click **Policy > Policy Configuration**.
2. In the menu on the left, select **Network Access**.
3. Select the policy to be removed.
4. Click **Delete**.
5. Click **OK** to confirm that you wish to remove the policy.

Network access configurations

Network Access Configurations define access treatments for connecting hosts and users. Hosts can be placed in a particular VLAN, have a CLI configuration applied or be passed a VPN Group Policy. The Network Access Configuration that is assigned to a particular host is determined by the pairing of a Network Access Configuration and a User/Host Profile within a Network Access Policy.

When a host requires network access, the host and user are compared to the User/Host Profile in each Network Access Policy starting with the first policy in the list. When a policy is found where the host and user data match the User/Host Profile in the policy, that policy is assigned. The Network Access Configuration contained within that policy specifies the treatment received by the host.



Network Access Configurations - Total: 4

Name	Access Value/VLAN	CLI	Last Modified By	Last Modified Date
Executive Access	10		root	07/03/12 09:43 AM EDT
Guest Access	12		root	07/03/12 09:42 AM EDT
Slow Data Transfer		Reduce Data Transfer Rate	root	07/05/12 08:50 AM EDT
Student Access	10		root	07/03/12 09:43 AM EDT

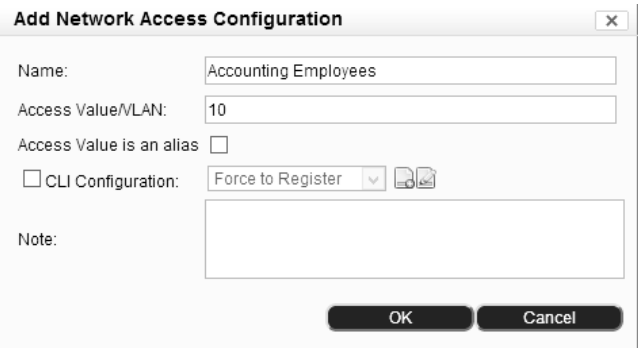
Settings

An empty field in a column indicates that the option has not been set.

Field	Definition
Name	User defined name for the Configuration.
Access Value/VLAN	Name or number of the Network Access identifier where the host or device will be placed, such as VLAN ID, VLAN Name or Aruba Role.

Field	Definition
CLI	CLI configuration that will be applied. CLI configurations are applied to the port where the host or device connects. See CLI configuration on page 928.
Note	User specified note field. This field may contain notes regarding the conversion from a previous version of FortiNAC.
Last Modified By	User name of the last user to modify the configuration.
Last Modified Date	Date and time of the last modification to this configuration.
Is Alias	Indicates whether the Access Value/VLAN field contains the actual VLAN Name, VLAN ID, Aruba Role, Group Policy or if it contains an Alias that represents many VLANs across multiple devices on your network. For example, if one device has a VLAN named Accounting that is actually VLAN 10 and another device has a VLAN named Accounting that is actually VLAN 20, both can be included in a Network Access Policy by using the VLAN Alias of Accounting. The **Access Value is an alias** option is supported only for Cisco and Brocade devices.
Right click options	
Delete	Deletes the selected Network Access Configuration.
In Use	Indicates whether or not the selected configuration is currently being used by any other FortiNAC element. See Configurations in use on page 414.
Modify	Opens the Modify Network Access Configuration window for the selected configuration.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.
Buttons	
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.

Add or modify a configuration



Add Network Access Configuration

Name: Accounting Employees

Access Value/VLAN: 10

Access Value is an alias □

□ CLI Configuration: Force to Register

Note:

1. Select **Policy > Policy Configuration**.
2. In the menu on the left click the **+** sign next to **Network Access**.
3. From the menu on the left, select **Configuration**.
4. On the **Network Access Configurations** window, click the **Add** button or select an existing configuration and click **Modify**.
5. Click in the **Name** field and enter a name for this configuration.
6. In the **Access Value/VLAN** field, type the network access identifier for this mapping, such as a **VLAN ID**, **VLAN Name**, **Aruba Role**, or for a VPN concentrator enter a **VPN group policy name**. If you use an alias to represent VLANs across multiple devices, enter the **Alias** here.
7. If you are using an alias instead of an actual Access Value, enable the **Access Value is an alias** check box. This indicates that the Access Value/VLAN field contains an Alias that represents many VLANs across multiple devices on your network.

   For example, if one device has a VLAN named Accounting that is actually VLAN 10 and another device has a VLAN named Accounting that is actually VLAN 20, both can be included in a Network Access Policy by using the VLAN Alias of Accounting. Using the Alias allows you to create one Network Access Policy that assigns users to VLAN 10 on one device and VLAN 20 on another device.

   The **Access Value is an alias** option is supported only for Cisco and Brocade devices.

8. To apply a CLI configuration to a device or port, click the **CLI** check box to enable it and select the CLI configuration from the drop-down list. This field is optional. For additional information on CLI configurations see CLI configuration on page 928.
9. You can use the icons next to the CLI Configuration field to add a new CLI Configuration or modify the CLI Configuration shown in the drop-down menu. Note that if you modify this CLI Configuration, it is modified for all features that make use of the CLI Configuration.
10. The **Note** field is optional.
11. Click **OK** to save the configuration.

Configurations in use

To find the list of FortiNAC features that reference a specific Network Access Configuration, select the Configuration from the Network Access Configurations View and click the In Use button. A message is displayed indicating whether or not the Configuration is associated with any other features. If the Configuration is referenced elsewhere, a list of each feature that references the Configuration is displayed.

Delete a configuration

If a configuration is in use by another feature in FortiNAC, it cannot be deleted. A dialog displays with a list of the features in which the configuration is used. Remove the association between the configuration and other features before deleting the configuration.

1. Click **Policy > Policy Configuration**.
2. In the menu on the left select **Network Access**.
3. Click on the **+** sign next to **Network Access** to open it.
4. Select **Configuration** from the menu on the left.
5. Select the configuration to be removed.
6. Click **Delete**.
7. Click **OK** to confirm that you wish to remove the configuration.

Endpoint compliance policies

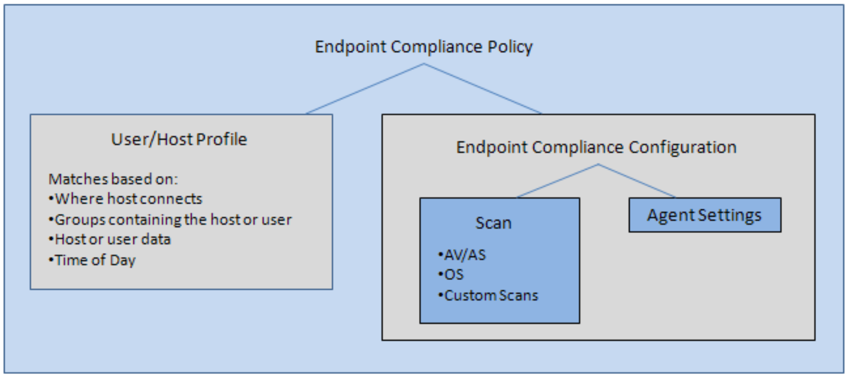
Endpoint Compliance Polices are used to assess hosts and determine if they are safe. An Endpoint Compliance Policy is composed of building blocks, including: a User/Host Profile and an Endpoint Compliance Configuration. Refer to Implementation on page 487 for information on the entire Endpoint Compliance feature.

When a host is evaluated and FortiNAC determines that the host requires an Endpoint Compliance Policy, the host and user are compared to the User/Host Profiles within each Endpoint Compliance Policy starting with the first policy in the list. When a match is found, the Endpoint Compliance Policy is applied. Once a policy is selected as a match for the host or user, the Endpoint Compliance Configuration within the policy determines the treatment that the host receives. An Endpoint Compliance Configuration specifies whether or not an agent is required and the scan parameters for scanning the host.

Endpoint Compliance policies created on the FortiNAC server will be ranked above global Endpoint Compliance Policies created on the NCM. The rank of a local Endpoint Compliance Policy can be adjusted above or below another local Endpoint Compliance Policy, but cannot be ranked below a global Endpoint Compliance Policy. The rank for a global Endpoint Compliance Policy cannot be modified from the FortiNAC server.

If the user/host does not match any policy, it is allowed to register with no scan and no policy.

There may be more than one Endpoint Compliance Policy that is a match for this host/user, however, the first match found is the one that is used.



If you create a User/Host Profile with fields Where (Location) set to Any, Who/What by Group set to Any, Who/What by Attribute left blank and When set to always, it matches ALL users and hosts. This is essentially a Catch All profile. If this User/Host Profile is used in a policy, all policies below that policy are ignored when assigning a policy to a user or a host. To highlight this, policies below the policy with the catch all profile are grayed out and have a line through the data.

The best way to use a Catch All profile is to create a general policy with that profile and place it last in the list of policies.

Endpoint Compliance Policies can be accessed from **Policy > Policy Configuration > Endpoint Compliance** or from **System > Quick Start > Policy Configuration**, however configuration steps point you to **Policy > Policy Configuration > Endpoint Compliance**. See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.

Settings

An empty field in a column indicates that the option has not been set.

Field	Definition
Rank Buttons	Moves the selected policy up or down in the list. Host connections are compared to Policies in order by rank.
Set Rank Button	Allows you to type a different rank number for a selected policy and immediately move the policy to that position. In an environment with a large number of policies, this process is faster than using the up and down Rank buttons. Rank can only be set on local policies, rank changes for global policies must be done at the NCM.
Table columns	
Rank	Policy's rank in the list of policies. Rank controls the order in which host connections are compared to Policies.
Name	User defined name for the policy.

Field	Definition
Endpoint Compliance Configuration	Contains the configuration for the Agent and Scan parameters that will be assigned if this Policy matches the connecting host and user. See Endpoint compliance configurations on page 420.
User/Host Profile	Contains the required criteria for a host or user, such as connection location, host or user group membership, host or user attributes or time of day. Host connections that match the criteria within the User/Host Profile are assigned the associated Endpoint Compliance Configuration. See User/host profiles on page 389.
Where (Location)	The connection location specified in the User/Host Profile. The host must connect to the network on a device, port or SSID contained within one of the groups shown here to be a match. When set to Any, this field is a match for all hosts or users.
Who/What by Group	User or Host group or groups specified in the User/Host Profile. These groups must contain the connecting user or host for the connection to be a match for this policy. When set to Any, this field is a match for all hosts or users.
Who/What by Attribute	User or Host attributes specified in the selected User/Host Profile. The connecting host or user must have the attributes to be a match. See Filter example on page 393.
When	The time frame specified in the selected User/Host Profile. The host must be on the network within this time frame to be a match. When set to Always this field is a match for all hosts or users.
Note	User specified note field. This field may contain notes regarding the data conversion from a previous version of FortiNAC.
Last Modified By	User name of the last user to modify the policy.
Last Modified Date	Date and time of the last modification to this policy.
Right click options	
Delete	Deletes the selected Endpoint Compliance Policy.
Modify	Opens the Modify Endpoint Compliance Policy window for the selected policy.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.
Buttons	
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.

Add or modify a policy

1. Select **Policy > Policy Configuration**.
2. In the menu on the left select **Endpoint Compliance**.
3. Click the **Add** button or select an existing policy and click **Modify**.
4. Click in the **Name** field and enter a name for this policy.
5. Select a **User/Host Profile** from the drop-down menu. You can use the icons next to the User/Host Profile field to add a new profile or modify the profile shown in the drop-down menu. Note that if you modify this profile, it is modified for all features that make use of the profile. Connecting hosts must match this User/Host Profile to be assigned the Endpoint Compliance Configuration specified in the next step.
6. Select an **Endpoint Compliance Configuration** from the drop-down menu. You can use the icons next to the Endpoint Compliance Configuration field to add a new configuration or modify the configuration shown in the drop-down menu. Note that if you modify this configuration, it is modified for all features that make use of it. See Add or modify a configuration on page 421.
7. The **Note** field is optional.
8. Click **OK** to save your policy.

Determining host operating system

FortiNAC uses the information configured in the Endpoint Compliance Policy and information received from the connecting host to determine if an agent is required and which agent should be offered to a host. If the operating system or host type is one for which there is no agent, FortiNAC can allow or deny network access based on the settings in the Endpoint Compliance Policy.

The host operating system is detected based on the information contained in the UserAgent string. When a host connects to a FortiNAC web page, its browser sends the user-agent string to the FortiNAC Server or Application Server. This string indicates which browser the host is using, its version number, and details about the host, such as operating system and version. The chart below outlines the criteria FortiNAC uses to determine the host operating system.

Operating system is considered unsupported unless it meets one of the following criteria:

Criteria	OS/Device
UserAgent contains "linux" and "android"	Android
User Agent contains "linux" only	Linux
User Agent contains "macOS"	macOS
User Agent contains "Macintosh" and "Silk"	Android
User Agent contains "Macintosh" and "Cloud9"	Android
User Agent contains "linux", "android" and "silk"	Kindle
User Agent contains any one of the following: "KFOT", "KFTT, "KFJWI", "KFJWA", "KFSOWI", "KFTHWI", "KFTHWA", "KFAPWI" or "KFAPWA"	Kindle Fire
User Agent contains "macOS" and "mobile" and "ipod"	iOS for iPod
User Agent contains "macOS" and "mobile" and "iphone"	iOS for iPhone

Criteria	OS/Device
User Agent contains "macOS" and "mobile" and "ipad"	iOS for iPad
User Agent contains "macOS" and "mobile"	Apple iOS
UserAgent contains "windows nt"	Windows
UserAgent contains "windows phone	Windows Phone
UserAgent contains "windows nt" and "ARM"	Windows RT
UserAgent contains "freebsd"	Free BSD
UserAgent contains "openbsd"	Open BSD
UserAgent contains "netbsd"	Net BSD
UserAgent contains "solaris" or "sunos"	Solaris
UserAgent contains "symbianos" or "symbos"	Symbian
UserAgent contains "webos"	Web OS
UserAgent contains "windows ce"	Windows CE
UserAgent contains "blackberry"	Blackberry OS
UserAgent contains "BB10" and "Mobile"	BlackBerry 10 OS
UserAgent contains "RIM Tablet OS"	RIM Tablet OS
UserAgent contains "CrOS"	Chrome OS

Add or modify a policy

1. Select **Policy > Policy Configuration**.
2. In the menu on the left, select **Endpoint Compliance**.
3. Click the **Add** button or select an existing policy and click **Modify**.
4. Click in the **Name** field and enter a name for this policy.
5. Select a **User/Host Profile** from the drop-down menu. You can use the icons next to the User/Host Profile field to add a new profile or modify the profile shown in the drop-down menu. Note that if you modify this profile, it is modified for all features that make use of the profile. Connecting hosts must match this User/Host Profile to be assigned the Endpoint Compliance Configuration specified in the next step.
6. Select an **Endpoint Compliance Configuration** from the drop-down menu. You can use the icons next to the Endpoint Compliance Configuration field to add a new configuration or modify the configuration shown in the drop-down menu. Note that if you modify this configuration, it is modified for all features that make use of it. See Add or modify a configuration on page 421.
7. The **Note** field is optional.
8. Click **OK** to save your policy.

Delete a policy

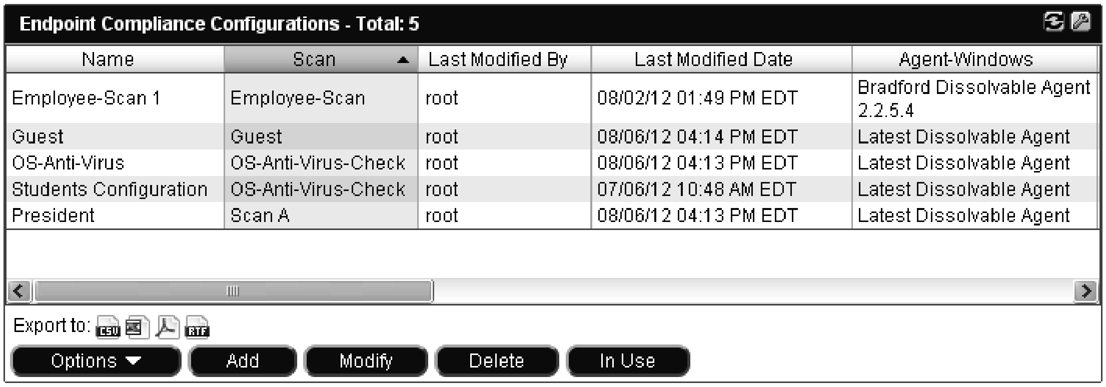
1. Click **Policy > Policy Configuration**.
2. In the menu on the left select **Endpoint Compliance**.
3. Select the policy to be removed.
4. Click **Delete**.
5. Click **OK** to confirm that you wish to remove the policy.

Endpoint compliance configurations

Endpoint Compliance Configurations define agent and scan parameters for hosts and users. Hosts can be required to download an agent and undergo a scan, permitted access with no scan or denied access. The Endpoint Compliance Configuration that is used for a particular host is determined by the pairing of an Endpoint Compliance Configuration and a User/Host Profile within an Endpoint Compliance Policy.

When a host is evaluated, the host, user and connection location are compared to each Endpoint Compliance Policy starting with the first policy in the list. When a policy is found where the host and user data and the connection location match the User/Host Profile in the policy, that policy is assigned. The Endpoint Compliance Configuration contained within that policy determines the security treatment received by the host.

See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.



Endpoint Compliance Configurations - Total: 5

Name	Scan	Last Modified By	Last Modified Date	Agent-Windows
Employee-Scan 1	Employee-Scan	root	08/02/12 01:49 PM EDT	Bradford Dissolvable Agent 2.2.5.4
Guest	Guest	root	08/06/12 04:14 PM EDT	Latest Dissolvable Agent
OS-Anti-Virus	OS-Anti-Virus-Check	root	08/06/12 04:13 PM EDT	Latest Dissolvable Agent
Students Configuration	OS-Anti-Virus-Check	root	07/06/12 10:48 AM EDT	Latest Dissolvable Agent
President	Scan A	root	08/06/12 04:13 PM EDT	Latest Dissolvable Agent

Settings

An empty field in a column indicates that the option has not been set.

Field	Definition
Name	User defined name for the Configuration.
Scan	Name of the scan used to evaluate a connecting host.
Note	User specified note field. This field may contain notes regarding the conversion from a previous version of FortiNAC.

Field	Definition
Collect Applications	If enabled, the agent assigned to the host will collect information about installed applications and add that information to the host record. An application inventory cannot be generated for a hosts unless an agent is in use.
Last Modified By	User name of the last user to modify the record.
Last Modified Date	Date and time of the last modification to this configuration.
Agent - OS	An Agent column is displayed for each operating system supported. The column contains the agent that will be used or treatment that applies to hosts with that operating system when the scan is applied. Some operating systems do not have agents and those hosts can only be allowed or denied access to the network. See the Settings in Add or modify a configuration on page 421 for information on the agent options for each operating system.
Right click options	
Delete	Deletes the selected Endpoint Compliance Configuration.
In Use	Indicates whether or not the selected configuration is currently being used by any other FortiNAC element. See Configurations in use on page 424.
Modify	Opens the Modify Endpoint Configuration window for the selected configuration.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847 You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671
Buttons	
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.

Add or modify a configuration

1. Select **Policy > Policy Configuration**.
2. In the menu on the left click the **+** sign next to **Endpoint Compliance**.
3. From the menu on the left, select **Configuration**.
4. On the Endpoint Compliance Configurations window, click the **Add** button or select an existing configuration and click **Modify**.
5. On the **General** tab, click in the **Name** field and enter a name for this configuration.
6. Select a **Scan** from the drop-down menu. You can use the icons next to the Scan field to add a new scan or modify the scan shown in the drop-down menu. Note that if you modify this scan, it is modified for all features that make use of it. See Add or modify a scan on page 433.
7. If you would like to add a list of installed applications to the host record, enable the **Collect Application Inventory** check box. This only applies to hosts that are assigned an agent. An application inventory cannot be generated for hosts unless an agent is in use.

8. If you would like to grant varying levels of access based on the host's role, select **Advanced Scan Controls**. This displays additional options that allow you to select and map a security action to scan success, failure, and warning. See Chaining configuration scans on page 424.

   You must have ATR access enabled to use the Advanced Scan Controls feature.
9. The **Note** field is optional.
10. Click the **Agent** tab to select it.
11. Select an agent for each operating system. You may choose not to use an agent for a particular operating system, however, scans can only be applied via an agent.
12. No agent exists for some operating systems. In those cases select either **None-Deny Access** or **None-Bypass**. Refer to the table below for information on each field.
13. Click **OK** to save the configuration.

Settings

Field	Definition
General tab	
Name	User specified name for this configuration.
Scan	Select the scan to be associated with this configuration. Hosts that match the Endpoint Compliance Policy containing this configuration will be scanned with the selected Scan.
Collect Application Inventory	If enabled, the agent assigned to the host will collect information about installed applications and add that information to the host record. An application inventory cannot be generated for a hosts unless an agent is in use.
Advanced Scan Controls	If enabled, allows you to select a security action mapped to an Endpoint Compliance activity that will be taken based on scan results. See Chaining configuration scans on page 424.
Note	User specified note field. This field may contain notes regarding the conversion of policies from a previous version of FortiNAC.
Agent tab	
Windows macOS Linux	Allows you to select a separate agent or treatment for each operating system. For example, a host with a Windows operating system may be scanned by the Persistent Agent while a host with a Mac operating system may be scanned with the Dissolvable Agent. See Determining host operating system on page 418. The names of all the agent versions and types available on the appliance are included in the list. The .exe is recommended for user-interactive installation. The .msi is recommended for use for a managed install by a non-user-interactive means. Agent options include: • **Persistent Agent:** Hosts with this operating system are required to download and install the selected version of the Persistent Agent. • **Dissolvable Agent:** Hosts with this operating system are required to download and run the selected version of the Dissolvable Agent. • **Latest Persistent Agent:** Hosts with this operating system are required to download and install the highest version of the Persistent Agent available on the FortiNAC Application server. Using the Latest Persistent Agent option prevents

Field	Definition
	you from having to update Policies each time a new Agent is released and loaded onto your server. • **Legacy Persistent Agent:** Hosts with this operating system are required to download and install the highest version of the Persistent Agent within the 2.X series. The Version 2.X agents do not require that a certificate be installed on the portal in order to run. • **Latest Dissolvable Agent:** Hosts with this operating system are required to download and run the highest version of the Dissolvable Agent available on the FortiNAC Application server. Using the Latest Dissolvable Agent option prevents you from having to update Policies each time a new Agent is released and loaded onto your server. • **Legacy Dissolvable Agent:** Hosts with this operating system are required to download and install the highest version of the Dissolvable Agent that is lower than V3.1.0. Dissolvable Agents with version numbers lower than Version 3.1.0 do not require that a certificate be installed on the portal in order to run. • **None-Deny Access**: No agent is assigned and hosts are denied access to the network if they have the matching operating system. • **None-Bypass**: No agent is assigned but hosts are allowed to access the network. If you select None - Bypass, hosts can register only if their IP address has been determined by FortiNAC. If IP address information has not been determined FortiNAC cannot determine the Physical Address and will not allow that host on the network. Users see the following message: "Registration Failed - Physical Address not Found" .
Android	• **None-Deny Access**: No agent is assigned and hosts are denied access to the network if they have the matching operating system. • **None-Bypass**: No agent is assigned but hosts are allowed to access the network if they have the matching operating system. • **Mobile Agent:** Mobile devices detected running the Android operating system are required to download and install the Mobile Agent. These devices are automatically directed to the Mobile Agent Download page in the captive portal where the host is prompted to download the Mobile Agent from Google Play (Android). • **Latest Mobile Agent**: Hosts with this operating system are required to download and install the highest version of the Mobile Agent availability Mobile Agent is downloaded from Google Play. See Mobile Agent on page 520.
Settings For Operating Systems Without Agents	This section provides a list of additional operating systems and allows you to select treatment for each one. For example, iPod devices could be set to None-Bypass indicating that no agent is necessary and allowing that device to connect to the network. Options for additional platforms include: • **None-Deny Access**: No agent is assigned and hosts are denied access to the network if they have the matching operating system. • **None-Bypass**: No agent is assigned but hosts are allowed to access the network if they have the matching operating system.

Field	Definition
	Use the **Set all to None-Bypass** or **Set all to None-Deny Access** buttons to modify settings for all additional platforms at once. The last platform labeled Other is used as a catch-all for devices with new or unsupported operating systems. Any platform not listed in the Policy, is treated as specified by the setting associated with Other.

Configurations in use

To find the list of FortiNAC features that reference a specific Endpoint Compliance Configuration, select the Configuration from the Endpoint Compliance Configurations View and click the In Use button. A message is displayed indicating whether or not the Configuration is associated with any other features. If the Configuration is referenced elsewhere, a list of each feature that references the Configuration is displayed.

Delete a configuration

If a configuration is in use by another feature in FortiNAC, it cannot be deleted. A dialog displays with a list of the features in which the configuration is used. Remove the association between the configuration and other features before deleting the configuration.

1. Click **Policy > Policy Configuration**.
2. In the menu on the left, select **Endpoint Compliance**.
3. Click on the **+** sign next to **Endpoint Compliance** to open it.
4. Select **Configuration** from the menu on the left.
5. Select the configuration to be removed.
6. Click **Delete**.
7. Click **OK** to confirm that you wish to remove the configuration.

Chaining configuration scans

When the Advanced Scan Controls option is enabled for an Endpoint Compliance Configuration, you can map a security action containing Run Endpoint Compliance Configuration activities to scan results.

The Run Endpoint Compliance Configuration activity will run scans for additional Endpoint Compliance Configurations. This allows further scans to be run on hosts when additional levels of access are needed. For example, if the host is part of a group requiring access to a secure VLAN, you can run additional scans the host must pass to be allowed onto this area of the network. Access is determined by the highest level scan that the host passes.

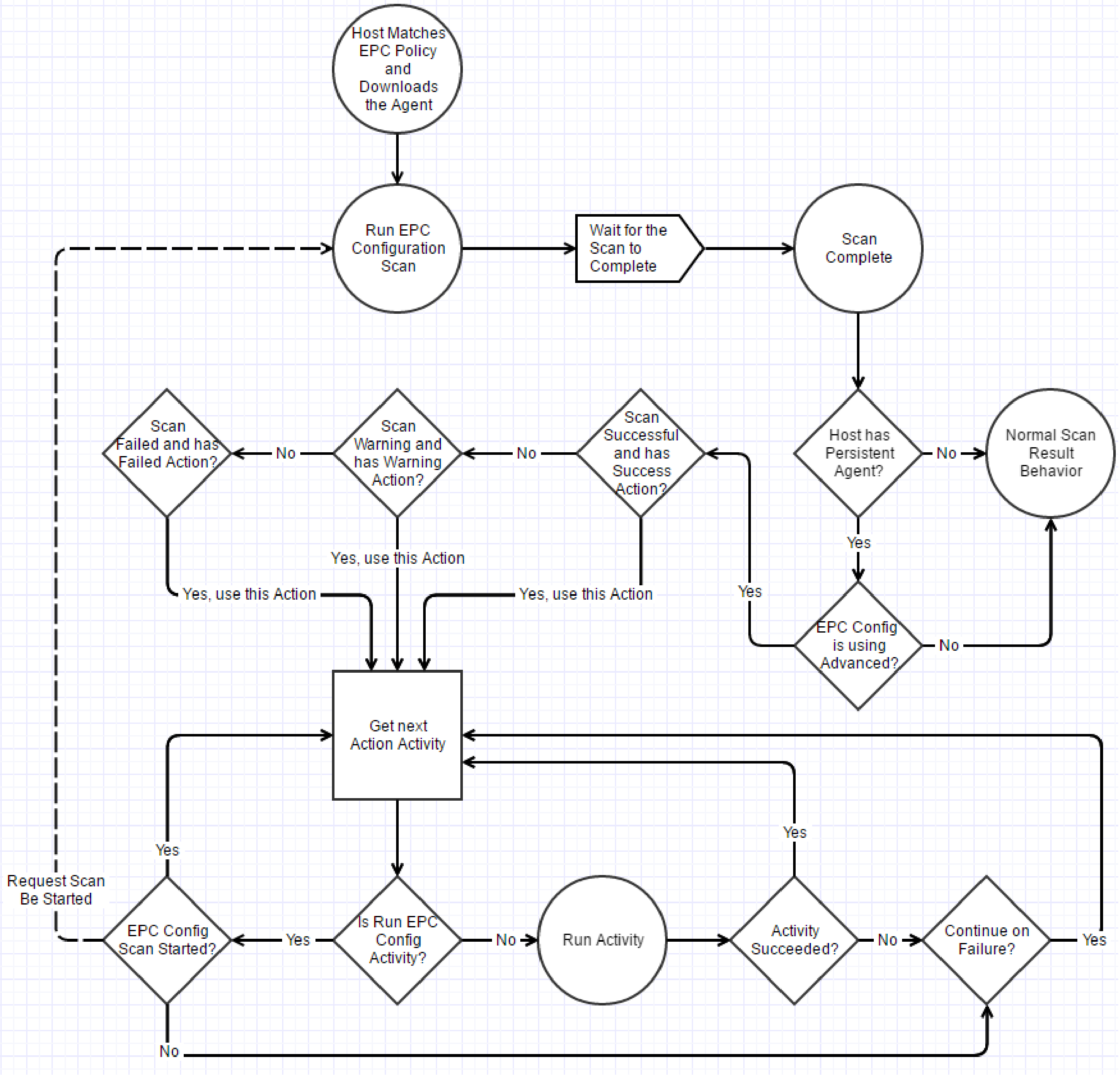
When a host is authenticated and matches an Endpoint Compliance Policy, the Endpoint Compliance Configuration scan is run. When the action is taken based on the scan results, if the Run Endpoint Compliance Configuration activity is performed and the Endpoint Compliance Configuration scan starts successfully, the action moves to the next activity in the list while the Endpoint Compliance Configuration scan is running.

If the Endpoint Compliance Configuration scan does not successfully start, additional activities are only performed if the On Activity Failure setting is set to Continue Running Activities.

There is no limit on the number of actions that can be run based on scan results.

The Persistent Agent must be installed on the host.

To enable and configure Advanced Scan Controls, go to **Policy > Policy Configuration. Click Endpoint Compliance > Configuration**, and then click the **Add** button or select an existing configuration and click **Modify**.


Host Matches EPC Policy and Downloads the Agent
Run EPC Configuration Scan
Wait for the Scan to Complete
Scan Complete
Scan Failed and has Failed Action?
No
Scan Warning and has Warning Action?
No
Scan Successful and has Success Action?
Host has Persistent Agent?
No
Normal Scan Result Behavior
Yes
Yes, use this Action
Yes, use this Action
Yes, use this Action
Yes
EPC Config is using Advanced?
No
Get next Action Activity
Yes
Yes
Request Scan Be Started
EPC Config Scan Started?
Yes
Is Run EPC Config Activity?
No
Run Activity
Activity Succeeded?
No
Continue on Failure?
Yes
No

Scans

The Scans View allows you to configure network scans or sets of rules that are used to scan hosts for compliance. Scans are included in Endpoint Compliance Configurations that are paired with User/Host Profiles, which form Endpoint Compliance Polices. When a host is evaluated and requires an Endpoint Compliance Policy, FortiNAC goes through the list of polices and compares user and host information to the associated User/Host Profile. When a match is found, the Endpoint Compliance Configuration inside the policy is applied to the host. That configuration contains the scan and agent information used to evaluate the host.

Scans typically consist of lists of permitted operating systems and required anti-virus software. In addition, Custom Scans can be created for more detailed scanning such as, searching the registry for particular entries, searching the hard drive for specific files, or verifying that hotfixes have been installed. Individual scans can be scheduled to run at regular intervals if your organization requires frequent rescans.

For a list of supported operating systems, anti-virus software software, use the Customer Portal on our web site.

The results of a scan are stored on the Host Health tab in the Host Properties view. Refer to Host health and scanning on page 803 for additional information.

Scanning with Agent 2.X

If your hosts are scanned by an Agent prior to Agent version 3.0, the agent tests every single item in the scan and presents extensive scan results. In some cases those items may not be relevant. For example, if Windows XP is required and that operating system is not installed, the agent will still test to see if the updates have been installed. In the scan results, the host fails for not having the operating system AND for not having the updates.

The opposite is also true. In some cases if an item is unchecked and therefore is not required, the host passes for that item and can pass the scan. See the example below:

OS/AV	Anti-Virus 1	Anti-Virus 2	Anti-Virus 3
Operating System 1	Unchecked	Unchecked	Checked
Operating System 2	Unchecked	Checked	Checked
Operating System 3	Checked	Checked	Checked

If the scan is set to Any indicating that any combination is acceptable, the goal of these scan settings would be as follows:

- Operating System 1 requires Anti-Virus 3
- Operating System 2 requires either Anti-Virus 1 or Anti-Virus 2.
- Operating System 3 requires either Anti-Virus 1, Anti-Virus 2 or Anti-Virus 3.

However, this is not supported because the agent tests for each combination. The actual process is as follows:

- Operating System 1 requires either no Anti-Virus 1 or no Anti-Virus 2 or Anti-Virus 3. Host passes if it does not have Anti-Virus 1 or 2 because those are unchecked, and the agent tests for that combination. It also passes if it has Anti-Virus 3.

- Operating System 2 requires either no Anti-Virus 1 or Anti-Virus 2 or Anti-Virus 3. Host passes if it does not have Anti-Virus 1 because that one is unchecked, and the agent tests for that combination. It also passes if it has Anti-Virus 2 or 3.
- Operating System 3 requires either Anti-Virus 1, Anti-Virus 2 or Anti-Virus 3. Host passes if it has any one of the three Anti-Viruses installed.

Scanning with Agent 3.X and higher

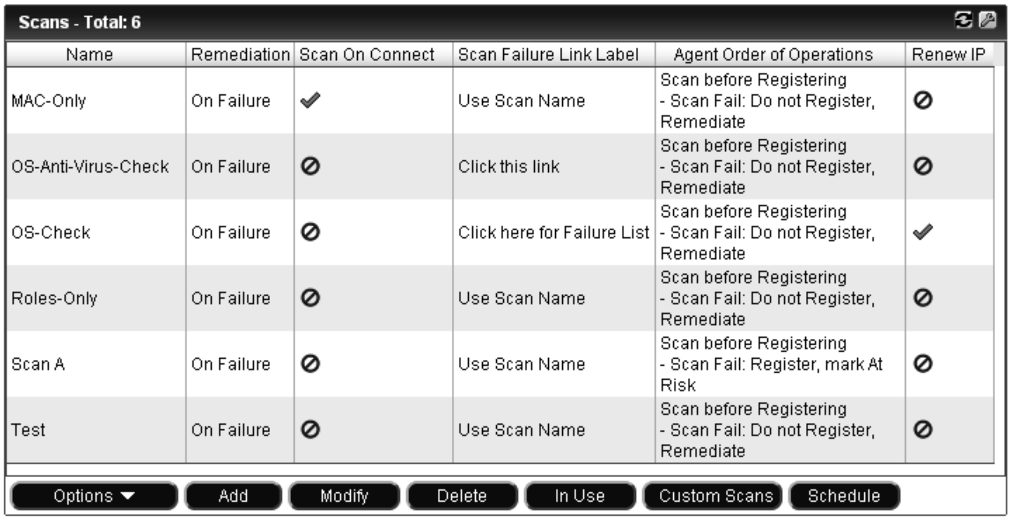
If your hosts are scanned using Agent version 3.0 or higher, the agent first checks to see if a required item is installed and then proceeds to scan for additional details about that item. For example, if the host is required to run Windows XP and that operating system is not installed, the agent does not check to see if the updates have been installed. Scan results, therefore, are reduced because needless scans are minimized. In the scan results, the host fails only for not having the operating system.

Using the example from the table shown above, Agent 3.X ignores items that are not checked or selected. With this agent, you would achieve the following results.

- Operating System 1 requires Anti-Virus 3. The agent does not test to see that Anti-Virus 1 and 2 are not installed, therefore, the host cannot pass the scan unless it has Operating System 1 with Anti-Virus 3.
- Operating System 2 requires either Anti-Virus 1 or Anti-Virus 2. The agent does not test for Anti-Virus 1.
- Operating System 3 requires either Anti-Virus 1, Anti-Virus 2 or Anti-Virus 3.

Scans view navigation

Scans can be accessed from **Policy > Policy Configuration > Endpoint Compliance** or from **System > Quick Start > Policy Configuration**, however configuration steps point you to **Policy > Policy Configuration > Endpoint Compliance**. See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.



Scans - Total: 6

Name	Remediation	Scan On Connect	Scan Failure Link Label	Agent Order of Operations	Renew IP
MAC-Only	On Failure	✓	Use Scan Name	Scan before Registering - Scan Fail: Do not Register, Remediate	⊘
OS-Anti-Virus-Check	On Failure	⊘	Click this link	Scan before Registering - Scan Fail: Do not Register, Remediate	⊘
OS-Check	On Failure	⊘	Click here for Failure List	Scan before Registering - Scan Fail: Do not Register, Remediate	✓
Roles-Only	On Failure	⊘	Use Scan Name	Scan before Registering - Scan Fail: Do not Register, Remediate	⊘
Scan A	On Failure	⊘	Use Scan Name	Scan before Registering - Scan Fail: Register, mark At Risk	⊘
Test	On Failure	⊘	Use Scan Name	Scan before Registering - Scan Fail: Do not Register, Remediate	⊘

Settings

Field	Definition
Scan Name	Each scan must have a unique name.
Remediation	Indicates when the host is moved to Remediation. Options include: **On Failure** — Host is moved to remediation immediately after failing a scan. **Delayed** — Host is moved to remediation after a user specified delay if the reason for the scan failure has not been addressed. **Audit Only** — Host is scanned and a failure report is generated, but the host is never moved to remediation.
Scan On Connect	Indicates whether this option is enabled or disabled. Scan On Connect forces a rescan every time the host assigned this scan connects to the network. See Scan on connect on page 430. This option only affects hosts running the Persistent Agent.
Renew IP (Supported by Dissolvable Agent Only)	Indicates whether the Renew IP option is enabled or disabled. When this option is enabled, it causes the Dissolvable Agent to actively release and renew the IP address of the host after it has completed its scan. The Renew IP option is only supported on the following systems that use the Dissolvable agent: • Windows: All Dissolvable Agent Versions • Mac-OS-X: Dissolvable Agent Versions 3.3.0.56+
Scan Failure Link Label	Label displayed on the failure page when a network user's PC has failed a scan. If no label is provided, the scan name is used. The label or scan name is a link that takes the user to a page indicating why the PC has failed the scan.
Agent Order Of Operations Remediation = On Failure	This set of options is available only when **Remediation** is set to **On Failure**. Determines the order in which the agent performs its tasks. Choose one of the following: **Scan Before Registering:** The host downloads the Agent and is scanned in the registration network before being registered. If the scan fails you must choose one of the following: • **Do not Register, Remediate:** Host remains a Rogue and stays in the registration network until it passes the scan. Note the host will not be marked "at risk." Default setting. • **Register and mark At Risk:** The host is registered immediately after the scan and then moved to Quarantine. Persistent Agent always registers and marks at risk. **Register, then Scan (if the scan fails, Remediate):** The host does not download an agent in the Registration network. Instead, the host is registered and moved to Quarantine to download the Agent and be scanned.
Agent Order Of Operations	The option below is available only when **Remediation** is set to **Delay** or **Audit Only**.

Field	Definition
Remediation = Delay or Audit Only	**If scan fails - Register or Remediate:** If the host fails a scan, a web page with a Register option and a Remediate option is displayed to the user. If the user chooses the Remediate option, the host is placed in remediation and the user must correct all issues and rescan. If the user chooses the Register option, the host is placed in production. The user can correct all of the issues and re-run the Agent.
Patch URL	URL for the web page to be displayed when a host using the Dissolvable Agent fails the scan. This web page allows the user to download the agent and rescan after addressing the issues that caused the failure. Hosts using the Persistent Agent have the agent installed and do not use this page.
Root Detection	Indicates whether this option is enabled or disabled. If enabled, rooted mobile devices are not allowed to register. Mobile Agent devices determines whether or not the device has been rooted. Rooting is a process allowing users of devices running the Android operating system to attain privileged control (known as "root access") within Android's subsystem.
Last Modified By	User name of the last user to modify the scan.
Last Modified Date	Date and time of the last modification to this scan.
Right click options	
Copy	Copy the selected Scan to create a new record.
Delete	Deletes the selected Scan. Scans that are currently in use cannot be deleted.
In Use	Indicates whether or not the selected Scan is currently being used by any other FortiNAC element. See Scans in use on page 441.
Modify	Opens the Modify Scan window for the selected Scan.
Schedule	Opens the Schedule Policy view for the selected scan and allows you to add a schedule for host rescans using that Scan. See Schedule a scan on page 441.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.
Buttons	
Custom Scans	Opens the Custom Scan Configuration window which allows you to add, remove or modify Custom Scans. Custom scan can be added to policies for more detailed host scans. See Custom scans on page 448.
Schedule	Opens the Schedule Policy view for the selected scan and allows you to add a schedule for host rescans using that Scan. See Schedule a scan on page 441.

Scan on connect

FortiNAC allows you to configure Scans that scan hosts each time they connect to the network. The Scan on Connect option is enabled on individual Scans. You may have hosts that are scanned each time they connect and hosts with a different Scan that are scanned periodically.

Scan on Connect can only be used on registered hosts that have the Persistent Agent installed. If you are using the Dissolvable Agent, this option is ignored.

When a host connects to the network, FortiNAC determines which Endpoint Compliance Policy should be applied to this host based on the criteria in the associated User/Host Profile. If a registered host has the Persistent Agent installed and Scan on Connect is enabled for the Scan that applies to this host, then the host is scanned. When the host disconnects from the network, the Persistent Agent modifies that host's Scan on Connect status to indicate that the host should be scanned again the next time it connects. If the host has more than one interface, such as wired and wireless, the host is scanned regardless of which one is used.

A rescan happens any time FortiNAC detects that the host has come online and the agent has communicated with the server, such as when a switch sends a linkdown/linkup trap.

To enable Scan on Connect you must go to the Scans window, select the appropriate Scan and enable the option. See Add or modify a scan on page 433 for step-by-step instructions on creating a Scan and enabling Scan on Connect.

Scan hosts without enforcing remediation

Hosts who are in Remediation are denied network access until they comply with the requirements of the Scan used to evaluate them. FortiNAC can scan hosts on the network without placing them in Remediation. This allows the administrator to determine host state or test new Endpoint Compliance Policies without interrupting network users as they work. To scan hosts without enforcing remediation you can disable the Quarantine switching option in FortiNAC Properties. Disabling Quarantine VLAN switching affects all hosts. However, you may need to scan selected hosts with no repercussions.

Two options have been provided to allow you to scan selected hosts without forcing "at risk" hosts into Remediation, Audit Only and Forced Remediation Exceptions group. You can use either one or both of these options. They work independently of each other. Audit Only controls remediation based on the scan applied. The Forced Remediation Exceptions group controls remediation based on group membership regardless of the scan used to evaluate the hosts.

Audit only

When the Audit Only option on a scan is enabled, hosts are scanned and the results of the scan are stored. Hosts that fail the scan are never marked "at risk" and therefore are not forced into Remediation or Quarantine. Administrators can then review all of the scan results and address issues of non-compliance without blocking users from the network.

Audit Only affects only those hosts evaluated by the scan in which Audit Only is enabled. If you have other scans with Audit Only disabled, hosts evaluated by those scans who fail are forced into Remediation. Using this option you can decide to force some groups of hosts into remediation while leaving others on the network. For example, you could have a scan for your executive staff that has Audit Only enabled and a different scan for administrative staff that has Audit

Only disabled. Executives that fail a scan would continue to work without disruption, while administrative staff that fail a scan would be forced to remediate.

1. Select **Policy > Policy Configuration**.
2. In the menu on the left, click the **+** symbol next to **Endpoint Compliance** to open it.
3. Click **Scans**.
4. Select an existing scan to modify or create a new one.
5. On the **Add** or **Modify Scan** window go to the **Scan Settings** section and enable **Audit Only** under the **Remediation** drop-down.

See Add or modify a scan on page 433 for additional information.

Forced remediation exceptions group

When hosts are placed in this group, they are evaluated by the scan that corresponds to them. See Policy assignment on page 378. Results of the scan are stored and hosts who fail are marked "at risk". Hosts in this group are never forced into remediation no matter which scan they fail. To prevent selected hosts from being forced to remediate, add them to this group.

The Forced Remediation Exceptions group is a system group that has already been created. System groups cannot be removed only modified. See System groups on page 843 and Modify a group on page 841.

Delayed remediation for scanned hosts

The Delayed Remediation scan feature allows you to scan hosts on your network, notify the user if the host has failed the scan and delay placing the host in the remediation VLAN for a specified number of days. This process gives the host's owner time to rectify the issues that triggered the failed scan and rescan without being removed from the network. If the user does not take care of the issues that caused the failure and successfully rescan the host by the time the specified delay has elapsed, the host is placed in remediation and cannot access the network.

Implementation

To implement Delayed Remediation, first implement the settings for Endpoint Compliance. See Implementation on page 487.

- This feature works with any agent (Passive, Persistent or Dissolvable). If you choose to use this feature with the Dissolvable Agent, note the following:
  - Using the Dissolvable Agent, Delayed Remediation can only be implemented during the registration process where the host is provided a link to the Dissolvable Agent. If the host fails, it is marked as Pending - At Risk, but can register and move to the production VLAN. The Dissolvable Agent remains on the host until all issues have been resolved and the host has been rescanned.
  - If you set up scheduled rescans for hosts, using Delayed Remediation does not prevent the scheduled rescan from marking the host "At Risk" at the scheduled interval. Therefore, it is recommended that you use Proactive Scanning with the Dissolvable Agent instead of Delayed Remediation. Proactive Scanning allows a user to rescan a host prior to a scheduled required rescan and if the host fails it is not marked "at risk" until the date of the scheduled rescan. See Schedule a scan on page 441.

    To rescan the user must open a browser and navigate to the following:

    ```
    https://<Server or Application Server>/remediation
    ```

The FortiNAC Server or Application Server in the URL can be either the IP address or Name of the server that is running the captive portal.

- Modify existing scans or create new ones and set the Delayed Remediation option for the number of days the host should be allowed to continue on the network after failing a scan. The default setting for Delayed Remediation is 0 days or no delay. See Add or modify a scan on page 433.
- If a host has already failed a scan with a Delayed Remediation setting and the delay setting is changed on the Scan, it does not change the delay for the associated host. For example, if Host A is scanned, fails Scan A and is assigned a delay of 2 days, changing Scan A to a delay of 5 days does not alter the delay for Host A. It remains 2 days.
- Configure events and alarms to notify you when a host is affected by the Delayed Remediation setting. See Enable and disable events on page 857. Events include:
  - **Host Pending At Risk** — Indicates that a host has failed a scan that has a Delayed Remediation set and has been set to Pending At Risk.
  - **Host Security Test - Delayed Failure** — A host has failed a scan and the scan has been set to Failure Pending in the Host Properties Health Tab.

Process

Below is a sample of the process FortiNAC goes through when Delayed Remediation is enabled.

1. A host connects to the network and is scanned by an agent with Scan A that has a 3 day delay configured.
2. The host fails the scan for Anti-Virus.
3. A failure page indicating the reason for the failure is displayed on the host.
4. A Delayed Remediation record is created for this host and Scan A, which was used to scan the host.
5. The host's status is set to Pending At Risk.
6. On the Host Properties - Health Tab the scan for Scan A is set to Failure Pending.
7. The host remains on the production network and is not sent to the remediation VLAN.
8. After one day the host connects in the Library and is scanned by an agent with Scan B that has a 5 day delay configured.
9. The host fails the scan for Operating System.
10. A failure page indicating the reason for the failure is displayed on the host.
11. A second Delayed Remediation record is created for this host and Scan B.
12. The host status remains Pending At Risk.
13. On the Host Properties - Health Tab the scan for Scan B is set to Failure Pending.
14. The user corrects the Anti-Virus issue and rescans with Scan A.
15. The Delayed Remediation record for this host and Scan A is removed.
16. On the Host Properties - Health Tab the scan for Scan A is set to Success.
17. The host's status remains Pending At Risk because the user has not corrected the Operating System issue and rescanned for Scan B.
18. Five days elapse and the user still has not corrected the Operating System issue and rescanned for Scan B.
19. The host is marked At Risk but it is not moved to the Remediation VLAN because Scan B is not the scan that currently applies to the host. Scan B will apply to the host if the host ever reconnects in the Library.
20. On the Host Properties - Health Tab the scan for Scan B is set to Failure.
21. The Delayed Remediation record for this host and Scan B is removed.
22. The host continues on the production network.

23. If the host ever reconnects in the Library, the host will be placed in Remediation. The User will have to resolve the Operating System issue and rescan the host for Scan B.

Each host failure and delay record is treated individually. Passing one scan and associated delay, does not remove failures for other scans and corresponding delays. However, if a failed scan does not apply to the host, the host will not be sent to Remediation. Refer to Host health and scanning on page 803.

Add or modify a scan

Use the Add or Modify Scan dialog to configure scan settings. Settings are divided into two tables. The first table details the fields on the General tab and the second details the Categories available under the remaining tabs.

1. Select **Policy > Policy Configuration**.
2. In the menu on the left click the + sign next to **Endpoint Compliance** to open it.
3. Click the **Scans** option to select it.
4. On the Scans View, click **Add** to add a new scan or select an existing Scan and click **Modify**.
5. Enter data in the fields as needed. See the Settings table below for information on each field.
6. For each operating system tab, there is a drop-down menu of categories that can be set, such as, anti-virus settings. Instructions for configuring each category are contained in the Scan Configuration Settings - Categories table.
7. The **Summary** tab provides an overview of the entire scan configuration for your review.
8. Click **OK** to save the scan.

Settings - general tab

Field	Definition
Scan Name	Each scan must have a unique name.
Scan settings	
Scan On Connect (Persistent Agent Only)	Forces a rescan every time the host assigned this scan connects to the network. This option only affects hosts running the Persistent Agent. See Scan on connect on page 430.
Renew IP (Supported Dissolvable Agent Only)	Indicates whether the Renew IP option is enabled or disabled. When this option is enabled, it causes the Dissolvable Agent to actively release and renew the IP address of the host after it has completed its scan. The Renew IP option is only supported on the following systems that use the Dissolvable agent: • Windows: All Dissolvable Agent Versions • Mac-OS-X: Dissolvable Agent Versions 3.3.0.56+

Field	Definition
Root Detection (Mobile Agent Only)	The Mobile Agent determines whether or not the device has been rooted. Rooting is a process allowing users of devices running the Android operating system to attain privileged control (known as "root access") within Android's subsystem. If enabled, rooted mobile devices are not allowed to register. If disabled, devices suspected of being rooted are allowed to register and (Rooted) is appended to the operating system information displayed in the Host View. If the agent detects that device has been altered, a **Potential Rooted Device** event is generated.
Remediation - On Failure	If enabled, the host is scanned and the information associated with the scan is recorded. If the host fails the scan, the user must resolve all of the issues for which the host failed and rescan before being allowed on the network. **Agent Order Of Operations:** This set of options is available only when Remediation is set to On Failure. Determines the order in which the agent performs its tasks. Choose one of the following: **Scan Before Registering:** The host downloads the Agent and is scanned in the registration network before being registered. If the scan fails you must choose one of the following: • **Do not Register, Remediate:** Host remains a Rogue and stays in the registration network until it passes the scan. Note the host will not be marked "at risk." Default setting. • **Register and mark At Risk:** The host is registered immediately after the scan and then moved to Quarantine. Persistent Agent always registers and marks at risk. **Register, then Scan (if the scan fails, Remediate):** The host does not download an agent in the Registration network. Instead, the host is registered and moved to Quarantine to download the Agent and be scanned.
Remediation - Delayed	Hosts who fail this scan are set to Pending at Risk for the number of days indicated in the Remediation Delay field. Hosts set to Pending at Risk are not placed in remediation until the number of days indicated has elapsed. The user is notified of the failure immediately. Changes to this setting do not affect hosts that are already marked as Pending At Risk. If a host was set to a delay of 3 days and you change the Remediation Delay field to 5 days, the host remains at a delay of 3 days. Hosts scanned after the change will use the 5 day setting. **Agent Order Of Operations:** **If scan fails - Register or Remediate:** If the host fails a scan, the Persistent Agent displays a message stating that the host is at risk. Click the message to display information about the scan. The host is automatically registered.

Field	Definition
	The Dissolvable Agent displays the results of the scan. You can choose to rescan or register. When the host is registered, the host is placed in production. The user can correct all of the issues and re-run the Agent.
Remediation - Audit Only	If enabled, the host is scanned and the information associated with the scan is recorded.If the host fails the scan, it is not marked "at risk". Therefore, it is not forced into Remediation and can continue using the network. The administrator can review the scan results and take corrective action without disrupting users on the network. **Agent Order Of Operations:** **If scan fails - Register or Remediate:** If the host fails a scan, a web page with a Register option and a Remediate option is displayed to the user. If the user chooses the Remediate option, the host is placed in remediation and the user must correct all issues and rescan. If the user chooses the Register option, the host is placed in production. The user can correct all of the issues and re-run the Agent.
Remediation	If On Failure is enabled, the host is scanned and the information associated with the scan is recorded. If the host fails the scan, the user must resolve all of the issues for which the host failed and rescan before being allowed on the network. If Delayed is enabled, hosts who fail this scan are set to Pending at Risk for the number of days indicated in the Remediation Delay field. Hosts set to Pending at Risk are not placed in remediation until the number of days indicated has elapsed. The user is notified of the failure immediately. If Audit Only is enabled, the host is scanned and the information associated with the scan is recorded.If the host fails the scan, it is not marked "at risk". Therefore, it is not forced into Remediation and can continue using the network. The administrator can review the scan results and take corrective action without disrupting users on the network.

Field	Definition
Agent Order of Operations	When Remediation is set to On Failure: Determines the order in which the agent performs its tasks. Choose one of the following: • **Scan Before Registering:** The host downloads the Agent and is scanned in the registration network before being registered. If the scan fails you must choose one of the following: • **Do not Register, Remediate:** Host remains a Rogue and stays in the registration network until it passes the scan. Note the host will not be marked "at risk." Default setting. • **Register and mark At Risk:** The host is registered immediately after the scan and then moved to Quarantine. Persistent Agent always registers and marks at risk. **Register, then Scan (if the scan fails, Remediate):** The host does not download an agent in the Registration network. Instead, the host is registered and moved to Quarantine to download the Agent and be scanned. When Remediation is set to Delayed or Audit Only: **If scan fails - Register or Remediate:** If the host fails a scan, a web page with a Register option and a Remediate option is displayed to the user. If the user chooses the Remediate option, the host is placed in remediation and the user must correct all issues and rescan. If the user chooses the Register option, the host is placed in production. The user can correct all of the issues and re-run the Agent.
Portal page settings	
Label For Scan Failure Link	Label displayed on the failure page when a network user's PC has failed a scan. If no label is provided, the scan name is used. The label or scan name is a link that takes the user to a page indicating why the PC has failed the scan.
Instructions For Scan Failure	If a host has failed a scan, the user must remedy the issue and rescan. This field allows you to provide the user with a brief set of instructions.
Patch URL For Dissolvable Agent Re-Scan	URL for the web page to be displayed when a host using the Dissolvable Agent fails the scan. This web page allows the user to download the agent and rescan after addressing the issues that caused the failure. Hosts using the Persistent Agent have the agent installed and do not use this page. Set this to /remediation To rescan the user must open a browser and navigate to the following: `https://<Server or Application Server>/remediation` The FortiNAC Server or Application Server in the URL can be either the IP address or Name of the server that is running the captive portal.

Field	Definition
In use by/Not currently in use	Indicates whether the scan is being used in User/Host Profile(s). When the scan is in use, click the link to view the User/Host Profile(s).

Settings - categories

For each operating system there is a Category drop-down that allows you to configure specific settings for categories such as anti-virus. The table below outlines these settings.

Default parameter values for individual anti-virus and operating systems packages are entered and updated automatically by the schedsuled Auto-Def Updates. If the values have been manually edited, the Auto-Def Updates will not override those changes.

Removing a check mark from a selected option causes any underlying changes to be lost. For example, if you modified settings for AVG antivirus and then unselected it, those changes are lost.

Field	Definition
Anti-virus	
Validation Options	• **Any** — Any one of the selected items must be present on the host to pass the scan. • **All** — All of the selected items must be present on the host to pass the scan.
Anti-Virus List	New anti-virus software is continually being created. As new anti-virus software becomes available, parameters for that software are made available as quickly as possible in FortiNAC. The default values for each anti-virus program are entered automatically by the scheduled Auto-Def Updates feature. You should not need to modify these. Select one or more types of **Anti-virus software** to check for on the host. To set additional parameters for any of the selected Anti-Virus programs, click the name of a program. A parameters window opens and displays all of the advanced options that can be set. Enter the custom parameter values for the selected program and click **OK**. See Anti-Virus parameters - Windows on page 1058 or Anti-Virus parameters - macOS on page 1062 for details on each parameter.
Preferred	Select the **Preferred** Anti-Virus from the drop-down list. If the host fails for all of the products selected for the scan, only the preferred item selected is displayed on the Failed Policy pages. If no Preferred product is selected, the list displayed on the Failed Policy pages contains a separate line for every product failure.
Custom scans	
Custom Scans List	Custom scans are user created scans that have been configured to scan hosts for things such as specific files, registry entries or programs. Custom scans must be created and saved before they can be included as part of a Security Policy. See Custom scans on page 448. When a Custom scan is added to a regular scan the custom scan is used across the board no matter what other options have been selected for the policy. Any host that is scanned with the regular scan is also scanned based on the Custom Scan. See Custom scan options - scan level on page 449.

Field	Definition
	Custom scans can be added within a category, such as Anti-Virus. For example, any host that has AVG Anti-Virus will be scanned using an associated custom scan. In this case, the Custom Scan is being used to enhance the scan for AVG Anti-Virus and it is not run on every host. See Custom scans options within a category level on page 449.
Operating systems	
Selection Options	• **All** — Marks every operating system with a check mark. • **None** — Removes the check mark from every operating system check box.
Operating Systems List	Scans for required or prohibited operating systems on hosts. Operating systems that are selected are required. See Operating system parameters - Windows on page 1064 The Windows-2003-Server-x64 product has been removed. Use the Windows 2003 Server and Windows XP x64 products.
Preferred	Select the **Preferred** Operating System from the drop-down list. If the host fails for all of the products selected for the scan, only the preferred item selected is displayed on the Failed Policy pages. If no Preferred product is selected, the list displayed on the Failed Policy pages contains a separate line for every product failure.
Monitors	
Scan List	Allows you to run a custom scan with greater frequency than the regular scan with which it is associated. For example, the original scan may only run once a week, but you may have a custom scan that needs to run every half an hour. Instead of running the entire scan policy every half an hour you can choose to run only a custom scan. Select a custom scan and enter the frequency with which it should run. Performance degradation may occur if you select an interval less than every five (5) minutes. It is recommended that monitoring intervals be set to five (5) minutes or more.

Custom scan options - scan level

Custom scans can be enabled for a regular scan. When a host is checked for compliance with the regular scan, the custom scan is also checked. Before adding a Custom Scan to a security scan you must create the custom scan.

To enable a Custom scan for a security scan:

1. Click **Policy > Policy Configuration**.
2. In the menu on the left click the + sign next to **Endpoint Compliance** to open it.
3. Click the **Scans** option to select it.
4. Modify the scan that will use this custom scan.
5. Click either the **Windows**, the **macOS**, or the **Linux** tab.
6. Select **Custom** from the drop-down menu at the top of the window.
7. Select the check box next to the Custom Scan for the security scan.
8. Click **OK** to save your changes.

Custom scans options within a category level

Custom scans can be enabled for various categories within a security scan such as the anti-virus or operating system requirements. When a host is checked for compliance with the security scan and one of the products within a category has a custom scan enabled, the custom scan is also used for hosts with the selected product. For example, if the security scan checks for the existence of AVG Anti-Virus and a Custom Scan has been associated with AVG, then hosts with AVG will also be scanned using the Custom Scan.

Before adding a custom scan to a security scan you must create the custom scan.

1. Click **Policy > Policy Configuration**.
2. In the menu on the left click the + sign next to **Endpoint Compliance** to open it.
3. Click the **Scans** option to select it.
4. Modify the security scan that will use this custom scan.
5. Click either the **Windows**, the **macOS**, or the **Linux** tab.
6. Click the **Category** drop-down on the Modify Scan view and select: anti-virus, operating system, etc.
7. Click the specific item within the sub-category (i.e. product name).
8. Click the **Custom Scans** tab and click next to the **Custom Scan** name to be applied to this sub-category.
9. Click **OK** to save the selected custom scan.
10. Click **OK** to save changes to the security scan.

Monitor custom scans

This feature allows you to run a custom scan with greater frequency than the security scan with which it is associated. For example, the original security scan may only run once a week, but you may have a custom scan that needs to run every half an hour. Instead of running the entire security scan every half an hour you can choose to run only a custom scan.

Use the monitor feature to periodically test for a specific status on hosts running the Persistent Agent. Monitors use Custom Scans to check the host. A monitor you configure as part of a scan can be the same or different for each scan. Configure monitors for each platform (Windows, macOS, or Linux) separately.

Hosts associated with the security scan are checked at the interval period set in the monitor. The agent on the host sends a message to the server after each time period has passed, indicating whether the host has passed or failed the scan. If several monitors are set to 1 minute intervals, traffic to the server is increased. For example, if there are 10 monitors running every minute on 5,000 hosts, the server might see up to 50,000 messages a minute.

Even though monitors use custom scans which can be set to warning, monitors will not send warnings to hosts. Monitors can only pass or fail. Hosts that fail are marked at risk and placed in remediation.

Enabling a monitor for a custom scan automatically enables the custom scan. However, disabling a monitor will not disable the associated custom scan.

For example, you have created Custom Scan A but have not selected it within any security scan. When you select Custom Scan A in the Monitor list select a time period, the custom scan is enabled.

Monitors ignore the severity flag of a custom scan.

Monitor example

All users have been notified that peer-to-peer software is not tolerated on the network. A web page explaining this policy is located in the remediation area where the host is moved after failing the scan.

Actions taken:

- A custom scan for a prohibited process has been created to check for LimeWire, a peer-to-peer software program, running on the host. The custom scan includes the URL of the web page where the host browser will be directed if the host fails the custom scan.
- The monitor is set to 10 minutes for the custom scan.

Results:

- Every 10 minutes the agent checks the host to determine if LimeWire is running.
  - If LimeWire is not running, the agent sends a message to the server indicating that the host has passed the security scan.
  - If LimeWire is running, the agent sends a message to the server indicating that the host has failed the scan. The host is immediately moved to the quarantine VLAN and the browser redirected to the web page specified in the Custom Scan.

Set up a custom scan monitor

Before adding a Custom Scan to a security scan you must create the custom scan.

1. Click **Policy > Policy Configuration**.
2. In the menu on the left click the **+** sign next to **Endpoint Compliance** to open it.
3. Click the **Scans** option to select it.
4. Click the security scan name and click **Modify**. If the security scan does not exist, it needs to be added. See Scans on page 426 for details on adding scans.
5. Click either the **Windows**, the **macOS**, or the **Linux** tab.
6. Click the **Category** drop-down and select **Monitors**.
7. Select the check box for the type of custom scan.
8. Select the time period that the agent waits before checking the host for compliance with the custom scan settings. The available intervals are every 15 seconds up to and including 1 minute, and every 5 minutes up to and including 1 hour.

   Performance degradation may occur if you select a very short interval or if you select a large number of monitors. It is recommended that monitoring intervals be set to five (5) minutes or more.
9. Click **OK**.

Reset default Anti-Virus values

Anti-Virus parameters contained in FortiNAC are updated weekly using the Auto-Def updates feature. This ensures that new version numbers and bug definition files for Anti-Virus software that you require are taken into account when users' computers are scanned.

If you have manually edited any parameters associated with a particular Anti-Virus software the Auto-Def update does not override your settings for that software. To reset Anti-Virus to the default values and allow the Auto-Def updates feature to update parameters do the following:

1. Click **Policy > Policy Configuration**.
2. In the menu on the left click the **+** sign next to **Endpoint Compliance** to open it.
3. Click the **Scans** option to select it.
4. Select a scan and click **Modify**.
5. Click either **Windows** or **Mac**, whichever applies.

6. Select **Anti-Virus** from the **Categories** drop-down.
7. Uncheck the checkbox for the software for which you have modified settings.
8. Click **OK**.
9. Open the same scan again and navigate back to the software you unchecked.
10. Check the checkbox for the previously modified settings and click **OK**.
11. Repeat this process for each Anti-Virus software that needs to be reset to defaults.
12. The next time the Auto-Def updates feature retrieves and installs an update, the Anti-Virus software that you reset will accept the updated parameters.

Delete a scan

If a Scan is in use by another feature in FortiNAC, it cannot be deleted. A dialog displays with a list of the features in which the scan is used. Remove the association between the scan and other features before deleting the scan.

1. Click **Policy > Policy Configuration**.
2. In the menu on the left click the **+** sign next to **Endpoint Compliance** to open it.
3. Click the **Scans** option to select it.
4. Click the scan to be removed.
5. Click **Delete**.
6. Click **OK** to remove the scan.

Deleting a scan automatically removes scheduled tasks for that scan.

Scans in use

To find the list of FortiNAC features that reference a specific Scan, select the Scan from the Scans View and click the In Use button. A message is displayed indicating whether or not the Scan is associated with any other features. If the Scan is referenced elsewhere, a list of each feature that references the Scan is displayed.

Schedule a scan

When hosts that use the Persistent Agent or the Dissolvable Agent connect to the network, they are checked against an Endpoint Compliance Policy. FortiNAC maintains a list of hosts that have passed the scan within the policy. When hosts that previously passed the scan connect to the network, they are given access.

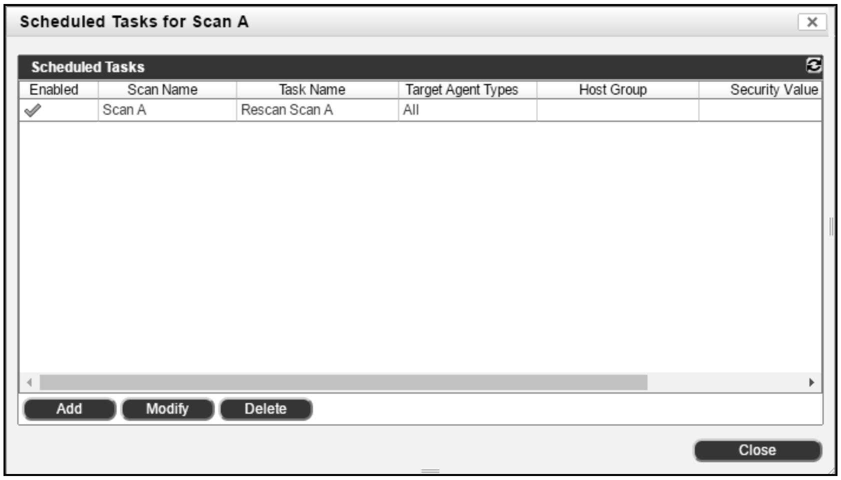
To recheck the hosts and ensure continued compliance, schedule the scan to be run at specific intervals. The hosts are rechecked the next time the scheduled task for the scan runs. Only hosts that have a valid operating system listed in Host Properties are rescanned. Valid operating systems include Linux, Windows, and Mac.

You can add more than one scheduled task for each scan to check different groups of network hosts at various times. This prevents an excessive load on the system. These groups are subgroups of the original group targeted by the scan. For example, if the original scan was set to scan all staff in the Building A group, the scheduled scan could target staff in subsets of the Building A group. Subsets would be created by placing staff from the Building A group into smaller groups. Then, the 1st floor group could be scanned on Mondays, the 2nd floor group could be scanned on Tuesdays, etc.

If FortiNAC has lost contact with the host's Persistent Agent, the host cannot be scanned.

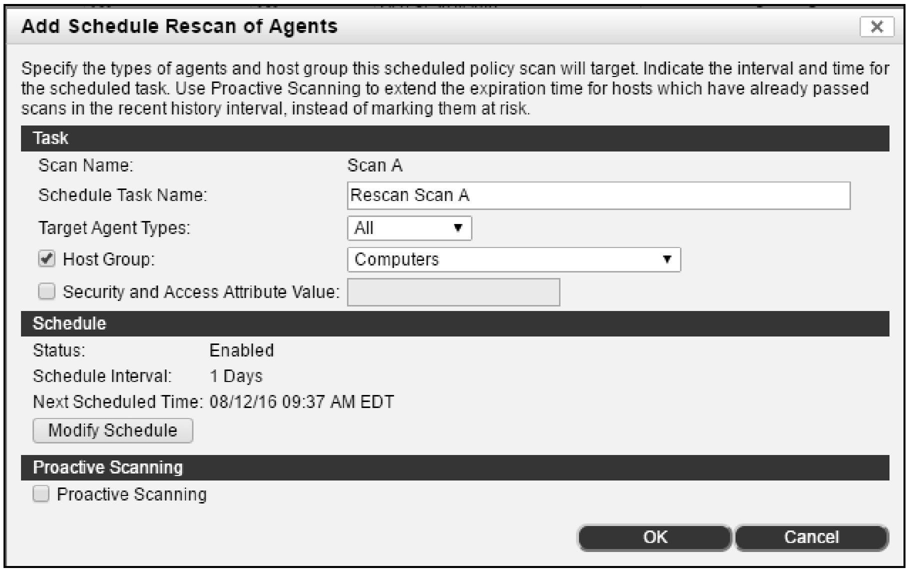
Offline hosts will be rescanned when they come back online.

1. Select **Policy > Policy Configuration**.
2. In the menu on the left click the **+** sign next to **Endpoint Compliance** to open it.
3. Click the **Scans** option to select it.
4. Click the scan to be scheduled.
5. Click **Schedule**. The Schedule Rescan of Agents window opens. Any existing scheduled tasks appear in the window.



Enabled	Scan Name	Task Name	Target Agent Types	Host Group	Security Value
✓	Scan A	Rescan Scan A	All		

6. Click Add.



Add Schedule Rescan of Agents

Specify the types of agents and host group this scheduled policy scan will target. Indicate the interval and time for the scheduled task. Use Proactive Scanning to extend the expiration time for hosts which have already passed scans in the recent history interval, instead of marking them at risk.

Task

Scan Name: Scan A

Schedule Task Name: Rescan Scan A

Target Agent Types: All

☑ Host Group: Computers

□ Security and Access Attribute Value:

Schedule

Status: Enabled

Schedule Interval: 1 Days

Next Scheduled Time: 08/12/16 09:37 AM EDT

Proactive Scanning

□ Proactive Scanning

7. Use the information in the table below to configure your schedule.

Field	Definition
Task	
Scan Name	Name of the Scan that will be used to rescan hosts.
Schedule Task Name	Each task for the selected scan must have a unique name.
Target Agent Types	Type of agent the hosts are using: ALL, Dissolvable, or Persistent.
Host Group	If selected, indicates the group of hosts that will be checked for scan compliance when this scheduled task runs. See Groups view on page 838 for information on creating groups. This group of hosts must be contained within the set of hosts targeted in the original scan.
Security And Access Attribute	If selected, filters hosts for rescan based on a field in the user record with matching data in the LDAP or Active Directory. This group must be the same as or a subset of the group targeted in the original scan.

If the Group option and the Security and Access Attribute option are both selected, the host must be a member of the group selected and the user must have a matching Security and Access Attribute value in order to be scanned.

If neither the Group option nor the Security and Access Attribute option are selected, all of the hosts targeted by the original scan are scanned.

Scans can be used in multiply policies, therefore, the set of hosts to be scanned could be quite large.

Field	Definition
Schedule	
Status	Indicates whether the scheduled task is current enabled or disabled.
Schedule Interval	How often the scheduled task is to run. Enter a number and select Days, Hours, or Minutes from the drop-down list.
Next Scheduled Time	The next date/time to run the scheduled task. Enter in the format MM/DD/YY HH:MM AM/PM
Modify Schedule	Opens the Modify Scheduled Activity dialog where you can configure the scan's schedule.
Proactive scanning	
Proactive Scanning	See the section below for additional information.

8. Click Modify Schedule to run the scheduled task automatically or on a fixed day.
   - To run the task automatically, select Repetitive Task to select the rate at which you wish to run the task. For example, selecting a Repetition Rate of two days and the Next Scheduled Time of today at 1:00 PM means the task will run today at 1:00 PM, and will continue to run every two days at 1:00 PM.
   - To run the task on a fixed day and time, select Fixed Day Task and then select the day(s). The task will automatically run on the selected day(s) and time each week.
9. Click **Apply**.

Add proactive scanning to a scheduled scan

Within FortiNAC you can schedule scans to run automatically. Hosts using the Dissolvable Agent can initiate a rescan on the production network. When a rescan is successful, the host has extended the time before another scan is required.

For example, assume the schedule is set to rescan every Sunday. The user rescans his host at his convenience on Friday and passes the scan. When Sunday comes, FortiNAC checks the scan history and determines that this host has had a successful scan. This host is not forced to rescan nor is it marked at risk.

If the host fails the scan, the user is presented with a list of reasons for the failure. The host is not marked at risk at this time. If the user resolves the issues and rescans before the scheduled scan date, the host is never marked at risk and is not forced to rescan on Sunday. If the user does not resolve the issues and rescan, when the scheduled scan date arrives the host is either marked at risk or aged out of the database. The host cannot access the network until it has been successfully scanned or until the host is reregistered and then is successfully scanned.

To rescan the user must open a browser and navigate to the following:

```
https://<Server or Application Server>/remediation
```

The FortiNAC Server or Application Server in the URL can be either the IP address or Name of the server that is running the captive portal.

Proactive scanning is enabled on the Schedule Rescan window. To provide your hosts access to the dissolvable agent, you can create a web page accessible from your network to download the dissolvable agent.

Scan results are central to FortiNAC's ability to determine when a host was last scanned. Scan results are removed based on the archive and purge schedule set up in FortiNAC properties. When configuring the archive and purge schedule be sure to make the interval long enough to allow the scan results to be used for Proactive Scanning. If the interval is too short, scan results will be purged too soon forcing all hosts to rescan regardless of when their last scan occurred. See Database archive on page 210 for information on archive and purge settings.

Schedule a scan—proactive scanning

Users can proactively rescan their computers to re-assess their system with or without any impact to their At Risk status. This feature helps to decrease the load around the re-registration process or rescan intervals.

To rescan the user must open a browser and navigate to the following:

```
https://<Server or Application Server>/remediation
```

The FortiNAC Server or Application Server in the URL can be either the IP address or Name of the server that is running the captive portal.

The time extension capability can not change a guest record’s age-out time; time extensions only apply to standard hosts.

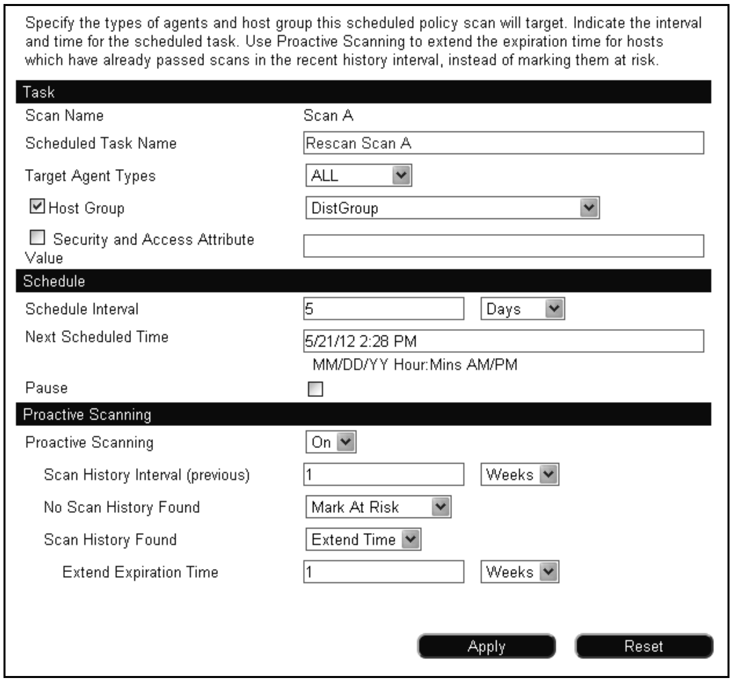
Use the options in the **Schedule Rescan** window to specify whether to apply a time extension if there is a successful scan history within the interval, and what actions to take if there is no scan history. For example if a host does not rescan proactively, the registered host can be set to age-out or be marked At Risk.

Once you have created a policy, do the following to configure the proactive scanning and specify subsequent actions.

Add proactive scanning to a scan schedule

1. Click **Policy > Policy Configuration**.
2. In the menu on the left click the **+** sign next to **Endpoint Compliance** to open it.
3. Click the **Scans** option to select it.
4. Select the scan to be scheduled.
5. Click **Schedule**. The **Schedule Rescan of Agents** window opens. Any existing scheduled tasks for the scan appear in the window.
6. Click **Add**.
7. For **Target**, select **Dissolvable**. Only hosts using the Dissolvable Agent can do a proactive scan.
8. For the **Proactive Scanning Option**, select **On**.
9. Click **Apply**.

In the example shown below, the **Scan History Interval** is set to one week. If hosts have successfully passed a scan during the week prior to the time and date specified in the **Next Scheduled Time** field, their expiration time is extended by one week and they will remain on their production network. If they do not have a successful scan within the previous week, they are marked at risk and moved to remediation to be rescanned.



Specify the types of agents and host group this scheduled policy scan will target. Indicate the interval and time for the scheduled task. Use Proactive Scanning to extend the expiration time for hosts which have already passed scans in the recent history interval, instead of marking them at risk.

Task	
Scan Name	Scan A
Scheduled Task Name	Rescan Scan A
Target Agent Types	ALL
☑ Host Group	DistGroup
□ Security and Access Attribute Value	
Schedule	
Schedule Interval	5 Days
Next Scheduled Time	5/21/12 2:28 PM MM/DD/YY Hour:Mins AM/PM
Pause	□
Proactive Scanning	
Proactive Scanning	On
Scan History Interval (previous)	1 Weeks
No Scan History Found	Mark At Risk
Scan History Found	Extend Time
Extend Expiration Time	1 Weeks

Settings

Field	Definition
Task	
Scan Name	Name of the Scan that will be used to rescan hosts.
Schedule Task Name	Each task for the selected policy must have a unique name.
Target Agent Types	Type of agent the hosts are using: ALL, Dissolvable, or Persistent.
Host Group	If selected, indicates the group of hosts that will be checked for scan compliance when this scheduled task runs. See Groups view on page 838 for information on creating groups. This group of hosts must be contained within the set of hosts targeted in the original policy.
Security And Access Attribute	If selected, filters hosts for rescan based on a field in the user record with matching data in the LDAP or Active Directory. This group of must be the same as or a subset of the group targeted in the original policy.

If the Group option and the Security and Access Attribute option are both selected, the host must be a member of the group selected and the user must have a matching Security and Access Attribute value in order to be scanned.

Field	Definition
	If neither the Group option nor the Security and Access Attribute option are selected, all of the hosts targeted by the original scan are scanned.
	Scans can be used in multiply policies, therefore, the set of hosts to be scanned could be quite large.
Schedule	
Schedule Interval	How often the scheduled task is to run. Enter a number and select Days, Hours, or Minutes from the drop-down list.
Next Scheduled Time	The next date/time to run the scheduled task. Enter in the format MM/DD/YY HH:MM AM/PM
Pause	When selected, the scheduled task is paused and will not run automatically. Go to the Scheduler View and run the task manually. See the Scheduler view on page 849 for more information.
Proactive scanning	
Proactive Scanning	Select **On**. If you select Off, the hosts are placed in Quarantine when the scheduled task runs.
Scan History Interval (previous)	Interval of time the previous scan history is considered valid.
No Scan History Found	If the host has not been successfully scanned within the scan history interval, you have the option of marking the host at risk or aging the record. If you select **At Risk**, the host is moved to Quarantine to be rescanned. If you select **Age Record**, the host is deleted and must be re-registered to regain network access.
Scan History Found	If the most recent scan in the scan history is a successful scan for the host and is within the scan history interval, you have the option of selecting No Action or Extend Time. Select **No Action** to let the account remain with the existing expiration date and time. If the system takes no action, the host is forced to rescan when the expiration date and time are met even if the host has a successful scan prior to the expiration date and time. Select **Extend Time** to specify a period in Extend Expiration Date (the next field).

Field	Definition
Extend Expiration Time	If Extend Time is selected and the host has had a successful scan within the Scan History Interval, the host’s expiration time is extended by this amount.

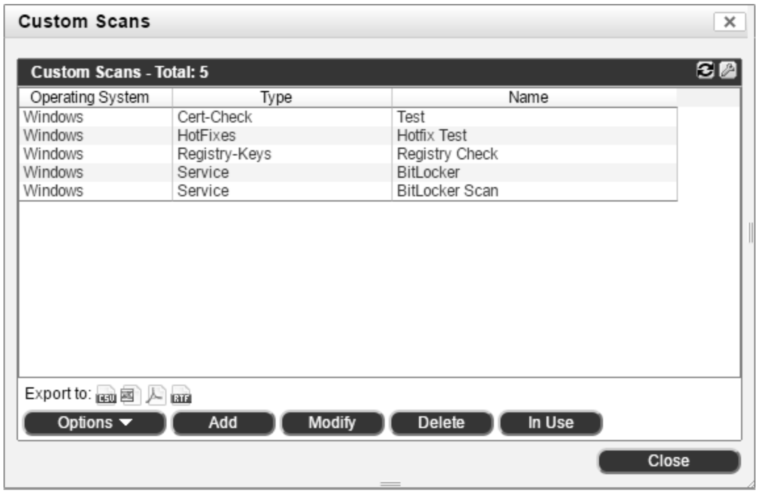
Custom scans

Scans are configured to evaluate hosts connecting to the network. These scans search the host computer for things such as anti-virus software or a particular version of an operating system. The categories within which the scan can search are fairly broad. To scan for very specific items, such as a file on the hard drive or a patch, you must create Custom Scans and then link Custom Scans to a general Scan.

The severity level set in the Custom Scan determines how the host is treated when it fails a Custom Scan. Levels can be set to deny the host access to the network or to just send a warning. See Severity level on page 469 for additional details.

Custom Scans that are associated with a Scan can be configured to run at more frequent intervals than the Scan itself by setting up a Monitor in the Scan. This requires that the host have the Persistent Agent installed.

In addition to running a Custom Scan on any host that is evaluated by the associated Scan, you can use Custom Scans to refine or enhance other Scans. For example, if you have set up a Scan to check hosts for one of the following anti-virus programs: AVG 8.5, Kaspersky, or Norton. Within the Kaspersky setting you can add a Custom Scan to search for a version that must be installed. This Custom Scan will not be run for hosts using AVG 8.5 or Norton. It will be run for hosts using Kaspersky.



Operating System	Type	Name
Windows	Cert-Check	Test
Windows	HotFixes	Hotfix Test
Windows	Registry-Keys	Registry Check
Windows	Service	BitLocker
Windows	Service	BitLocker Scan

Custom Scans are created differently depending on the operating system on which they will run. You must create separate Custom Scans for each operating system.

When hosts fail a Custom Scan, they are redirected to the web page designated within the Custom Scan configuration. These web pages are not provided as part of the Portal Configuration. They must be created and stored on your FortiNAC appliance in the following directory:

```
/bsc/Registration/registration/site
```

Within the directory listed above there are other web pages that might serve as a template for the custom scans web pages. One option is to copy the antivirus.jsp file to a new name and edit the text within that file to accommodate your custom scans.

> User created web pages that display when a host fails a custom scan are now stored in `/bsc/Registration/registration/site`. If you are using Portal Version 1 and have legacy pages that are stored in `/bsc/Registration/registration/sma` you do not need to move them to the new directory, they will continue to display to hosts as needed.

Custom scan options - scan level

Custom scans can be enabled for a regular scan. When a host is checked for compliance with the regular scan, the custom scan is also checked. Before adding a Custom Scan to a security scan you must create the custom scan. See Windows on page 450, macOS on page 462, or Linux on page 465.

To enable a Custom scan for a security scan:

1. Click **Policy > Policy Configuration**.
2. In the menu on the left click the + sign next to **Endpoint Compliance** to open it.
3. Click the **Scans** option to select it.
4. Modify the scan that will use this custom scan.
5. Click either the **Windows**, the **macOS**, or the **Linux** tab.
6. Select **Custom** from the drop-down menu at the top of the window.
7. Select the check box next to the Custom Scan for the security scan.
8. Click **OK** to save your changes.

Custom scans options within a category level

Custom scans can be enabled for various categories within a security scan such as the anti-virus or operating system requirements. When a host is checked for compliance with the security scan and one of the products within a category has a custom scan enabled, the custom scan is also used for hosts with the selected product. For example, if the security scan checks for the existence of AVG Anti-Virus and a Custom Scan has been associated with AVG, then hosts with AVG will also be scanned using the Custom Scan.

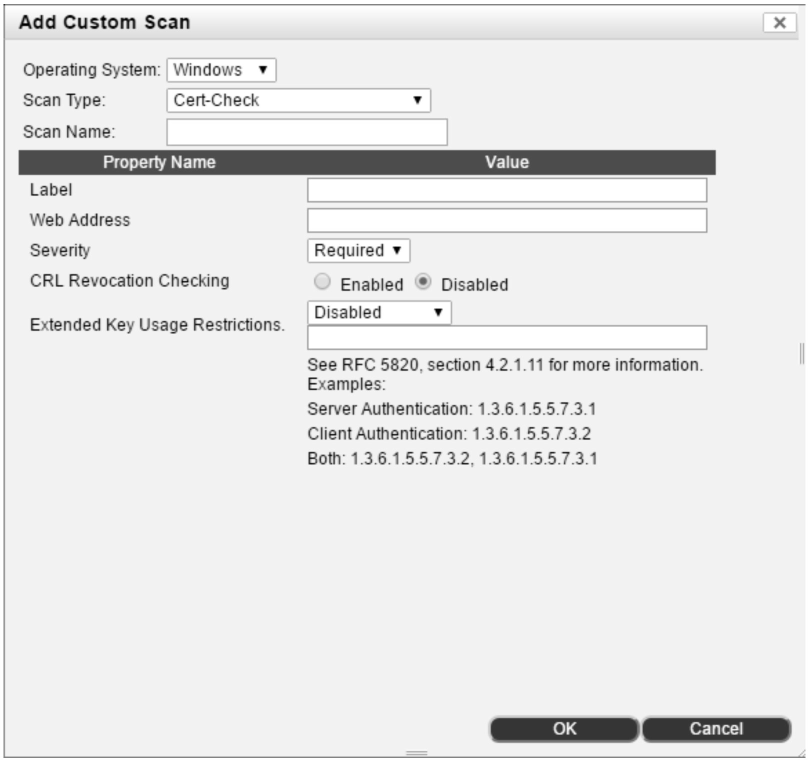
Before adding a Custom Scan to a security scan you must create the custom scan. See Windows on page 450 or macOS on page 462.

1. Click **Policy > Policy Configuration**.
2. In the menu on the left click the + sign next to **Endpoint Compliance** to open it.
3. Click the **Scans** option to select it.
4. Modify the security scan that will use this custom scan.
5. Click either the **Windows**, the **macOS**, or the **Linux** tab.
6. Click the **Category** drop-down on the Modify Scan view and select: anti-virus, operating system, etc.
7. Click the specific item within the sub-category (i.e. product name).
8. Click the **Custom Scans** tab and click next to the **Custom Scan** name to be applied to this sub-category.
9. Click **OK** to save the selected custom scan.
10. Click **OK** to save changes to the security scan.

Windows

The Custom Scans feature allows you to search host computers for very specific information. Custom Scans must be created separately for different operating systems. Within each operating system, there are different types of scans that can be created. Refer to Add A Windows Custom Scan below for a list of scan types and general instructions on adding scans. Refer to the instructions for each scan type for field level information. You can modify or delete the scans at any time. When a scan is modified it affects any existing Scan that use that Custom Scan.

Add a custom scan


Add Custom Scan

Operating System: Windows

Scan Type: Cert-Check

Scan Name:

Property Name	Value
Label	
Web Address	
Severity	Required
CRL Revocation Checking	○ Enabled ● Disabled
Extended Key Usage Restrictions.	Disabled

See RFC 5820, section 4.2.1.11 for more information.
Examples:
Server Authentication: 1.3.6.1.5.5.7.3.1
Client Authentication: 1.3.6.1.5.5.7.3.2
Both: 1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.1

1. Click **Policy > Policy Configuration**.
2. In the menu on the left click the **+** sign next to **Endpoint Compliance** to open it.
3. Click the **Scans** option to select it.
4. At the bottom of the window, click the **Custom Scans** button.
5. In the Custom Scans dialog, click **Add**.
6. Select **Windows** from the **Operating System** drop-down list.
7. Select the type of scan desired. Each scan type has a special set of fields that are specific to that type. Use the table below for settings.

Scan Type	Description
Cert-Check	Test for a valid certificate on the host.

Scan Type	Description
	Requires Agent Version 3.5 or higher. See Certificate check settings on page 451
Domain-Verification	Test for the domain joined by the host. See Domain verification scan settings on page 459. Note: Requires Agent Version 2.2.2 or higher. Using a lower version of the agent causes all hosts to pass the scan regardless of the domain returned.
File	Test for the existence and version of a specific file. If the file exists and is an executable the program can be forced to run. See File scan settings on page 453.
HotFixes	Test for the existence of specific HotFixes for the specified Operating systems. See HotFixes scan settings on page 456.
Processes	Test for the existence of a specific process name for the indicated Windows operating system. See Processes scan settings on page 458.
Prohibited - Domain-Verification	Test for the domain joined by the host. See Prohibited domain verification scan settings on page 460. Note: Requires Agent Version 2.2.2 or higher. Using a lower version of the agent causes all hosts to pass the scan regardless of the domain returned.
Prohibited-Processes	Test for the existence of a specific prohibited process for the indicated Windows operating system(s). See Prohibited processes scan settings on page 459.
Registry-Keys	Test for a specific registry key and its associated data. See Registry keys scan settings on page 454.
Registry-Version	Test for a specific program and its version. The program can be required for specific versions of the Windows Operating System. See Registry version scan settings on page 457.
Service	Test the state of a service running on the operating system. See Service scan settings on page 461. Requires Agent Version 3.5 or higher.

8. Enter the **Name** for the custom scan.
9. Enter the information for the custom scan.
10. Click **OK**.
11. The name of the Custom Scan displays in the Custom Scans section for each scan. You can select the Custom Scan to be part of the creation or modification of scan parameters.

Certificate check settings

The certificate being scanned must be obtained from the CA (e.g., Windows AD server), and installed on the host in the Certificate Store under **Local Computer > Personal > Certificates**. The certificate must then be uploaded to

FortiNAC's Certificate management to the Persistent agent cert-check target. Go to **System > Settings** and under **Security** click **Certificate Management**. Click **Upload Certificate**, and then select the **Persistent Agent Cert Check** target.

Requirements for client certificates:

- The certificate must be signed by a CA specified by the customer.
- The certificate selected by the agent should adhere to the uses as specified:
- The certificate is a client certificate that is located in the Certificate Store on the host under **Local Computer > Personal > Certificates**.
- The host name can be found in the certificate as part of the certificate's subject alternative name (SAN). For example, `DNS Name=Win7QA.qatest.com`.
- The agent must also be able to sign data using the certificate's private key, so the Key Usage must have "Digital Signature".

This refers to the Key Usage and not the Enhanced Key Usage.

To create a custom scan for a Cert-Check, enter the information shown in the table below into the custom scan window after selecting the Cert-Check scan type.

Scan Parameter	Description
Label (required)	This label appears in the Results page information to identify which scan the host failed.

Web Address (optional)	The URL of the page with information about this cert-check. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:
	`/bsc/Registration/registration/site`
	When completing this field you must enter part of the path for the page not just the page name, such as:
	`site/pagename.jsp`

Severity (required)	The severity of the failure if the certificate is not on the host. If you select Required and the certificate does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See Severity level on page 469 for more details.
CRL Revocation Checking (optional)	If enabled, CRL Revocation Checking ensures the certificate has not been revoked by the Certificate Authority (CA). If the certificate is revoked, the host fails the custom scan. The application server must have access to the web server. When CRL Verification is enabled, the server reads the CRL Distribution point URIs from the client certificate. The application server will directly download a CRL from an "http://" URI, or indirectly download a CRL from a "ldap://" URI through your configured LDAP servers.

Scan Parameter	Description
Extended Key Usage Restrictions (optional)	If enabled, determines how the private key may be used. Multiple extensions must be comma-separated. For example, if you select this option and enter "1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.1" as the specified extensions, • **Disabled** - There are no restrictions on key usage extensions. • **All of** - The certificate must include all of the specified extensions. • **Exactly** - The certificate must include only the specified extensions. • **One or More of** - The certificate must have at least one of the specified extensions. • **None of** - The certificate may have extensions, but it must not have one of the specified extensions.

File scan settings

To create a custom scan for a specific file, enter the information shown in the table below into the custom scan window after selecting the File scan type.

Scan Parameter	Description
Label	This label appears in the Results page information to identify which scan the host failed.
Severity	The severity of the failure if the file is not on the host. If you select Required and the file does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See Severity level on page 469 for more details.
File Name	The name of the file being checked.
File Contains String	Enter the content that must be present within the file in order for the host to pass the scan (e.g., the version number of a product in a configuration file). When the information is found, the host passes the scan. If the information is not found, the host fails the scan. Requires Agent 4.0.4 or greater. Requires AV/AS Definition Updates as of May 2, 2016.
Registry Key	To speed up the search for a file you can first check the registry to determine the folder in which the file is installed. In this field you would enter the section of the registry where the information about the file you seek resides. For example, if you want to make sure that Windows Messenger is installed on the host, the scan needs to look for **msmsgs.exe**. Enter the registry key that points to the Value Name containing the location of msmsgs.exe, such as:

Scan Parameter	Description
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MessengerService
Registry Value Name	The Value Name that contains the path to the file the custom scan is seeking. To continue the example above, the Registry Key listed in the previous field tells the custom scan the part of the registry to access to determine where msmsgs.exe is installed. Once the custom scan is looking in the correct section, it needs to know the specific "container" or Value Name in the registry that has the path to msmsgs.exe, such as: InstallationDirectory The custom scan can begin its search in the directory specified in the "InstallationDirectory" Value Name, such as: "C:\Program Files\Messenger"
Execute	Default = No. Select Yes to run the file when it is located.
Command-Line Options	Command line options to be used when executing the file.
Wait for Execution to Complete Before Continuing	Default = No. If set to Yes, the scan waits until the execution of the program is complete before continuing.
File Version (>=)	The version number of the file has to be greater than or equal to the version number entered here.

Web Address	The URL of the page with information about this file. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:
	`/bsc/Registration/registration/site`
	When completing this field you must enter part of the path for the page not just the page name, such as:
	`site/pagename.jsp`

Windows OS	Select the check box next to the version(s) of Windows OS for which this key is required. Select the OS within the Custom Scan to apply the custom scan to hosts with that OS. If you do not select an OS in the Custom Scan, and the host has that OS, the host automatically passes the general scan.
Prohibit this product	If the file is found and this is set to true, the host fails the scan for a prohibited product. Default = false.

Registry keys scan settings

To create a custom scan for a specific Registry key, enter the information shown in the table below into the custom scan window after selecting the Registry-Keys scan type.

Scan Parameter	Description
Label	This label appears in the Results page information to identify which scan the host failed.

Scan Parameter	Description
Web Address	The URL of the page with information about this registry key. If entered, this link appears on the Results page. This is a user created web page. It must be stored in: /bsc/Registration/registration/site When completing this field you must enter part of the path for the page not just the page name, such as: site/pagename.jsp
Severity	The severity of the failure if the key is not on the host. If you select Required and the registry key does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See Severity level on page 469 for more details.
Hive	The name of the hive to be searched. Supported hives are: • HKEY_CLASSES_ROOT • HKEY_CURRENT_USER • HKEY_LOCAL_MACHINE • HKEY_USERS • HKEY_CURRENT_CONFIG Scanning for registry keys in the HKEY_CURRENT_USER hive will not be successful because the user running Persistent Agent differs from the user logged on to the host.
Key Name	Name of the Registry Key that contains the value being located.
Value Name	The Value Name to be located.
Type	• REG_SZ • REG_DWORD You must enter the REG_DWORD setting as a decimal value, not hexadecimal.
Data	The data to be contained in the selected type.
Action	Select an action from the drop-down list: • **Match Value Exactly**—The ***Value Name*** is used as a path to find the specified ***Key Name*** in the tree. ***Data*** listed in the scan is compared to the data on the key. If the value and data in the key are exact matches to the specified entries, the scan passes. Otherwise, it fails. • **Search keys and values**—The ***Key Name*** is used as a starting point. The search is for whatever is contained in ***Data***. The data must be found in a key name, a Value name, or the data of all sub-keys of the key entered. • **Value contains Data**—The ***Value Name*** is used as a path to find the specified ***Key Name*** in the tree. ***Data*** listed in the scan is compared to the data in the

Scan Parameter	Description
	value. If the contents in the value contains the data, the scan passes. Otherwise, it fails. • **Key has a value**—The ***Value Name*** is used as a path to find the specified ***Key Name*** in the tree. If the key is found by using the name in the value and the data is not empty, the scan passes. Otherwise, it fails. • **Sets the value (Use Caution)**— When checked, this scan ALWAYS PASSES. The scan checks to see if the key exists in the registry key. If it does, the scan overwrites the key to have the specified data. If it does not exist, the scan creates the key and sets the data as specified. When the Type is **REG_DWORD**, the only actions available are **Match Value** and **Sets the value (Use Caution)**. **Example**: **Hive Name** HKEY_LOCAL_MACHINE **Key Name** SOFTWARE\Widgets\Setup **Value Name** Version **Data** 1.0
DWORD Comparison Operation	This field is enabled only when **Type** is set to REG_DWORD and **Action** is set to Match Value. The operator selected here is used in the comparison of the value in the **Data** field to the Data value in the registry. For example, if this field is set to = then both values must match exactly. If the operator is set to >= the Data value in the host registry must be greater than or equal to the Data value in the custom scan.
Prohibit	If the Registry Key is found and this is set to True, the host fails the scan for a prohibited product. Default = False.
Require for Windows...	Select the check box next to the version(s) of Windows OS for which this key is required. You must select the OS within the Custom Scan to apply the scan to hosts with the selected OS. If you do not select an OS in the Custom Scan and the host has that OS, the host automatically passes the general scan.

HotFixes scan settings

You can create a custom scan for a specific HotFix. Enter the information shown in the table below into the custom scan window after selecting the HotFix scan type.

As a best practice, add HotFix custom scans to a particular operating system within a general Scan. If you enable the HotFix custom scan at the Scan level, every host that is evaluated by the scan is also scanned for the HotFix. Since HotFixes are operating system specific you could inadvertently deny access to the network to many hosts.

Scan Parameter	Description
Label	Label in the Results page information identifying which scan the host failed.

Web Address	The URL of the page with information about this HotFix. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:
	`/bsc/Registration/registration/site`
	When completing this field you must enter part of the path for the page not just the page name, such as:
	`site/pagename.jsp`

Severity	The severity of the failure if the hotfix is not on the host. If you select Required and the hotfix does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See Severity level on page 469 for more details.
HotFix ID	The name of the HotFix, such as, KB123456.
Bypass Service Pack (>=)	Select the Bypass Service Pack check box to display a text field. Enter the numeric value for the Service Pack level in this field. The host must have the specified hotfix (HotFix ID above) OR a service pack level equal to or greater than the set value to pass the scan.
Require for Windows...	Select the check box next to the version(s) of Windows OS for which this key is required. You must select the OS within the Custom Scan to apply the scan to hosts with the selected OS. If you do not select an OS in the Custom Scan and the host has that OS, the host automatically passes the general scan.

Registry version scan settings

Create a custom scan to verify that a specific version of an application, such as Internet Explorer, is installed on the host. Enter the information shown in the table below into the custom scan window after selecting the Registry-Version scan type. When the scan runs, the registry is checked to see if the installed application has the required version.

Scan Parameter	Description
Label	This label appears in the Results page information to identify which scan the host failed.

Web Address	The URL of the page with information about this registry version. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:
	`/bsc/Registration/registration/site`
	When completing this field you must enter part of the path for the page not just the page name, such as:
	`site/pagename.jsp`

Scan Parameter	Description
Severity	The severity of the failure if the file is not on the host. If you select Required and the version of the application does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See Severity level on page 469 for more details.
Hive	The name of the Hive to be searched. Supported hives are: • HKEY_CLASSES_ROOT • HKEY_CURRENT_USER • HKEY_LOCAL_MACHINE • HKEY_USERS • HKEY_CURRENT_CONFIG
Key Name	Name of the Registry Key that contains the value being searched for.
Value Name	The Value Name that must be in the key entry.
Version	The Version that must be in the key entry.
Operation	Select an Operator for the version number: > = >=
Prohibit	If the Registry Key is found and this is set to True, the host fails the scan for a prohibited product. Default = False.
Version Delimiter	The character used to identify the delimiter.
Require for Windows...	Select the check box next to the version(s) of Windows OS for which this key is required. You must select the OS within the Custom Scan to apply the scan to hosts with the selected OS. If you do not select an OS in the Custom Scan and the host has that OS, the host automatically passes the general scan.

Processes scan settings

Create a custom scan for a specific process. Process names for various applications may differ between operating systems. Enter the process name for each OS if this is the case. Enter the process name(s) information into the custom scan window for Processes.

Scan Parameter	Description
Label	This label appears in the Results page information to identify which scan the host failed.
Web Address	The URL of the page with information regarding this process. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:

Scan Parameter	Description

	`/bsc/Registration/registration/site`
	When completing this field you must enter part of the path for the page not just the page name, such as: When completing this field you must enter part of the path for the page not just the page name, such as:
	`site/pagename.jsp`

Severity	The severity of the failure if the process is not running on the host. If you select Required and the process does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See Severity level on page 469 for more details.
Process Name for ...	Enter the name of the process that is required for the specific Operating System(s).

If you do not want to scan for a process on a particular Operating System, leave the corresponding field blank. When you click **Apply**FortiNAC fills each blank field with the word SYSTEM. This indicates that the corresponding Operating System should be passed for this scan.

Prohibited processes scan settings

Create a custom scan to prohibit a specific process on a host with selected Operating System(s). Process names for various applications may differ between operating systems. Enter the process name for each OS if this is the case. Enter the process name(s) information into the custom scan window for Prohibited-Processes.

Scan Parameter	Description
Label	This label appears in the Results page information to identify which scan the host failed.

Web Address	The URL of the page with information regarding this prohibited process. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:
	`/bsc/Registration/registration/site`
	When completing this field you must enter part of the path for the page not just the page name, such as:
	`site/pagename.jsp`

Severity	The severity of the failure if the prohibited process is running on the host. If you select Required and the process does exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See Severity level on page 469 for more details.
Process Name for ...	Enter the name of the process that is prohibited for the specific Operating System(s).

Domain verification scan settings

Create a custom scan to verify that a host has joined the appropriate domain when it connected to the network. Domain names may differ between operating systems. Enter a comma separated list of domain names for each OS. Attach this custom scan to any Policies that require domain verification. A host will pass this scan if it is joined with any domain contained in the list for the host's operating system.

Requires Agent Version 2.2.2 or higher. Using a lower version of the agent causes all hosts to pass the scan regardless of the domain returned.

Scan Parameter	Description
Label	This label appears in the Results page information to identify which scan the host failed.

Web Address	The URL of the page with information regarding domain verification. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:
	`/bsc/Registration/registration/site`
	When completing this field you must enter part of the path for the page not just the page name, such as:
	`site/pagename.jsp`

Severity	The severity of the failure if the host is not part of any of the domains specified. If you select Required and the host is not in the correct domain, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See Severity level on page 469 for more details.
Domain Names for ...	Enter a comma separated list of the NetBIOS domain names that are required or permitted for the specific Operating System(s).

Prohibited domain verification scan settings

Create a custom scan to verify the domain a host is attempting to join and prohibit access to the network based on that domain. Domain names may differ between operating systems. Enter a comma general scan to prevent access based on domain verification. A host will fail this scan if it is joined with any domain contained in the list for the host's operating system.

Requires Agent Version 2.2.2 or higher. Using a lower version of the agent causes all hosts to pass the scan regardless of the domain returned.

Scan Parameter	Description
Label	This label appears in the Results page information to identify which scan the host failed.

Web Address	The URL of the page with information regarding domain verification. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:
	`/bsc/Registration/registration/site`
	When completing this field you must enter part of the path for the page not just the page name, such as:
	`site/pagename.jsp`

Scan Parameter	Description
Severity	The severity of the failure if the host is part of any of the domains specified. If you select Required and the host is not in the correct domain, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See Severity level on page 469 for more details.
Domain Names for ...	Enter a comma separated list of the NetBIOS domain names that are prohibited for the specific Operating System(s).

Service scan settings

You can create a custom scan to check the status of a Windows Service. Enter the information shown in the table below into the custom scan window after selecting the Service scan type.

Scan Parameter	Description
Label	This label appears in the Results page information to identify which scan the host failed.
Severity	The severity of the failure if the service is not in the desired state on the host. If you select Required and the service is not in the desired state, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See Severity level on page 469 for more details.
Service Name	The name of the service on the Windows OS. To retrieve the service name, open the Microsoft Management Console Local Services view. See Find the service name on page 461 for information on how to locate the Service Name on your system.
Desired State	Select the the state of the service on the host to be scanned. Select Running to indicate the host must be running the service. Select Stopped to indicate the host must not be running the service.

Web Address	The URL of the page with information about this service. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:
	`/bsc/Registration/registration/site`
	When completing this field you must enter part of the path for the page not just the page name, such as:
	`site/pagename.jsp`

Find the service name

1. Open Microsoft Management Console on your system.
2. Navigate to the Local Services view.
3. Right-click the process you want to create the custom scan for, and click **Properties**.
4. Find the service name in the Properties view and enter it in the **Service Name** field of the custom scan.

macOS

The Custom Scans feature allows you to search host computers for very specific information. Custom Scans must be created separately for different operating systems. Within each operating system, there are different types of scans that can be created. Refer to Add A macOS Custom Scan below for a list of scan types and general instructions on adding scans. Refer to the instructions for each scan type for field level information. You can modify or remove the scans at any time. When a Custom Scan is modified it affects any existing general Scans that use that Custom Scan.

Add a custom scan

1. Click **Policy > Policy Configuration**.
2. In the menu on the left click the **+** sign next to **Endpoint Compliance** to open it.
3. Click the **Scans** option to select it.
4. At the bottom of the window click the **Custom Scans** button.
5. In the Custom Scans dialog, click **Add**.
6. Select **macOS** from the **Operating System** drop-down list.
7. Select the type of scan desired. Each scan type has a special set of fields that are specific to that type. Use the table below for settings.

Scan Type	Description
File	Test for the existence of a specific file on the host. See File scan settings on page 462.
Package	Test for a existence of a specific installer package on the host. An inclusive range of macOS Versions can be specified for this scan. See Package scan settings on page 463.
Processes	Test for the existence of a specific process. See Processes scan settings on page 464.
Prohibited-Processes	Test for the existence of a specific prohibited process. See Prohibited processes scan settings on page 464.

8. Enter the **Name** for the custom scan.
9. Enter the information for the custom scan.
10. Click **OK**.
11. The name of the custom scan will now appear in the **Custom Scans** section for each macOS scan and can be selected as part of the creation or modification of the general scan parameters.

File scan settings

To create a custom scan for a specific file, enter the information shown in the table below into the custom scan window after selecting the File scan type.

Scan Parameter	Description
Label	This label appears in the Results page information to identify which scan the host failed.

Scan Parameter	Description
Severity	The severity of the failure if the file is not on the host. If you select Required and the file does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See Severity level on page 469 for more details.
File Name	The name of the file being checked for on the host.
Starting Path	The search for the file starts with the directory indicated here and includes all sub-directories and files. **Important:** Use the forward slash (/) to delimit directory names. Do NOT use a colon (:).

Web Address	The URL of the page with information regarding this file. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:
	`/bsc/Registration/registration/site`
	When completing this field you must enter part of the path for the page not just the page name, such as:
	`site/pagename.jsp`

Prohibit this product	If the file is found and this is set to true, the host fails the scan for a prohibited product. Default = false.

Package scan settings

To create a custom scan for a specific installer package, enter the information shown in the table below into the custom scan window after selecting the Package scan type.

Use this custom scan to check whether particular updates or patches have been applied to the host.

If the package name is installed on a host with an OS version outside the range, the host will pass the scan.

Scan Parameter	Description
Label	This label appears in the Results page information to identify which scan the host failed.
Severity	The severity of the failure if the package is not on the host. If you select Required and the package does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See Severity level on page 469 for more details.
Package Name	name.pkg The name of the installer package being searched for on the host. The custom scan searches the /Library/Receipts directory for install receipts.

Scan Parameter	Description
Minimum macOS Version	The inclusive minimum version of the macOS software.
Maximum macOS Version	The inclusive maximum version of the macOS software.

Web Address	The URL of the page with information regarding this installer package. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:
	`/bsc/Registration/registration/site`
	When completing this field you must enter part of the path for the page not just the page name, such as:
	`site/pagename.jsp`

Processes scan settings

To create a custom scan for a specific process, enter the information shown in the table below into the custom scan window after selecting the Processes scan type.

Scan Parameter	Description
Label	This label appears in the Results page information to identify which scan the host failed.

Web Address	The URL of the page with information regarding this process. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:
	`/bsc/Registration/registration/site`
	When completing this field you must enter part of the path for the page not just the page name, such as:
	`site/pagename.jsp`

Severity	The severity of the failure if the process is not running on the host. If you select Required and the process does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See Severity level on page 469 for more details.
Process Name	The name of the process being scanned for on the host. This name is seen when you use ps at the command line. This is not necessarily the name in the Activity Monitor list. For example, iChat, iChatAgent, iTunes, iTunesHelper.

Prohibited processes scan settings

To create a custom scan for a specific prohibited process, enter the information shown in the table below into the custom scan window after selecting the Prohibited Processes scan type.

Scan Parameter	Description
Label	This label appears in the Results page information to identify which scan the host failed.

Scan Parameter	Description

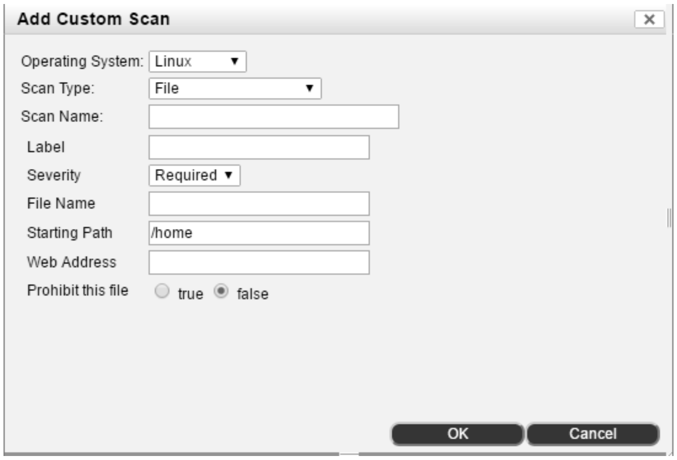
Web Address	The URL of the page with information regarding this prohibited process. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:
	`/bsc/Registration/registration/site`
	When completing this field you must enter part of the path for the page not just the page name, such as:
	`site/pagename.jsp`

Severity	The severity of the failure if the prohibited process is running on the host. If you select Required and the prohibited process does exist, the host fails the custom scan. If you select Warning, the host pass the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See Severity level on page 469 for more details.
Process Name	Name of the prohibited process being scanned for on the host.

Linux

The Custom Scans feature allows you to search host computers for very specific information. Custom Scans must be created separately for different operating systems. Within each operating system, there are different types of scans that can be created. Refer to Add A Linux Scan below for a list of scan types and general instructions on adding scans. Refer to the instructions for each scan type for field level information. You can modify or remove the scans at any time. When a Custom Scan is modified it affects any existing general Scans that use that Custom Scan.

Add a custom scan



Add Custom Scan

Operating System: Linux

Scan Type: File

Scan Name:

Label

Severity Required

File Name

Starting Path /home

Web Address

Prohibit this file ○ true ● false

1. Click **Policy > Policy Configuration**.
2. In the menu on the left click the **+** sign next to **Endpoint Compliance** to open it.
3. Click the **Scans** option to select it.
4. At the bottom of the window, click the **Custom Scans** button.
5. In the Custom Scans dialog, click **Add**.
6. Select **Linux** from the **Operating System** drop-down list.

7. Select the type of scan desired. Each scan type has a special set of fields that are specific to that type. Use the table below for settings.

Scan Type	Description
File	Test for the existence of a specific file on the host. See File scan settings on page 466.
Package	Test for a existence of a specific rpm/deb packages on the host. See Package scan settings on page 467.
Processes	Test for the existence of a specific process. See Processes scan settings on page 467.
Prohibited-Processes	Test for the existence of a specific prohibited process. See Prohibited processes scan settings on page 468.
Script	Allows users to upload a script toFortiNAC to be executed on the host. See Script settings on page 468.

8. Enter the **Name** for the custom scan.
9. Enter the information for the custom scan.
10. Click **OK**.

The name of the Custom Scan will now appear in the Custom Scans section for each Linux scan and can be selected as part of the creation or modification of the general scan parameters.

File scan settings

To create a custom scan for a specific file, enter the information shown in the table below into the custom scan window after selecting the File scan type.

Scan Parameter	Description
Label	This label appears in the Results page information to identify which scan the host failed.
Severity	The severity of the failure if the file is not on the host. If you select Required and the file does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See Severity level on page 469 for more details.
File Name	The name of the file being checked for on the host.
Starting Path	The search for the file starts with the directory indicated here and includes all sub-directories and files. **Important:** Use the forward slash (/) to delimit directory names. Do NOT use a colon (:).
Web Address	The URL of the page with information regarding this file. If entered, this link appears on the Results page. This is a user created web page. It must be stored in: `/bsc/Registration/registration/site`

Scan Parameter	Description
	When completing this field you must enter part of the path for the page not just the page name, such as: `site/pagename.jsp`
Prohibit this product	If the file is found and this is set to true, the host fails the scan for a prohibited product. Default = false.

Package scan settings

To create a custom scan for a specific rpm or deb package, enter the information shown in the table below into the custom scan window after selecting the Package scan type.

Use this custom scan to check whether particular updates or patches have been applied to the host.

Scan Parameter	Description
Label	This label appears in the Results page information to identify which scan the host failed.
Severity	The severity of the failure if the package is not on the host. If you select Required and the package does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See Severity level on page 469 for more details.
Package Name	The name of the rpm or deb package being searched for on the host. The custom scan runs rpm or dpkg commands to search for installed packages.
Version	The inclusive minimum version of the Linux software.

Web Address	The URL of the page with information regarding this rpm or deb package. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:
	`/bsc/Registration/registration/site`
	When completing this field you must enter part of the path for the page not just the page name, such as:
	`site/pagename.jsp`

Processes scan settings

To create a custom scan for a specific process, enter the information shown in the table below into the custom scan window after selecting the Processes scan type.

Scan Parameter	Description
Label	This label appears in the Results page information to identify which scan the host failed.
Web Address	The URL of the page with information regarding this process. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:

Scan Parameter	Description

	`/bsc/Registration/registration/site`
	When completing this field you must enter part of the path for the page not just the page name, such as:
	`site/pagename.jsp`

Severity	The severity of the failure if the process is not running on the host. If you select Required and the process does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See Severity level on page 469 for more details.
Process Name	The name of the process being scanned for on the host. This name is seen when you use ps at the command line.

Prohibited processes scan settings

To create a custom scan for a specific prohibited process, enter the information shown in the table below into the custom scan window after selecting the Prohibited Processes scan type.

Scan Parameter	Description
Label	This label appears in the Results page information to identify which scan the host failed.

Web Address	The URL of the page with information regarding this prohibited process. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:
	`/bsc/Registration/registration/site`
	When completing this field you must enter part of the path for the page not just the page name, such as:
	`site/pagename.jsp`

Severity	The severity of the failure if the prohibited process is running on the host. If you select Required and the prohibited process does exist, the host fails the custom scan. If you select Warning, the host pass the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See Severity level on page 469 for more details.
Process Name	Name of the prohibited process being scanned for on the host.

Script settings

To create a custom scan for a specific script, enter the information shown in the table below into the custom scan window after selecting the Script scan type.

Scan Parameter	Description
Label	This label appears in the Results page information to identify which scan the host failed.

Scan Parameter	Description
Upload Script	Users can select a script to upload to FortiNAC. The name of the uploaded script appears in the text field.
Return Value	The value that the script must return after the agent executes the script.

Web Address	The URL of the page with information regarding this prohibited process. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:
	`/bsc/Registration/registration/site`
	When completing this field you must enter part of the path for the page not just the page name, such as:
	`site/pagename.jsp`

Severity level

You can configure custom scans with a Severity Level setting. The Severity Level controls whether a host loses access to the network or only receives a warning when it is not in compliance with the scan. When the host fails a custom scan with a severity level set to warning, the experience varies, depending on the type of security agent that is being used.

Setting severity level to required

When a custom scan severity level is set to Required, if the host fails the scan, the host is set to At Risk. The browser is redirected to a web page that contains details about the requirements the host failed. The host self-remediates (corrects the issues causing the failure) and rescans until it meets all requirements. When the host passes the requirements, it is moved to the production network.

The Scan Results section of the Health Tab on the Host Properties window shows a Failed or Passed result. See Host health and scanning on page 803.

Setting severity level to warning

When the host fails a custom scan with a severity level set to Warning, the experience will vary depending on the type of security agent that is being used.

Dissolvable Agent

When a host fails the scan, the browser is redirected to a web page that contains details about the requirements the host failed. The web page is divided into two sections. One section contains required severity level items the host failed; the other contains warning severity level items the host failed.

If the host failed only warning severity level items, a **Register Now** button is available on the web page. The user clicks the button and is moved to the Success web page.

If the host failed required and warning severity level items, the host must self-remediate until all items in the Required section are corrected. When only Warning level items are listed in the Warning section of the web page, the **Register Now** button becomes available. The user clicks the button and is moved to the Success web page. The host is not fully compliant with the Endpoint Compliance Policy, but is allowed on the production network.

Persistent Agent

If the host fails the scan for only items with the severity level set to warning, a **Warning** message is sent to the host and the host is moved to the production network.

If the host fails items with severity levels set to Required and Warning, the host is moved to the remediation network. The browser is redirected to a web page containing details about the requirements the host failed. The web page is divided into two sections. One section contains Required severity level items the host failed; the other contains Warning severity level items the host failed.

The host must self-remediate until all items in the Required section are corrected. When the only items listed are in the section containing the failures for severity level set to Warning, the user receives a warning message that his computer is not fully compliant with the Endpoint Compliance Policy. The host is then allowed on the production network.

Configure the Warning message in **System > Settings > Persistent Agent > Security Management**. See Security management on page 140.

The **Scan Results** section of the **Health Tab** on the **Host Properties** window shows a warning result. See Host health and scanning on page 803.

Use case

The company network rules prohibit registered hosts on the network from having LimeWire installed on the host. Hosts are required to have a Persistent Agent and are scanned daily to maintain compliance. If LimeWire is installed, the host will receive three warnings before being removed from the network.

To set up a custom scan to enforce this rule:

1. Create a custom scan for Registry Key, enter the details for LimeWire, set Prohibit to True, and set the Severity level to Warning. See Add a custom scan on page 450 or Add a custom scan on page 462.
2. Create a regular Scan and enable the custom scan within that scan. See Add or modify a scan on page 433.
3. Schedule the regular Scan to be rerun daily. See Schedule a scan on page 441.
4. Create an Endpoint Compliance Policy that contains the regular Scan. See Endpoint compliance policies on page 415.
5. Map the Security Risk Host event to an alarm that will take action on the third occurrence of the event, and set the host At Risk and Send a message. See Add or modify alarm mapping on page 892.
6. Configure the Security Management Properties Warning message block. See Security management on page 140.
7. Configure the web page that the host will be redirected to when moved to Remediation. The web page used is created outside the program. In order to keep this page from being overwritten during an upgrade, it should be stored in /bsc/Registration/registration/site . Then, return to your custom scan and modify it to contain the new web address.

   If the host fails the scan, the first two times, the Warning message is sent. On the third failure, the host is sent the Warning message, is marked At Risk, and moved to Remediation. The web page informs the user about the failure to meet policy requirements. The host self-remediates and rescans. When the host passes the policy, the host is moved back to the production network.

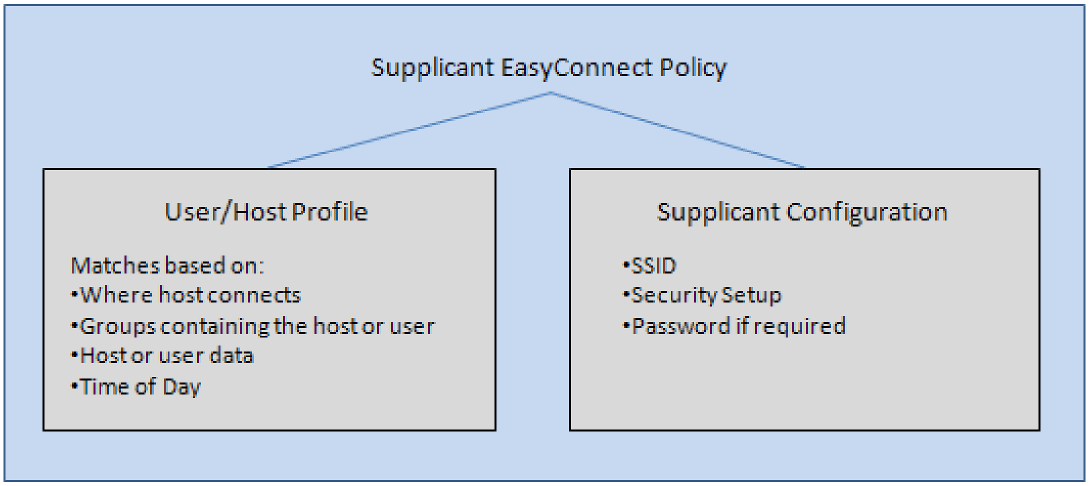
Supplicant EasyConnect policies

Supplicant EasyConnect policies are used to help your network users connect to the network quickly in a wireless environment. Supplicant policies contain a Supplicant Configuration and a User/Host Profile. When a host needs a supplicant, FortiNAC compares the user and host data to the User/Host Profile in each Supplicant Policy starting with the first policy in the list. When a match is found, the Supplicant Policy is applied to the connecting host and the Supplicant Configuration is used to setup the supplicant on the host.

There may be more than one Supplicant Policy that is a match for this host/user, however, the first match found is the one that is used.

If you create a User/Host Profile with fields Where (Location) set to Any, Who/What by Group set to Any, Who/What by Attribute left blank and When set to always, it matches ALL users and hosts. This is essentially a Catch All profile. If this User/Host Profile is used in a policy, all policies below that policy are ignored when assigning a policy to a user or a host. To highlight this, policies below the policy with the catch all profile are grayed out and have a line through the data.

The best way to use a Catch All profile is to create a general policy with that profile and place it last in the list of policies.



Supplicant Policies are applied to the host using an agent, except in the case of iOS devices where the user is prompted to download the configuration from the Captive Portal. The Dissolvable Agent or the Persistent Agent is used for Windows and macOS hosts and the Mobile Agent is used for Android devices.

The host connection location does not determine the Supplicant Configuration applied unless the location is part of the User/Host Profile. Therefore, a host could connect on an SSID, and actually be configured for a different SSID because the User/Host Profile matched a Supplicant Policy with a higher rank that contained the configuration for a different SSID.

Host configuration process

The host Supplicant Configuration setup process is as follows:

1. Host connects to the network.
2. Host connects to an Open SSID based on the operating system of the host. If authenticating through LDAP, the user must be in the selected Directory Group configured in the SSID Mapping for this SSID. The SSID Mapping has been configured with a Supplicant Configuration.
3. If the user is on a Windows or macOS device, the user downloads either the Persistent Agent or the Dissolvable Agent. The agent applies the Supplicant Configuration after scanning and registering the host.
4. If the user is on an Android device, the user downloads and runs the Mobile Agent. The agent applies the Supplicant Configuration after scanning and registering the host. See Mobile Agent on page 520 for download requirements.
5. FortiNAC compares user and host data to Supplicant Policies and finds the first match starting from the top of the list of policies.
6. The user registers or authenticates.
7. The Supplicant Configuration is applied.
8. The Agent attempts to move the host to the SSID that was just configured.

FortiNAC supports the configuration of encrypted networks as follows:

- Open
- WEP (PSK)
- WPA (PSK)
- WPA2 (PSK)
- WEP Enterprise
- WPA Enterprise(PEAP)
- WPA2 Enterprise(PEAP)

WPA Enterprise and WPA2 Enterprise are limited to PEAP-MSCHAPv2.

Requirements

To use Supplicant EasyConnect Policies to configure the supplicant on hosts that connect to your wireless network, the following requirements must be met:

- If your RADIUS Server is configured with a certificate it must be a trusted third-party certificate from a Certificate Authority such as Verisign or Thawte. If you have used a self-signed certificate it must be distributed to all hosts or you must replace it with a trusted third-party certificate. FortiNAC will not be able to configure the supplicant unless these certificates are correct.
- You must have at least one Isolation VLAN, such as Registration or Remediation. If you do not, use the Configuration Wizard to configure an Isolation context. See the *Appliance Installation Guide* for instructions on running the Configuration Wizard.
- Supplicant Easy Connect Policies are only supported on the following operating systems:

  Having the required Windows Service Packs installed ensures that the host is transitioned to the secure SSID without having to close the browser and reopen:

  - Windows 7 Service Pack 1 and higher
  - Windows 8, 8.1, 10 and higher

Windows 10 hosts using Random Hardware Address functionality may experience unpredictable and undesired results with the Supplicant Easy Connect feature.

  - macOS 10.7 and higher
  - Android 2.3.3 or higher
  - iOS 4.0 or higher
- Supplicant EasyConnect Configurations can only be applied as follows:
  - For Windows and macOS hosts you must use the Dissolvable Agent Version 3.0.2.8 or higher or the Persistent Agent Version 3.1 or higher.
  - For Android devices you must use the Mobile Agent contained in Agent package Version 3.0.x or higher.

Mobile Agent requires the use of a Certificate from a Certificate Authority. A Self-Signed Certificate cannot be used. See SSL certificates on page 523

iOS and macOS users need to select the secure SSID because they will not be switched to that SSID automatically after applying the Supplicant Configuration.

- Supplicant Configurations are applied to the host using an agent, except in the case of iOS devices where the user is prompted to download the configuration from the Captive Portal. The Dissolvable Agent or Persistent Agent are used for Windows and macOS hosts and the Mobile Agent is used for Android devices.
- Supplicant Configurations for Windows hosts connecting on an SSID that uses WEP Enterprise, WPA Enterprise, WPA2 Enterprise for security require that you upload the CA or Root Certificate for the valid SSL Certificate used to secure the RADIUS server. FortiNAC parses the CA Certificate in order to read the CA fingerprint. This allows the Supplicant Configuration to be applied correctly and to switch the Windows host from the Open SSID to the Secure SSID. CA or Root Certificates can be downloaded from the Certificate Authority that issued your SSL Certificate. See Add or modify a configuration on page 478 and Open SSID for device onboarding on page 996.
- If you would like to modify the text displayed to Apple iOS users in the captive portal, go to the Portal Content Editor and modify Profile Configuration Download under the appropriate Isolation context, such as Registration or Remediation. See Portal content editor on page 250.
- Configure Isolation VLANs on the Model configuration for the wireless devices being used or the individual SSIDs being used. See Model configuration on page 767 or SSID configuration on page 788.
- Create an Endpoint Compliance Policy that uses the Dissolvable Agent or the Persistent Agent for Windows and macOS hosts and the Mobile Agent hosts. The User/Host Profile created for this Endpoint Compliance Policy must have information in it that will match a connecting host that needs to have a supplicant configured. For example, the User/Host profile could have a group of wireless devices as the connection location and Host operating system in the Who/What by Attribute field. See Endpoint compliance policies on page 415 and Agent packages on page 226.

It is recommended that you modify the associated scan to require Service Pack 3 for Windows XP and Service Pack 1 and higher for Windows 7. Having these Service Packs installed ensures that the host is transitioned to the secure SSID without having to close the browser and reopen.

In some cases, when the Supplicant Configuration is applied using the Persistent Agent, the host cannot be transitioned to the secure SSID automatically. The user must connect to the SSID manually.

- Create at least one User/Host Profile that has criteria that matches the hosts who will need a Supplicant, such as Operating System or connection location. See User/host profiles on page 389.
- Create at least one Supplicant Configuration with the setup parameters for the SSID that hosts will use. See Supplicant configurations on page 476.
- Create at least one Supplicant EasyConnect Policy that maps the Supplicant Configuration to a User/Host Profile. See Supplicant EasyConnect policies on page 471.

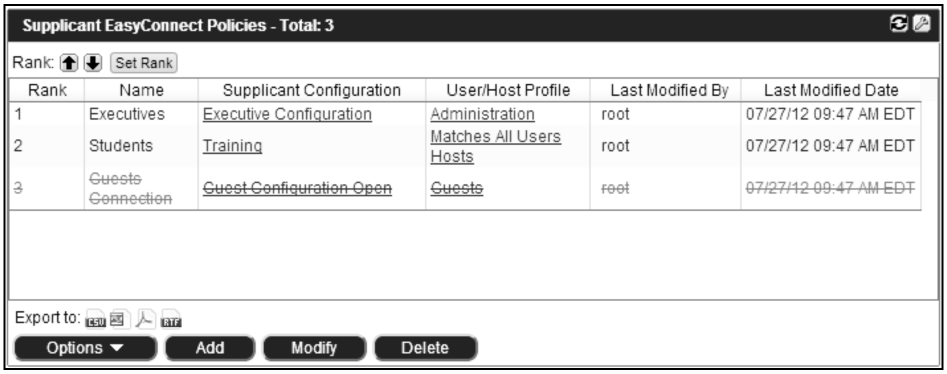
Manage policies

Add, modify or delete Supplicant EasyConnect Policies used to configure Supplicants on connecting hosts. See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.

If the user/host does not match any policy, no Supplicant Configuration is provided.

If you create a User/Host Profile with fields Where (Location) set to Any, Who/What by Group set to Any, Who/What by Attribute left blank and When set to always, it matches ALL users and hosts. This is essentially a Catch All profile. If this User/Host Profile is used in a policy, all policies below that policy are ignored when assigning a policy to a user or a host. To highlight this, policies below the policy with the catch all profile are grayed out and have a line through the data.

The best way to use a Catch All profile is to create a general policy with that profile and place it last in the list of policies.



Supplicant EasyConnect Policies - Total: 3

Rank	Name	Supplicant Configuration	User/Host Profile	Last Modified By	Last Modified Date
1	Executives	Executive Configuration	Administration	root	07/27/12 09:47 AM EDT
2	Students	Training	Matches All Users Hosts	root	07/27/12 09:47 AM EDT
~~3~~	~~Guests Connection~~	~~Guest Configuration Open~~	~~Guests~~	~~root~~	~~07/27/12 09:47 AM EDT~~

Settings

An empty field in a column indicates that the option has not been set.

Field	Definition
Rank Buttons	Moves the selected policy up or down in the list. Host connections are compared to Policies in order by rank.
Set Rank Button	Allows you to type a different rank number for a selected policy and immediately move the policy to that position. In an environment with a large number of policies this process is faster than using the up and down Rank buttons.
Table columns	
Rank	Policy's rank in the list of policies. Rank controls the order in which host connections are compared to Policies.
Name	User defined name for the policy.
Supplicant Configuration	Contains the configuration for the SSID, Security Settings and password if required. See Supplicant configurations on page 476.
User/Host Profile	Contains the required criteria for a connecting host, such as connection location, host or user group membership, host or user attributes or time of day. Host connections that match the criteria within the User/Host Profile are assigned the associated Supplicant Configuration. See User/host profiles on page 389.
Where (Location)	The connection location specified in the User/Host Profile. The host must connect to the network on a device, port or SSID contained within one of the groups shown here to be a match. When set to Any, this field is a match for all hosts or users.
Who/What by Group	User or Host group or groups specified in the User/Host Profile. These groups must contain the connecting user or host for the connection to be a match for this policy. When set to Any, this field is a match for all hosts or users.
Who/What by Attribute	User or Host attributes specified in the selected User/Host Profile. The connecting host or user must have the attributes to be a match. See Filter example on page 393.
When	The time frame specified in the selected User/Host Profile. The host must connect to the network within this time frame to be a match. When set to Always this field is a match for all hosts or users.
Note	User specified note field. This field may contain notes regarding the data conversion from a previous version of FortiNAC.
Last Modified By	User name of the last user to modify the policy.
Last Modified Date	Date and time of the last modification to this policy.
Right click options	
Delete	Deletes the selected Supplicant EasyConnect Policy.
Modify	Opens the Modify Supplicant EasyConnect Policy window for the selected policy.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847.

Field	Definition
	You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.
Buttons	
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.

Add or modify a policy

1. Select **Policy > Policy Configuration**.
2. In the menu on the left select **Supplicant EasyConnect**.
3. Click the **Add** button or select an existing policy and click **Modify**.
4. Click in the **Name** field and enter a name for this policy.
5. Select a **User/Host Profile** from the drop-down menu. You can use the icons next to the User/Host Profile field to add a new profile or modify the profile shown in the drop-down menu. Note that if you modify this profile, it is modified for all features that make use of the profile. Connecting hosts must match this User/Host Profile to be assigned the Supplicant Configuration specified in the next step.
6. Select a **Supplicant Configuration** from the drop-down menu. You can use the icons next to the Supplicant Configuration field to add a new configuration or modify the configuration shown in the drop-down menu. Note that if you modify this configuration, it is modified for all features that make use of it. See Add or modify a configuration on page 478.
7. The **Note** field is optional.
8. Click **OK** to save your policy.

Delete a policy

1. Click **Policy > Policy Configuration**.
2. In the menu on the left select **Supplicant EasyConnect**.
3. Select the policy to be removed.
4. Click **Delete**.
5. Click **OK** to confirm that you wish to remove the policy.

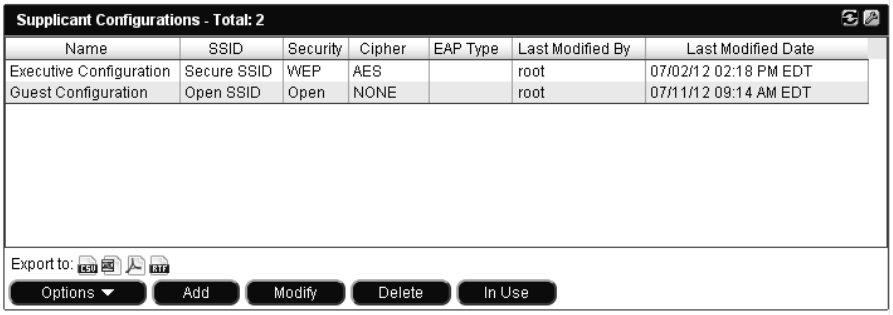
Supplicant configurations

Supplicant Configurations define an SSID and security parameters required to configure the native supplicant available on a connecting host as part of its operating system. The Supplicant Configuration that is used for a particular host is determined by the pairing of a Supplicant Configuration and a User/Host Profile within a Supplicant Policy.

When a host connects to the network and requires the use of a supplicant, the host and user data are compared to each Supplicant Policy starting with the first policy in the list. When a policy is found where the host and user data match the

User/Host Profile in the policy, that policy is applied. The Supplicant Configuration contained within that policy configures the supplicant on the host.

See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.



Supplicant Configurations - Total: 2

Name	SSID	Security	Cipher	EAP Type	Last Modified By	Last Modified Date
Executive Configuration	Secure SSID	WEP	AES		root	07/02/12 02:18 PM EDT
Guest Configuration	Open SSID	Open	NONE		root	07/11/12 09:14 AM EDT

Settings

An empty field in a column indicates that the option has not been set.

Field	Definition
Name	User defined name for the Configuration.
SSID	Name of the SSID being configured. This is not necessarily the SSID to which the host is connected. However, the agent will attempt to move the host to this SSID when the configuration is applied. A host can have Supplicant Configurations stored for multiple SSIDs.
Security	Indicates the type of encryption that will be used for connections to this SSID. Options include: • Open • WEP (PSK) • WPA (PSK) • WPA2 (PSK) • WEP Enterprise (PEAP) • WPA Enterprise (PEAP) • WPA2 Enterprise (PEAP) WPA Enterprise and WPA2 Enterprise are limited to PEAP-MSCHAPv2.
Cipher	Encryption/decryption method used in conjunction with the information in the Security field to secure this connection. Options include: • AES • NONE • TKIP

Field	Definition
EAP Type	Currently only PEAP is supported.
Note	User specified note field. This field may contain notes regarding the conversion from a previous version of FortiNAC.
Last Modified By	User name of the last user to modify the record.
Last Modified Date	Date and time of the last modification to this configuration.
Right click options	
Delete	Deletes the selected Supplicant Configuration.
In Use	Indicates whether or not the selected configuration is currently being used by any other FortiNAC element. See Configurations in use on page 480.
Modify	Opens the Modify Supplicant Configuration window for the selected configuration.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.
Buttons	
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.

Add or modify a configuration

1. Select **Policy > Policy Configuration**.
2. In the menu on the left click the **+** sign next to **Supplicant EasyConnect**.
3. From the menu on the left select **Configuration**.
4. On the **Supplicant Configurations** window, click the **Add** button or select an existing configuration and click **Modify**.
5. Click in the **Name** field and enter a name for this configuration.
6. In the **Security** field, select a type from the drop-down list. Options include: Open, WEP, WPA, WPA2, WEP Enterprise, WPA Enterprise, WPA2 Enterprise.
7. Click in the **Password** field to open the Password pop-up. This is the Pre-Shared Key. Enter the key twice to confirm that it is correct and click **OK**. The Password field does not display if Open, WPA2 Enterprise or WPA Enterprise is selected in the Security field.
8. Click in the **Cipher** field and select AES, NONE or TKIP.
9. In the **EAP Type** field, PEAP is the only option. EAP type does not display when Open, WEP or WPA is selected in the Security field.
10. The **Validate Server Certificate** field applies only to Windows 7 and higher hosts.

- If disabled, it disables the Validate Server Certificate setting on the host and any certificate will be accepted.
- If enabled, the host validates the Certificate with the list of Trusted Root Certificate Authorities listed in the host's Certificate Manager. If the Certificate Authority is not listed on the host, the user may have to connect to the secure SSID manually.

11. If you have enabled WEP Enterprise, WPA Enterprise or WPA2 Enterprise the **CA Certificate** field is displayed. Browse to the CA or Root Certificate from the certificate authority that issued the SSL Certificate used on your RADIUS server. Select the file and click Open.
12. The **CA Fingerprint** field is displayed and automatically populated after a CA or Root Certificate is uploaded and the Supplicant Configuration is saved.
13. The **Note** field is optional.
14. Click **OK** to save the configuration.

Settings

Field	Definition
Name	User defined name for the Configuration.
SSID	Name of the SSID being configured. This is not necessarily the SSID to which the host is connected. However, the agent will attempt to move the host to this SSID when the configuration is applied. A host can have Supplicant Configurations stored for multiple SSIDs.
Security	Indicates the type of encryption that will be used for connections to this SSID. Options include: • Open • WEP (PSK) • WPA (PSK) • WPA2 (PSK) • WEP Enterprise (PEAP) • WPA Enterprise (PEAP) • WPA2 Enterprise (PEAP) WPA Enterprise and WPA2 Enterprise are limited to PEAP-MSCHAPv2.

Field	Definition
Password	Opens the Password pop-up. This is the Pre-Shared Key. Enter the key twice to confirm that it is correct and click **OK**. The Password field does not display if Open, WPA2 Enterprise or WPA Enterprise is selected in the Security field. The XML predefined characters **' " < > &** are not supported.
Cipher	Encryption/decryption method used in conjunction with the information in the Security field to secure this connection. Options include: - AES - NONE - TKIP
EAP Type	Currently only PEAP is supported.
Validate Server Certificate	Applies only to Windows 7 and higher hosts. Default = Disabled. If disabled, it disables the Validate Server Certificate setting on the host and any certificate will be accepted. If enabled, the host validates the Certificate with the list of Trusted Root Certificate Authorities listed in the host's Certificate Manager. If the Certificate Authority is not listed on the host, the user may have to connect to the secure SSID manually.
CA Fingerprint	Fingerprint parsed from the CA or Root Certificate from the certificate authority that issued the SSL Certificate used to secure the RADIUS server. This field does not display until after the certificate has been uploaded and the Supplicant Configuration has been saved.
CA Certificate	This field is only displayed if you select WEP Enterprise, WPA Enterprise or WPA2 Enterprise in the Security field. Use the **Choose File** button to browse to and select the CA or Root certificate from the certificate authority that issued the SSL Certificate used to secure the RADIUS server. CA or Root certificates can be downloaded from the certificate authority web site. Either PEM or binary format can be used.
Note	User specified note field. This field may contain notes regarding the conversion from a previous version of FortiNAC.

Configurations in use

To find the list of FortiNAC features that reference a specific Supplicant Configuration, select the Configuration from the Supplicant Configurations View and click the In Use button. A message is displayed indicating whether or not the Configuration is associated with any other features. If the Configuration is referenced elsewhere, a list of each feature that references the Configuration is displayed.

Delete a configuration

If a configuration is in use by another feature in FortiNAC, it cannot be deleted. A dialog displays with a list of the features in which the configuration is used. Remove the association between the configuration and other features before deleting the configuration.

1. Click **Policy > Policy Configuration**.
2. In the menu on the left select **Supplicant EasyConnect**.
3. Click on the **+** sign next to **Supplicant EasyConnect** to open it.
4. Select **Configuration** from the menu on the left.
5. Select the configuration to be removed.
6. Click **Delete**.
7. Click **OK** to confirm that you wish to remove the configuration.

Remediation configurations

Use the Remediation Configuration to set up the Admin Scan Configurations used for options such as denying access to guests or other users by time of day or day of week.

To manage scans, you can add, modify, and remove scan scripts and profiles. You may also view performance statistics for the scan scripts and profiles. Schedule scans from the Modify Scan dialog box.

Add a scan

1. Click **Policy > Remediation Configuration**.
2. Click **Add**.
3. Use the settings in the table below to enter the parameters for the script or profile you are adding.
4. Click **Apply**.

Settings

Field	Definition
Type	The type of scan you are adding: • **System** - These scans runs scripts on the FortiNAC platform. • **Admin** - These scans indicate the reason why a host was manually marked at risk. They are not actually scanning the host but provide a configuration or profile with which to associate the host state. Admin Scans are also used to mark hosts At Risk or Safe based on an alarm action triggered by an event.
Script/Profile	**System scripts** • **ForceCSARescan** - Forces the Target Group of hosts using the Dissolvable agent to be rescanned by setting the hosts in the group to At-Risk. • **ForcePersistentAgent** - Forces the Target Group of hosts using the Persistent

Field	Definition
	agent to be rescanned by setting the hosts in the group to At-Risk. • **PassAllClients** - Sets the Target Group of hosts to Safe. • **FailAllClients** - Sets the Target Group of hosts to AtRisk. **Admin scans** Enter a name for the scan. This scan is initiated on the Host Properties under the Health tab.
Label	Displayed on the failure page when a network user's PC has failed a scan. If no label is provided, the scan name is used. The label or scan name is a link that takes the user to a page indicating why the PC has failed the scan.
Max Scan Execution Time (sec)	The maximum length of time FortiNAC will wait for the scan to return a status of passed or failed. If the elapsed time is greater than this value, a script failed error is generated and the host returns to the queue of hosts waiting to be scanned.
Status	Enable or Disable the scan. This setting can be modified to allow the scan to run or to stop it from running.
Target	The sub-set of FortiNAC hosts that will be scanned. • All Hosts • All Hosts & Servers • All Registered • All Rogues • All Servers • All VPN Clients • Group: See below. • Security and Access Attribute Value. See below.
Group	Specify the FortiNAC host group to be scanned. This option is only available if you select Group as the Target.
Security and Access Attribute Value	Used to determine which scan is to be applied to hosts connecting to the network whose associated user has this value set in the Active Directory Security and Access attribute. The host inherits this value from the user. This option is only available if you select Directory Attribute as the Target.
Patch URL	The location of the URL containing instructions for users whose hosts fail the scan. This must be a local URL.
Patch Information	If a host has failed a scan, the user must remedy the issue and rescan. Use this second field to provide the user with a brief set of instructions. For this field to be displayed to the user, you must use the portal pages distributed with FortiNAC and the Use Portal Version 1 check box on the Portal Configuration window must be disabled.

View scan status

1. Click **Policy > Remediation Configuration**.
2. Click the radio button next to a script/profile.
3. Click **View**. The **Scan Status** window is displayed.

Settings

Field	Definition
Script/Profile	Name of the scan.
Type	The type of scan.
Target	Sub-set of FortiNAC hosts that are being scanned by this script or profile.
Execution Time (sec)	Maximum length of time FortiNAC waits for the scan to return a status of passed or failed. If the elapsed time is greater than this value, a script failed error is generated and the host returns to the queue of hosts waiting to be scanned.
Servers Failed	Total number of servers that failed the scan.
Hosts Failed	Total number of hosts that failed the scan.
Elements Scanned	Number of elements scanned.
Queue Count	Number of elements waiting to be scanned.
Status	Whether the scan is Enabled or Disabled.

Click the **Details** button for additional information.

The Scan Details window displays the overall details of the scan and the specific host results for the scan.

Details settings

Field	Definitions
Script/Profile	Name of the scan.
Elements Scanned	Number of elements scanned.
Execution Time (sec)	Maximum length of time FortiNAC will wait for the scan to return a status of passed or failed. If the elapsed time is greater than this value, a script failed error is generated and the host returns to the queue of hosts waiting to be scanned.
Average Execution Time	Average length of time the scan was run against an individual host in the group being scanned.
Filter Status	Filter setting for script performance results: • **All** - All scanned hosts results • **Safe** - Only scanned hosts that are safe • **At Risk** - Only scanned hosts that are at risk • **Script Failed** - Only hosts that failed the scan
Start Record	Number of the first record to be displayed in the range of records selected.

Field	Definitions
End Record	Number of the last record to be displayed in the range of records selected.
Clear List of Scanned Hosts	Clears the list of hosts that have been scanned against this scan profile. Click **Now** to clear the list immediately. Click **Schedule** to schedule when to clear the list.
Hosts Details	Specific information on each scanned host. • **Name** - MAC Address or name of host • **IP address** - IP address of host • **Server** - Server that performed the scan • **Execution Time (sec)** - The length of time in seconds that it took to run the scan against the host • **Status** - Safe, At Risk, or Script Failed

Click the icon next to a host name to view the Host Properties. The Health Tab provides details regarding the Scan Report for the host so you can rescan the host immediately if you want. See Properties on page 801 for more information.

Clear scanned hosts list

Under Remediation Configuration - Modify or View you have the option to clear the list of Scanned Hosts. This forces the hosts in the results list to be rescanned. You may clear the list immediately or schedule the list to be cleared at specific intervals. On the Modify Scan view:

- Click **Now** to clear the list immediately.
- Click **Schedule** to set the interval that the list will be cleared.

1. Click **Policy > Remediation Configuration**.
2. Click the radio button next to a scan to select it.
3. Click **Modify**.
4. Click **Schedule**.
5. Enter the **Schedule Interval** (the number of minutes, hours, or days) that the scanned host list is to be cleared.
6. Select the time increment from the drop-down list.
7. Enter the **Next Scheduled Time** for the scan to run. The format for the entry is MM/DD/YY hh:mm AM/PM.
8. Check the **Pause** option if you want to pause the scan until you run it manually from the Scheduler view. See Scheduler view on page 849 for more information. If you leave this option unchecked, the scan runs according to the parameters you entered.
9. Click **Apply**.

Modify or remove a scan

1. Click **Policy > Remediation Configuration**.
2. Click the radio button next to the scan you want to select it.
3. To remove the scan, click **Remove**.

4. To modify the scan, click **Modify**. See Add a scan on page 481 for settings.
5. The list of Scanned Hosts may be cleared immediately or be scheduled to be cleared at a specified interval. See Remediation configurations on page 481 for additional information.
6. Click **Apply**.

Endpoint compliance

Endpoint compliance is a feature set used to ensure that hosts connecting to your network comply with network usage requirements. The cornerstone of endpoint compliance are endpoint compliance policies. Use these policies to establish the parameters for security that will be enforced when hosts connect to the network. If you do not create policies, when hosts connect to the network and users enter their credentials, they will be automatically registered without a policy being applied. See Endpoint compliance policies on page 415.

Endpoint compliance can also use an agent on the host to ensure that compliance with established policies is maintained. The Dissolvable Agent is downloaded during registration and is removed when the host is registered. The Persistent Agent remains on the host. Mobile Agent devices are installed on and remain installed on mobile devices. The Passive Agent is not installed, but is served as the user logs onto the network and does a scan in the background.

Access andpoint compliance options from the **Policy** menu.

Features

Feature	Description
Agent Distribution	Download Agents for alternative distribution. See Agent packages on page 226.
Auto-Def Update Schedule	Schedule the task to automatically update virus definitions, spyware definitions and operating systems for which you can scan. See Auto-Definition updates on page 549.
NAT Detection	Enter the IP ranges where an agent will detect NAT'd hosts. IP addresses outside this range could be NAT'd hosts and can generate an event and an alarm to notify the network administrator. See NAT detection on page 118.
Passive Agent Configuration	Create customized configurations that register and scan hosts associated with network users contained in your LDAP or Active directory. See Passive Agent on page 495.
Policy Configuration	Add, Delete, Modify, or Schedule Endpoint Compliance Policies. See Endpoint compliance policies on page 415.
Persistent Agent Properties	Enter text that will be displayed in the header and footer area on any messages sent to a host running the Persistent Agent. Enable status pop-ups. Configure server communication. See Persistent Agent settings on page 133.
Remediation Configuration	Add, Remove, Modify, or Schedule Security and Admin Script profile configurations. See Remediation configurations on page 481.

Endpoint compliance policies contain scans used to evaluate hosts and ensure that each host complies with your configured list of acceptable operating systems and anti-virus software. For a list of supported operating systems and anti-virus software, use the Customer Portal on our web site.

Implementation

Endpoint Compliance allows you to create security policies and use those policies to scan network users' computers for compliance with your organization's network usage rules. The implementation of this feature set can vary widely from one organization to another based on how restrictive or open you choose to make it. You can simply monitor hosts for non-compliance or go so far as to completely block network access. You can institute scans based on simple options included in FortiNAC or create your own custom scans. This section of the documentation discusses the implementation in the approximate order in which it should be done. It also details optional features that you may or may not choose to implement. As the options are discussed, links to additional information are provided.

Before implementing Endpoint Compliance, it is recommended that you notify all users about your network usage requirements. This helps users anticipate the changes and reduces calls to your IT Staff.

Agent

Choose one or more agents

The first step in implementing Endpoint Compliance is determining whether you will use the Persistent Agent, the Dissolvable Agent, the Passive Agent, the Mobile Agent or a combination.

- The **Persistent Agent** is installed on the host and remains there to scan the computer as needed.
- The **Dissolvable Agent** is downloaded to the host and removes itself once the host has passed the security scan. If the host does not pass the scan, the Dissolvable Agent remains on the host for the user to run again after compliance issues have been resolved.
- The **Passive Agent** is provided using an external method, such as Group Policy Objects, and launched when the user logs into the domain. Users experience a slight delay while logging in but are unaware that their hosts are being scanned. See Passive Agent on page 495.
- The **Mobile Agent** is installed on Android devices and is downloaded from either the captive portal or Google Play.

You may have situations in which one agent works better than others. For example, network users who log into your network every day could use the Persistent Agent and guest users could use the Dissolvable Agent. See Agent overview on page 491 for additional information.

Use the latest agents

You may not have the most recent version of the selected agent on your FortiNAC appliance. Use the Agent Distribution window to see which agents are installed. From this window download the latest agent from Fortinet, if you need it. See

Agent packages on page 226 . Not all agent versions are compatible with all FortiNAC versions. It is recommended that you check with a sales or support representative before using a new agent.

Deploy selected agents

Once you have determined which agents to use, you must decide how to deploy them. Typically agents are deployed using the portal pages or web pages that users see when they connect to your network. These web pages allow users to download an agent and install it on their hosts. If this is the method you use to give the agent to your hosts, no special setup is required. FortiNAC takes care of making the agent available via its own web pages based on the options selected in the Endpoint Compliance Policy. Go to the Portal Configuration window and edit the content displayed on those web pages in order to customize them. See Portal content editor on page 250.

Deployment options for each agent are as follows:

- **Dissolvable Agent**—Can be deployed from the captive portal or a separate web page.
- **Passive Agent**—Deployed using an external method, such as Group Policy Objects. This agent is launched and served to the host when the users logs onto the network.
- **Mobile Agent**—Deployed using the captive portal or Google Play.
- **Persistent Agent**—Deployed using the captive portal, a separate web page or some other software distribution method.
  - If you choose to deploy the agent outside of FortiNAC you must download the agent and make it available for your chosen distribution method. See Agent packages on page 226 for information on downloading the latest agent.
  - Go to the Persistent Agent Settings to configure agent behavior and the server with which the agent must communicate. See Persistent Agent settings on page 133.

Agent / server communications

All Agents must be configured to communicate with the FortiNAC server while they are scanning the host. The default configuration is for the agent to communicate based on the server alias "ns8200". To ensure that this communication is successful the alias must be resolvable through DNS. Agents distributed through the captive portal are set automatically to communicate with the server. Additional settings in both FortiNAC and your Production DNS direct the agent to the correct server. See and .

Agents at V3.0 or higher are designed to use a secure communication protocol with the FortiNAC Server or Application Server, however, that does require some configuration.

Endpoint compliance policy

When you have determined the agent or agents to be used, you are ready to begin configuring your Endpoint Compliance Policies.

- Create User/Host Profiles to determine which users/hosts will match a policy. See User/host profiles on page 389.
- Create Endpoint Compliance Policies to evaluate the hosts connecting to your network. See Endpoint compliance policies on page 415.
- Policies contain Scans that rely on having up-to-date information about Anti-Virus and Operating Systems. In order to ensure that you have the latest information at all times you should configure a schedule for and run the Auto Def Updates.

- If you plan to use Custom Scans, you must create them first and then associate them with a Scan. This can be done at any time you feel that a custom scan is necessary. New custom scans can be associated with existing Scans. See Custom scans on page 448.
- For each Scan that you create, decide how often to rescan hosts assigned to that policy. Setup a rescan schedule. See Schedule a scan on page 441.
- If you are using the Dissolvable Agent and you want to allow hosts to rescan at their convenience, enable Proactive scanning.
- When a host fails a scan the user sees a web page with a list of reasons for the failure. To comply with your organization's requirements, that host may need access to certain web sites. For example, if the host failed because virus definitions were not up to date, that host needs to access the anti-virus software manufacturer's web page to download new virus definitions. FortiNAC has a list of web sites that are made accessible even when a host has failed a scan. Make sure that the web sites for the software you require are included in that list.
- To understand what determines the policy that is assigned to a host, see Policy assignment on page 378.

Events & alarms

- Make sure the Security Risk Host event is enabled, so that an event is generated any time a host fails a scan. The event message provides you with information about the host and why they failed. This is optional, but may be helpful in troubleshooting. See Enable and disable events on page 857.
- You can view the list of events that have been generated by going to the Events View. See Events view on page 867.
- If you would like to be notified that a host has failed a scan, map the Security Risk Host event to an alarm. Within the alarm configuration you can specify that you would like to be notified via email or you can use the Alarm Panel on the dashboard. This alarm notifies you when a host has failed a scan and helps you trouble shoot any problems. You can also set up e-mail notification for users so they are aware that their host failed a scan. See Map events to alarms on page 888 and Alarm on page 38.
- Make sure that your administrator e-mail address and your e-mail server have been configured or FortiNAC will not be able to send e-mail notifications. See Email settings on page 169.

Ports - control access

- Place ports for wired switches in a Forced Registration group. This forces hosts connecting on those ports to the Registration VLAN and displays the registration page. From this page they can download an agent and be scanned. See and .
- Hosts who have an agent and have already registered are not forced to the registration page. They are sent directly to the network. They are rescanned based on the schedule you have implemented for their policy.
- If you have a Remediation or Quarantine VLAN where hosts are placed when they fail a scan, you must place ports in a Forced Remediation group. Placing ports in this group enables the Quarantine VLAN switching option. If you are not ready to begin placing hosts in Remediation, you can disable this option.
- When Quarantine VLAN switching is disabled, hosts are scanned and can see the passed and failed items from their scans, but they are given access to the network instead of being put into the Quarantine VLAN. This is a good option to use when testing out the system. See Quarantine on page 117.
- Other groups you may choose to use are Forced Authentication, Dead End and Role Based Access.

Scan hosts without enforcing remediation (optional)

To scan hosts without placing "at risk" hosts in remediation you can enable one or more options. See Scan hosts without enforcing remediation on page 430 for more details.

- Disable Quarantine VLAN switching to scan hosts but not mark them "at risk".
- Enable the Audit Only option on an Endpoint Compliance Policy. Hosts that fail when scanned with that policy are not marked "at risk" .
- Add hosts to the Forced Remediation Exceptions Group. Hosts in this group are scanned with the policy that corresponds to them. Hosts that fail the scan are marked "at risk" but are not forced into remediation.

Delayed remediation for scanned hosts (optional)

Allows you to scan hosts, notify the users of hosts that fail the scan of any pending issues, but not place the host in Remediation for a specified number of days. See Delayed remediation for scanned hosts on page 431.

- Enable the Delayed Remediation setting on one or more Endpoint Compliance Policies by entering the number of days for the delay.

Switches - model configuration

- Go to the Model Configuration for your wired and wireless switches and configure your VLANs. See Model configuration on page 767.

Authentication

- If you are using the Persistent Agent, you must set the method for authenticating your users in the Credential Configuration and in Portal Configuration. The authentication method selected must be the same in both places. See Credential configuration on page 139.
- If you are using the Dissolvable Agent or the Mobile Agent, you must set the method for authenticating your users in the Portal Configuration window.

Monitoring

- Use the Scan Results View to see a list of hosts with their current scan status. This view provides information on the Scan used and whether or not the host passed the scan. See Scan results view on page 925.
- Use Standard Reports to view lists of policies, the number of scans run that were passed or failed and details on the Pass/Fail. See Standard report templates on page 897.
- Use the Health Tab under Host Properties to view detailed scan information for an individual host. See Host health and scanning on page 803.

Testing

It is recommended that you spend considerable time testing your Endpoint Compliance Policies, web pages and VLAN switching before fully implementing Endpoint Compliance. Use your own hosts and go through as many failure scenarios as possible to make sure that hosts are being managed correctly.

Agent overview

Agents are used to scan hosts and determine whether the host complies with the Endpoint Compliance Policy assigned to that host. Agents can perform additional functions, such as, installing a Supplicant Configuration for a secure network. Several types of agents are available with FortiNAC, the Dissolvable Agent, the Passive Agent, the Persistent Agent and the Mobile Agent.

When hosts are scanned by an agent and fail, there are several options:

- Administrators can simply receive a warning that the host has failed the scan along with a list of what the failures were, but the host is given access to the network.
- Users can receive a warning that they have failed and be given access to the network.
- The network can be configured to move failed hosts off the production VLAN into the quarantine or remediation VLAN. This happens regardless of the agent type being used. Once remediation has taken place and the host has passed the scan, the host is moved back to the production VLAN.

Custom scans using HKEY_CURRENT_USER or HKEY_CLASSES_ROOT may not behave the same with Fortinet Persistent Agent as they do with Fortinet Dissolvable Agent. If HKEY_CLASSES_ROOT exists in HKEY_LOCAL_MACHINE\Software\Classes, it should work the same for both agents.

Agents have only been validated against English language versions of supported operating systems.

Dissolvable Agent

The Dissolvable Agent is downloaded to the host by the user. The user runs the agent and the agent scans the host. If the computer is compliant with the Endpoint Compliance Policy used for the scan, it is allowed on the network and the agent removes itself from the computer. If the computer is not compliant with the Endpoint Compliance Policy, the Dissolvable Agent remains on the host to be used in a future scan after compliance issues have been addressed.

This agent can run custom scans, verify that Hotfixes are installed, check for AntiVirus and AntiSpyware and Operating System information.

The Dissolvable Agent files are different for Windows, macOS and Linux.

All version 2.2.6, 3.x and higher agents are signed except the Windows Dissolvable Agent. The Windows Dissolvable Agent is signed as of version 3.1.

Passive Agent

The Passive Agent is not installed, but is served as the user logs onto the network and does a scan in the background. See Passive Agent on page 495. This agent can run custom scans, verify that Hotfixes are installed, check for AntiVirus and AntiSpyware and Operating System information. This agent runs only on Windows.

Persistent Agent

The Persistent Agent can be downloaded to the host and installed by the user, by a login script or by any other software distribution method your organization might use. The Persistent Agent remains installed on the host at all times. Once the agent is installed it runs in the background and communicates with FortiNAC at intervals established by the FortiNAC administrator.

The Persistent Agent can be configured to provide messages to the user when the host is scanned indicating the results of the scan. In addition you can provide pop-up messages indicating the host's current state, such as disabled, requires authentication or network access is normal. See Persistent Agent settings on page 133.

The Persistent Agent can run custom scans and monitors, verify that Hotfixes are installed, check for AntiVirus and AntiSpyware and Operating System information and allow an administrator to send a message to the host.

Mobile Agent

The Mobile Agent is downloaded and installed either from the captive portal or from Google Play depending on device settings. The Mobile Agent assist with authentication and registration and provide an inventory of installed apps. The Mobile Agent can determine whether the device is rooted or not. A device is considered rooted when a user has accessed the secure areas of the operating system on the device.

Dissolvable Agent

The Dissolvable Agent is an application that works on Windows, macOS or Linux hosts to identify them to FortiNAC. The agent scans them for compliance with an Endpoint Compliance Policy. This Agent is downloaded and installed on the host until the host passes the scan. The Agent then removes itself.

In a Windows environment, there are some operations that the Dissolvable Agent cannot perform unless the user has administrator privileges on the PC, such as, release and renew the IP address on the PC.

All version 2.2.6, 3.x and higher agents are signed except the Windows Dissolvable Agent. The Windows Dissolvable Agent is signed as of version 3.1.

Setup requirements and options

- Make sure the latest Agent Package is installed on the FortiNAC server.
- The Dissolvable Agent can be downloaded and installed by the user through the captive portal. The portal itself can be modified and personalized. Dissolvable Agent 3.1 (or higher) also has some settings in the portal under Agent > Dissolvable. See Portal configuration on page 248.
- If you are using Dissolvable Agent 3.X or higher, the FortiNAC appliance must be configured with SSL and must have a valid third party SSL certificate from a certificate authority. A self-signed certificate cannot be used.
- Dissolvable Agent Version 3.1 (or higher) discovers the server to which it should connect using DNS SRV records. If for any reason, it cannot discover the server, the user is presented with an option to enter either the URL or the FQDN of the server. The URL field will accept an HTTPS address, the FQDN of the server which it uses to create an HTTPS address or an HTTP address. If an HTTP address is used, a warning is displayed asking the user to confirm that they wish to access the server over an insecure connection. Depending on your configuration you may need to supply this information to users running the Dissolvable Agent. See and .

Host requirements and options

- See the Operating System for Hosts section, which is found under System Compatibility in the Release Notes.
- For an overview of the host registration and scanning process using the Dissolvable Agent, refer to .

Using the Dissolvable Agent

The Persistent Agent only works with the FortiNAC Control Server and FortiNAC Application Server pair or the FortiNAC Server. If the FortiNAC Control Server is not paired with the FortiNAC Application Server, the Dissolvable Agent must be used.

If you have chosen to use the Dissolvable Agent to scan Windows or macOS systems, the Dissolvable Agent is downloaded to the host. Once the Dissolvable Agent runs and the host has successfully passed the scan, the agent is removed from the host.

In a Windows environment, there are some operations that the Dissolvable Agent cannot perform unless the user has administrator privileges on the PC, such as, release and renew the IP address on the PC.

Registration

When an unknown host connects to the network and attempts to access the Internet, an entry in the DNS server redirects the host to the Login page for registration.

During registration FortiNAC determines which Endpoint Compliance Policy should be applied to this host based on the User/Host Profile that the connecting user and host match.

Endpoint Compliance Policies contain a series of requirements for hosts that want to access the network. Endpoint Compliance Policies contain scans that are configured by the Administrator and are run by the Agent. Policy requirements can include scans for specific Anti-Virus, Operating System version and Custom Scans. Custom Scans are created by the Administrator. These allow the administrator to scan for the existence of things such as, a specific file, a registry entry, an installer package, a specific process or a domain.

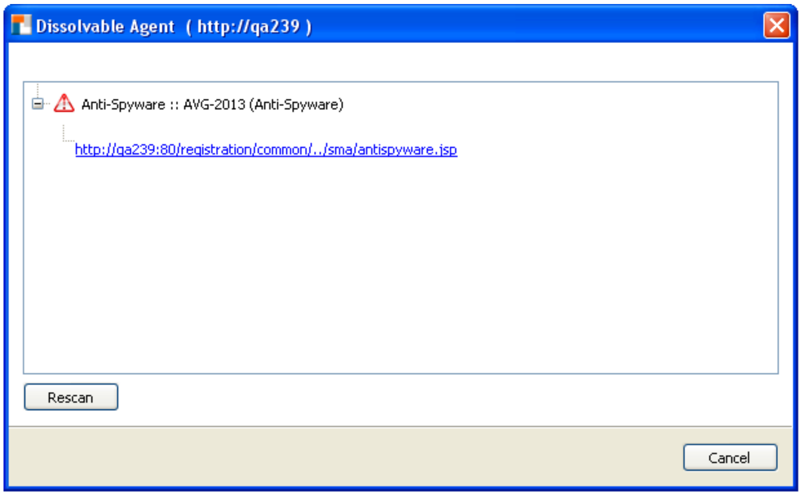
The Endpoint Compliance Policy determines which agent is made available to the user for download, such as Dissolvable or Persistent.

Hosts connecting to the network will go through the process outlined below:

Version 3.1 and higher

1. User connects to the network and is placed in Registration. The registration web page is displayed.
2. User downloads the Dissolvable Agent to the default downloads location for the operating system.
3. Run the downloaded file and install it on the device.
4. After the Dissolvabe Agent is installed, run the program. An Agent window is displayed and remains on the screen until the user closes it.
5. The Dissolvable Agent uses the DNS SRV records to locate the appropriate FortiNAC server.
6. If the Dissolvable Agent cannot locate the server, a message is displayed asking for the URL of the server. The user is presented with an option to enter either the URL or the FQDN of the server. The URL field will accept an HTTPS address, the FQDN of the server which it uses to create an HTTPS address or an HTTP address. If an HTTP address is used, a warning is displayed asking the user to confirm that they wish to access the server over an insecure connection.

7. The Agent window displays the results of the scan.



Dissolvable Agent (http://qa239)

Anti-Spyware :: AVG-2013 (Anti-Spyware)

http://qa239:80/registration/common/../sma/antispyware.jsp

8. If the host fails scan, a Rescan button is displayed allowing the user to Rescan after correcting any issues.
9. When the host passes the scan, the user closes the Agent window and the Dissolvable Agent dissolves.

Version 3.0 and lower

1. User connects to the network and is placed in Registration. The registration web page is displayed.
2. User downloads the Dissolvable Agent to the default Downloads location for their operating system.
3. Run the downloaded file and install it on the device.
4. After the Dissolvable Agent is installed, run the program. An Agent window is displayed and remains on the screen until the user closes it.
5. Once the security check has completed, the results are stored in a results.html file on the computer and launched in a browser. If the host failed to meet the requirements of the Endpoint Compliance Policy, the results page lists the items that failed and passed. The user must correct the issues indicated in the results page and run the Dissolvable Agent again.

   You can configure a link to a separate page that provides information about items that failed and what to do to correct the problem. Enter this link when you configure the policy. See Endpoint compliance policies on page 415 for more information.

   If you do not provide a link, modify the failure page to provide information for the user to correct the problem and find assistance.
6. If the host fails scan, the Dissolvable Agent remains on the host.
7. Once the user has corrected any issue(s) that caused the host to fail the scan, the Dissolvable Agent security check must be run again. The original Dissolvable Agent downloaded at the beginning of this process is still on the host and can be run again.

   Navigate to the Desktop.

   Double-click the Dissolvable Agent.exe file.

   This process may need to be completed again if additional issues remain that cause the host to fail the Endpoint Compliance Policy.
8. Once all the items causing the host to fail the policy have been corrected, the host is registered and the Success page is displayed in the browser. At this point the Dissolvable Agent file is removed from the host. The Dissolvable Agent does not remove itself from the host until the host successfully passes a security scan.

Passive Agent

Passive Agent Registration allows you to create customized configurations that register and scan hosts associated with network users contained in your LDAP or Active directory. Scanning requires an agent, however, the agent does not need to be installed by the user. The agent is provided using an external method, such as Group Policy Objects, and launched when the user logs into the domain. Users experience a slight delay while logging in but are unaware that their hosts are being scanned.

When a user connects to the network and logs in, FortiNAC determines the directory group to which the user belongs. Based on that group, a Passive Agent Configuration is used. The configuration registers the user and the associated host in FortiNAC. If enabled, the agent scans the host to verify that it is in compliance with the appropriate Endpoint Compliance Policy. The scan can be specified in the configuration or determined by FortiNAC based on the User/Host Profile of the user or host.

Registration

- To implement Passive Agent Registration you must complete the following tasks:
- Integrate your Directory with FortiNAC. See Directories on page 79 for configuration and integration information.
- Create one or more Passive Agent Configurations. See Add or modify configuration on page 497.
- If the **Passive Agent Configuration Modified** event is enabled, the Event Log tracks each Passive Agent Configuration as it is added, modified or removed. In addition, the user name of the user who made the changes and the current configuration settings are included in the event message. See Event management on page 856 to enable or disable this event. See Events view on page 867 to view the event log.
- If you plan to scan users' computers when they log in, create one or more security policies. See Endpoint compliance policies on page 415.
- If you have more than one FortiNAC Server or Control Server and you want to control which server responds to which hosts, configure IP address ranges for each server. See IP ranges on page 499.
- Go to the Agent Distribution window and download the passive agent (FortiNAC Passive Agent. exe). It is recommended that you rename this file, and remove the spaces in the filename before you distribute it. See Agent packages on page 226.

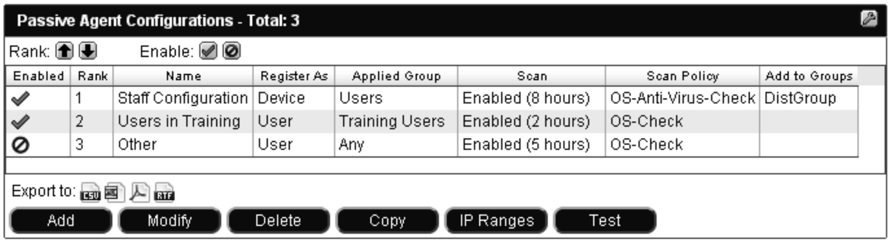
The Passive Agent filename for versions prior to 4.0.1.4 must be renamed to remove spaces to avoid issues when deploying with scripts.

- To scan user's computers the agent downloaded in the previous step must be set up to deploy or to be served to the host when the user logs into or off of the network. The agent can be served using Group Policy Objects, Desktop Management Software or any method that allows the network administrator to deploy and run the agent on a remote host as users login or logout of the domain. The method of deployment is up to the Network Administrator.
- If you choose to use Group Policy Objects to deploy the agent, you must also download the Administrative Templates provided on the Agent Distribution window, install them on your Windows Server and configure the appropriate settings. See Administrative templates for GPO on page 501.
- When the Passive Agent is run using a script, there are additional arguments that must be used to indicate whether the agent is attempting login or logout. See CLI arguments on page 508.

Manage configurations

The Passive Agent Configurations window displays the set of configurations you have created. Use this window to add, modify or delete configurations. Disabled configurations are ignored when users log in.

See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.



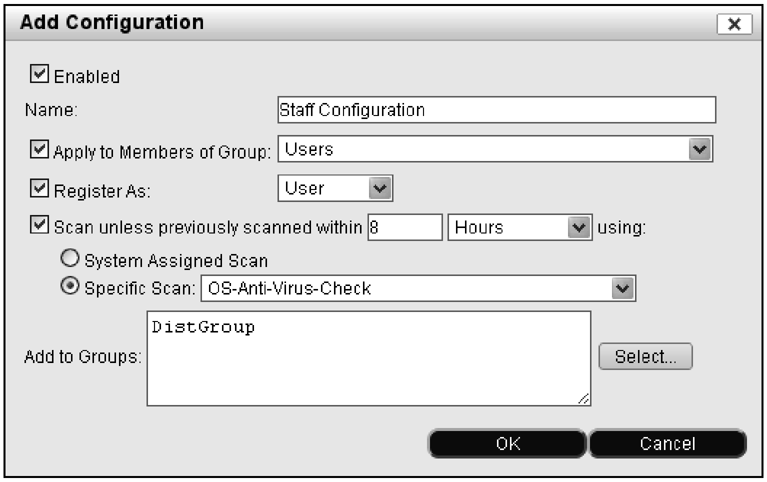
Enabled	Rank	Name	Register As	Applied Group	Scan	Scan Policy	Add to Groups
✓	1	Staff Configuration	Device	Users	Enabled (8 hours)	OS-Anti-Virus-Check	DistGroup
✓	2	Users in Training	User	Training Users	Enabled (2 hours)	OS-Check	
⊘	3	Other	User	Any	Enabled (5 hours)	OS-Check	

Settings

Field	Definition
Table configuration	
Rank Buttons	Moves the selected configuration up or down in the list. If a user matches more than one configuration based on the selected directory group, the configuration with the higher rank is used. One is the highest rank.
Enable Buttons	Enables or disables the selected configuration. Disabled configurations are ignored when a user logs onto the network.
Table columns	
Enabled	A green check mark indicates that the configuration is enabled. A red circle indicates that the configuration is disabled.
Rank	Configuration's rank in the list of configurations. Rank controls the configuration used if a user matches more than one configuration based on the selected directory group.
Name	Name for the configuration.
Register As	Indicates whether the host will be registered based on the login name of the user as a host or based on host name as a device.
Applied Group	Directory group to which this configuration will be applied. Users within this group are registered in FortiNAC and scanned based on the rules in the associated configuration. If this is not enabled in the configuration, the word Any is displayed, indicating that directory group is not used to select the appropriate configuration. It is recommended that such a configuration be placed at the end of the list as a catch all because it could apply to a large group of users.
Scan	Indicates whether scanning is enabled or disabled. When scanning is enabled, the scan can be repeated the next time the user logs in or out if the time interval shown has been exceeded.

Field	Definition
Scan Policy	Scan used to evaluate the host when this configuration is applied. Either a specific scan or the scan contained in the Endpoint Compliance Policy selected by FortiNAC based on the User/Host Profile.
Add To Groups	FortiNAC groups where hosts are added as they log in.
Last Modified By	User name of the last user to modify the configuration.
Last Modified Date	Date and time of the last modification to this configuration.
Right click options	
Export	Exports data to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.
Copy	Copy the selected Configuration to create a new record.
Delete	Deletes the selected Configuration.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.
Modify	Opens the Modify Configuration window for the selected configuration.
IP Ranges Button	Configures the host IP addresses that this FortiNAC server will respond to when a host logs on to or off of the network. If this is not configured, requests are accepted from all hosts.
Test Button	Allows you to test a single directory user, based on user name to determine which configuration would apply to that user on login or logout.

Add or modify configuration



Add Configuration

☑ Enabled

Name: Staff Configuration

☑ Apply to Members of Group: Users

☑ Register As: User

☑ Scan unless previously scanned within 8 Hours using:

○ System Assigned Scan

● Specific Scan: OS-Anti-Virus-Check

Add to Groups: DistGroup

1. Select **Policy > Passive Agent Configuration**.
2. Click the **Add** button or select a configuration and click **Modify**.
3. Refer to the table below for information on each option for this window.
4. Click **OK** to save.

Agent selections contained within the Endpoint Compliance Policy used to scan the host are ignored when the Passive Agent is used. The Passive agent scan will only occur if there is a connected adapter, or if the scan name is provided in the Passive Registration Configuration.

Settings

Field	Definition
Enable	Enables or disables this configuration. Disabled configurations are ignored when a user logs onto the network.
Name	Name for the configuration.
Apply to Members of Group	Directory group to which this configuration will be applied. Users within this group are registered in FortiNAC and scanned based on the rules in the associated configuration. If this is not enabled, the word Any is displayed on the list of configurations, indicating that directory group is not used to select the appropriate configuration. It is recommended that such a configuration be ranked at the end of the list as a catch all because it could apply to a large group of users.
Register As	Indicates whether the host will be registered as a host based on the login name of the user or based on the host name as a device with no user association.
Scan Unless Previously Scanned Within	Enables scanning. The time interval determines whether or not the host is scanned the next time the user logs on or off. For example, if the time interval is one hour and the user logs out after 30 minutes, the host is not scanned again. If the user remains logged out for two hours and then logs back in again, the host is scanned because the time interval has been exceeded. Only login and logout after the selected time interval has elapsed trigger scans.
System Assigned Scan	If this option is selected the Endpoint Compliance Policy used to select the scan is determined by FortiNAC based on the User/Host Profile associated with the policy.
Specific Scan	If this option is selected the scan in the drop-down list is used to scan the host regardless of the host state. Scans in the drop-down list are created in Policy Configuration under Endpoint Compliance. See Add or modify a scan on page 433.
Add To Groups	FortiNAC groups to which hosts are added as they log in. If new groups are added to the list, the host is added the next time the user logs in. If groups are removed from this field, the host is not removed from those groups automatically. You must remove the host manually from the Groups View. See Groups view on page 838. Click the **Select** button to view or modify the list of groups. On the Select Groups window the All Groups column displays a list of available groups and the Selected Groups column displays a list of the groups to which hosts will be added. Use the arrows in the center of the window to move groups from one column to the other.

Delete configuration

1. Select **Policy > Passive Agent Configuration**.
2. Select a configuration and click **Delete**.
3. A message displays asking if you are sure. Click **Yes** to continue.

Copy configuration

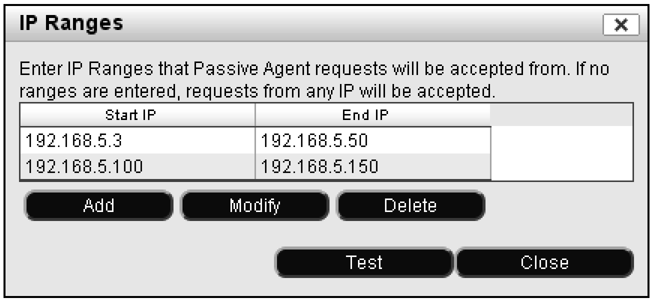
1. Select **Policy > Passive Agent Configuration**.
2. Select a configuration and click **Copy**.
3. The **Add Configuration** window displays with the information from the selected configuration.
4. You must, at minimum, modify the name of the configuration. Modify other fields as needed and click **OK** to save.
5. For settings, see Add or modify configuration on page 497.

IP ranges

Under the Passive Agent Configurations window you have the option of limiting the FortiNAC Servers or Control Servers to hosts from within selected IP address ranges. If you have multiple FortiNAC Servers or Control Servers, you can control which servers respond to which user login/logout requests based on the IP address of the host connecting to the network. If IP address ranges are configured on this server it will only respond to requests from hosts within the range. If no IP address ranges are configured, the server responds to all requests.

Configure IP ranges

1. Select **Policy > Passive Agent Configuration**.
2. Click the **IP Ranges** button at the bottom of the window.

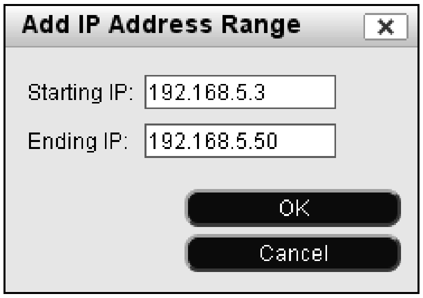


IP Ranges

Enter IP Ranges that Passive Agent requests will be accepted from. If no ranges are entered, requests from any IP will be accepted.

Start IP	End IP
192.168.5.3	192.168.5.50
192.168.5.100	192.168.5.150

3. Click the **Add** button to add an IP address Range. Enter the Starting and Ending IP addresses and click **OK**.



Starting IP: 192.168.5.3

Ending IP: 192.168.5.50

4. To modify a range, select it from the list and click **Modify**.
5. To delete a range, select it from the list and click **Delete**.
6. When the ranges are configured correctly, click **Close**.

Test IP addresses

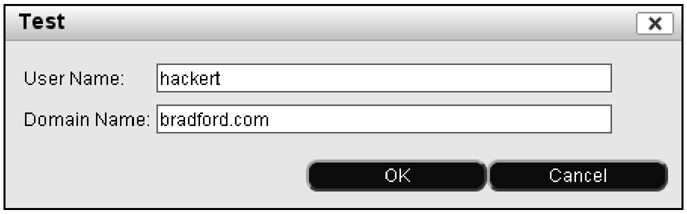
Use the Test button to test an individual IP to make sure it is contained within one of the IP address ranges in the list.

1. Select **Policy > Passive Agent Configuration**.
2. Click the **IP Ranges** button at the bottom of the window.
3. Click the **Test** button.
4. Enter a single IP address and click **OK**.
5. A message is displayed indicating either that the IP Passed or the IP Failed. If the IP failed you must either update your ranges or configure the appropriate range on a different FortiNAC Server.

Test a directory user

The Test feature on the Passive Agent Configurations window allows you to test a single directory user and determine which configuration would apply to that user on login or logout. The test tool takes a sample user and tries to match that user with a configuration. Users are matched to configurations based on the directory group in the Applied Group field. Users may match more than one configuration depending on the groups in which they are members. If a user matches more than one configuration, the configuration with the highest rank is used. The lower the rank number the higher the rank, for example a configuration with Rank 1 would be the highest on the list. Disabled configurations are ignored. Run the test as follows:

1. Select **Policy > Passive Agent Configuration**.
2. Click the **Test** button at the bottom of the window.
3. Enter the **User Name** and **Domain Name** of your sample user.

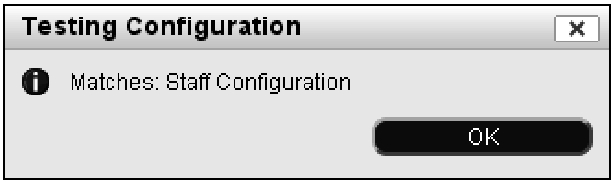


User Name: hackert

Domain Name: bradford.com

4. Click **OK** to display the results of the test. If the user matched a configuration because they were a member of the associated directory group, the name of the configuration displays in the Test Configuration window. If the user did

not match any configuration, the Testing Configuration window displays No Configuration Found.



Testing Configuration

Matches: Staff Configuration

Administrative templates for GPO

Administrative templates are used to configure registry settings on Windows endpoints through Group policy objects. For the Persistent Agent and the Passive Agent, there are templates to configure the Server URL of the FortiNAC Application Server with which the agent will communicate. There are also per-computer and per-user templates to enable or disable the System Tray Icon or Balloon Notifications of status changes. The Balloon Notification template does not affect the Server IP and is not required.

FortiNAC does not support an Administrative Template for deploying configuration changes to macOS computers or users through GPO. You can investigate 3rd party applications, such as Likewise Enterprise that support macOS computers using Group Policy Object editor. The modifications shown in the tables below can be made in the Preferences file on macOS hosts, using the tool of your choice.

The Persistent Agent running on a macOS computer can determine the server to which it should connect via DNS server records it does not require changes to Preferences.

If you are using Persistent Agent version 2.2.2 or higher your Windows login credentials are automatically passed to FortiNAC. You can modify the Administrative Template to hide the Persistent Agent Login dialog and use the Windows login credentials sent by the Persistent Agent by modifying the settings in the Administrative Template. See Using Windows domain logon credentials on page 516.

If you are using Agent package version 3.0 or higher, security is enabled by default. It is recommended that you update to the latest template files and configure the templates for the new security settings.

Requirements:

- Active Directory
- Group Policy Objects
- Template Files From Fortinet

Templates:

The templates listed below are provided by Fortinet. You must run the installation program for the templates on your Windows server . Be sure to select the appropriate MSI for your Windows server architecture.

- 32-bit (x86): Bradford Networks Administrative Templates.msi
- 64-bit (x86_64): Bradford Networks Administrative Templates-x64.msi

Install a GPO template

1. In FortiNAC select **System > Settings > Updates > Agent Packages**.
2. At the top of the Agent Distribution window click either the **32-bit (x86)** or the **64-bit (x86_64)** link to download the appropriate template file.
3. Copy the template file to the domain server.
4. On the domain server, double-click the msi file to start the installation wizard.
5. Click through the installation wizard. When installation has completed, the Microsoft Group Policy Management Console is required to complete the installation. Refer to the Windows Server documentation for details.
6. Navigate to the **Group Policy Object** you want to edit, right-click and select **Edit** to display the GPO Editor pane.
7. Right-click **Computer Configuration > Administrative Templates** and select **Add/ Remove Templates**, shows the current templates pop-up.
8. Click **Add** and browse to `Program Files\Bradford Networks\Administrative Templates`.
9. To use the Persistent Agent, select `Bradford Persistent Agent.adm` and click **Open**.
10. To use the Passive Agent, select `Bradford Passive Agent.adm` and click **Open**.
11. Click **Close**, and the Administrative Templates will be imported into the GPO.

Install an updated template with balloon notifications

If you already have a Fortinet Administrative Template installed for the Persistent Agent and the Balloon Notifications were ever set to anything other than Not Configured (e.g. enabled or disabled), you must unconfigure the Balloon Notifications and push the settings to your clients. When your clients have all been updated, then the new template can be installed. These templates affect the registry settings on the client host. In the case of the Balloon Notifications, removing the previous configuration before installing the new one ensures that the keys will be set correctly.

Before updating a template, be sure to record the current template settings. Existing template settings are lost when the new template is installed.

1. In FortiNAC, navigate to **System > Settings > Persistent Agent Properties**.
2. Select **Security Management** and make sure that Display Notifications is disabled. When you have uploaded and configured the new template, come back to this view and restore the Display Notifications option to its original state.
3. Log into your Windows Server.
4. On your Windows server open the Group Policy Management Tool.
5. Navigate to the **Group Policy Object** you want to edit, right-click and select **Edit** to display the GPO Editor pane.
6. Select **Computer Configuration > Administrative Templates > Bradford Persistent Agent**.
7. In the pane on the right, right-click on the Balloon Notifications setting and select Properties.
8. On the **Setting** tab in the Properties window, select **Not Configured** and click **OK**.
9. When all of your clients have received the updated settings, the new template can be installed.
10. Navigate to the **Group Policy Object** you want to edit, right-click and select **Edit** to display the **GPO Editor** pane.
11. Right-click **Computer Configuration > Administrative Templates** and select **Add/ Remove Templates** to show the current templates pop-up.

12. Select the old template and click **Remove**. Follow the instructions in Install a GPO template on page 502 to install the new template.

Install an updated template without balloon notifications

Before updating a template, be sure to record the current template settings. Existing template settings are lost when the new template is installed.

1. On your Windows server, open the Group Policy Management Tool.
2. Navigate to the **Group Policy Object** you want to edit, right-click and select **Edit** to display the **GPO Editor** pane.
3. Right-click **Computer Configuration > Administrative Templates** and select **Add/ Remove Templates** to show the current templates pop-up.
4. Select the old template and click **Remove**. Follow the instructions in Install a GPO template on page 502 to install the new template.

Modify template settings

See the table below for settings which can be configured using the Administrative Templates provided.

Settings

Option	Definition
Persistent Agent template	
Host Name	Fully qualified host name of the FortiNAC Application Server or the FortiNAC Server if you are not using a pair. It is pushed out to the connecting host(s) to ensure that the Persistent Agent is communicating with the correct host in a distributed environment. Note: This is an option for Persistent Agent Version 2.9.x and lower. Persistent Agent Versions 3.0 and higher do not use this setting.
Balloon Notifications	Enables or Disables Balloon Notifications on a per-host or per-user basis. This setting is not required for configuring Server IP information. Options include: • **Enabled** — Forces balloon notifications for host state changes to be enabled on the host. • **Disabled** — Forces balloon notifications for host state changes to be disabled on the host. • **Not Configured** — Use the non-policy setting (Enabled).
Login Dialog	Enables or Disables the login dialog on a per-host or per-user basis. This setting is not required for configuring Server IP information. See Using Windows domain logon credentials on page 516 for further instructions. Options include: • **Enabled** — The login dialog is enabled. This can be used per-user to override a per-host setting of Disabled. • **Disabled** — The login dialog is disabled. The agent will never prompt the user for credentials. This is useful in certain Single-sign-on configurations.

Option	Definition
	• **Not Configured** — The login dialog is enabled, unless overridden by a per-user configuration.
System Tray Icon	Enables or Disables the System Tray Icon on a per-host or per-user basis. This setting is not required for configuring Server IP information. (Requires Persistent Agent 2.2.3 or higher). Options include: • **Enabled** — The System Tray Icon is enabled. This can be used per-user to override a per-host setting of Disabled. • **Disabled** — The System Tray Icon is disabled. Disabling the System Tray Icon also disables the following functionality: Status Notifications (Show Network Access Status, Login, Logout), Message Logs and the About dialog. • **Not Configured** — The System Tray Icon is enabled, unless overridden by a per-user configuration.
Max Connection Interval	The maximum number of seconds between attempts to connect to FortiNAC.
Security settings	
Security Mode	Indicates whether security is enabled or disabled.
Home Server	Server with which the agent always attempts to communicate first. Protocol configuration change requests are honored only when they are received from this server. If this servers is not set, it is automatically discovered using Server Discovery. On upgrade, this is populated by the contents of ServerIP.
Limit Connections To Servers	**Enabled** — Agent communicates only with its Home Server and servers listed under Allowed Servers list displayed. **Disabled** — Agent searches for additional servers when the home server is unavailable. **Allowed Servers List** — In large environments there may be more than one set of FortiNAC servers. If roaming between servers is limited, list the FQDNs of the FortiNAC Application Servers or FortiNAC Servers with which the agent can communicate.
Passive Agent template	
Passive Agent	**Server URL List**— Comma separated list of URLs (HTTP(s)://<server_name>/<context> formatted) for the FortiNAC servers that hosts running an agent should contact. Hosts must be able to reach all of the URLs in order to run properly. Example: http://qa228/registration NOTE: The context portion of the Server URL is the area of the captive portal the agents should contact, such as, registration, remediation, or authentication.

Registry keys

The template setup shown in the table above modifies the Windows host's registry settings. The table below shows the modifications made to the host's registry keys by the Group Policy Object using the administrative template. If you use a tool other than GPO, you must make sure to set the appropriate keys on each host.

Upon installation of the Persistent Agent, the following key is created by default (and can be viewed using the Windows registry editor on the endstation):

```
HKLM\Software\Bradford Networks\Client Security Agent
```

When registry settings are pushed to a host via software, one or both of the following keys are created (depending upon the values pushed):

```
HKEY_USERS\ … \Software\Policies\Bradford Networks\Persistent Agent
HKLM\Software\Policies\Bradford Networks\Persistent Agent
```

When the settings are pushed, the values for HKLM\Software\Bradford Networks\Client Security Agent will remain the same, but any settings altered via the software push will override those listed in the original key.

On 64-bit operating systems in RegEdit, these registry values will appear in the following key: `HKLM\Software\wow6432node`

Key	Value	Data
Persistent Agent		
HKLM\Software\Policies\Bradford Networks\Persistent Agent	ServerIP	The fully-qualified hostname to which the agent should communicate. **Data Type:** String **Default:** Not Configured
HKLM\Software\Policies\Bradford Networks\Persistent Agent	ClientStateEnabled	**0** — Do not show balloon notifications on status changes. **1** — Show balloon notifications on status changes. Data Type: DWORD Default: Not Configured
HKEY_USERS\ … \Software\Policies\Bradford Networks\Persistent Agent	ClientStateEnabled	**0** — Do not show balloon notifications on status changes. **1** — Show balloon notifications on status changes. Data Type: DWORD **Default:** Not Configured
HKLM\Software\Policies\Bradford Networks\Persistent Agent	LoginDialogDisabled	**0** — Enable Login Dialog. **1** — Disable Login Dialog. **Data Type:** DWORD **Default:** Not Configured (Login Dialog displayed)

Key	Value	Data
HKEY_USERS\ … \Software\Policies\Bradford Networks\Persistent Agent	LoginDialogDisabled	**0** — Enable Login Dialog. **1** — Disable Login Dialog. **Data Type:** DWORD **Default:** Not Configured (Login Dialog displayed)
HKEY_USERS\ … \Software\Policies\Bradford Networks\Persistent Agent	ShowIcon	**0** — Do not show the tray icon. **1** — Show the tray icon. **Data Type:** DWORD **Default:** Not Configured (Tray icon displayed)
HKLM\Software\Policies\Bradford Networks\Persistent Agent	ShowIcon	**0** — Do not show the tray icon. **1** — Show the tray icon. **Data Type:** DWORD **Default:** Not Configured (Tray icon displayed)
HKEY_LOCAL_ MACHINE\SOFTWARE\Policies\ Bradford Networks\Persistent Agent	maxConnectInterval	The maximum number of seconds between attempts to connect to FortiNAC. **Data Type:** Integer **Default:** 960
HKEY_LOCAL_ MACHINE\SOFTWARE\Policies\ Bradford Networks\Persistent Agent	securityEnabled	**0** — Disable Agent Security. **1** — Enable Agent Security **Data Type:** Integer **Default:** 1
HKEY_LOCAL_ MACHINE\SOFTWARE\Policies\ Bradford Networks\Persistent Agent	homeServer	The fully-qualified hostname of the default server with which the agent should communicate. **Data Type:** String **Default:** Empty
HKEY_LOCAL_ MACHINE\SOFTWARE\Policies\ Bradford Networks\Persistent Agent	restrictRoaming	**0** — Do not restrict roaming. Allow agent to communicate with any server. **1** — Restrict roaming to the home server and the allowed servers list. **Data Type:** Integer **Default:** 0

Key	Value	Data
HKEY_LOCAL_ MACHINE\SOFTWARE\Policies\ Bradford Networks\Persistent Agent	allowedServers	Comma-separated list of fully-qualified hostnames with which the agent can communicate. If restrict roaming is enabled, the agent is limited to this list. The home server does not need to be included in this list (for example, a.example.com, b.example.com, c.example.com). **Data Type:** String **Default:** Empty
Passive Agent		
HKEY_USERS\{SID}\Software\ Policies\Bradford Networks \PASSIVE	ServerURL	**Server URL List** — Comma separated list of URLs for the FortiNAC servers that an agent should contact. Example: http://qa228/registration NOTE: The context portion of the Server URL is the area of the captive portal the agents should contact, such as, registration, remediation, or authentication.
HKLM\Software\Policies\Bradford Networks\PASSIVE	ServerURL	**Server URL List** — Comma separated list of URLs for the FortiNAC servers that an agent should contact. Example: http://qa228/registration NOTE: The context portion of the Server URL is the area of the captive portal the agents should contact, such as, registration, remediation, or authentication.

Deploy the Passive Agent

1. On your Windows server open the Group Policy Management Tool.
2. Navigate to the Group Policy Object you want to edit.
3. Right-click the Group Policy Object and select **Edit** to display the GPO Editor pane.
4. Click **User Configuration > Policies > Windows > Settings Scripts (Logon/Logoff)** to display the Logon and Logoff script configurations.
5. Double click **Logon** for Logon Properties.
6. Click **Add** and then browse to the location of `FortiNAC_Passive_Agent.exe`.
7. Select `FortiNAC_Passive_Agent.exe` to add it to the **Script Name** field.
8. Enter `-logon` in the **Script Parameters** field.
9. Click **OK**.

To ensure the user is logged off the host upon logging out, do the following:

1. Follow steps 1-4, and then double-click **Logoff**.
2. Add `FortiNAC_Passive_Agent.exe` to the Script Name field, and then enter `-logoff` in the Script Parameter field.
3. Click **OK**.

CLI arguments

The Passive Agent is designed to be run via an external script when a user logs onto or off of the network. Creating the script is the responsibility of the Administrator. When running the agent CLI arguments that indicate whether the agent is attempting to logon or logoff. If no argument is used, the agent defaults to login. Arguments are case sensitive.

The Passive Agent filename for versions prior to 4.0.1.4 must be renamed to remove spaces to avoid issues when deploying with scripts.

Type	Arguments	Description

Logon	`-login`
	`/login`
	`-logon`
	`/logon`
	`-on`
	`/on`
	`-in`
	`/in`
	`-authenticate`
	`/authenticate`
		Any one of these arguments can be used to indicate Logon. There must be a space between the name of the agent file and the argument.
		Example: `FortiNAC_Passive_Agent.exe -login`

Logoff	`-logout`
	`/logout`
	`-logoff`
	`/logoff`
	`-off`
	`/off`
	`-out`
	`/out`
	`-deauthenticate`
	`/deauthenticate`
		Any one of these arguments can be used to indicate Logoff. There must be a space between the name of the agent file and the argument.
		Example: `FortiNAC_Passive_Agent.exe -logout`

Persistent Agent

The Persistent Agent is an application that works on Windows,macOS, or Linux hosts to identify them to FortiNAC and scan them for compliance with an Endpoint Compliance Policy. This Agent is downloaded and installed on the host permanently.

Communication

The Persistent Agent installed on a host is designed to "check in" through a periodic heartbeat sent to the Persistent Agent server. This lets the server know that the Persistent Agent is still installed and running on the host host. When this does not happen, a "Lost Contact with Persistent Agent" event is generated indicating that the server cannot communicate with the host. When the Persistent Agent eventually contacts the server again a "Regained Contact with Persistent Agent" event is generated.

Lost contact with the persistent agent is intended to communicate to FortiNAC Administrators that hosts that are marked as having the Persistent Agent are online and not communicating to the FortiNAC agent server. Lost contact with the Persistent Agent detection can take up to approximately 90 minutes from the first failure to communicate detection to generate the Event. This also depends on the L2 poll interval of the Network Device.

The Persistent Agent communicates using the following ports:

- udp 4567
- tcp 4568
- tcp 80 (required for upgrades)

The "Lost Contact with Persistent Agent" event only detects that the agent is no longer successfully communicating. This loss of contact could be caused by many things including: a missing or disabled agent, a lack of network connectivity, a lack of network activity that would prevent FortiNAC from polling to discover that the host was offline, a firewall that prevents communication between the agent and the server or any other issue that would interrupt communication.

The Persistent Agent does work within the context of FortiNAC's VPN integration.

Setup requirements and options

- Make sure the latest Agent Package is installed on the FortiNAC server.
- Add SRV records to your production DNS server that allow the agent to locate the FortiNAC Server or Application server to which it should connect. See and .
- If you are using Persistent Agent 3.X or higher, the FortiNAC appliance must be configured with SSL and must have a valid third party SSL certificate from a certificate authority. A self-signed certificate cannot be used.
- The 3.x Persistent Agent communication method requires not only SSL certificates be installed for the Persistent agent target in FortiNAC, but also the root certificate be installed on the endstation hosting the agent. The Persistent Agent reads all certificates from the trusted root certification authorities store of the system account. If the Certificate Authority is not listed in this store, the Persistent Agent will not trust the connection to FortiNAC and will not communicate.

  FortiNAC does not push root certificates to endstations. Root certificates come pre-installed with the host's operating system. Any additions or updates to root certificates are distributed via the host's OS updates.
- The Persistent Agent can be downloaded and installed by the user through the captive portal, by a login script or by any other software distribution method your organization might use. Determine your distribution method.
- If you plan to deliver the agent via the captive portal, configure the portal styles. See Portal configuration on page 248.
- You can configure FortiNAC to authenticate users with their Windows domain logon credentials eliminating the need for the Persistent Agent to ask for credentials. See Using Windows domain logon credentials on page 516.

- The Persistent Agent can be configured to provide messages to the user when the host is scanned indicating the results of the scan. In addition you can provide pop-up messages indicating the host's current state, such as disabled, requires authentication or network access is normal. See Persistent Agent settings on page 133.
- In addition to the settings contained within the Admin UI, registry settings on Windows hosts can be configured using Group Policy Objects. These registry settings contain the URL of the FortiNAC Application Server, enable and disable the System Tray Icon or Balloon Notifications and various security settings. See Agent packages on page 226.
- The Persistent Agent has different files for macOS and Windows operating systems. FortiNAC can be configured to update the Persistent Agent automatically with a user-specified version or an updated agent can be pushed to a specific host.
- Persistent Agent Version 3.1 and higher can be used to apply a Supplicant Configuration to a host. See Supplicant EasyConnect policies on page 471.

Host requirements and options

- The host must be running Windows, macOS, or Linux. Refer to the Agent Comparison table in Agent overview on page 491 or the Release Notes for more detailed information about operating system versions that are supported.
- If the host is running a Virtual Machine (VM) with the Persistent Agent inside the VM, the VM must be bridged. The Persistent Agent is not fully functional when it runs in a NATed Virtual Machine on a host. The agent can contact the FortiNAC server and receive a response. However, unsolicited messages from the FortiNAC server fail to reach the agent.
- For the Persistent Agent to detect guest VMs running on the host, the VMs must be bridged. The VM adapters will then be associated with the host with the Medium of VirtualGuest.
- If the Persistent Agent is delivered via the captive portal, the user must install it manually. See Installion for Windows on page 510 and Installation for macOS on page 511.
- For an overview of the host registration and scanning process using the Persistent Agent, refer to Using the Persistent Agent on page 514.

Troubleshooting

- If you are troubleshooting an issue with the Persistent Agent, review the logs generated on the host. See Logging on page 519.

Installion for Windows

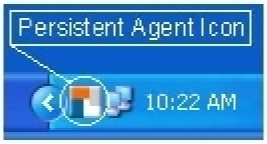
When a new host connects to the network, it is directed to a special web page that allows the user to download the Persistent Agent. Once the Persistent Agent has been downloaded, it must be installed on the host.

The Persistent Agent can also be delivered as an .msi file. This allows it to be pushed automatically from Active Directory.

Install

1. On the host, locate `Persistent Agent.exe` file that was downloaded. Double-click the to begin the installation process.

2. The Welcome window displays. Click **Next** to continue.
3. A progress window appears showing the status of the installation. The Installation Complete window displays.
4. Click **Finish**.
5. The Agent Icon appears in the system tray on the right.



Several right click options are available:

Option	Description
About	Displays the agent version, copyright, and other information.
Show Messages	Displays the list of the messages sent through the Persistent Agent that have been received by the host. If any URLs have been sent separate from a message, a list of these are also be displayed.
Login	Appears when host is in isolation requiring registration or authentication. When selected, opens a login dialog.
Log off the Network	Appears when host is logged in and authenticated. When selected, the host is logged off the network and is placed into isolation requiring authentication.
Show Network Access Status	Appears when the host is isolated for remediation or being disabled. When selected, the user is sent to either the remediation page for rescan or the dead end page if disabled.

6. The Agent automatically communicates with the FortiNAC Application Server to authenticate the user credentials.
7. Enter **User Name** and **Password**, then click **OK**. The user is authenticated and registered.

Host firewall

When a host is running a Windows Firewall, the Persistent Agent automatically adds a program exception for itself to the Windows Firewall configuration. This is added to the currently active user profile, unless the "Domain" profile is active. For hosts using a different firewall you must meet the following requirements:

- An exception for the Persistent Agent must be added to the firewall
- UPD/TCP ports 4567 and 4568 must be available for agent communication

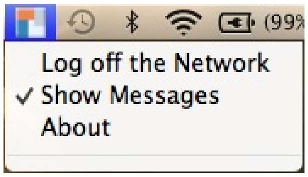
Installation for macOS

When a new host connects to the network, it is directed to a special web page that allows the user to download the Persistent Agent. Once the Persistent Agent has been downloaded it must be installed on the host.

Install

1. On the host, locate and open the Persistent Agent.dmg folder that was downloaded.
2. Double-click the Persistent Agent.pkg on the desktop to begin the installation process. Then click Continue to start the installation.

3. Select the drive where the persistent agent is to be installed, then click Continue.
4. Click Install to begin the installation of the agent on the local host.
5. Enter the local host’s administrator credentials and click OK.
6. Click Close when the installation is complete.
7. Go to the desktop and unmount the Persistent Agent Installer by dragging it to the trash bin. The trash bin icon turns into an eject icon.
8. The Persistent Agent Icon appears in the system tray on the right. Click options for the icon are About and Show Messages.



Several options are available when you click the icon:

Option	Description
About	Displays the agent version, copyright, and other information.
Show Messages	Displays the list of the messages sent through the Persistent Agent that have been received by the host. If any URLs have been sent separate from a message, a list of these are also be displayed.
Login	Appears when host is in isolation requiring registration or authentication. When selected, opens a login dialog.
Log off the Network	Appears when host is logged in and authenticated. When selected, the host is logged off the network and is placed into isolation requiring authentication.
Show Network Access Status	Appears when the host is isolated for remediation or being disabled. When selected, the user is sent to either the remediation page for rescan or the dead end page if disabled.

9. The Agent automatically communicates with the FortiNAC Application Server to authenticate the user's credentials. Enter User Name and Password, then click OK. The user is authenticated and registered.

If the Agent will not run (e.g., there is no icon displayed), uninstall the PA and run the following command from the command line (Terminal). Then, re-install the PA.

```
sudo /usr/sbin/pkgutil --forget
com.bradfordnetworks.PersistentAgent
```

Installation for Linux

When a host connects to the network, it is directed to a special web page that allows the user to download a rpm or deb package of the Persistent Agent. Once the Persistent Agent has been downloaded, it must be installed on the host.

Install

1. On the host, locate the directory where the `bni-persistent-agent-3.X.X.X-1.x86_64.rpm` or `bin-persistent-agent-3.X.X.X-1.amd64.deb` was downloaded.
2. To install the Persistent Agent package, do the following:
   a. To install rpm, type: `$ sudo rpm -Uvh bni-persistent-agent-3.X.X.X-1.x86_64.rpm`
   b. To install deb, type: `$ sudo dpkg -i bni-persistent-agent-3.X.X.X-1.amd64.deb`
3. The Persistent Agent Icon appears.

   Several options are available when you click the icon:

Option	Description
About	Displays the agent version, copyright, and other information.
Show Messages	Displays the list of the messages sent through the Persistent Agent that have been received by the host. If any URLs have been sent separate from a message, a list of these are also be displayed.
Login	Appears when host is in isolation requiring registration or authentication. When selected, opens a login dialog.
Log off the Network	Appears when host is logged in and authenticated. When selected, the host is logged off the network and is placed into isolation requiring authentication.
Show Network Access Status	Appears when the host is isolated for remediation or being disabled. When selected, the user is sent to either the remediation page for rescan or the dead end page if disabled.

4. The Agent automatically communicates with the FortiNAC Application Server to authenticate the user's credentials. Enter the User Name and Password, then click OK.

   The user is authenticated and registered.

If FortiNAC's DNS does contain the specific SRV records used by the Persistent Agent to locate the server, the end user must run the setup script to edit the configuration file for the Linux Persistent Agent.

To run the setup script, do the following:

1. To stop the Linux Persistent Agent service type: `$ sudo service bndaemon stop`
2. Run the setup script.
   a. Type `$ cd /opt/com.bradfordnetworks/PersistentAgent`
   b. Type `$ sudo ./setup`
   c. Enter the following configuration values from the setup:
      - Home Server: Enter the FQDN of your the FortiNAC Application Server
      - Allowed Servers: Enter any other FortiNAC servers the Agent would need to communicate with.
      - Restrict roaming: Restrict the agent to only communicate with servers listed in the Home Server and Allowed Servers fields.
3. To start the Linux Persistent Agent service type: `$ sudo service bndaemon start`

Right-click options

Option	Description
About	Displays the agent version, copyright, and other information.
Show Messages	Displays the list of the messages sent through the Persistent Agent that have been received by the host. If any URLs have been sent separate from a message, a list of these are also be displayed.
Login	Appears when host is in isolation requiring registration or authentication. When selected, opens a login dialog.
Log off the Network	Appears when host is logged in and authenticated. When selected, the host is logged off the network and is placed into isolation requiring authentication.
Show Network Access Status	Appears when the host is isolated for remediation or being disabled. When selected, the user is sent to either the remediation page for rescan or the dead end page if disabled.

Host firewall

When a host is running a firewall (iptables), the Persistent Agent will need the ports 4567, 4568 open in order to communicate with FortiNAC.

Uninstall

On the host, use the following commands to remove the Persistent Agent:

1. To uninstall rpm, type: `$ sudo rpm -ev bni-persistent-agent`
2. To uninstall deb, type: `$ sudo dpkg --purge bni-persistent-agent`

Using the Persistent Agent

If you have chosen to use the Persistent Agent to scan Windows, macOS, or Linux systems, hosts connecting to the network will go through the following process. The PA is downloaded to the host and installed. Once PA is installed it runs in the background and communicates with FortiNAC at intervals established by the Network Administrator.

The Persistent Agent will not detect the addition of a guest to a virtual host record unless the "Append to Host" or "Register as New Host" options are enabled in the VM Detection settings, and the port they are connected to may be subject to isolation and registration policies. See Security management on page 140.

The Persistent Agent only works with the FortiNAC Control Server and FortiNAC Application Server pair or the FortiNAC Server. If the FortiNAC Control Server is not paired with the FortiNAC Application Server, the Dissolvable Agent must be used.

Registration

When an unknown host connects to the network and attempts to access the Internet, an entry in the DNS server redirects the host to the Login page for registration.

The Persistent Agent can also be used to register hosts passively (behind the scenes).

To begin the registration and policy check process, the user on the unknown host does the following:

1. Enter the User Name.
2. Enter the Password.
3. Click Download.
4. Save the file to the Desktop as directed by the browser download functionality or runs the file.

If a Persistent Agent is being used, the host must install the Persistent Agent the first time. If a Dissolvable Agent is being used, the agent runs without installing any files.

Results

Once the security check has completed, if the host failed to meet the security policy, a results page shown in a browser lists the items that failed and passed.

You can configure a link that the user can click that provides information about items that failed and what to do to correct the problem. Enter this link when you configure the policy. See Add or modify a scan on page 433 for more information.

If you do not provide a link, modify the failure page to provide information for the user to correct the problem and find assistance.

Rescan

Once the user has corrected any issue(s) that caused the failure, the Persistent Agent security check must be run again.

1. Open a browser window.
2. Host is placed in Remediation.
3. Click on the link associated with the security policy.
4. Click Rescan.

This process may need to be completed again if additional issues remain that cause the host to fail the security policy.

Successfully registered notification

Once all the items causing the host to fail the security policy have been corrected, the host is registered and the Success message window is displayed.

Using Windows domain logon credentials

With Persistent Agent Version 2.2.2 and higher you can configure FortiNAC to authenticate users with their Windows domain logon credentials eliminating the need for the Persistent Agent to ask for credentials. You must use Active Directory and Group Policy Objects to manage your Windows hosts. To implement this feature your system must meet the following requirements:

- **Active Directory** — You must be using Active Directory to authenticate users. The Directory must be configured in **System > Settings > Authentication > LDAP**. See Directories on page 79 for configuration information.
- **Authentication** — In **Policy > Policy Configuration**. Under **Authentication**, click **Configuration**. Click **Add**, or select a configuration and click **Modify**. Make sure that **Enable Authentication** is selected.
- **Passive Agent Configuration** — At least one Passive Agent rule or configuration must be set up. The Persistent Agent uses this configuration to process session notification information from the host. Navigate to **Policy > Passive Agent Configuration**. Add a configuration that is enabled and that applies to a directory group that contains all the users for whom this feature is being implemented. If you plan to have the Persistent Agent register hosts as devices, you must also include that setting in the Passive Agent Configuration you are creating.
- **Persistent Agent Properties** — Navigate to **Policy > Persistent Agent Properties**. Under **Status Notifications**, disable the **Provide a Log Off** functionality from the tray icon for authenticated hosts option. This can remain enabled, however, if the user were to log off using the Persistent Agent icon, the host would be automatically logged on again the next time the server requests credentials. If you plan to have the Persistent Agent register hosts as devices, click the **Credential Configuration** tab and enable the **Register as Device** option.

  If you want to prevent users from being able to log off the network using the Agent Icon you must also disable the Display a special "Needs to Authenticate" icon when a host needs to authenticate. option on the Status Notification Tab. This is optional, not required.
- **GPO Templates** — Download and install the latest Persistent Agent Administrative Templates.

  After installing the templates on your Windows server you must modify the following Persistent Agent Template settings:
  - **Host Name** — Ensures that the Persistent Agent is communicating with the correct FortiNAC server.
  - **Login Dialog** — Allows you to enable or disable the Login dialog that is presented by the Persistent Agent during authentication. Disable the Login dialog to use the users' Windows login credentials.

GPO settings for high availability

If you are using Persistent Agent version 3.X or higher, this issue does not apply.

For the Persistent Agent to communicate with a FortiNAC appliance the agent must know the name or IP address of that appliance. Group Policy Objects can leverage templates distributed by Fortinet to modify the host registry and provide the Persistent Agent with the host name of the FortiNAC appliance. However, in a High Availability environment, the agent must also know how to communicate with the secondary server in the event of a failover.

High Availability or redundant servers can be set up in two ways. In an L2 or single subnet configuration, the FortiNAC servers share a virtual IP address and server name. In a failover situation, the transition is seamless because agents continue to communicate with the same virtual IP address or name no matter which FortiNAC appliance is in control. In an L3 environment where redundant servers are on different subnets, there is no shared IP address. The agent must know how to connect to both servers.

If you are running in a High Availability environment, you must analyze the HA configuration, the version number of the agent being used and the method used to establish communication between the FortiNAC appliance and the Persistent Agent. You may need to alter the way you inform the Persistent Agent of the server name or IP address.

When a template is served to a host, the template writes to the following keys in the Windows registry:

- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Bradford Networks\Persistent Agent
- HKEY_LOCAL_MACHINE\SOFTWARE\Bradford Networks\Client Security Agent

The Persistent Agent key takes precedence over the Client Security Agent key. However, in an L3 environment with redundant servers on different subnets, if there is a fail over, FortiNAC can only update the value in the Client Security Agent key. Since the Persistent Agent key takes precedence, the agent does not communicate with the correct server.

The sections below provide an overview of successful configuration combinations for Persistent Agent / Server communication in a High Availability environment. This is particularly important when hosts are configured using templates served by Group Policy Objects to modify the host registry.

When FortiNAC is running on a Control Server/Application Server pair, the Persistent Agent communicates with the Application Server. Be sure to use the correct server name or IP address during configuration.

L2 high availability

In this environment, redundant servers share a virtual IP address and a server name. There are two options for configuring communication between the agent and the FortiNAC server.

Option 1: Use GPO to deliver a template

Use GPO to deliver a template to the host where the Agent is installed. All values in the template, including ServerIP can be configured. If the primary FortiNAC server fails over, the secondary server uses the same server name and virtual IP address, therefore, no change is required in the host registry.

Option 2: Use Persistent Agent properties

Navigate to **Policy > Persistent Agent Properties > Security Management**. Add the shared name of the primary and secondary FortiNAC servers. See Security management on page 140.

L3 high availability

In this environment, redundant servers are on different subnets and have different IP addresses. In this scenario, there is only one option.

You can use GPO to deliver a template to the host where the Persistent Agent is installed, however, you must NOT configure ServerIP in the template. It is important that the associated registry keys not be configured on the host.

You must navigate to **Policy > Persistent Agent Properties > Security Management**. Add the server name of both the primary and secondary FortiNAC servers.

In the event of a failover, the name of the secondary FortiNAC server is pushed to the Persistent Agent.

Certificate validation

The Persistent Agent can be configured using a Windows custom scan to validate the certificate on a host against the certificate provided by the administrator on Active Directory.

Persistent Agent 3.5 or higher must be installed.

The application server must have access to the web server.

The Cert-Check Custom Scan allows the Persistent Agent to verify whether the certificate on the host matches the certificate on the network. The Persistent Agent scans the host and sends the timestamp, client certificate, and signature to the server. The server then completes the following process:

- Validates the certificate against a trusted Certificate Authority that is provided by the administrator
- Verifies the revocation against the CRL (Certificate Revocation List) provided through the LDAP or web server.
- Verifies the timestamp is within five minutes of receipt by the server.
- Verifies the signature with the certificate's public key.
- Updates the scan result to change the default failure state to success, and updates the overall result from failure to success, if necessary.

Implementation

1. Upload and install the certificate from a trusted Certificate Authority (CA) for validation by the server, and select **Persistent Agent Cert Check** as the target. See SSL certificates on page 523.
2. Create a Windows Cert-Check Custom Scan to verify the certificate on the host. See Windows on page 450.
3. Add the Cert-Check Custom Scan to a scan that is enabled within your Endpoint Compliance Policy. See Custom scan options - scan level on page 449.

Upgrade the Persistent Agent

Global update

Hosts on your network that have a Persistent Agent installed can be updated automatically using the settings in **System > Settings > Persistent Agent > Agent Update**. See Global updates on page 134 for instructions.

Update on a single host

Hosts on your network that already have a version of the Persistent Agent installed can be updated individually. The FortiNAC administrator may choose to selectively update a few hosts to test a new version of the Agent or to install an earlier version of the agent on an older host.

Clients upgrading the Persistent Agent must have access to Port 80 on the FortiNAC appliances.

The update is sent immediately to the host. The host must be running and connected to the network for the update to be successful.

If the host has software installed to reset the host to its original configuration after a re-boot, the agent reverts to the previous version. The software must be disabled before updating the Agent.

A special group, **Global Agent Update Exceptions**, has been created to stop selected hosts from being automatically updated. Any host in this group is not updated. If you update a host to an agent version that is different from the version selected for Global Agent Updates, this host is automatically moved to the Global Agent Update Exceptions Group. If necessary, this host must be manually removed from that group. See Group membership on page 811 for instructions.

To select and update a host:

1. Click **Hosts > Hosts View**.
2. Right–click on the host and select **Host Properties**.
3. A window displays containing the host information. If the host has more than one MAC Address, all are displayed.
4. In the Policy Agent/Access section of the window, locate the **Agent Version** field. The agent version that is currently installed on the host is displayed.
5. Click the **Update** button.
6. Select the new Persistent Agent version from the drop-down list and click **OK**.

When the **OK** button on the Update window is clicked FortiNAC “polls” the host to determine the point at which the Agent Version number changes to the new version. This “polling” times out after a minute or when the new version number is returned. If the update times out without returning a new version number, a message that the update has failed is displayed. If the new version number is returned, a message that the update was successful is displayed.

No events are generated based on the success or failure of an individual host update.

Logging

Persistent Agent Versions 2.2.0.114 and higher have a logging feature for Persistent Agent Packet activity on the host. The log file automatically rotates every 24 hours based on the installation time of the Persistent Agent. The Log file is stored in the following locations:

Windows

For Windows Operating systems look in the Common Application Data directory at `%ProgramData%\Bradford Networks\bndaemon_log.txt`

macOS

For macOS log messages are sent to the system log via the "debug" syslog priority.

- On 10.5 and 10.6 messages show up in `system.log`
- On 10.4 these messages show up in `console.log`

Linux

- On Linux (Debian Based), these messages show up in `/var/log/syslog`
- On Linux (Red Hat Based), these messages show up in `/var/log/messages`

Time stamps included in the log file are displayed in UTC time. Coordinated Universal Time (UTC) is a high precision atomic time standard that corresponds roughly to Greenwich Mean Time.

Mobile Agent

Mobile Agent is an application that works on Android devices to identify them to FortiNAC, assist with authentication and provide an inventory of installed Apps. The Mobile Agent can scan the device for indicators of rooting. Rooting is a process allowing users of devices running the Android operating system to attain privileged control (known as "root access") within Android's subsystem.

FortiNAC will only require or respond to a Mobile Agent if the Policy that applies to the host includes settings requiring the Mobile Agent. If for any reason a mobile device had a Mobile Agent installed, the user would not be able to register the device unless the policy assigned included the Mobile Agent. If the policy assigned is set to None-Deny, the mobile device is not allowed to register. If the policy is set to None-Bypass, the mobile device can be registered but not using the installed Mobile Agent.

The Mobile Agent does work within the context of FortiNAC's VPN integration.

Setup Requirements

- Make sure the latest Agent package is installed on the FortiNAC server.
- Add SRV records to your production DNS server that allow the agent to locate the FortiNAC Server or Application server to which it should connect. See and .
- The Mobile device must be running Android operating system 2.3.3 or higher.
- Users can download the agent one of two ways:
  - If the Android device is configured to allow downloads from unknown sources, the Mobile Agent can be downloaded from the captive portal. For example, configure an Android phone by choosing Settings from a Home screen, then selecting Applications and enabling the Unknown Sources option.

  - If the Android device does not allow downloads from unknown sources, the Mobile Agent must be downloaded through Google Play.
- FortiNAC appliance must be configured with SSL and must have a valid third party SSL certificate from a certificate authority. A self-signed certificate cannot be used. See Agent server communications on page 521.
- Create an Endpoint Compliance Policy for Android devices to control whether or not an agent is required and whether or not the device can register. See Endpoint compliance policies on page 415.
- To prevent Rooted devices from registering, enable Root Detection in the Scans used for Mobile devices. See Add or modify a scan on page 433. When Root Detection is not enabled, the Mobile Agent still determines whether the device is rooted, but allows the device to register and appends (Rooted) to the operating system information displayed in the Host View.

Root Detection happens only during registration. If a user registers a device and then later alters that device causing it to be Rooted, FortiNAC is not notified. You may want to age these devices out of the database quickly so the user is forced to re-register periodically.

- Enable the **Potential Rooted Device** event and alarm to be notified when the Mobile Agent determines that the devices may be rooted. The event message contains the username of the user and the MAC addresses of the device. See Enable and disable events on page 857.
- Mobile device users are authenticated based on the settings for Standard User Login. Navigate to **System > Portal Configuration > Content Editor**. In the tree on the left select **Global > Settings** and verify that the Standard User Login Type is correct.
- You can modify the default text shown in the captive portal as mobile device users connect to the network. Navigate to **System > Portal Configuration > Content Editor**. In the tree on the left scroll to the **Registration > Mobile Agent Download** section to review or modify the download page. In the tree on the left, scroll to the Agent > Mobile section to review or modify the Login page.

Notes

- If the Mobile device attempts to connect to the network but never reaches the agent download page and is never prompted for credentials, verify that the device is receiving an IP address within the Registration VLAN. Verify that the device is connected to the correct SSID.
- If the user receives a message indicating that they do not have rights to access the network, verify that there is a Policy in place for mobile devices and that it is configured correctly.

Agent server communications

The sections below provide instructions for securing communications between the agent and the FortiNAC server with a trusted SSL certificate, setting up communication between the agent and the server, and the host registry settings or preferences that can be modified to customize Persistent Agent behavior.

Implementation

Update FortiNAC

Requires FortiNAC version 5.3.3 or higher to enable security.

You must have the latest Auto-Definition files installed. See Auto-Definition updates on page 549.

Certificates

You must have a separate certificate for each FortiNAC server that runs the captive portal, such as the FortiNAC Application server or the stand-alone FortiNAC Server.

Certificates must be from a trusted certificate authority, such as VeriSign, Thawte, or GeoTrust.

Self-signed certificates are not recommended. If you use a self-signed certificate, end users will receive constant pop-up warnings indicating that the site is not secure and asking them to confirm that they wish to continue. In addition, the Mobile Agent absolutely require a Certificate from a trusted certificate authority. The Mobile Agent cannot communicate with FortiNAC when Self-signed certificates are used.

If you already have a certificate that you are using to secure your portal, you can import that certificate into the FortiNAC server configuration and use it for both the portal and agent/server communications.

If you do not have a certificate for your portal, generate a certificate request and purchase a certificate. When the certificate is returned, import that certificate into the FortiNAC server configuration and use it for both the portal and agent/server communications.

Persistent and Dissolvable Agents Version 3.1 or higher and the Mobile Agent require the use of a certificate.

The 3.x Persistent Agent communication method requires not only SSL certificates be installed for the Persistent agent target in FortiNAC, but also the root certificate be installed on the endstation hosting the agent. The Persistent Agent reads all certificates from the trusted root certification authorities store of the system account. If the Certificate Authority is not listed in this store, the Persistent Agent will not trust the connection to FortiNAC and will not communicate.

FortiNAC does not push root certificates to endstations. Root certificates come pre-installed with the host's operating system. Any additions or updates to root certificates are distributed via the host's OS updates.

For instructions on generating and installing SSL certificates, see the document entitled **FortiNAC SSL Certificates How To**.

DNS server configuration

If you use agents for macOS and some Linux systems, using a .local suffix in Domain fields in the Configuration Wizard may cause communications issues.

Example:

Incorrect DNS suffix for reg: `tech-reg.megatech.local`
Correct DNS suffix for reg: `tech.megatech-reg.edu`

- On upgrade to V6.0 or higher, SRV records indicating the port and FQDN of the FortiNAC appliance where the portal is located are automatically added to the domain.zone.* files for named. These files are created by the Configuration Wizard, which can also add the SRV records to the domain.zone.* files during the initial appliance configuration.
- If you are unable to configure the agent through Agent Configuration, the same SRV records may be added to the corporate production DNS servers. Agents can then query the DNS servers to determine the FortiNAC server with which they should communicate.
- Any references to the FortiNAC server's FQDN in DNS must match the name in the certificate used to secure the

portal.

See DNS server configuration on page 531 and Agent server discovery on page 536.

Server configuration

If the time on FortiNAC is inaccurate and is updated after Agent Security is enabled, Agents may ignore packets received from the server until the agent is restarted because the new timestamp deviates significantly from previous timestamps.

Make sure that the server is configured to use NTP for time synchronization. Go to **System > Settings > System Management > NTP and Time Zone** to configure the NTP server. This is typically set during installation.

Host configuration

- Host machines should not have the fully qualified domain name of the FortiNAC Server or Application Server in the hosts file on the hard drive. Typically network users would not have this information in their hosts file. However, administrator users may have the FQDN in their hosts file to accommodate accessing java applets. Modify the hosts file to use the short name, such as, qa233 instead of qa233.example.com. If a host has the FQDN in its hosts file, the Persistent Agent cannot communicate with the FortiNAC Server or Application Server and cannot register the host.
- For Windows hosts, download and configure Administrative Templates for Group Policy Objects to update the registry on each host with values that pertain to agent security.
- For macOS hosts, update Preferences to provide security values to the agent.

See Persistent Agent on Windows on page 538.

Agent configuration

- Requires Agent version 3.0 or higher. Download the latest Agent Package from Fortinet to your FortiNAC server.

SSL certificates

The following components of FortiNAC are able to utilize SSL Certificates for encrypting communications:

- Administrative User Interface: browser traffic between user managing FortiNAC through the UI and the FortiNAC Control Server.
- Persistent Agent: traffic between Persistent Agent (PA) installed on a host and the FortiNAC Application Server. Functions that utilize this communication include, but are not limited to, registration/authentication and scanning.
- Portal: browser traffic between host in isolation using the captive portal (Registration, Remediation, Authentication, Dead End) and the FortiNAC Application Server. This is also used for traffic between the Dissolvable Agent (DA), Mobile Agent, and the Application Server.

These components are secured independently of each other. However, the same SSL Certificate can be used if multiple components are to be secured.

The following sections describe how to obtain, upload, and renew SSL certificates.

Implementation considerations

If you are running a High Availability (HA) configuration using a shared IP address, the certificate information for the Portal target is replicated from the primary server to the secondary server. If you are running a HA configuration where primary and secondary servers are on separate subnets (L3 HA) contact Support for assistance.

You may act as your own Certificate Authority (CA) and use your own internal certificate, as long as all systems in your domain use the same certificate.

The Persistent and Dissolvable Agents cannot use the Self-Signed Certificate.

Wildcard certificates

Wildcard certificates may be imported to secure the Captive Portal. They can either be generated from a Certificate Signing Request (CSR) created via FortiNAC or a third party.

To generate a wildcard CSR using FortiNAC, see Obtaining an SSL certificate from a Certificate Authority (CA) on page 525

To use a wildcard certificate already generated, proceed to Upload a certificate received from the CA on page 528.

Ensure the following when importing a wildcard certificate:

- The wildcard private key cannot be password protected.
- The actual Fully-Qualified Host Name must be entered in the Fully-Qualified Host Name Field in the General tab under **Go > Tasks > Portal Configuration**. Entering the wildcard name in this field will cause the application of the certificate to fail.

Subject Alternative Name (SAN) certificates

A SAN certificate can be used to secure multiple host names and/or IP addresses. For example, in a Layer 2 HA environment the virtual, primary, and secondary appliance host names and their corresponding IP addresses can all be secured with one certificate.

To generate a SAN Certificate using FortiNAC, see Obtaining an SSL certificate from a Certificate Authority (CA) on page 525.

Create a keystore for LDAP

If you choose to use SSL or TLS security protocols for communications with your LDAP directory, you must have a security certificate. You must obtain a valid certificate from a Certificate Authority. That certificate must be saved to a specific directory on your FortiNAC.

SSL or TLS protocols are selected on the Directory Configuration window when you set up the connection to your LDAP directory. Follow the steps below to import your certificate. You should be logged in as root to follow this procedure.

1. When you have received your certificate from the Certificate Authority, copy the file to the /bsc/campusMgr/ directory on your FortiNAC server.
2. Use the keytool command to import the certificate into a keystore file.

   For example, if your certificate file is named MainCertificate.der, you would type the following:

```
keytool -import -trustcacerts -alias <MyLDAP> -file MainCertificate.der -
keystore .keystore
```

Depending on the file extension of your certificate file, you may need to modify the command shown above. For additional information on using the keytool key and certificate management tool go to www.oracle.com.

3. When the script responds with the Trust this certificate? prompt, type Yes and press Enter.
4. At the prompt for the keystore password, type in the following password and press Enter: `^8Bradford%23`
5. To view the certificate, navigate to the `/bsc/campusMgr/` directory and type the following: `keytool -list -v -keystore .keystore`
6. Type the password used to import the certificate and press Enter.

The keystore is cached on startup. Therefore, it is recommended that you restart FortiNAC after making any changes to the keystore.

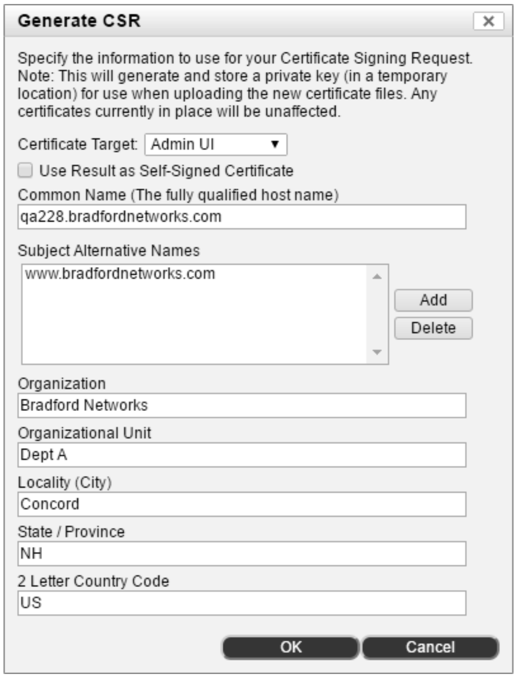
Obtaining an SSL certificate from a Certificate Authority (CA)

If you do not have a certificate, you must obtain a certificate from a CA.

To obtain a valid third party SSL certificate from a CA, you must generate a CSR and send it to the CA.

To generate a CSR, and self-signed certificate:

1. Select **System > Settings**.
2. Expand the **Security** folder.
3. Select **Certificate Management** from the tree.
4. Click **Generate CSR**.



Generate CSR

Specify the information to use for your Certificate Signing Request. Note: This will generate and store a private key (in a temporary location) for use when uploading the new certificate files. Any certificates currently in place will be unaffected.

Certificate Target: Admin UI

□ Use Result as Self-Signed Certificate

Common Name (The fully qualified host name): qa228.bradfordnetworks.com

Subject Alternative Names: www.bradfordnetworks.com

Organization: Bradford Networks

Organizational Unit: Dept A

Locality (City): Concord

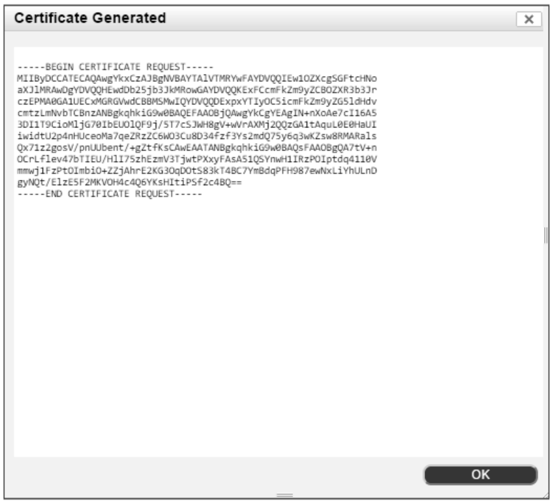
State / Province: NH

2 Letter Country Code: US

5. Select the certificate target (the type of certificate you want to generate).
   - Select **Admin UI** to generate a CSR for the administrative user interface.
   - Select **Persistent Agent** to generate a CSR for the PA communications.
   - Select **Portal** to generate a CSR to secure the captive portal and DA communications.
   - Select **RADIUS Server** to generate a CSR for integrated FortiNAC RADIUS server set to use 802.1x and PEAP.

The Private Key that corresponds with the CSR is stored on the appliance. Once the SSL Certificate is uploaded, to view the Private Key, click the **Details** button and select the **Private Key** tab.

6. Enter the Common Name (Fully-Qualified Host Name). This is the Host Name to be secured by the certificate. If generating a wildcard CSR, enter the desired domain specifying the wildcard in the Common Name Field (Example: *.example.com).
7. Enter the Subject Alternative Names (leave blank if not requesting a SAN certificate). Click **Add** to enter each additional host name and/or IP address.
8. Enter the remaining information for the certificate in the dialog box:
   - **Organization**: The name of the server's organization.
   - **Organizational Unit**: The name of the server's unit (department).
   - **Locality (City)**: The city where the server is located.
   - **State/Province**: The state/province where the server is located.
   - **2 Letter Country Code**: The country code where the server is located.
9. Click **OK** to generate the CSR.



```
-----BEGIN CERTIFICATE REQUEST-----
MIIByDCCATECAQAwgYkxCzAJBgNVBAYTAlVTMRYwFAYDVQQIEw1OZXcgSGFtcHNo
aXJlMRAwDgYDVQQHEwdDb25jb3JkMRowGAYDVQQKExFCcmFkZm9yZCBOZXR3b3Jr
czEPMA0GA1UECxMGRGVwdCBBMSMwIQYDVQQDExpxYTIyOC5icmFkZm9yZG5ldHdv
cmtzLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAgIN+nXoAe7cI16A5
3DI1T9CioMljG70IbEUOlQF9j/5T7cSJWH8gV+wVrAXMj2QQzGA1tAquL0E0HaUI
iwidtU2p4nHUceoMa7qeZRzZC6WO3Cu8D34fzf3Ys2mdQ75y6q3wKZsw8RMARals
Qx71z2gosV/pnUUbent/+gZtfKsCAwEAATANBgkqhkiG9w0BAQsFAAOBgQA7tV+n
OCrLflev47bTIEU/HlI75zhEzmV3TjwtPXxyFAsA51QSYnwH1IRzPOIptdq4110V
mmwj1FzPtOImbiO+ZZjAhrE2KG3OqDOtS83kT4BC7YmBdqPFH987ewNxLiYhULnD
gyNQt/ElzE5F2MKVOH4c4Q6YKsHItiPSf2c4BQ==
-----END CERTIFICATE REQUEST-----
```

10. Copy the section with the certificate request to include the following:

```
-----BEGIN CERTIFICATE REQUEST-----
...Certificate Request Data...
-----END CERTIFICATE REQUEST-----
```

11. Paste it into a text file, and save the file with a .txt extension. Note the location of this file on your PC.

Make sure there are no spaces, characters or carriage returns added to the Certificate Request.

12. Send the Certificate Request file to the CA to request a Valid SSL Certificate.

Important Notes:

- Do not click OK in the Generate CSR screen after saving the Certificate Request file and sending to the CA. Each time OK is clicked on the Generate CSR screen, a new CSR and private key are created, overwriting any previous private key. Consequently, if a Certificate Request file has been submitted to the CA, and the OK button has been clicked since the original Certificate Request was generated, the returned certificate will not match the current private key, and a new request will have to be issued and sent to the CA.
- Not all Certificate Authorities ask for the same information when requesting a certificate. For example, some CA's ask for a server type (Apache, etc) while others do not. FortiNAC requires a non-encrypted certificate in one of the following formats:
  - PEM
  - DER
  - PKCS#7
  - P7B

  This will allow the certificate to be applied to any of the desired components.

  If the certificate is in PEM format, opening the certificate in a text editor should look something like the following format:

```
-----BEGIN CERTIFICATE1-----
fjkghwjernlsfuigylerkjlkfjnu23jnlkjbliu5ghl6kh4
fjkjlkfjnu23jnlkjbliu5ghl6khkghwjernlsfuigyler4
ghwjernlsfuigylerkjlkfjnu23jnlkjbliu5fjkghl6kh4
-----END CERTIFICTATE1-----
-----BEGIN CERTIFICATE2----
```

```
fjkghwjernlsfuigylerkjlkfjnu23jnlkjbliu5ghl6kh4
fjkjlkfjnu23jnlkjbliu5ghl6khkghwjernlsfuigyler4
ghwjernlsfuigylerkjlkfjnu23jnlkjbliu5fjkghl6kh4
-----END CERTIFCATE2-----
```

Certificate requests generated on FortiNAC use the SHA1 RSA encryption signature. However, certificates with SHA2 encryption can be requested using this CSR.

- Agent versions prior to 3.1.5 are not compatible with SHA2. Contact Support to verify appropriate SHA version based on current deployment.
  - Select **Admin UI** to generate a CSR for the administrative user interface.
  - Select **Persistent Agent** to generate a CSR for the PA communications.
  - Select **Portal** to generate a CSR to secure the captive portal and DA communications.

The Private Key that corresponds with the CSR is stored on the appliance. Once the SSL Certificate is uploaded, to view the Private Key, click the **Details** button and select the **Private Key** tab.

Upload a certificate received from the CA

Upload the valid SSL certificate to the appliance when the certificate file is returned from the CA. Certificate files can be returned to you in one of several configurations. Depending upon the CA, one or multiple certificate files may be returned.

1. Save the file(s) received from the CA to your PC.
2. Select **System > Settings**.
3. Expand the **Security** folder.
4. Select **Certificate Management** from the tree.
5. Click **Upload Certificate**.
6. Select the target where the certificate will be uploaded:
   - Select **Admin UI** to install the certificate for the administrative user interface.
   - Select **Persistent Agent** to install certificate for the PA communications.
   - Select **Portal** to install the certificate to secure the captive portal.
7. Select one of the following:
   - **Use Private Key from Last Generated CSR** to use the key from the most recent CSR for the selected target.
   - **Reuse Private Key from Existing Certificate** to use the private key for the certificate currently in use. This option is for renewing an existing installed certificate.
   - **Upload Private Key** to upload a key. Click **Choose** to find and upload the private key.
8. Click the Choose File button to find and select the certificate to be uploaded. Users can also upload CA certificates and CA bundles.

Upload any relevant intermediate certificate files needed for the creation of a completed certificate chain of authority. The Certificate Authority should be able to provide these files. Without a complete certificate chain of authority, the target functionality may produce error/warning messages.

9. Click the **Add Certificate** button if multiple certificates were returned. Use this to enter each additional certificate file.
10. Click **OK**.

Copying a certificate to another target

If the certificate is intended to be used for multiple targets, copy the certificate to the new target:

1. Highlight the target with the desired certificate installed.
2. Click **Copy Certificate**.
3. Select the new target from the drop-down menu.
4. Click **OK**.

Activating certificates

Certificates for the administrative user interface and Persistent Agent are activated automatically upon installation. No further action is required.

1. Navigate to **System > Settings**.
2. Expand the **Security** fold and then click **Portal SSL**.
3. In the **SSL Mode** field, select **Valid SSL Certificate**.
4. Click **Save Settings** (this may take several minutes).

Prevent the use of port 8080

Modify server.xml file

To ensure that users connect to the Admin UI using a secure port, you must modify the server.xml file.

1. Log in as `root`.
2. Navigate to the following directory: `/bsc/services/tomcat-admin/conf`
3. Use vi or another editor to open the server.xml file.
4. Locate the line shown below.
   ```
   <Connector port="8080" redirectPort="8443" address="nac" />
   ```
5. Modify the line as follows to comment it out:
   ```
   <!-- <Connector port="8080" redirectPort="8443" addresss="nac" /> -->
   ```
6. Save the changes to the server.xml file.
7. Restart Tomcat.
8. For your server to use the new certificates and acknowledge the changes made to server.xml, you must restart Tomcat. Type the following at the prompt:
   ```
   service tomcat-admin restart
   ```

Modify web.xml file

To ensure that users connect to the Admin UI using a secure port, you must modify the web.xml file.

This change must be made after each upgrade because the web.xml is overwritten during the upgrade. A README should be put in place as a reminder to follow this procedure upon upgrade.

1. Use vi or another editor to open the following file in a text editor:
   `/bsc/campusMgr/ui/ROOT/WEB-INF/web.xml`
2. Locate the security-constraint for ALL.
3. Change the transport-guarantee to CONFIDENTIAL. This value matches the API security-constraint.
4. Save the changes to the file.

Create expiration warning alarms

Three events are enabled by default in FortiNAC:

- **Certificate Expiration Warning**: Generated when a certificate is due to expire within 30 days.
- **Certificate Expiration Warning (CRITICAL)**: Generated when a certificate is due to expire within 7 days.
- **Certificate Expired**: Generated when a certificate has expired.

You must create alarms to send emails when these events are generated.

1. Navigate to **Logs > Event to Alarm Mappings**.
2. Create one alarm for each event with the following settings:
   - Select the **Notify Users** setting.
   - Select the type of messaging (Email or SMS) and admin group desired to be notified.
   - Set the **Trigger Rule** to **One Event to One Alarm**.
3. For detailed instructions on creating alarms, see Add or modify alarm mapping on page 892.

Renew a certificate

SSL certificates must be renewed periodically or they expire. However, the existing certificate must be used until the new one arrives. Some Certificate Authorities allow managing certificates such that it can be renewed without generating a new request file. In these cases, the private key will remain the same and the new certificate can be imported when it arrives.

1. Save the file(s) received from the CA to your PC.
2. Select the target where the certificate will be uploaded. See Step 6 under Upload a certificate received from the CA on page 528.
3. Select Reuse Private Key from Existing Certificate to use the private key for the certificate currently in use. See Step 7 under Upload a certificate received from the CA on page 528.
4. Follow Steps 8-10 under Upload a certificate received from the CA on page 528 to complete the process.

Troubleshooting

If something is wrong with the uploaded certificate files, FortiNAC will display an error and will not apply the certificate.

Common causes for upload errors

- The wildcard name (e.g., *.example.com) was placed in the Fully-Qualified Host Name Field in the Portal SSL view under System > Settings > Security. To correct, change the entry to the true Fully-Qualified Host Name and click Save Settings.
- There are extra spaces, characters, and/or carriage returns above, below, or within the text body of any of the files.
- The certificate was not generated with the current key and there is mismatch.

  This can happen if the OK button in the Generate CSR screen had been clicked after saving the Certificate Request. Each time OK is clicked on the Generate CSR screen, a new CSR and private key are created, overwriting any previous private key.

  To confirm the certificate and key match, use the following tool:

  https://www.sslshopper.com/certificate-key-matcher.html

  If the key and certificate do not match, generate a new CSR and submit for a new certificate.
- An error displays indicating the private key is invalid. This can occur if the Private Key is not a RSA Private Key. To confirm, (if the certificate is in PEM format), open the certificate in a text editor. If the content looks something like the following:

  ```
  ----BEGIN PRIVATE KEY----
  MIIEowIBAAKCAQEAtozSKRv4mpPVk0L4Xz2RzadYym5pRH+Cp1du4uJ2yGKepFmF
  HoB/yOuBt0PAJz9SAT+CkK7j5ocWbAlkjtZxdSs5T2aABWIWTmu0l5T8GYD6KQ9T
  ----END PRIVATE KEY----
  ```

  then the key will need to be converted to a RSA key.
- The following error displays in UI: "Unable to update Apache configuration." This can occur if SSH communication is failing (as the appliance establishes a SSH session to restart apache service). If appliance is a pair, verify Control Server can SSH to Application Server. If appliance is a single device, verify appliance can SSH to itself (without being prompted to enter a password).

For additional troubleshooting assistance, contact Fortinet Support.

DNS server configuration

FortiNAC has its own DNS server used to manage page resolution in the captive portal. For secure communications between the agent and the server, this DNS server must contain specific SRV records used by the agent to locate the server while in isolation. Adding these SRV records is handled for you by FortiNAC.

On upgrade to FortiNAC V6.0 or higher, SRV records indicating the port and FQDN of the FortiNAC appliance where the portal is located are automatically added to the domain.zone.* files for named. If this is a new installation, the domain.zone.* files are created by the Configuration Wizard. The Configuration Wizard also adds the SRV records to the domain.zone.* files during the initial appliance configuration. Manual edits to files are not needed and should not be attempted.

If you use agents for macOS and some Linux systems, using a .local suffix in Domain fields in the Configuration Wizard may cause communications issues.

Example:

Incorrect DNS suffix for reg: `tech-reg.megatech.local`
Correct DNS suffix for reg: `tech.megatech-reg.edu`

If you are unable to configure the agent through Agent Configuration, the same SRV records may be added to the corporate production DNS servers. These are particularly important in a High Availability environment because the SRV records provide the agent with a prioritized list of servers with which it can communicate. In a facility were multiple FortiNAC appliances are being managed by a FortiNAC Control Manager, SRV records make it easier for the agent to locate a FortiNAC server.

When using the FortiNAC Control Manager to manage multiple FortiNAC servers, enabling the Require Connected Adapter check box in Security Management eliminates the need to use ACLs to block access to the FortiNAC Application server when the host is connecting on a device managed by a different FortiNAC Control Server/Application Server pair. This setting will require a host reported by the agent to be connected to a device managed by FortiNAC in order to communicate.

To enable the Require Connected Adapter check box, go to **Settings > Persistent Agent > Security Management**.

The agent must be configured with security enabled. Requires Persistent Agent 4.0.3 or higher.

When the Require Connected Adapter check box is not enabled, or for Agent Versions below 4.0.3, you must use ACLs to block access to a FortiNAC Application server when the host is connecting on a device managed by a different FortiNAC Control Server/Application Server pair. For example, assume the host initially connects to the network on Device A which is managed by Server A. When the host later connects to the network on Device B which is managed by Server B, the agent continues to communicate with Server A. If access to Server A is denied, the agent will go through the server discovery process to locate another server.

Entries in DNS are different for each agent. Currently, the DNS mechanism used for the agent to discover the server is used by the Android, Dissolvable and Persistent Agents. As new types of agents are added to FortiNAC you may be required to update DNS SRV records to accommodate them. See Agent server discovery on page 536.

Verify the SRV records

1. Log into the CLI of the FortiNAC appliance that is running the captive portal, typically this is a FortiNAC Application Server.
2. Navigate to the following directory: `/var/named/chroot/etc`
3. There is a special zone file for the Mobile Agent labeled `discovery.portal.bradfordnetworks.com.zone`. Type `ls *.zone` and verify that this file is in the list of files.
4. Type `ls domain.zone.*` to display a list of all of the domain.zone files.
5. Display the contents of one of the files by typing `cat <file name>`, for example, `cat domain.zone.reg.`
6. Within the contents displayed look for the lines beginning with `_bradfordagent`.

If those lines are included in the file, then the SRV records have been added to the domain.zone.* files. You should see records similar to the following:

```
$TTL 15s
example.com.              IN SOA reg.example.com. root.reg.example.com. (
                          1
                          10800
                          3600
                          604800
                          86400
                          )
                IN NS      reg.example.com.
                IN TXT     "Registration Domain"
$ORIGIN example.com.

b._dns-sd._udp  PTR @
lb._dns-sd._udp  PTR  @
_networksentry._tcp  PTR AgentConfig._networksentry._tcp

;Insert agent line here
; Needs to be here for BN_OTHER_HOSTNAME
AgentConfig._networksentry._tcp SRV 0 0 443 servername.domainname.com.
                                TXT path=/registration/agent/config
_networksentry._tcp             SRV 0 0 443 servername.domainname.com.
                                TXT path=/registration/agent/config

_bradfordagent._udp             SRV 0 0 4567 servername.domainname.com.
_bradfordagent._tcp             SRV 0 0 4568 servername.domainname.com.
*.example.com.            IN      A   172.16.28.1
```

Adding a DNS SRV record

DNS servers will vary based on the operating system of the computer used to house them. The example below is for a DNS server running on a Windows operating system with the SRV records added from a command prompt. You may prefer to use another method to add records to your DNS Server.

1. On the Windows Desktop click **Start > Run**.
2. On the **Run** dialog in the **Open** field, type `command` and click **OK**.
3. At the command prompt type the following:

```
> dnscmd /RecordAdd yourdomain.com _bradfordagent._udp.yourdomain.com. SRV 0 0
4567 servername.domainname.com.
```

4. To add the next record type the following:

   ```
   > dnscmd /RecordAdd yourdomain.com _bradfordagent._tcp.yourdomain.com. SRV 0 0
   4568 servername.domainname.com.
   ```

In the commands above yourdomain.com is the zone supplied via DHCP (Connection-specific DNS Suffix on a Windows station in "ipconfig /all" output). servername.domainname.com is the FQDN of the FortiNAC Application Server or server that is running the captive portal. Note that there is a period (.) after .com at the end of the FQDNs and node names.

The two zeros (0) in the example indicate priority and weight of this record. Priority is used when there are multiple servers to which the agent can connect, such as in a High Availability environment.

DNS server examples

From the DNS example in the section above you must include specific entries in your production DNS server. The examples below list each entry and provide notes about its function and the agents affected.

Entry 1

This entry is used only by the Dissolvable Agent Version 3.1 or higher. It is always required.

```
_networksentry._tcp  PTR AgentConfig._networksentry._tcp


AgentConfig._networksentry._tcp SRV 0 0 443 servername.domainname.com.

                                TXT path=/registration/agent/config
```

These lines work together to define the AgentConfig service. The first line indicates the name of the service and sets the type (_networksentry._tcp).

The second and third lines are the SRV record and indicate the FQDN of the server to which the agent will connect. The two zeros (0) in the example indicate priority and weight of this record. Priority is used when there are multiple servers to which the agent can connect, such as in a High Availability environment. 443 is the port and should not be changed. In the example, the name of the server is servername.domainname.com. This must match the name in the valid certificate used to secure the portal. Note that the period (.) at the end of servername.domainname.com. is required. The TXT line contains the path.

The agent uses the information contained in these entries to construct a URL for the server to which it should connect. Using the records shown above the agent would construct the following:

```
https://servername.domainname.com:443/registration/agent/config
```

Entry 2

This entry is used by the Mobile Agent and is always required.

```
_networksentry._tcp.discovery.portal.bradfordnetworks.com             SRV 0 0 443 server-
name.domainname.com.

_networksentry._tcp.discovery.portal.bradfordnetworks.com             TXT path-
h=/registration/agent/config
```

These lines are SRV record and indicate the FQDN of the server to which the agent will connect. They are the detailed version of the lines below that are included in the domain.zone.reg file shown above. It is recommended that you use the detailed entry when editing your production DNS, however, either entry is acceptable.

```
_networksentry._tcp             SRV 0 0 443 servername.domainname.com.

                                TXT path=/registration/agent/config
```

The two zeros (0) in the examples indicate priority and weight of this record. Priority is used when there are multiple servers to which the agent can connect, such as in a High Availability environment. 443 is the port and should not be changed. In the example, the name of the server is servername.domainname.com. This must match the name in the valid certificate used to secure the portal. Note that the period (.) at the end of servername.domainname.com. is required. The TXT line contains the path.

The agent uses the information contained in these entries to construct a URL for the server to which it should connect. Using the records shown above the agent would construct the following:

```
https://servername.domainname.com:443/registration/agent/config
```

Entry 3

This entry must be done on each site that uses the Persistent Agent.

```
_bradfordagent._udp             SRV 0 0 4567 servername.domainname.com.


_bradfordagent._tcp             SRV 0 0 4568 servername.domainname.com.
```

These SRV records indicate the FQDN of the server to which the agent will connect. The two zeros (0) in the example indicate priority and weight of this record. Priority is used when there are multiple servers to which the agent can connect, such as in a High Availability environment. 4567 and 4568 are the ports on which the server listens and should not be changed. In the example, the name of the server is servername.domainname. Note that the period (.) at the end of servername.domainname.com. is required.

This entry is used by the Persistent Agent and is required. The Persistent Agent has other mechanisms for determining where its server is such as registry entries on the host or information contained in Persistent Agent Properties on the server. However, if those options are not available, the Persistent Agent does use DNS to locate a server.

See Agent server discovery on page 536.

Entry 4

These records are used by the Persistent Agent.

In a High Availability environment where redundant servers are not on the same sub-net and there is no shared IP address, you must add SRV records for all of the servers in order by priority. Priority is the first number after SRV in the example. If your High Availability servers share an IP address you do not need to provide these entries. Use the entries for the stand-alone server as shown in the examples above for Entry 1 through Entry 4.

```
_bradfordagent._tcp.example.com   SRV  0 0 4568 primaryas.example.com.

_bradfordagent._udp.example.com   SRV  0 0 4567 primaryas.example.com.

_bradfordagent._tcp.example.com   SRV  1 0 4568 secondaryas.example.com.

_bradfordagent._udp.example.com   SRV  1 0 4567 secondaryas.example.com.
```

Entry 5

These records are used by the Persistent Agent.

In an environment where multiple FortiNAC servers are managed by a FortiNAC Control Manager, the best practice is to set the registry keys via software push. If this is not possible, there should be an entry in DNS for each FortiNAC appliance that runs a captive portal. If all servers are reachable across all segments of the network, you may need to create ACLs that block access for the Persistent Agent from one segment to another. When a host with the Persistent Agent installed moves from one location to another on the network the Persistent Agent will continue to connect to its original FortiNAC server. The agent will not connect to the server that is managing the port to which it is connected. If an ACL denies the Persistent Agent access to a FortiNAC server based on the hosts location on the network, the Persistent Agent will search for a different server.

The following shows DNS configuration entries for two FortiNAC configurations.

```
_bradfordagent._tcp.example.com   SRV   0 0 4568 appserver1.example.com.

_bradfordagent._udp.example.com   SRV   0 0 4567 appserver1.example.com.

_bradfordagent._tcp.example.com   SRV   0 0 4568 appserver2.example.com.

_bradfordagent._udp.example.com   SRV   0 0 4567 appserver2.example.com.
```

In the commands above example.com is the zone. appserver1.example.com and appserver2.example.com are the FQDNs of the FortiNAC Application Servers or servers that are running the captive portal. Note that there is a period (.) after .com. at the end of the FQDNs and node names.

Agent server discovery

Agent server discovery is a mechanism used by different types of agents to determine the identity of the FortiNAC Server or Application Server to which the agent should connect. Some agents use SRV and TXT records contained within both FortiNAC's DNS server (for when agents are in isolation) and your production DNS server. The records used by the Agent for identifying and connecting to the FortiNAC server vary depending on the type of Agent used.

FortiNAC agents discover the FortiNAC Application Server to which they should connect in variety of ways. The discovery process for each agent is outlined in this section.

The FortiNAC Application Server name used by the agent must match the server name in the Certificate securing the appropriate Certificate Target or the agent and the server will not be able to communicate. The Certificate Target used is dependent upon the agent type. Refer to the discovery process below.

Persistent Agent

Persistent Agent v3.0 and higher determines the FortiNAC Application Server to which it should connect in several ways. If you have used the Administrative Templates distributed with FortiNAC and used Group Policy Objects to set registry entries on each host, then the Persistent Agent can use those entries to find the appropriate FortiNAC Application Server.

The Persistent Agent communicates on the following ports:

- udp 4567
- tcp 4568

- tcp 80 (required for upgrades)

The discovery process is as follows:

1. The Persistent Agent starts.
2. The agent checks DNS for SRV records of _bradfordagent._udp.*example.com* and _bradfordagent._tcp.*example.com*.
3. The agent looks at the host registry (Windows), preferences (macOS), or .conf (Linux).
4. First it checks the entry for lastConnectedServer. If lastConnectedServer is set it adds the server to the top of the list.**
5. Then it checks the entry for HomeServer. If HomeServer is set, it adds it to a list.
6. Then the agent checks the entry for AllowedServers. This entry contains a list of additional servers to which the agent can connect. It adds each of these servers to the list.
7. If SRV records are returned, the agent processes them in reverse priority order (highest value first). If homeServer is not already set, the name contained in the SRV response is written to the host registry HKLM\Software\Bradford Networks\Client Security Agent (Windows) or preferences (macOS, Linux).*
8. For each SRV record:
   a. If the name is not already in the list, and restrictRoaming is disabled, the agent adds the name to the top of the list and to the lastConnectedServer value.**
   b. Otherwise, if the name is already in the list, the agent moves the name to the top of the list.
9. Now that the list of servers is complete, the agent tries to connect to each server over SSL/TLS until it successfully connects to one. Unless security is disabled on the agent, this is done over SSL/TLS (requires valid certificate installed for the Persistent Agent Certificate Target).
10. Once the agent has successfully connected to a server, that server will be set to the lastConnectedServer value, and moved to the top of the list.**
11. Once a server has been added to the lastConnectedServer, if restrictRoaming is enabled, it will remain at the top of the list until that server is no longer reachable by the agent. At that point the list will be parsed until the agent connects to a server and then that server will be moved to lastConnectedServer and to the top of the list.**

*registry/preferences settings remain until one of the following occurs:

- Entry is manually changed.
- Agent is uninstalled.
- Agent is updated.

**Requires Agent Version 4.1.4 and higher.

If the agent cannot be configured through Agent Configuration, the same SRV records may be added to the corporate production DNS servers. Agents can then query the DNS servers to determine the FortiNAC server with which they should communicate.

Mobile Agent

Mobile Agent 3.0 and higher determines the FortiNAC Application Server to which it should connect by checking DNS as follows:

1. The Mobile Agent starts.
2. It checks DNS and is directed to a service type _networksentry.tcp called AgentConfig.
3. It checks the SRV record for that service type for the server to which it should connect.

4. It connects to the FortiNAC Application Server over SSL/TLS (requires valid certificate installed for the Portal Certificate Target).
5. For Mobile Agent 3.1 or higher, if for any reason it cannot connect to the FortiNAC Application Server, a request for the appropriate URL is presented to the user. The URL field will accept an HTTPS address, the FQDN of the server which it uses to create an HTTPS address or an HTTP address. If an HTTP address is used, a warning is displayed asking the user to confirm that they wish to access the server over an insecure connection.

Passive Agent

The Passive Agent determines the FortiNAC Application Server to which it should connect by checking the host registry.

1. The network user logs onto the network.
2. The login triggers a script that is served from a corporate server on the network.
3. The script checks the registry entry ServerURL for the list of servers to which it can connect.
4. It tries the servers in order until it connects to one.

Dissolvable Agent v3.1 and higher

The Dissolvable Agent determines the FortiNAC Application Server to which it should connect by checking DNS as follows:

1. The Dissolvable Agent starts.
2. It checks DNS and is directed to a service type _networksentry.tcp called AgentConfig.
3. It checks the SRV record for that service type for the server to which it should connect.
4. It connects to the FortiNAC Application Server over SSL/TLS (requires valid certificate installed for the Portal Certificate Target).
5. If for any reason it cannot connect to the FortiNAC Application Server, a request for the appropriate URL is presented to the user. The URL field will accept an HTTPS address, the FQDN of the server which it uses to create an HTTPS address or an HTTP address. If an HTTP address is used, a warning is displayed asking the user to confirm that they wish to access the server over an insecure connection.

Dissolvable Agent v3.0 and lower

The Dissolvable Agent knows the FortiNAC Application Server to which it should connect because the server URL is embedded in the agent when it is downloaded.

Persistent Agent on Windows

To take advantage of the Agent Security feature some settings must be configured on the host. Settings for Windows hosts are configured in the registry. Settings for Mac OS X hosts are configured in Preferences.

Administrative templates are used to configure registry settings on Windows endpoints through Group policy objects. These templates can be downloaded from the Agent Distribution view in FortiNAC. Customers can opt to edit registry settings on hosts using another tool.

Requirements:

- Active Directory
- Group Policy Objects
- Template Files From

Templates:

The templates listed below are provided by Fortinet. You must run the installation program for the templates on your Windows server or another Windows system and then copy files to your server. Be sure to select the appropriate MSI for your architecture.

- 32-bit (x86): Bradford Networks Administrative Templates.msi
- 64-bit (x86_64): Bradford Networks Administrative Templates-x64.msi

Install ADMX template

1. In FortiNAC select **Policy > Agent Distribution**.
2. At the top of the Agent Distribution window click either the **32-bit (x86)** or the **64-bit (x86_64)** link to download the appropriate template file.
3. Copy the template file to the domain server or another Windows system with access to the Central Store or local PolicyDefinitions directory.
4. On the Windows system, double-click the msi file to start the installation wizard.
5. Click through the installation wizard.
6. Browse to `Program Files\Bradford Networks\Administrative Templates\admx`.
7. Copy the `Bradford Networks.admx` and `en-US` directory to the `PolicyDefinitions` directory of your central store.
8. Open the Group Policy Editor and navigate to the **Group Policy Object** you want to edit, right-click and select **Edit** to display the **GPO Editor** pane.
9. Browse to **Computer Configuration > Administrative Templates > Bradford Networks**.

Install GPO template

1. In FortiNAC select **Policy > Agent Distribution**.
2. At the top of the Agent Distribution window click either the **32-bit (x86)** or the **64-bit (x86_64)** link to download the appropriate template file.
3. Copy the template file to the domain server.
4. On the domain server, double-click the msi file to start the installation wizard.
5. Click through the installation wizard. At the end, the Microsoft Group Policy Management Console will be launched, if available.
6. Navigate to the **Group Policy Object** you want to edit, right-click and select **Edit** to display the GPO Editor pane.
7. Right-click **Computer Configuration > Administrative Templates** and select **Add/Remove Templates**, shows the current templates pop-up.
8. Click **Add** and browse to `Program Files\Bradford Networks\Administrative Templates`.
9. Select `Bradford Persistent Agent.adm` and click **Open**.
10. Click **Close**, and the administrative templates will be imported into the GPO.

Install an updated template

Occasionally new templates are made available to incorporate additional features. If you already have a Fortinet Administrative Template installed but it does not have Balloon Notifications enabled, follow the instructions below to update it. If you do have Balloon Notifications enabled, see Agent packages on page 226 for instructions on installing an updated template.

1. On your Windows server open the Group Policy Management Tool.
2. Navigate to the **Group Policy Object** you want to edit, right-click and select **Edit** to display the GPO Editor pane.
3. Right-click **Computer Configuration > Administrative Templates** and select **Add/Remove Templates**, to show the current templates pop-up.
4. Select the old template and click **Remove**. Follow the instructions above to install the new template.

Persistent Agent settings

The table below outlines settings that can be configured for the Persistent Agent.

Setting	Options
Allowed Ciphers and Authentication Schemes	Indicates the cipher and authentication schemes that can be used.
CA Trust Length/ Depth	Indicates how deep a chain of certificates to allow between the server's certificate and the certificate's Central Authority.
CA File path	The absolute path to a file containing root and intermediate Certificate Authority certificates in PEM format.
Security	Indicates whether security is enabled or disabled.
Home Server	The fully-qualified hostname of the default server with which the agent should communicate. If this server is not set, it is automatically discovered using Server Discovery. On upgrade, this is populated by the contents of ServerIP.
Allowed Servers	In large environments there may be more than one set of FortiNAC servers. If roaming between servers is limited, list the FQDNs of the FortiNAC Application Servers or FortiNAC Servers with which the agent can communicate.
Restrict Roaming	If enabled, the agent communicates only with its Home Server and servers listed under Allowed Servers. If disabled, the agent searches for additional servers when the home server is unavailable.
Server IP	Server used for communication by agents lower than Agent Version 3.0.
maxConnectInterval	The maximum number of seconds between attempts to connect to FortiNAC. **Data Type**: Integer **Default**: 960
Last Connected Server	Server that the agent last connected to and with which the agent always attempts to communicate first. Protocol configuration change requests are honored only when they are received from this server. If this server is not set, it is automatically discovered using Server Discovery.

Setting	Options
	Requires Agent Version 4.1.4 and higher.

Refer to the Registry Keys section in Administrative templates for GPO on page 501 for more information about the registry keys that correspond to the Persistent Agent settings.

Registry keys

The table below shows the host's registry keys that are not modified by the Group Policy Object. These keys can be set manually.

Key	Value	Data
Persistent Agent		
HKLM\Software\Bradford Networks\Client Security Agent For 64-bit operating systems see Note.	ServerIP	The fully-qualified hostname to which the agent should communicate. **Data Type:** String **Default:** ns8200
HKLM\Software\Bradford Networks\Client Security Agent For 64-bit operating systems see Note.	ClientStateEnabled	**0** — Do not show balloon notifications on status changes. **1** — Show balloon notifications on status changes. **Data Type:** DWORD **Default:** 1
HKLM\Software\Bradford Networks\Client Security Agent	ShowIcon	**0** — Do not show the tray icon. **1** — Show the tray icon. **Data Type:** DWORD **Default:** Not Configured (Tray icon displayed)
HKLM\Software\Bradford Networks\Client Security Agent For 64-bit operating systems see Note.	allowedServers	Comma-separated list of fully-qualified hostnames with the agent can communicate. If restrict roaming is enabled, the agent is limited to this list. The home server does not need to be included in this list (for example, a.example.com, b.example.com, c.example.com). **Data Type:** String **Default:** Empty
HKLM\Software\Bradford Networks\Client Security Agent	homeServer	The fully-qualified hostname of the default server with which the agent should communicate.

Key	Value	Data
		Data Type: String **Default:** Empty
HKLM\Software\Bradford Networks\Client Security Agent	restrictRoaming	**0** — Do not restrict roaming. Allow agent to communicate with any server. **1** — Restrict roaming to the home server and the allowed servers list. **Data Type**: Integer **Default**: 0
HKLM\Software\Bradford Networks\Client Security Agent	securityEnabled	**0** — Disable Agent Security. **1** — Enable Agent Security **Data Type**: Integer **Default**: 1
HKLM\Software\Bradford Networks\Client Security Agent	ServerIP	The fully-qualified hostname to which the agent should communicate. **Data Type:** String **Default:** ns8200
HKLM\Software\Bradford Networks\Client Security Agent For 64-bit operating systems see Note.	maxConnectInterval	The maximum number of seconds between attempts to connect to FortiNAC. **Data Type**: Integer **Default**: 960
HKLM\Software\Bradford Networks\Client Security Agent For 64-bit operating systems see Note.	lastConnectedServer	The last server that the Agent successfully connected to. This will be automatically populated by the agent upon successfully connection to a server discovered through SRV records, or from homeServer, or allowedServers list. This value will remain unchanged until the lastConnectedServer is unreachable by the agent and the agent has connected to another server. Requires Agent Version 4.1.4 and higher. **Data Type:** String **Default:** Empty

On 64-bit operating systems in RegEdit, these registry values will appear in the following key: `HKLM\Software\wow6432node`

Disabling the tray icon via the registry requires the use of Persistent Agent 2.2.3 or higher.

Individual User keys are required only when the user’s settings differ from those for a group of users. Typically, keys are set based on a group of users who have a common Policy using the HKLM\Software\Bradford Networks\Client Security Agent key shown in the table.

Persistent Agent on macOS

To take advantage of the Agent Security some settings must be configured on the host. Settings for Mac OS X hosts are configured in Preferences. At this time we do not have a recommendation for a tool to set preferences.

Security settings

The table below outlines settings that can be configured for Agent Security.

Setting	Options
Allowed Ciphers and Authentication Schemes	Indicates the cipher and authentication schemes that can be used.
CA Trust Length/ Depth	Indicates how deep a chain of certificates to allow between the server's certificate and the certificate's Central Authority.
CA File path	The absolute path to a file containing root and intermediate Certificate Authority certificates in PEM format.
Security	Indicates whether security is enabled or disabled.
Home Server	The fully-qualified hostname of the default server with which the agent should communicate. If this server is not set, it is automatically discovered using Server Discovery. On upgrade, this is populated by the contents of ServerIP.
Allowed Servers	In large environments there may be more than one set of FortiNAC servers. If roaming between servers is limited, list the FQDNs of the FortiNAC Application Servers or FortiNAC Servers with which the agent can communicate.
Restrict Roaming	If enabled, the agent communicates only with its Home Server and servers listed under Allowed Servers. If disabled, the agent searches for additional servers when the home server is unavailable.
Server IP	Server used for communication by agents lower than Agent Version 3.0.
maxConnectInterval	The maximum number of seconds between attempts to connect to FortiNAC. **Data Type**: Integer **Default**: 960
Last Connected Server	Server that the agent last connected to and with which the agent always attempts to communicate first. Protocol configuration change requests are honored only when they are received from this server. If this server is not set, it is automatically discovered using Server Discovery. Requires Agent Version 4.1.4 and higher.

Preferences

The table below shows the modifications that need to be made to the host's Preferences. If you use a tool other than GPO, you must make sure to set the appropriate keys on each host.

Value	Data
allowedServers	Comma-separated list of fully-qualified hostnames with the agent can communicate. If restrict roaming is enabled, the agent is limited to this list. The home server does not need to be included in this list (for example, a.example.com, b.example.com, c.example.com). **Data Type:** String **Default:** Empty
homeServer	The fully-qualified hostname of the default server with which the agent should communicate. **Data Type:** String **Default:** Empty
restrictRoaming	**0** — Do not restrict roaming. Allow agent to communicate with any server. **1** — Restrict roaming to the home server and the allowed servers list. Data Type: Integer Default: 0
securityEnabled	**0** — Disable Agent Security. **1** —Enable Agent Security Data Type: Integer Default: 1
ServerIP	The fully-qualified hostname to which the agent should communicate. **Data Type:** String **Default:** ns8200
ShowIcon	**0** — Do not show the tray icon. **1** — Show the tray icon. **Default:** Not Configured (Tray icon displayed) If both com.bradfordnetworks.bndaemon and com.bradfordnetworks.bndaemon.policy are configured on the system, the com.bradfordnetworks.bndaemon.policy configuration takes precedence over the com.bradfordnetworks.bndaemon configuration.
maxConnectInterval	The maximum number of seconds between attempts to connect to FortiNAC. **Data Type**: Integer **Default**: 960

Value	Data
lastConnectedServer	The last server that the Agent successfully connected to. This will be automatically populated by the agent upon successfully connection to a server discovered through SRV records, or from homeServer, or allowedServers list. This value will remain unchanged until the lastConnectedServer is unreachable by the agent and the agent has connected to another server. Requires Agent Version 4.1.4 and higher. **Data Type:** String **Default:** Empty

There are manual commands that can be used to modify the Preferences as follows:

1. On the macOS host, navigate to a command prompt (Terminal).
2. Before editing the preferences, it is recommended that you unload the launchDaemon plist. Type the following:
   ```
   sudo launchctl unload /Library/LaunchDaemons/com.bradfordnetworks.agent.plist
   ```
3. To read the configuration, type the following:
   ```
   sudo defaults read /Library/Preferences/com.bradfordnetworks.bndaemon
   ```
4. To write configuration values use the table above for the value names and type a command similar to the following:
   ```
   sudo defaults write /Library/Preferences/com.bradfordnetworks.bndaemon
   homeServer -string qa225.bradfordnetworks.com
   ```
   In the example above, homeServer is the value name, -string is the data type, qa225.bradfordnetworks is the data or setting that should be added to Preferences.
5. While some elements require a string data value, others require an integer data value. For these elements, type a command similar to the following:
   ```
   sudo defaults write /Library/Preferences/com.bradfordnetworks.bndaemon
   restrictRoaming -int 1
   ```
   In the example above, restrictRoaming is the value name, -int is the value data type and 1 is the setting added to the value. In this case 1 is equal to enabled and 0 is disabled.
6. To reload the launchDaemon plist, type the following:
   ```
   sudo launchctl load /Library/LaunchDaemons/com.bradfordnetworks.agent.plist
   ```

Persistent Agent on Linux

To take advantage of the Agent Security some settings must be configured on the host. Settings for Mac OS X hosts are configured in Preferences. At this time we do not have a recommendation for a tool to set preferences.

Security settings

The table below outlines settings that can be configured for Agent Security.

Setting	Options
Allowed Ciphers and Authentication Schemes	Indicates the cipher and authentication schemes that can be used.

Setting	Options
CA Trust Length/ Depth	Indicates how deep a chain of certificates to allow between the server's certificate and the certificate's Central Authority.
CA File path	The absolute path to a file containing root and intermediate Certificate Authority certificates in PEM format.
Security	Indicates whether security is enabled or disabled.
Home Server	The fully-qualified hostname of the default server with which the agent should communicate. If this server is not set, it is automatically discovered using Server Discovery. On upgrade, this is populated by the contents of ServerIP.
Allowed Servers	In large environments there may be more than one set of FortiNAC servers. If roaming between servers is limited, list the FQDNs of the FortiNAC Application Servers or FortiNAC Servers with which the agent can communicate.
Restrict Roaming	If enabled, the agent communicates only with its Home Server and servers listed under Allowed Servers. If disabled, the agent searches for additional servers when the home server is unavailable.
Server IP	Server used for communication by agents lower than Agent Version 3.0.
maxConnectInterval	The maximum number of seconds between attempts to connect to FortiNAC. **Data Type**: Integer **Default**: 960
Last Connected Server	Server that the agent last connected to and with which the agent always attempts to communicate first. Protocol configuration change requests are honored only when they are received from this server. If this server is not set, it is automatically discovered using Server Discovery. Requires Agent Version 4.1.4 and higher.

Configuration settings

The table below shows the modifications that need to be made to the host's Preferences. If you use a tool other than GPO, you must make sure to set the appropriate keys on each host.

Value	Data
allowedServers	Comma-separated list of fully-qualified hostnames with the agent can communicate. If restrict roaming is enabled, the agent is limited to this list. The home server does not need to be included in this list (for example, a.example.com, b.example.com, c.example.com). **Data Type:** String **Default:** Empty
homeServer	The fully-qualified hostname of the default server with which the agent should communicate. **Data Type:** String

Value	Data
	Default: Empty
restrictRoaming	**False** — Do not restrict roaming. Allow agent to communicate with any server. **True** — Restrict roaming to the home server and the allowed servers list. **Data Type**: Boolean **Default**: False
securityEnabled	**False** — Disable Agent Security. **True** — Enable Agent Security **Data Type**: Boolean **Default**: True
ServerIP	The fully-qualified hostname to which the agent should communicate. **Data Type:** String **Default:** ns8200
caFile	The absolute path to a file containing root and intermediate Certificate Authority certificates in PEM format. **Data type**: String **Default**: /etc/ssl/certs/ca-bundle.crt (RPM) or /etc/ssl/certs/ca-certificates.crt (DEB)
ShowIcon	**0** — Do not show the tray icon. **1** — Show the tray icon. **Default:** Not Configured (Tray icon displayed) If both PersistentAgent.conf and PersistentAgentPolicy.conf are configured on the system, the PersistentAgentPolicy.conf configuration takes precedence over the PersistentAgent.conf configuration.
maxConnectInterval	The maximum number of seconds between attempts to connect to FortiNAC. **Data Type**: Integer **Default**: 960
macpollinterval	The maximum number of seconds between attempts to learn of new MAC address added to the host. This is intended to facilitate the quick discovery of VM Guests that have been deployed for use with the VM-Detection feature. **Data Type**: Integer **Default**: 5
lastConnectedServer	The last server that the Agent successfully connected to. This will be automatically populated by the agent upon successfully connection to a server discovered through SRV records, or from homeServer, or allowedServers list. This value will remain unchanged until the lastConnectedServer is unreachable by the agent and the agent has connected to another server. Requires Agent Version 4.1.4 and higher.

Value	Data
	Data Type: String **Default:** Empty

Disable agent security

1. Open the etc/xdg/com.bradfordnetworks/PersistentAgent.conf file to edit. Type:
   `sudo vi /etc/xdg/com.bradfordnetworks/PersistentAgent.conf`
2. Change the value of '`securityenabled=`' to "`false`"
3. Save the file.
4. Restart the agent service. Type: `sudo service bndaemon restart`

Host logging for agent security

Log files located on the host that include information pertaining to Agent Security will vary by platform.

Windows

For Windows, look in the Common Application Data directory at `%ProgramData%\Bradford Networks\`

Log files include:

- stderr.txt: output of stderr.
- stdout.txt: output of stdout.
- bndaemon_log.txt: Logged packets, same as pre-3.0.

macOS

For macOS, log messages are sent to the system log via the "debug" syslog priority.

- Messages display in console.log

Linux

For Linux, the log file is found at /var/log/bndaemon

- All logs are consolidated into this common file.

Time stamps included in the log file are displayed in UTC time. Coordinated Universal Time (UTC) is a high precision atomic time standard that corresponds roughly to Greenwich Mean Time.

Auto-Definition updates

Fortinet provides weekly updates called Auto-Definition updates that contain support for the following:

- Information on the latest Anti-Virus definitions
- Support for new versions of Anti-Virus
- Support for new operating system versions
- Any new Vendor OUIs released by the IEEE Standards Association
- New or modified Custom Scan options

Downloading these updates keeps your FortiNAC software current allowing your hosts and users to access the network easily without having to contact your IT department.

Typically, Fortinet provides an update file every Monday. If Monday is a holiday, the update is posted on the next business day. An alert is posted on the Fortinet web site in the Customer Portal when the update file is ready for download. For customers who prefer to download updates on a delayed schedule, Fortinet maintains the current update plus updates from the previous three weeks.

To implement Auto-Definition updates you must do the following:

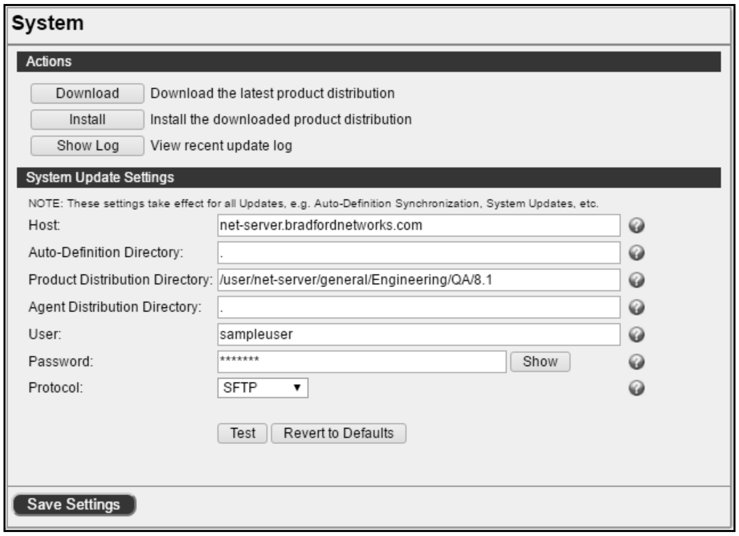
- Configure your FortiNAC server to communicate with the Fortinet download site.
- Configure the schedule for retrieving and installing updates.

Download settings

To download auto-definition updates from the download site, you must configure a connection to that site.

Configure settings

Configure the connection settings for the download location so the Auto-Def Synchronizer, Agent Packages, and the Software Distribution Updates can be completed. You need to change the default settings if another server is used to host the auto-definition or updated distribution files.



System

Actions

Download — Download the latest product distribution
Install — Install the downloaded product distribution
Show Log — View recent update log

System Update Settings

NOTE: These settings take effect for all Updates, e.g. Auto-Definition Synchronization, System Updates, etc.

Host:	net-server.bradfordnetworks.com
Auto-Definition Directory:	.
Product Distribution Directory:	/user/net-server/general/Engineering/QA/8.1
Agent Distribution Directory:	.
User:	sampleuser
Password:	*******
Protocol:	SFTP

To set the host and protocol settings for the System Update:

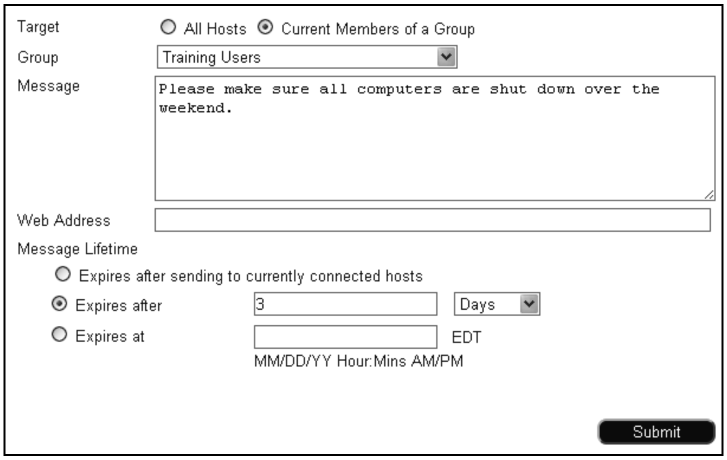
1. Click **System > Settings**.

Settings

Field	Definition
Host	IP address, host name, or fully-qualified name of the server that is hosting the updates.
Auto-Definition Directory	The sub-directory where the weekly anti-virus and operating system updates are located. Default setting for this field is a period (.). If you are downloading these files from a server on your network, specify the directory containing the updates. If you prefer to download and install updates on a delayed schedule, you can choose system updates from one, two, three or four weeks ago by modifying this field with an additional sub-directory. For example, entering /week1 gives you an update that is one week old. Available directories are: **./week1** contains updates that are one week old. **./week2** contains updates that are two weeks old. **./week3** contains updates that are three weeks old. **./week4** contains updates that are four weeks old.
Product Distribution Directory	The sub-directory where the product software files are located. This field will vary depending on the version of the software being updated. A forward slash (/) may be required in the path configuration. Click the Test button to confirm the configuration. Refer to the System Update Settings section of the Release Notes on our web site for information about the distribution directory for the specific version package you wish to download and install.
Agent Distribution Directory	The sub-directory where the Agent update files are located. This field will vary depending on the version of the software being updated. A forward slash (/) may be required in the path configuration. Click the Test button to confirm the configuration. Refer to the System Update Settings section of the Release Notes on our web site for information about the distribution directory for the specific agent package you wish to download and install.
User	The user name for the connection.
Password	The password for the connection.
Protocol	**HTTP**—Hypertext Transfer Protocol. **HTTPS**—Secure communication over HTTP. **SFTP**—Secure FTP. This protocol provides a more secure connection. **FTP**—File Transfer Protocol. **PFTP**—Passive FTP. A more secure form of data transfer in which the flow of data is set up and initiated by the FTP client rather than by the FTP server program.

Field	Definition
Buttons	
Test	Tests the connection between the FortiNAC program and the update server.
Revert To Defaults	Returns the window to the factory default settings.

Send a message to group/all hosts



Target ○ All Hosts ● Current Members of a Group

Group: Training Users

Message: Please make sure all computers are shut down over the weekend.

Web Address:

Message Lifetime

○ Expires after sending to currently connected hosts

● Expires after 3 Days

○ Expires at EDT

MM/DD/YY Hour:Mins AM/PM

Use the Send Message option on the Bookmarks menu to send a real-time message to all hosts. This provides a method for you to get a message directly to the desktop of the selected hosts.

User can send messages to hosts with the Persistent Agent or Mobile Agent installed.

See Send a message to a host on page 814 in the Host Properties section for details on sending a message to an individual host.

1. Select **Bookmarks > Send Message**.
2. Click **All Hosts** to send the message to all hosts, or click Group and select a group of hosts to receive the message.

   The message is sent only to the members of the selected group. Hosts who register and are assigned to the group after the message is sent will not receive the message, even if the message is still active.

3. Enter the message in the **Message** block.
4. If desired, enter a **Web Address** that will be sent as part of the message. Make sure the web address includes the http:// or ftp:// or other information. The page must also be in a location that the host(s) can access from their current VLAN, such as Remediation, Quarantine, Dead End, or other.
5. Click the radio button next to a **Message Lifetime** option and enter the information.

The server can only send messages to hosts with which it is communicating. If you have entered an expiration date and time, hosts who connect or communicate before that date and time also receive the message.

Message Lifetime Options	Description
Expires after sending to currently connected hosts	The message expires immediately after it has been sent.
Expires after	The message expires after the specified amount of time. Enter a number and select the timeframe of Minutes, Days, or Hours. The message remains active on the server for the selected timeframe. The server sends the message the next time it communicates with a host as long as communication occurs before the message expires.
Expires at	The message expires on the specified date and time. The format is MM/DD/YY hh:mm AM/PM. The message remains active on the server until the specified date and time. The server sends the message the next time it communicates with a host as long as communication occurs before the message expires.

6. Click **Submit**.

Role management

Roles are used in two different ways in FortiNAC. Roles assigned to hosts managed in the Host View or Users are attributes of those elements. In this case the role is another way to group users and hosts. Roles can be used in User/Host Profiles to filter for specific Users or Hosts when applying Network Access Policies, Endpoint Compliance Policies and Supplicant EasyConnect Policies.

For devices or hosts managed in the Topology View Roles are used to determine the network access given to those elements based on their connection location. In this case Roles are used with Network Device Roles. The Role is simply a name or identifier that is assigned to the host or device. The Network Device Role maps the connection location with device, port or SSID groups to a specific Role. For example, when a device connects to the network with Role A on Switch 1, FortiNAC searches through the Network Device Roles for a record with Role A that has a connection location containing Switch 1. The first matching Network Device Role is used. The configuration of this Network Device Role can place the device in a specific VLAN or can apply a CLI Configuration.

Role Management relies on the configuration of both Roles and Network Device Roles. The Roles View contains the list of possible Role names and controls assigning roles to users and hosts based on group membership. Roles for hosts managed in the Host View and Users do not need a corresponding Network Device Role. Network access for those hosts and users is handled by Network Access Policies. Roles for devices or hosts managed in Topology View require a corresponding Network Device Role to control network access. See Roles view on page 557.

If a role has more than one mapping for the same device or port group, the order of precedence is determined by the order of the role mappings on the Network Device Roles View. Starting from the top of the list, the first mapping match found is used.

See Configuration on page 553 for an overview of setup requirements.

Configuration

1. Determine which device(s) will be used to support a specific role.
2. Configure the device(s) with the VLAN or Interface ID information for the role.
3. Create a device group and add the device(s) for each set of devices that will be used for roles. For example, you might have a group of devices that provide network access in Building A. That group of devices will provide different types of access than the devices in Building B, therefore you would create two separate device groups. See Groups view on page 838 for information on groups.
4. If only some ports on a device or devices will be used for Role Management, you can place just the required ports in a Port group specifically for roles. First, determine which ports will participate in Role Management and place those ports in the Role Based Access Group. Ports that are not in this group cannot apply roles. Once ports are in the Role Based Access group, place them in groups that will be associated with roles. See Groups view on page 838 for information on groups.

Ports that are assigned roles are typically included in the Role Based Access Group. If a port is assigned a role but is not included in the Role Based Access Group, devices connecting to that port are placed in the default VLAN entered on the Model Configuration window for that device. They are not placed on the VLAN defined for the role. However, if the role is used as a filter for any policy, that policy is still used.

5. Create a list of Roles. See Roles view on page 557.
6. Determine which hosts or users will be identified by the role.
7. Associate the hosts or users with the role. See Assigning roles on page 554.

Use only one method to associate a host or a user with a role. If more than one method is used, the role is assigned based on the ranking of roles and the first piece of data that matches.

Roles are only applied to hosts that are registered.

8. Once roles have been created, configure Network Device Roles. Network Device Roles indicate the actions to be taken when a device in that role connects to a group of devices or ports. There can be multiple mappings for a single role. For example, Role A can have a mapping for Port/Device Group A and a different mapping for Port/Device Group B. Select the Device or Port group and enter the Network Access IDs. See Network device roles on page 560.

Assigning roles

Roles can be assigned to users, hosts, network devices and ports. Each one of these entities has a role field on its corresponding Properties window. Assignment of roles is accomplished by setting the role field for the user, host, device or port either manually or using one of the options listed in the table.

When a user and a host have different roles, the user role is applied if the user logs into the host. In the case of a gaming device that the user does not log into, it has its own role that may or may not be the same as the user's.

In the event that multiple methods are used to set a role, the order of precedence is determined by the order of the roles on the Roles View. Starting from the top of the list, the first role match found is used. For example, assume you have assigned roles to hosts based on groups. Later you add the host to a new group, if that group is associated with a role that is ranked above the host's original role, the host's role will be changed.

Roles created on the FortiNAC server will be ranked above global roles created on the NCM. The rank of a local role can be adjusted above or below another local role, but cannot be ranked below a global role. The rank for a global role cannot be modified from the FortiNAC server.

In the event that multiple methods are used to assign a role to a host, a hierarchy determines which role to assign. Roles assigned through Portal pages (typically for gaming), have the lowest precedence and will be overwritten by a role determined by any other method. Roles assigned by Directory Attributes have the highest precedence and will overwrite a role that is assigned by any other method. Roles assigned by Group Membership have the middle level of precedence, overwriting roles assigned through Portal Pages, but being overwritten by roles assigned via Directory Attributes. Roles assigned via Group Membership will change when the host's group membership changes. When this occurs, the roles are ranked, with low-numbered ranks having the highest precedence.

Settings

Setting	Definition
User roles	
User Roles Based On Groups	Users can be assigned roles by placing them in a group and then associating that group with a role on the Role View. See Add a role on page 559 for additional information on adding roles. Once the group of users has been created and you have assigned them a role, you must associate that role with a device group or a port group and a corresponding VLAN or CLI configuration. User groups can also be created based on groups in the Directory. These groups are treated the same as groups created manually within FortiNAC. If a user is a member of more than one group the group that is found first when matching users to roles determines the role assigned to the user. When assigning Roles to users, the use of Directory attributes over Directory groups is recommended. Attribute data is retrieved directly from the directory as the user registers, while group information is retrieved from data cached on the FortiNAC server and could be out-dated.
User Roles Based On A Directory Field	Network users can be assigned a role based on a field in LDAP or Active Directory. For example, you might choose to have roles based on a field in the directory called Department. The data within the Department field would be the name of the role, such as, Accounting or Customer Service. In a university environment a user might have a role based on whether he is a Student or Faculty. To assign roles based on a field in a directory you must indicate which field in the directory is to be used as a role. See to map the role field. Users in the directory with matching data in this field constitute a group, even though the group is not shown anywhere. For example, users with Accounting in their department field are treated as an Accounting group for the purpose of assigning roles. Next, you must create a Role with the exact same name as the data contained in the directory field. For example, if the user's role in the directory is Accounting, you must create a Role on the Role View that is named Accounting. When a user registers, the role field in User Properties is set to match the data in that user's role field in the directory.
User Roles Based On Fields In Captive Portal	When registering a host through the Captive Portal, if the user fields on the portal page have a role set, that role is assigned to the user, such as during registration or authentication.

Setting	Definition
Individual User Roles	In some situations you may want to assign a role to a single user. First create the role on the Roles View. Then, navigate to the User Properties window and modify the Role field.
Host roles	
Host Roles Inherited From Users	When registering a rogue to a user on the Host View, you have the option to use the user's role or to select a different role for the device. See Add or modify a host on page 807. When registering a host through the Captive Portal, if the portal does not have a role set, the host inherits the role of the user. If the users role changes, regardless of how it is changed, any host registered to that user that has the same role will be changed also. **Example:** John Doe is a student and has two registered hosts. • John Doe’s Role: **Student** • John Doe’s Host 1 Role: **Student** • John Doe’s Host 2 Role: **Gaming** John Doe graduates and becomes faculty, so the University makes the change in AD and runs a Directory Sync. John's role is changed to Faculty. • John Doe’s Role: **Faculty** • John Doe’s Host 1 Role: **Faculty** • John Doe’s Host 2 Role: **Gaming** Host 2 did not match John's original role of Student, so it is not changed.
Host Roles Assigned Through Captive Portal	When registering a host through the Captive Portal, if the portal page has a role set, that role is assigned to the host during registration. If the role field is blank, the host inherits the role of the user.
Host Roles Based On Groups	Hosts can be assigned roles by placing them in a group and then associating that group with a role on the Roles View. See Add a role on page 559 for additional information on adding roles.
Host Roles Assigned Manually	This would typically be used to assign a role to hosts, such as a medical device that connects to the network. To register rogues and set their role: Select one or more rogues on the Host View. Right-click on the selected records and choose Register as Device from the menu. On the registration pop-up you can select device type and role. See Register a host as a device on page 812. To set roles for registered devices: Select one or more devices on the Host View. Right-click on the selected records and choose Set Host Role. Select the new role from the drop-down list in the pop-up window.
Host Roles Assigned By Device Profiler	This would typically be used to assign a role to hosts, such as a medical device that connects to the network. Devices that are hosts, such as, medical devices, gaming devices, or printers can be assigned a role and a device type based on Device Profiling Rules.

Setting	Definition
	If you are using the Device Profiler feature, you can create or use default rules that allow FortiNAC to determine the device type and assign the device to a role. When a new host device connects to the network it becomes a rogue because it is unknown. FortiNAC compares information received from the device with the Device Profiling Rules in its database until it comes up with a match. Based on the parameters defined in the rule, the device is assigned a type and a role. See Device profiler on page 348 and Rules on page 350. The role assigned by Device Profiler takes precedence over any role associated with the Vendor OUI.

Roles view

This view allows you to setup Role Names. Roles are assigned to Users, Hosts and Devices. For hosts managed in the Host View and users roles are attributes that are used in User/Host Profiles as filters. For devices and hosts managed in Topology View, such as a printer, roles are used to control network access based on where they connect. If you are using roles to control network access for hosts and devices you must also configure Network Device Roles to provide a set of connection instructions for role and device or port group combinations.

For example, if Role A is assigned to all of the printers in the Accounting Department, then when a printer connects to a port in the accounting office, the Network Device Role for accounting office ports is configured to move them to VLAN 10.

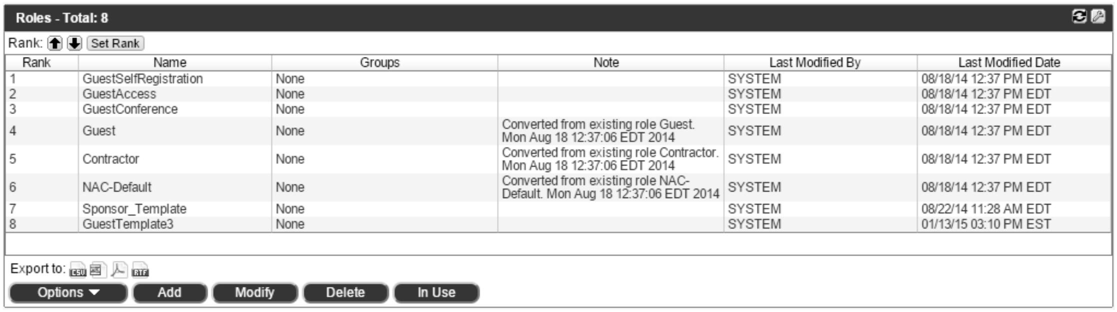
In the case of a host managed in the Host View, if Role B is assigned to that host, then when the host connects to a port in the accounting office, FortiNAC reviews the Network Access Policies until it finds a policy for a host with Role B connected to accounting ports based on the User/Host Profile in the policy.

Roles can be assigned in many different ways. In the case of the Roles View, roles are assigned based on directory groups or FortiNAC groups. When a user or a host is added to a group, FortiNAC searches the list of roles for a match starting with the role ranked number 1. When a match is found, the role is assigned to the user or the host. In the case of directory attributes, when a user is registered and FortiNAC checks the list of roles, a role with a name that exactly matches the attribute will be assigned to the user if it is the first piece of data about the user that matches the role criteria.

Roles created on the FortiNAC server will be ranked above global roles created on the NCM. The rank of a local role can be adjusted above or below another local role, but cannot be ranked below a global role. The rank for a global role cannot be modified from the FortiNAC server.

For additional information on all methods for role assignment, see Assigning roles on page 554.

See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.



Roles - Total: 8

Rank: Set Rank

Rank	Name	Groups	Note	Last Modified By	Last Modified Date
1	GuestSelfRegistration	None		SYSTEM	08/18/14 12:37 PM EDT
2	GuestAccess	None		SYSTEM	08/18/14 12:37 PM EDT
3	GuestConference	None		SYSTEM	08/18/14 12:37 PM EDT
4	Guest	None	Converted from existing role Guest. Mon Aug 18 12:37:06 EDT 2014	SYSTEM	08/18/14 12:37 PM EDT
5	Contractor	None	Converted from existing role Contractor. Mon Aug 18 12:37:06 EDT 2014	SYSTEM	08/18/14 12:37 PM EDT
6	NAC-Default	None	Converted from existing role NAC-Default. Mon Aug 18 12:37:06 EDT 2014	SYSTEM	08/18/14 12:37 PM EDT
7	Sponsor_Template	None		SYSTEM	08/22/14 11:28 AM EDT
8	GuestTemplate3	None		SYSTEM	01/13/15 03:10 PM EST

Export to:

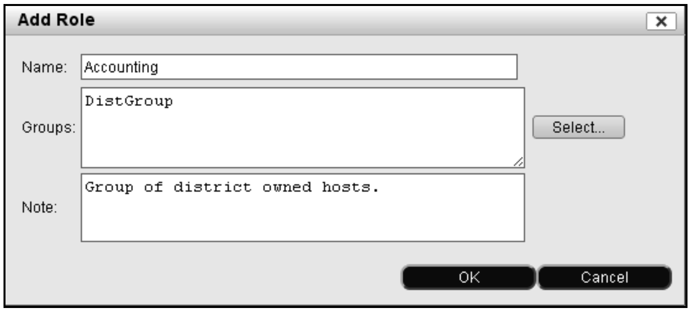
Settings

Field	Definition
Rank Buttons	Moves the selected role up or down in the list. Users and hosts are compared to roles in order by rank.
Set Rank Button	Allows you to type a different rank number for a selected role and immediately move the role to that position. In an environment with a large number of roles, this process is faster than using the up and down Rank buttons.
Name	Name of the role. If you are assigning roles based on the directory attribute specified in Attribute Mappings in the Role field, the name of the role in the Roles View must match the data in the user's directory attribute. For example, if the directory attribute is department and the user's field is set to Accounting, then the role name must be Accounting in order to match.
Groups	One or more groups whose members will be assigned to this role. List includes Groups both in FortiNAC and in the Directory, if one is being used with FortiNAC. If no groups are selected, None is displayed in this field. This effectively disables the role for group assignment. However, the role can still be assigned manually, by Device Profiler or through the Captive Portal.
Note	User specified note field. This field may contain notes regarding the conversion of roles from a previous version of FortiNAC.
Last Modified By	User name of the last user to modify the role. SYSTEM indicates that the role was modified by FortiNAC itself.
Last Modified Date	Date and time of the last modification to this role
Right click options	
Export	Exports data to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.
Copy	Copy the selected Role to create a new record.
Delete	Deletes the selected Role. Roles that are currently in use cannot be deleted.
In Use	Indicates whether or not the selected role is currently being used by any other FortiNAC element. See Role in use on page 560.
Modify	Opens the Modify Role window for the selected role.

Field	Definition
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.

Add a role

Once you have created and configured the host, user and device groups, create the roles associated with these groups.


Add Role

Name: Accounting

Groups: DistGroup

Note: Group of district owned hosts.

1. Select **Policy > Roles**.
2. Click **Add** at the bottom of the Roles View.
3. In the **Name** field, enter a name for the new role. If this role corresponds to an LDAP attribute value, the spelling of the role name must be an exact match for the data contained in the user's directory record and you do not need to select a group in the Groups field.
4. Click the **Select** button next to the Groups field. Choose one or more user or host groups by clicking on the names in the **All Groups** column and clicking the right arrow to move them to the **Selected Groups** column. Click **OK** to continue.
5. If you are creating a role that you do not want to have automatically assigned, but wish to assign manually or through the captive portal, then do not enter any groups.
6. Click in the **Note** field to add any user defined information needed for this role.
7. Click **OK** to save the role.
8. If this role will be used to control network access for hosts managed in Topology View and devices, go to the Network Device Roles View and configure the role mapping there. See Network device roles on page 560.

Modify or delete roles

You can modify the role settings as needed. All devices, users and hosts in the database are required to have a role. You cannot remove a role from these elements. You can only change the role to something else. If no role is specified devices, users and hosts default to the NAC Default role.

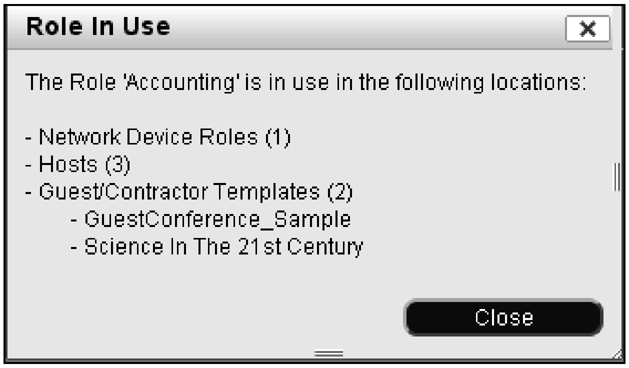
If a role is in use by a Device Profiling Rule, Guest Template or assigned to a Host, User, or Device, the role cannot be removed from the database. If a role is simply mapped to a device based on the device's membership in a group and not assigned specifically to the device, the role can be removed.

1. Select **Policy > Roles**.
2. Select the role from the list.
3. To remove the role from the database, click the **Delete** button.
4. On the confirmation window, click **Yes** to remove the role.
5. If the role is in use, a warning message is displayed and the role is not deleted. Click the **In Use** button for a complete list of places where this role is referenced.
6. To modify the role, click the **Modify** button.
7. Modify settings as needed and click **OK** to save.

Role in use

To find the list of FortiNAC features that reference a role, select the role from the Roles View and click the In Use button. A message is displayed indicating whether or not the role is associated with any other features. If the role is referenced elsewhere, a list of each feature that references the configuration is displayed. A role can be used in the following locations:

- Network Device Roles
- Hosts
- Users
- Devices
- Device Profiling Rules
- Vendor OUIs
- Guest Templates
- Scheduled Tasks with an action of "Role Assignment"
- Event to Alarm Mappings with an Action of "Host Role Action"



The Role 'Accounting' is in use in the following locations:

- Network Device Roles (1)
- Hosts (3)
- Guest/Contractor Templates (2)
  - GuestConference_Sample
  - Science In The 21st Century

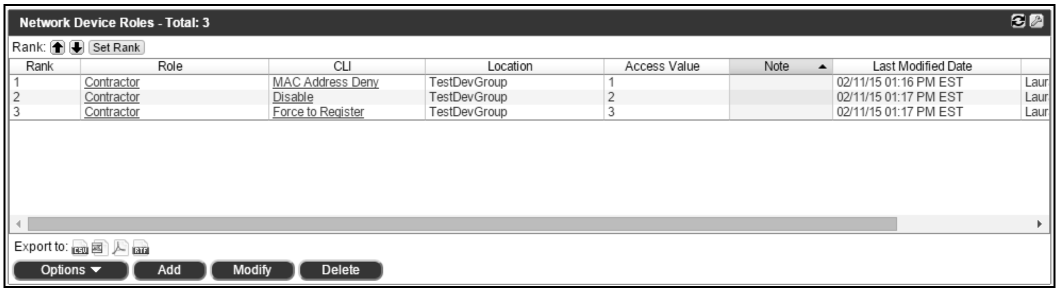
Network device roles

Network Devices that request network services are provided with those services based on the role assigned to the device and the connection location. Network Device Roles allow you to map Device Roles and connection locations to network access configurations for connecting devices. These roles apply only to hosts managed in Topology View, such as a printer, and devices.

A role can have more than one mapping to provide different results when a device with the selected role connects to a different port or device group. For example, you could map Role A to a group of ports in the Accounting Group and place connecting printers with Role A in VLAN 10. You could also map Role A to a group of ports in the Lobby Group and place connecting printers with Role A in VLAN 20. Because roles can have more than one mapping, FortiNAC must determine which mapping is appropriate for each connecting device. When a device connects each mapping is evaluated starting with Rank 1 and working down the list until a match is found. The first match found is used.

To view Network Device Roles, go to **Policy > Roles**, and then click **Network Device Roles**.

See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.



Network Device Roles - Total: 3

Rank	Role	CLI	Location	Access Value	Note	Last Modified Date	
1	Contractor	MAC Address Deny	TestDevGroup	1		02/11/15 01:16 PM EST	Laur
2	Contractor	Disable	TestDevGroup	2		02/11/15 01:17 PM EST	Laur
3	Contractor	Force to Register	TestDevGroup	3		02/11/15 01:17 PM EST	Laur

Settings

Field	Definition
Rank Buttons	Moves the selected device role up or down in the list. Connecting devices, roles and connection location combinations are compared to mappings in order by rank.
Set Rank Button	Allows you to type a different rank number for a selected device role and immediately move the device role to that position. In an environment with a large number of device roles, this process is faster than using the up and down Rank buttons.
Role	Name of the role to which this mapping applies. If Any is displayed, this indicates that the role is not being used as a selection requirement for this mapping. When set to Any, the role field is a match for all roles.
CLI	CLI configuration that will be applied. CLI configurations are applied to the port where the device connects. See CLI configuration on page 928.
Location	One or more groups of devices or ports where the device must be connected in order for this mapping to apply. If Any is displayed, this indicates that the field has been left blank when configuring the mapping and that location is not being used as a selection requirement for this mapping. When set to Any, the location field is a match for all locations.
Access Value	Name or number of the Network Access identifier where the device will be placed based on its role, such as VLAN ID, VLAN Name or Aruba Role.
Note	User specified note field. This field may contain notes regarding the conversion of roles from a previous version of FortiNAC.
Last Modified By	User name of the last user to modify the mapping. SYSTEM indicates that the mapping was modified by FortiNAC itself during an upgrade.
Last Modified Date	Date and time of the last modification to this mapping.

Field	Definition
Right click options	
Export	Exports data to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.
Copy	Copy the selected mapping to create a new record.
Delete	Deletes the selected mapping.
Modify	Opens the Modify Network Device Role window for the selected mapping.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.

Add role mappings

Network Device Role mappings tie roles to connection locations and network access options, such as VLANs.

Settings

Field	Definition
Role	If the checkbox is enabled, you can select an existing Role from the drop-down list for this mapping. If the checkbox is not enabled, this mapping is not tied to a specific role, however the other criteria in the mapping, such as Location must match the connecting device or the mapping will not be used. If you configure a mapping with no Role, you may want to make sure its Rank places it towards the bottom of the list of rankings. Device connections are compared to the mappings from the lowest (1) to the highest. The first match is used.
CLI	CLI configuration that will be applied. CLI configurations are applied to the device or port where the device connects. See CLI configuration on page 928 for additional information.
Location	One or more groups of devices or ports where the device must be connected in order for this mapping to apply. If this field has been left blank, then location will not be used as a selection requirement for this mapping.
Access Value	Name or number of the Network Access identifier where thedevice will be placed based on its role, such as VLAN ID, VLAN Name or Aruba Role.
Note	User specified note field. This field may contain notes regarding the conversion of roles from a previous version of FortiNAC.

1. Select **Policy > Network Device Roles**.
2. Click the **Add** button at the bottom of the view.
3. Click the **Role** check box to enable the role drop-down. If this is not enabled, this mapping can apply to any device that matches the other criteria in the mapping, such as Location. The word Any displays in the Role column on the Network Device Roles View if this box is unchecked.
4. Select a role from the drop-down list.
5. To apply a CLI configuration to a device or port, click the **CLI** check box to enable it and select the CLI configuration from the drop-down list. This field is optional. For additional information on CLI configurations see CLI configuration on page 928.
6. In the **Access Value** field, type the Network Access identifier for this mapping, such as a VLAN ID, VLAN Name, Aruba Role or for a VPN concentrator enter a group policy name.
7. Click the **Select** button next to the Location field. Choose one or more device or port groups by clicking on the names in the **All Groups** column and clicking the right arrow to move them to the **Selected Groups** column. Click **OK** to continue.
8. Click in the **Note** field to add any user defined information needed for this mapping.
9. Click **OK** to save the mapping.

Modify or delete role mapping

1. Select **Policy > Network Device Roles**.
2. Select the mapping from the list.
3. To remove the mapping from the database, click the **Delete** button.
4. On the confirmation window, click **Yes** to remove the mapping.
5. To modify the mapping, click the **Modify** button. See Add role mappings on page 562 for settings.
6. Modify settings as needed and click **OK** to save.

Guest manager

Your enterprise may occasionally need to augment staff with contractors for short term projects. More often, you need to provide controlled network access for guests or remote attendees of conferences. Guest Manager meets these demands by providing you with a set of tools to create limited network accounts for Guests and Contractors that are secure, role-based and provide access for a specified time period. Guest Manager allows you to:

- Control the point of access for guests and contractors.
- Manage guest and contractor authorization.
- Ensure that guests and contractors receive the appropriate network resources for the amount of time the services are needed.
- Provide IT staff with control and tracking capabilities.
- Provide administrative accounts that allow non-IT staff to create accounts and manage accounts for visiting users.

You must have a license for the Guest Manager feature. You must be sure to have enough Concurrent Licenses to provide a connection to the network for each guest. When a host connects to the network it uses one Concurrent license. The license is released as soon as that host disconnects from the network. See Licenses on page 7 for additional information.

If you have not purchased a Guest Manager license you will not be able to create Guest/Contractor accounts.

When guests or contractors enter their temporary user name, password, and other required information, Guest Manager checks the credentials against the guest or contractor account. Guest Manager denies access if the credentials do not match the entries in the Guest Manager database or LDAP directory, depending on which is being used for guest or contractor authentication. In addition, guests and contractors can be scanned to ensure that they have up-to-date anti-virus software and pose no threat to the network.

Implementation

Guest Manager is implemented at several levels. The initial setup is done by a FortiNAC administrator. Guest and Contractor Accounts are created and managed by an administrative user called a sponsor. Finally, Guests and Contractors themselves follow a login process. The initial setup of Guest Manager can be done using the Quick Start wizard under **System > Quick Start**. This section of the documentation outlines the implementation process in the order in which it should be done if you are implementing Guest Manager without using the wizard or enabling additional features not configured by the wizard.

Administrators

Administrators have full rights to all parts of the FortiNAC system and can fully implement Guest Manager without needing a sponsor user to create accounts. However, in most organizations these responsibilities are divided up.

- Make sure that e-mail settings for your FortiNAC server or control server have been configured. If they are not configured you will not be able to send email to guests with their account credentials.
- If you intend to use Endpoint Compliance Policies and scan guest/contractor's computers, set up the policies before creating templates.
- Each guest account that is created must be associated with a template that controls configuration details about that account, such as, how long the account is valid or when the guest can access the network. Guest account types include Guest, Contractor, Conference and Self-Registered Guest. See Guest/contractor templates on page 566.
- Guest Manager templates allow you to limit guest access to the network based on time of day or day of week. During the time that the guest is not allowed to access the network it is marked "At Risk" for the Guest No Access admin scan. If you choose to implement this feature for any template, the following requirements must be met:
  - You must have a quarantine or remediation VLAN on your network.
  - Under **System > Settings > Control > Quarantine**, enable the Quarantine VLAN option.
  - Ports through which a guest would connect must be in the Forced Remediation Group (applies only to wired ports).
  - The Model Configuration for all switches to which guests connect must have an entry for the Quarantine VLAN. This applies to both wired and wireless switches and access points.
- Admin User Profiles control what administrative users can do when they are working in FortiNAC. If you intend to have an administrative user create and manage guest accounts you must create an Admin User Profile to provide that user with the appropriate permissions. Sponsors profiles determine whether the sponsor can manage Guest accounts, Kiosk Accounts or Self-Registered Guest accounts.
- Create any administrative users or sponsors that will be responsible for creating and managing guests. Administrative users can also be created and associated with an Administrative User Profile automatically based on users and groups in your Directory.
- To force guests and contractors to register and/or authenticate when they connect to the network, the ports to which they connect must be in a controlled access group such as Forced Registration.
- When guests or contractors connect to the network they are presented with a registration page. This page can be set up either by editing the existing registration pages directly (Portal V1) or using the Portal Configuration Content Editor (Portal V2).
- If you would like to provide guests with badges containing their login credentials, you must make sure the printer is set up correctly.
- If you would like to send guests their login credentials via an SMS message, enable any necessary Mobile Providers. See Mobile providers on page 175. For guest account type Self-Registered Guest, SMS messages are enabled by default and requires that you enable Mobile Providers.
- If you decide to use Network Access Policy features of FortiNAC you must configure User/Host Profiles that correspond to guests. Then map a User/Host Profile to a Network Access Configuration using a Network Access Policy. See Network access policies on page 407 for additional information.

Sponsors

Sponsors have the following responsibilities. Administrators can perform these functions also.

- When all of the preliminary setup steps have been completed, either the Sponsor or the Administrator can create guest/contractor accounts.
- If Self-Registration Requests permission has been granted, sponsors can also approve or deny account requests for accounts from guests using the Self-Registration feature. See or .
- To facilitate your guests connection to the network you must give them information about their login credentials.
- If you are managing a large group of guests or contractors, you can use the Locate feature to find and manage guests. See Locate on page 58.

Sponsors with management permissions in their Admin Profile can locate guests, contractors, registered hosts, and other sponsors.

Sponsors who are limited in their Admin User Profile to managing their own hosts, can not search for any other hosts. The Sponsor field in the Locate screen is automatically filled in with the sponsor’s name and can not be changed.

Guest/contractor templates

Guest/Contractor Templates can be accessed from **Users > Guest/Contractor Templates** or from **System > Quick Start > Authentication Settings**, however configuration steps point you to **Users > Guest/Contractor Templates**.

As an administrator, you control Guest, Contractor, Conference and Self-Registration accounts by creating templates for each account type. The templates include privileges you specify, such as account duration, and credential requirements. Each time a visitor account is created one of these templates must be applied.

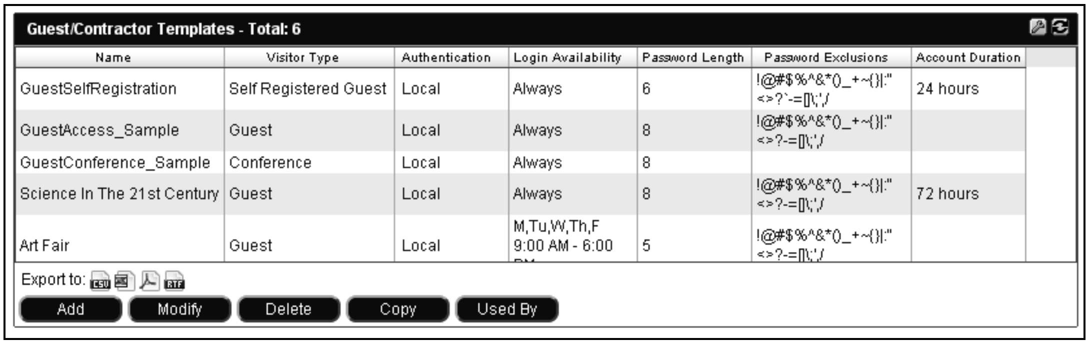
The templates you define:

- Restrict or allow certain privileges for the sponsors who create guest, contractor, and conference accounts.
- Ensure that sponsors set up appropriate accounts for guests and contractors.
- Define the number of characters in the automatically generated passwords.
- Make sure data from the guest or contractor is provided to the sponsor.

You may grant sponsor privileges to an administrative user who uses the templates to create and manage temporary guest and contractor accounts. Sponsors may also provide account details to guests by email, SMS message or printout. The entire process, from account creation to guest network access, is stored for audit and reporting.

From the Guest/Contractor Templates window you can add, delete, modify or copy templates.

See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.



Guest/Contractor Templates - Total: 6

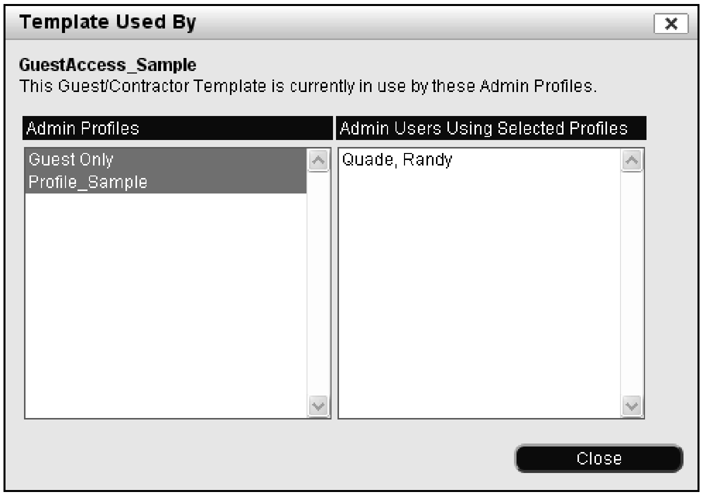
Name	Visitor Type	Authentication	Login Availability	Password Length	Password Exclusions	Account Duration
GuestSelfRegistration	Self Registered Guest	Local	Always	6	!@#$%^&*()_+~{}|:" <>?`-=[]\;',/	24 hours
GuestAccess_Sample	Guest	Local	Always	8	!@#$%^&*()_+~{}|:" <>?-=[]\;',/	
GuestConference_Sample	Conference	Local	Always	8		
Science In The 21st Century	Guest	Local	Always	8	!@#$%^&*()_+~{}|:" <>?-=[]\;',/	72 hours
Art Fair	Guest	Local	M,Tu,W,Th,F 9:00 AM - 6:00	5	!@#$%^&*()_+~{}|:" <>?-=[]\;',/	

Settings

Field	Definition
Name	Descriptive name for the template. Sponsors use this name when they select a template to create accounts.
Visitor Type	User type for the template. Corresponds to the account types of Guest and Contractor so that the correct view is presented to the user.

Field	Definition
Role	Role is an attribute added to the user and the host. Roles can be used in User/Host Profiles as a filter. Note that these roles must first be configured in the Role Management View. If they are not configured, no role-based restrictions apply. Any additional roles you have configured are also listed here. The available default options are Contractor, Guest and NAC-Default. If you have not configured a Guest or Contractor role, any Host you register has the NAC-Default common role applied to it. See Visitor types on page 569. For more on Roles see Role management on page 553.
Authentication	Indicates type of authentication used for Guests or Contractors associated with this template. Options include: **Local**—User name and password credentials are stored in the local database. For Conference accounts, authentication is Local only. **LDAP**—The email of the user is required, and is what guests and contractors use to log in. The email address maps to the created Guest user. When the email address is located in the LDAP directory, it is compared with the given password for the user. If it matches, the guest or contractor's credentials are accepted and they are granted access. **RADIUS**—Checks your RADIUS server for the email address (required) in the user's created account. If a match is found, it is compared with the given password for the user. If it matches, the guest or contractor's credentials are accepted and they are granted access.
Login Availability	Indicates when guests or contractors with this template can login to the network. Login Availability is within the timeframe you specify for the Account Duration. The available options are: • Always • Time range Guests created using this template are marked "At Risk" for the Guest No Access admin scan during the times they are not permitted to access the network.
Password Length	Required length of guest or contractor passwords. Must be between 5 and 64 characters.
Account Duration	There are two methods that work together for determining the length of time a guest account is active. The shortest duration of the two is the one that is used to remove a guest account from the database. **Account Duration (Hours)**— Option included in the Guest Template to limit the time a guest account created with this template remains in the database. If this is blank, the guest account end date is used. The Account Duration starts only when the guest user first logs in. For example, you could create a guest account with a date range that spans one week and if the account duration was 24 hours, they would be able to log in for one 24 hour period any time during that week

Field	Definition
	Account End Date— Option included on the Add Guest Account dialog to determine the date on which the guest account expires. This field is required when a guest account is created.
Reauth Period (hours)	Number of hours the guest or contractor can access the network before reauthentication is required.
Security & Access Value	User specified text associated with guests created using this template that can be used as a filter. Used to assign a policy to a guest by filtering for this value.
Password Exclusions	List of characters that will not be included in generated passwords.
Last Modified By	User name of the last user to modify the template.
Last Modified Date	Date and time of the last modification to this template.
Right click menu options	
Export	Exports data to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.
Copy	Copy the selected Template to create a new record.
Delete	Deletes the selected Template. Accounts that were created with the template prior to deletion are still valid and retain the data that was in the template.
Modify	Opens the Modify Guest/Contractor Template window for the selected template.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.
Used By	Display a list of users by Admin Profile that are associated with the selected template. Click on a specific Admin Profile to see the associated users. To select more than one profile use the Ctrl key.


Template Used By

GuestAccess_Sample

This Guest/Contractor Template is currently in use by these Admin Profiles.

Admin Profiles	Admin Users Using Selected Profiles
Guest Only Profile_Sample	Quade, Randy

Visitor types

Guest Manager supports four basic types of accounts. They are identified on the Guest templates as Visitor types and are loosely defined as follows:

Guest—A visitor to your facility with limited or Internet-only network access. For example, a guest might be on the premises for a one-day sales call or a three-day presentation. Any number of guest accounts may be created at one time as bulk accounts. In this case, the email address is the same as the user name. Guests who need access for one day only may be managed by administrative users with permission to manage guest self-registration or self-serve kiosks. For more on Kiosks see Using a kiosk on page 606.

Self-Registered Guest—A visitor to your facility with limited or Internet-only network access who connects to your network on their own device to request a temporary account. The account request goes to a sponsor via e-mail. The sponsor can log into FortiNAC and approve or deny the request or, depending on your configuration, can approve or deny the request for the account directly from the e-mail. The account is created when the request is approved.

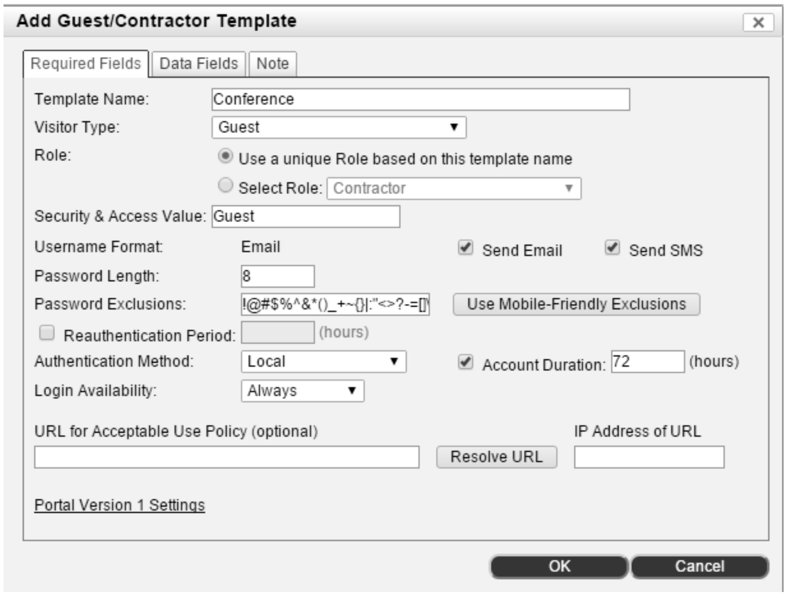
Conference—A group of short- or long-term visitors to your organization who require identical but limited access to your network for typically one to five days. Conferences are often bulk accounts, in which attendees receive notification of the conference via, for example, email. Conference members may be given an identical generated user name and password that is specific to the conference—for example, *conference-1* or *training123*, individual passwords for individual attendees, or individual attendee names with a shared password. See Conference accounts on page 602. When the conference members register they enter their email address. Once they have registered, they fill in their name and other information.

Contractor—A temporary employee of your organization who may be granted all or limited network access for a specific time period generally defined in weeks or months. Any number of contractor accounts may be created at one time as bulk accounts. In this case, the email address is the same as the user name.

Create templates

Use this option to create multiple templates for each of the Guest, Contractor, Conference and Self-Registered Guest visitor types with a variety of permissions. Data fields allow you to collect data from your guests and store it in User Properties. If you are a FortiNAC administrator you have access to all templates and can assign any template of the correct type to any guest, contractor or conference user when you create their accounts. If you choose to create a sponsor user who is responsible for creating visitor accounts, the sponsor must be assigned a set of templates through the Admin Profile. When the sponsor creates visitor accounts, he can only choose templates from the list you have assigned.

1. Log into your administrator account.
2. Click **Users > Guest/Contractor Templates**.
3. The Templates window appears. Click **Add**.
4. The **Add Guest/Contractor Template** window appears. Enter the information in the **Required Fields** tab as described in Settings on page 570.
5. Click the **Data Fields** tab to determine which fields will be required when a guest logs onto the network.
6. Click the **Note** tab to add a note to the printed access information to give the guest/contractor special login instructions or an SSID. See Provide login information on page 601.
7. Click **OK** to create the template and add it to the list of templates.


Add Guest/Contractor Template
✕
Required Fields
Data Fields
Note
Use Mobile-Friendly Exclusions
Resolve URL
Portal Version 1 Settings
OK
Cancel

Template Name: Conference

Visitor Type: Guest ▼

Role: ● Use a unique Role based on this template name

○ Select Role: Contractor ▼

Security & Access Value: Guest

Username Format: Email ☑ Send Email ☑ Send SMS

Password Length: 8

Password Exclusions: !@#$%^&*()_+~{}|:"<>?-=[]

☐ Reauthentication Period: (hours)

Authentication Method: Local ▼ ☑ Account Duration: 72 (hours)

Login Availability: Always ▼

URL for Acceptable Use Policy (optional)

IP Address of URL

Settings

All possible fields are included in this table. The fields shown on your screen will vary depending on the Visitor Type you select.

Field	Definition
Template Name	Type a descriptive name for the template. Sponsors use this name when they select a template to create accounts.
Visitor Type	User type for the template. Corresponds to the account types of Guest and Contractor so that the correct view is presented to the user. See Visitor types on page 569.
Use A Unique Role Based On This Template Name	Creates a role based on the template name and assigns that role to guests with accounts created using this template. Using the template name as a role allows you to limit network access based on the Guest Template by using the new role as a filter in a User/Host Profile. See User/host profiles on page 389.

Field	Definition
	When using the Wireless Security feature to configure SSID mappings, the name of the Guest Template selected is used to create the appropriate User/Host Profile allowing you to limit SSID access based on Guest Template.
Select Role	Role is an attribute added to the user and the host. Roles can be used in User/Host Profiles as a filter. Note that these roles must first be configured in the Role Management View. If they are not configured, no role-based restrictions apply. Any additional roles you have configured are also listed here. The available default options are Contractor, Guest and NAC-Default. If you have not configured a Guest or Contractor role, any Host you register has the NAC-Default common role applied to it. See Visitor types on page 569. For more on Roles see Role management on page 553.
Security & Access Value	Enter a value, such as, Guest or Visitor. This field is added to each guest user account that is created based on this template and can be used as a filter. When creating User/Host Profiles, you can filter for the contents of the Security & Access Value field to control which Endpoint Compliance Policy is used to scan guest hosts.
Send Email	For Conference accounts, email cannot be sent until a guest has registered or you have modified the account via the **User View > Modify** option to enter an email address. Select this check box if you want a sponsor with this template to be able to send an e-mail confirmation to the guest's/contractor's email address. If not selected (default) guest or contractor credentials need to be printed or sent via SMS. For Self-Registered Guest accounts this option is automatically checked and cannot be disabled.
Send SMS	For Guest or Contractor accounts, select this check box if you want a sponsor with this template to be able to send an SMS confirmation to the guest's/contractor's mobile phone. If not selected guest or contractor credentials need to be e-mailed or printed. For Self-Registered Guest accounts this option is automatically checked and cannot be disabled. Requires that the guest or contractor provide both a mobile number and the mobile provider. These fields default to Required in the Data Fields tab.
Max Number Of Accounts	Only available when Visitor Type is set to Conference. Typically used when generating a large number of accounts for a conference. Limits the total number of accounts that can be created on the Conference Account window when this template is selected. To limit accounts, enable the check box and enter the maximum number of accounts that can ever be created using this template. For an unlimited number of accounts, leave the check box empty.
Password Length	Between 5 and 64 characters. Passwords that are automatically generated by Guest Manager contain at least one capital letter, one lower case letter, one alphanumeric character, and one symbol. If you have characters listed in Password Exclusions, those characters will not be used. Note that for Conference accounts, once a template has been created, the sponsor may specify the individual different passwords for attendees when the sponsor creates the conference account. See Conference accounts on page 602.

Field	Definition
	FortiNAC does not recognize or restrict system-generated passwords that may be offensive.
Password Exclusions	List of characters that will not be included in generated passwords.
Use Mobile Friendly Exclusions	Removes any existing entries and then populates the Password Exclusions field with a list of symbols that are typically difficult to enter on a mobile device. Modify the list of characters as needed. Characters include: !@#$%^&*()_+~{}|:"<>?-=[]\;',/
Reauthentication Period (hours)	Specify the number of hours the guest or contractor can access the network before reauthentication is required. To specify a reauthentication period you must first select the check box. Next fill in the reauthentication period in hours. If you do not select this check box, you will not have to specify a reauthentication period for guests or contractor accounts created with this template.
Authentication Method	Specify where authentication occurs: • **Local**—User name and password credentials are stored in the local database. For Conference accounts, authentication is Local only. • **LDAP**—The email of the user is required, and is what guests and contractors use to log in. The email address maps to the created Guest user. When the email address is located in the LDAP directory, it is compared with the given password for the user. If it matches, the guest or contractor's credentials are accepted and they are granted access. • **RADIUS**—Checks your RADIUS server for the email address (required) in the user's created account. If a match is found, it is compared with the given password for the user. If it matches, the guest or contractor's credentials are accepted and they are granted access.
Account Duration	Select the check box to specify the duration of the account in hours. For all guests except those with shared conference accounts: The duration governs how long from creation the account remains in the database, regardless of the end date that is entered when creating the guest account. For shared conference accounts: The duration governs how long from guest Login the account remains in the database, regardless of the end date that is entered when creating the conference. For Self-Registered Guest accounts this option is automatically checked and cannot be disabled. You must enter a duration. There are two methods that work together for determining the length of time a guest account is active. The shortest duration of the two is the one that is used to remove a guest account from the database.

Field	Definition
	• **Account Duration (Hours)**— Option included in the Guest Template to limit the time a guest account created with this template remains in the database. If this is blank, the guest account end date is used. The Account Duration starts only when the guest user first logs in. For example, you could create a guest account with a date range that spans one week and if the account duration was 24 hours, they would be able to log in for one 24 hour period any time during that week • **Account End Date**— Option included on the Add Guest Account dialog to determine the date on which the guest account expires. This field is required when a guest account is created.
Propagate Hosts	Controls whether the Propagate Hosts setting is enabled or disabled on the user record for guest users created with this template. If enabled, the record for the host owned by the guest user is copied to all managed FortiNAC appliances. This field is only displayed if the FortiNAC server is managed by a FortiNAC Control Manager.
Login Availability	Select when guests or contractors with this template can login to the network. Login Availability is within the timeframe you specify for the Account Duration. The available options are: • Always • Specify Time: If you select this option, a window displays in which you specify the time range and select the days of the week. Click OK. Guests created using this template are marked "At Risk" for the Guest No Access admin scan during the times they are not permitted to access the network.
URL for Acceptable Use Policy	Optional. Directs the guest or contractor to the page you specify with the network policies when they login.
Resolve URL	Click to acquire the IP addresses for the URLs for Acceptable Use Policy and Successful Landing page. If the URL is not reachable, specify the IP address in the IP address field.
Portal version 1 settings	
URL for Successful Landing Page	Directs the guest or contractor to a certain page when they have successfully logged into the network and passed the scan in an Endpoint Compliance Policy. This field is optional and is used only if you have Portal V1 enabled in Portal Configuration. If you are using the portal pages included with FortiNAC and controlled by the Content Editor in the Portal Configuration, this field is ignored.

Login availability time

This option allows you to limit network access for a guest or contractor based on the time of day and the day of the week. Any guest associated with a template, can only access the network as specified in the Login Availability field for the template.

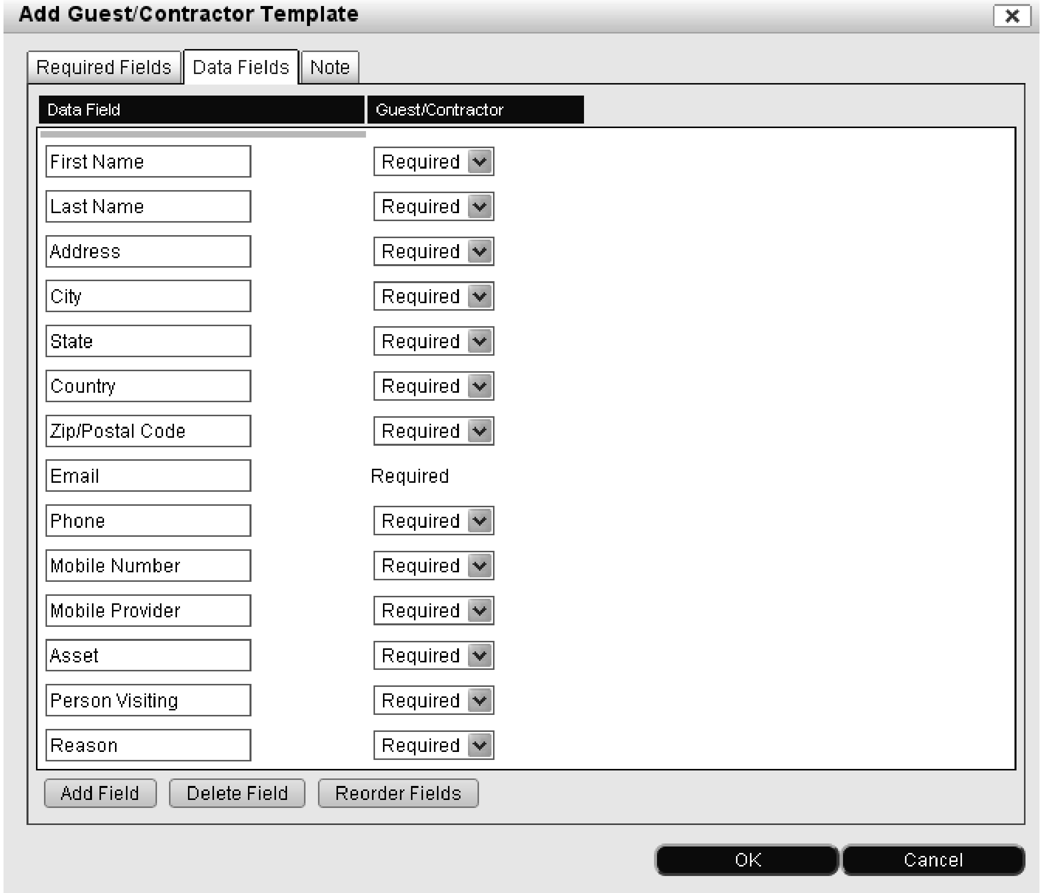
If you set times for Login Availability, FortiNAC periodically checks the access time for each guest associated with the template. When the guest is not allowed to access the network the host associated with the guest is marked "At Risk" for the Guest No Access admin scan. When the time is reached that the guest is allowed to access the network, the "At Risk" state is removed from the host. These changes in state occur on the guest host record whether the guest is connected to the network or not. If the guest host connects to the network outside its allowed timeframe, a web page is displayed with the following message: "Your Network Access has been disabled. You are outside of your allowed time window. To regain network access call the help desk.".

Data fields

Specify which pieces of data will appear on the form the guest or contractor will be required to fill out in the captive portal. For Self-Registered Guests this information is filled out with the request for an account. For Guests with an existing account, this information is filled out after they enter their user name and password on the login page. If the field has a corresponding database field, it is stored there and displayed on the User Properties window. If the field does not have a corresponding database field, it is stored and displayed in the Notes tab of the User Properties window and the Host Properties window. Hover over the field name to display a tool tip indicating where the data entered by the guest will be stored.

- **Required**—The data in this field must be entered in order for the guest or contractor to log in.
- **Optional**—Appears on the form, but is not required data from the guest or contractor.
- **Ignored**—Will not appear on the form.

The E-mail Field is required. The fields listed below are default fields that are included with the original setup of Guest Manager. Field names can be modified by typing over the original name. Therefore, the fields on your template window may not match any of the fields in this list. If you rename a field, the data entered into that field by the guest is still stored in its original location. For example, if you modify the title of the Last Name field to say Mother's Maiden Name, the data is still stored in the Last Name field on the User Properties window.



Data Field	Guest/Contractor
First Name	Required
Last Name	Required
Address	Required
City	Required
State	Required
Country	Required
Zip/Postal Code	Required
Email	Required
Phone	Required
Mobile Number	Required
Mobile Provider	Required
Asset	Required
Person Visiting	Required
Reason	Required

Original Field Name	Definition
Last Name	Maximum length 50 characters. Stored in the Last Name field.
First Name	Maximum length 50 characters. Stored in the First Name field.
Address	Maximum length 50 characters. Stored in the Address field.
City	Maximum length 50 characters. Stored in the City field.
State (or Province/County)	Standard two-letter state abbreviation, or up to 50 characters. Stored in the State field.
Country	Maximum length 50 characters. Stored on the Notes tab.
Zip or Postal Code	Maximum length of 16. Stored in the Zip Code field.
Email	Email address of the guest or contractor. Stored in the E-mail field. This field can be modified however FortiNAC expects the contents of the field to be an email address. This field tests for a valid email address and will not allow the user to proceed without one. If the label is something other than email and other types of data are entered, the guest account may not be able to be created.
Phone	Telephone number including international country codes (for example, +1, +44). Maximum length 16. Stored in the Phone field.
Mobile Phone	Mobile Telephone number. Maximum length 16. Stored in the Add/Modify User window.
Mobile Provider	The name of the company that provides the guest with Mobile service. The guest is provided with a list of possible providers. Stored in the Add/Modify User window.
Asset	Text field for computer serial numbers, manufacturer's name and model number, or any other asset identifier of the guest's or contractor's computing platform. Stored in the Serial Number field. Max.length 80 characters.
Reason	The reason for the guest's or contractor's visit. Max. length 80 characters. Stored on the Notes tab.
Person Visiting	Maximum length 50 characters. Stored on the Notes tab.
Buttons	
Add Field	Click to add new data fields to track additional guest or contractor data, such as license plate numbers or demo equipment details. Maximum length 80 characters. Type the name of the field in the pop-up window. Select whether to make the field required or optional. Once new fields have been added they are stored in the Notes tab of the user's account. To see these fields go to the User Properties window.
Delete Field	Click this button to delete a data field from the list. Only those fields that have been created by an Admin user can be deleted. System fields can be set to Ignore so they do not display, but cannot be deleted from the template.

Original Field Name	Definition
Reorder Fields	Changes the order of the fields as they appear in the Guest or Contractor Form. Click this button to reorder account information fields. In the pop-up window, click Move Up or Move Down and OK.

Notes

The Notes tab on the template creation window allows you to provide additional information to guests and contractors. After you have created a Guest or Contractor account, you may want to provide that user with his login information. Login information can be printed, viewed on the screen, sent via text message to a mobile telephone or included in an amalgamate text added on the Notes tab is appended to the guest information included in the printout, email or text message. See Provide login information on page 601 for additional information.

Endpoint compliance policies for guests

Endpoint Compliance Policies and the agents that run associated scans are assigned based on the rules contained within the Policy. FortiNAC selects a scan and an agent by comparing guest and host data to the User/Host Profile in each policy beginning with the policy ranked number 1 until a match is found. When a match is found the scan and agent are assigned and the guest's computer is scanned. If you want to create a specific policy for guests, you must define a policy that searches for user data that only guests will match and place it at the beginning of the list of policies.

Example 1

In this example the policy will apply to guests based on their Role. Create a policy that has the following settings:

User/Host Profile

- **Where (Location)** — Leave this field blank.
- **Who/What by Group** — Leave this field blank.
- **Who/What by Attribute** — Add a filter for users. Within the filter enable Role and enter the name of the Role assigned to guests. Typically the Role is named Guest, but you may have chosen to use a different role for Guests. Roles are assigned by the Guest Template used to create the guest account.
- **When** — Set to Always.

Scan

- **Scan** — Create a scan to evaluate guest computers for compliance.

Endpoint Compliance Configuration

- **Scan** — Select the scan you wish to apply to guests.
- **Agent Tab** — Select the agent that should be used.

Endpoint Compliance Policy

- **User/Host Profile** — Select the profile that determines who is assigned this policy.
- **Endpoint Compliance Configuration** — Select the configuration that determines the scan and agent used.

Example 2

In this example the policy will apply to guests based on their Security & Access Value. Create a policy that has the following settings:

User/Host Profile

- **Where (Location)** — Leave this field blank.
- **Who/What by Group** — Leave this field blank.
- **Who/What by Attribute** — Add a filter for users. Within the filter enable Security & Access Value and enter the name of the Security & Access Value assigned to guests. These values are assigned by the Guest Template used to create the guest account.
- **When** — Set to Always.

Scan

- **Scan** — Create a scan to evaluate guest computers for compliance.

Endpoint Compliance Configuration

- **Scan** — Select the scan you wish to apply to guests.
- **Agent Tab** — Select the agent that should be used.

Endpoint Compliance Policy

- **User/Host Profile** — Select the profile that determines who is assigned this policy.
- **Endpoint Compliance Configuration** — Select the configuration that determines the scan and agent used.

Modify templates

1. Log into your administrator account.
2. Click **Users > Guest/Contractor Templates**.
3. The Guest/Contractor Template Management window opens with a list of created templates.
4. Select the template and click **Modify**. Change the name of the template, or other information and parameters.

   Once the template has been modified the modifications will only apply to new accounts created from the template. All old accounts made from the template remain the same.

5. Click OK.

Copy templates

You may copy a template, save it under another name, and use it as the basis for a new template.

1. Log into your administrator account.
2. Click **Users > Guest/Contractor Templates**.
3. The Guest/Contractor Template Management window opens with a list of created templates.
4. Select the template and click **Copy**.
5. Change the name of the template, or other information and parameters.
6. Click **OK**.

Delete templates

You may delete a template at any time. Accounts that were created with the template prior to deletion are still valid and retain the data that was in the template.

1. Log into your administrator account.
2. Click **Users > Guest/Contractor Templates**.
3. The Guest/Contractor Template Management window opens with a list of created templates.
4. Select the template and click **Delete**.
5. A confirmation message is displayed. Click **Yes** to delete the template.

Admin profiles

In FortiNAC, you can create an administrative user and give that user an Admin Profile that contains special permissions for the Guest/Contractor feature set. These privileges are designed to restrict this user to certain parts of the program. See Admin profiles and permissions on page 657.

For Guest Manager, this type of user is referred to as a Sponsor in documentation because that person sponsors incoming guests and contractors. Creating a Sponsor Admin Profile allows the user to manage guest, contractor, conference or Self-Registered Guest accounts. For more information on the types of accounts, see Visitor types on page 569.

Guest Manager supports multiple UPN formats (for example, @gcs.xyztech.com) so sponsors do not have to type their full user login name. As administrative users create guest or contractor accounts, their administrative login name within Guest Manager is added as a part of the guest or contractor record for reporting purposes.

Additional permissions can be given to Sponsors based on the parameters of their responsibilities. Create one or more Admin Profiles for these types of users. Sponsor Admin User Profiles determine whether the sponsor can manage Guest accounts, Kiosk Accounts or Self-Registered Guest accounts.

Add a guest manager profile

This procedure describes how to create a specific Admin User Profile for an administrative user with permissions for Guest Manager. As a sponsor, the administrative user can create guest or contractor accounts. For details on all of the options that can be include in an Admin User Profile see Add an admin profile on page 671.

If an Admin User Profile has Kiosk Mode enabled, the corresponding user can only log into the Kiosk computer to make it available to arriving guests. That user cannot create accounts. You may need to create a sponsor who can manage accounts and a second sponsor to use for the self-service Kiosk. See Add a guest kiosk profile on page 581

To create an Admin User Profile you must first be logged into your Administrator account. Follow the steps below to add an Admin User Profile for an Administrative User that is considered a Sponsor for incoming guests:

1. Click **Users > Admin Profiles**.
2. Click **Add**. The **Add Admin Profile** screen appears with the **General** tab highlighted.
3. On the **General** tab, enter a name for the profile, such as **Guest Sponsor**.
4. Under **Manage Hosts and Ports** select **All**.
5. Leave the defaults for the remaining fields and click on the **Permissions** tab.
6. On the Permissions tab note that some permissions are dependent on each other. Refer to the Permissions list on page 666 for additional information.
7. The minimum that this sponsor must have is the **Guest/Contractor Accounts** permission set. Select all of the check boxes for this set including the **Custom** check box.
8. When you select the Guest/Contractor permission set, the Landing Page field defaults to Guest Contractor Accounts.
9. In addition you may want include Self Registration Requests, which allow a Sponsor to Allow or Deny guest access to a user who has registered through the captive portal. This is not required.
10. The Manage Guests tab is enabled when Custom is selected for the Guest/Contractor Accounts permission set. Click on the **Manage Guests** tab.
11. Use the table below to configure the settings.
12. Click **OK** to save.

Settings

Field	Definition
Guest Account Access	You can give Administrative Users with this profile privileges that allow them to manage all guest contractor accounts, regardless of who created them, only their own accounts, or no accounts. The privileges include whether the sponsors can add or modify accounts, locate guests or contractors, and view reports. **No**—Users can only see guest accounts they create and send credentials to those guests. Users cannot modify or delete any guest accounts. **Own Accounts**—Users can see guest accounts they create, send credentials to those guests, and modify or delete their own guest accounts. All Accounts—User can see all Guest accounts in the database, send credentials to guests and modify or delete any guest accounts.

Field	Definition
Account Types	**Individual**—Sponsor can create single guest accounts. Within the constraints of the template, the sponsor may specify account start and end date. Each account has a unique name and password associated with it. **Bulk**—Sponsors may create multiple accounts with unique passwords by importing a bulk account file. **Conference**—Sponsors may create any number of conference accounts, or the number may be limited by a template. Conference accounts may be named identically but have a unique password for each attendee, have the same name and password, or have unique names and passwords.
Create Accounts Days in Advance (Maximum)	The maximum number of days in advance this sponsor is allowed to create accounts.
Create Accounts Active For Days (Maximum)	Determines the length of time the guest account remains active in the database. There are two methods that work together for determining the length of time a guest account is active. The shortest duration of the two is the one that is used to remove a guest account from the database. **Account Duration (Hours)**— Option included in the Guest Template to limit the time a guest account created with this template remains in the database. If this is blank, the guest account end date is used. The Account Duration starts only when the guest user first logs in. For example, you could create a guest account with a date range that spans one week and if the account duration was 24 hours, they would be able to log in for one 24 hour period any time during that week **Account End Date**— Option included on the Add Guest Account dialog to determine the date on which the guest account expires. This field is required when a guest account is created.
Allowed Templates	Indicates whether the Administrative User can use all guest templates or only those in the Specify Templates > Selected Templates field. Default = All. Options include: **All Templates**—Profile gives the Administrative User access to all templates in the database when creating guest accounts. **Specify Templates**—Profile gives the Administrative User access to the templates listed in Selected Templates.
Specify Templates	Allows you to select guest/contractor templates available for Administrative Users with this Admin User Profile. Use the arrows to place the templates needed in the Selected Templates column and the unwanted templates in the Available Templates column. If All Templates is selected in the Allowed Templates field, all templates are moved to the Selected Templates column and the arrows are hidden.
Available Templates	Shows the templates that have not been selected to be included in this Admin User Profile.
Selected Templates	Shows the templates selected to be included in this Admin User Profile.
Add Icon	Click this button to create a new Guest/Contractor template.

Field	Definition
	For information on templates, see Create templates on page 569.
Modify Icon	Click this button to modify the selected Guest/Contractor template. For information on templates, see Create templates on page 569.

Add a guest kiosk profile

A kiosk allows visitors to your facility to create their own account. Guests have a maximum of 24 hours of access to your network, which may be only during certain hours of the day, or a pre-defined number of hours from when they log on. Guests may simply be queried for pre-defined contact data. In any case, at 11:59 PM each day, or after the allowed number of hours has elapsed, kiosk guest accounts expire.

All other profile options are disabled if Kiosk Mode is enabled, because guests creating their own accounts would not need access to other options.

For added security, sponsors should use a kiosk browser. Kiosk browsers block users from accessing other programs on the host or other web sites.

This procedure describes how to create a profile that gives a sponsor permission to manage a kiosk. A sponsor with Kiosk Mode enabled cannot access any of the regular FortiNAC windows. That user can log in to display the Guest Login web page and make it available on the Kiosk PC.

To create a profile you must first be logged into your Administrator account.

1. Click **Users > Admin Profiles**.
2. Click **Add**. The **Add Admin Profile** screen appears with the **General** tab highlighted.
3. On the **General** tab, enter a name for the profile, such as Kiosk Sponsor.
4. Use the table below to fill out the settings.
5. Under **Manage Hosts and Ports** select **All**.
6. Select **Enable Guest Kiosk**.
7. In the **Kiosk Template** field select a Guest/Contractor Account template. All guest accounts created through the Kiosk will use this template.
8. In the **Kiosk Welcome Text** field type the message that a guest will see when they create a guest account through the Kiosk.
9. Click **OK** to save.

Settings

Field	Definition
Name	Enter a name that describes the profile, such as Kiosk Sponsor.
Logout After	User is logged out after this amount of time has elapsed without any activity in the user interface.
Login Availability	Specify when this sponsor can log into the network: • **Always** • **Specify Time**

Field	Definition
	The Specify Time option requires you to specify an hourly time range and the days of the week the sponsor can log in.
Manage Hosts And Ports	Restricts an Administrative User to a specific set of hosts or ports. The set is defined by host and port groups that are assigned to be managed by a specific group of Administrative Users. Any Administrative User that has a profile with this option enabled can only view and or modify a subset of the data in FortiNAC. Typically, this type of user would ONLY have the Manage Hosts & Ports permission set on the Permissions tab, therefore, this setting is not used frequently. Default = All. • **All**—All groups containing hosts and ports can be accessed. • **Restrict By Groups**—Enables the restriction of Administrative Users to specific hosts and ports. For an overview and additional setup information see Limit admin access with groups on page 691.
Note	User specified note field. This field may contain notes regarding the data conversion from a previous version of FortiNAC for an existing Admin Profile record.
Enable Guest Kiosk	If you enable this mode, sponsors can log into FortiNAC to provide visitors self-serve account creation through a kiosk. For added security, use a kiosk browser. See Using a kiosk on page 606 to read the sponsor's procedure. Note: Sponsors with this profile cannot do anything except log into the Kiosk PC to display the Guest Login page. Sponsors who need to manually create visitor accounts cannot have Kiosk mode enabled.
Kiosk Template	Select a Kiosk template for this sponsor. All visitors who use the self-service Kiosk when this sponsor is logged in will be assigned this template.
Kiosk Welcome Message	Enter the message that will appear when the kiosk user creates a guest account.

Add a guest self registration profile

Guest Self-Registration allows visitors to request a temporary or guest account from their own device. A sponsor receives an email indicating that a request has been received from a guest. The sponsor responds to the request by approving or denying it. Sponsors with the Guest Self Registration Admin Profile or with a Guest Manager Admin Profile and Administrators can respond to a Self-Registration request from a guest.

Anyone in your organization can be a sponsor for Guest Self-Registration. They must be entered into FortiNAC as an Administrative User and that user account must have a Guest Self-Registration Admin Profile applied. You can quickly create Sponsors by using Directory Groups. See Set admin privileges based on directory groups on page 692.

Guests can access your network for the length of time specified by the Account Duration. Availability can be 24 hours a day or limited to specific hours during the day.

To create a profile you must first be logged into your Administrator account.

1. Click **Users > Admin Profiles**.
2. Click **Add**. The **Add Admin Profile** screen appears with the **General** tab highlighted.
3. On the **General** tab, enter a name for the profile, such as Self-Registered Guest Sponsor.

4. Use the table below for details on the fields in the General Tab.
5. Under **Manage Hosts and Ports** select **All**.
6. Leave the defaults for the remaining fields and click on the **Permissions** tab.
7. On the **Permissions** tab note that some permissions are dependent on each other. Refer to thePermissions list on page 666 for additional information.
8. The minimum that this sponsor must have is the **Self Registration Requests** permission set. Select all of the check boxes for this set.
9. When you select the **Self Registration Requests** permission set, the Landing Page field defaults to Self Registration Requests.
10. Click **OK**.

Settings

Field	Definition
Name	Enter a name that describes the profile, such as Kiosk Sponsor.
Logout After	User is logged out after this amount of time has elapsed without any activity in the user interface.
Login Availability	Specify when this sponsor can log into the network: • **Always** • **Specify Time** The Specify Time option requires you to specify an hourly time range and the days of the week the sponsor can log in.
Manage Hosts And Ports	Restricts an Administrative User to a specific set of hosts or ports. The set is defined by host and port groups that are assigned to be managed by a specific group of Administrative Users. Any Administrative User that has a profile with this option enabled can only view and or modify a subset of the data in FortiNAC. Typically, this type of user would ONLY have the Manage Hosts & Ports permission set on the Permissions tab, therefore, this setting is not used frequently. Default = All. • **All**—All groups containing hosts and ports can be accessed. • **Restrict By Groups**—Enables the restriction of Administrative Users to specific hosts and ports. For an overview and additional setup information see Limit admin access with groups on page 691.
Note	User specified note field. This field may contain notes regarding the data conversion from a previous version of FortiNAC for an existing Admin Profile record.
Enable Guest Kiosk	Do not enable this field for the Self Registered Guest Admin User Profile. If you enable this mode, sponsors can log into FortiNAC to provide visitors self-serve account creation through a kiosk. For added security, use a kiosk browser. See Using a kiosk on page 606 to read the sponsor's procedure. Note: Sponsors with this profile cannot do anything except log into the Kiosk PC to display the Guest Login page. Sponsors who need to manually create visitor accounts cannot have Kiosk mode enabled.

Administrative users

When you create or modify an administrative user, you must attach an Admin User Profile to the account. Before adding Administrative Users to manage guests, create an Admin User Profile that contains the set of permissions that allow the administrative user to sponsor guest, contractor, or conference accounts. The profile limits the administrative user's access to FortiNAC features.

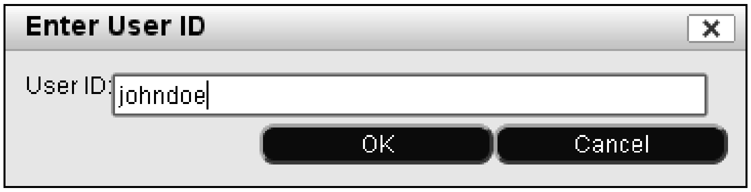
When an administrative user with an Admin Profile logs into FortiNAC, the system presents the views available based on the user's default permissions. You can configure administrative accounts to authenticate locally or externally via RADIUS or LDAP. If the administrative user cannot be authenticated, an error message specifying the problem displays.

Add an admin user

If you are creating Admin Users to manage guests or devices, you must create an Administrative User who has the appropriate Admin User Profile associated. See Admin profiles and permissions on page 657.

1. Select **Users > Admin Users**.
2. Click the **Add** button.
3. In the User ID window displayed, enter an alphanumeric **User ID** for the new Admin user and click **OK**. As you enter the User ID, the network user database is checked to see if there is a current user with the same ID and a drop-down list of matching users is displayed. If you enter an ID that already exists as a regular network user, the network user and the Admin user become the same person with a single account.

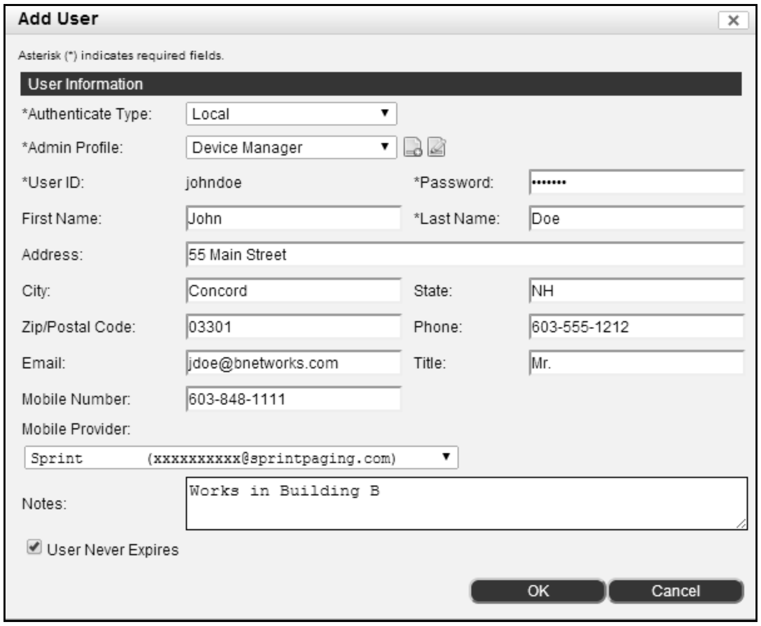
   This allows you to give a network user administrator privileges to help with some administrative tasks.



Enter User ID

User ID: johndoe

4. Use the table of Settings below to complete the information in the Add User dialog.
5. Click **OK** to save the new user.



Add User

Asterisk (*) indicates required fields.

User Information

*Authenticate Type: Local

*Admin Profile: Device Manager

*User ID: johndoe

*Password: •••••••

First Name: John

*Last Name: Doe

Address: 55 Main Street

City: Concord

State: NH

Zip/Postal Code: 03301

Phone: 603-555-1212

Email: jdoe@bnetworks.com

Title: Mr.

Mobile Number: 603-848-1111

Mobile Provider: Sprint (xxxxxxxxxx@sprintpaging.com)

Notes: Works in Building B

☑ User Never Expires

Settings

Field	Definition
Authentication Type	Authentication method used for this Admin user. Types include: • **Local** — Validates the user to a database on the local FortiNAC appliance. • **LDAP** — Validates the user to a directory database. FortiNAC uses the LDAP protocol to communicate to an organization’s directory. • **RADIUS** — Validates the user to a RADIUS server.
Admin Profile	Profiles control permissions for administrative users. See Admin profiles and permissions on page 657. • **Add** — Opens the Admin Profiles window allowing you to create a new profile without exiting the Add User window. • **Modify** — Allows you to modify the selected Admin Profile. Note that modifications to the profile affect all Administrative Users that have been assigned that profile.
User ID	Unique alphanumeric ID for this user.
Password	Password used for local authentication. If you authenticate users through LDAP or RADIUS, the password field is disabled and the user must log in with his LDAP or RADIUS password.
First Name	User's first name.
Last Name	User's last name.

Field	Definition
Address	Optional demographic information.
City	
State	
Zip/Postal Code	
Phone	
E-mail	E-mail address used to send system notifications associated with features such as alarms or profiled devices. Also used to send Guest Self-Registration Requests from guests requesting an account. For multiple e-mail addresses, enter addresses separated by commas or semi-colons. Messages are sent to all e-mail addresses provided.
Title	User's title, such as Mr. or Ms.
Mobile Number	Mobile Phone number used for sending SMS messages to administrators.
Mobile Provider	Mobile provider for the mobile phone number entered in the previous field. Used to send SMS messages to administrators. This field also displays the format of the SMS address that will be used to send the message. For example, if the provider is US Cellular, the format is xxxxxxxxxx@email.uscc.net, where the x's represent the user's mobile phone number. The number is followed by the email domain of the provider's message server.
Notes	Free form notes field for additional information.
User Never Expires	If enabled, Admin users are never aged out of the database. The default is enabled. Admin Users assigned the Administrator Profile cannot be aged out.
Propagate Hosts	The Propagate Hosts setting controls whether or not the record for the host owned by the user is copied to all managed FortiNAC appliances. This field is only displayed if the FortiNAC server is managed by a FortiNAC Control Manager.

Portal page setup for version 1

Applies only to Version 1 Portal Pages.

If you are adding the Guest Manager feature to your existing FortiNAC system and you are using the Version 1 portal pages, you will need to modify your Registration page so that it links to the Guest Manager Guest Login page. The default link is for the Guest Account Guest Login page.

Guest Account is a feature that provides limited guest access to your network. Each guest account is created individually by an administrator.

Guest Manager is a feature that provides a suite of tools for creating and managing large numbers of guests.

When any unknown user connects to your network a Registration page is displayed. If you are using Guest Manager this page should contain separate links for regular network users and Guests or Contractors. When a user clicks the Guest link a Guest Login page is displayed asking them for their credentials. To display the guest page associated with the Guest Manager feature, your normal registration page must be edited to include a link to that page.

To edit your current registration page so that it calls the new guest manager guest login page, see the instructions below.

If you choose to disable all legacy or Version 1 portal pages and use the Content Editor in Portal Configuration to manage your pages, the option above will not apply. You can edit your Guest pages from the Content Editor. See Portal content editor on page 250.

Update guests link on the registration page

When users connect to the network a registration page is displayed. This page is usually index.html, however you may have chosen to use a different html file. To allow guests created with Guest Manager to connect to your network , the Guests link on the registration page or index.html must be modified so that it opens the appropriate Guest Login page.

Do the following to edit the Guests link on an existing portal page. The file is assumed to be index.html. If this is not the file you normally call GuestLogin.html from, edit the file you use instead.

1. Use an ssh utility to reach the appliance.
2. Use vi to edit the content of each of the following files. Within each file change `GuestLogin.html` or `GuestLogin2.html` to `GuestLoginGCS.html`. Each file contains two references to `GuestLogin.html` or `GuestLogin2.html`.

   ```
   /bsc/Registration/registration/index.html
   /bsc/Remediation/remediation/index.html
   /bsc/Authentication/authentication/index.html
   ```

Example:

```
<td width="25%" rowspan="2" class="opte"><a href="GuestLoginGCS.html"
onMouseOver="MM swapImage('Image2','','img/acguest.gif',1)" onMouseOut="MM_
swapImgRestore()">

<img src="img/ac.gif" alt="Guest Access" name="Image2" width="100" height="100"
border="0" id="Image2"></a></td>
```

The only difference from the standard web pages is that the href is `GuestLoginGCS.html` instead of `GuestLogin.html`.

Portal page setup for version 2

If you are using the Portal Pages distributed with FortiNAC you may need or want to edit some of the settings that apply to guest users. Below is a list of settings that should be edited for Guests. For a description of each field and how to use it either hover over the field in the Portal Content editor or

The Portal Content Editor is arranged in a tree configuration. As you select an item on the left, the pane on the right displays corresponding options or settings that can be edited to manipulate how guests are treated in the portal and what is displayed on the web pages used by guests.

Options marked with an asterisk are not limited to being used for Guest. These options may be displayed on many portal pages. For example, the Instructions page can be enabled as a link on the Guest Registration page and the regular User Registration page.

Tree Option	Settings
Registration > Login Menu Authentication > Login Menu	• Guest Login Enabled • Guest Login Title • Guest Login Link • Guest Login Order
Registration > Login Menu	• Self Registration Guest • Self Registration Guest Login Title • Self Registration Guest Login Link • Anonymous Authentication Enabled • Anonymous Authentication Title • Anonymous Authentication Link • Anonymous Authentication Order
Registration > Self Registration Login	• Window Title • Left Column Content • Request Page Title • Request Page Introduction • Request Page Form Title • Request Access Button Text • Pending Page Title • Default Sponsor Email • Sponsor Email Label • Notify Sponsor of Guest Details • Accept Notification • Login Username Label • Login Password Label • Require Sponsor Approval • Guest Request Expiration (minutes) • Request Pending Message • Deny Notification • Expired Notification

Tree Option	Settings
	• Cancel Request Button Text • Message from Sponsor Header • Sponsor Email Intro Text • Sponsor Approval Link Requires Login • Sponsor Email Login Link Text • Sponsor Email Approve Link Text • Sponsor Email Deny Link Text • Notify User via Portal Page • Show Password in Portal Page Notification • Notify User via Email • Notify User via SMS • Default Guest Template • Acceptable Use Policy • Acceptable Use Policy Checkbox Text • URL for Acceptable Use Policy • Link text for Acceptable Use Policy URL • Text for Acceptable Use Policy • Instructions
Registration > Primary Guest Login Authentication > Primary Guest Login	• Window Title • Title • Left Column Content • Introduction • Form Title • User Name Label • Password Label • Missing Fields • Instructions
Registration > Secondary Guest Login Authentication > Secondary Guest Login	• Window Title • Title • Left Column Content • Main Content • Introductory Paragraph • Form Button Text • Account Expiration Label • Login Availability Label
*Registration > Instructions *Authentication > Instructions	• Window Title • Title • Left Column Content • Introduction • Show Windows Instructions • Windows Instructions • Show macOS Instructions • macOS Instructions

Tree Option	Settings
	• Show Linux Instructions • Linux Instructions • Show Other Instructions • Other Instructions Title • Other Instructions • Display as Accordion View
*Registration > Success *Authentication > Success	• Window Title • Title • Left Column Content • Progress Bar Enabled • Progress Bar Title • Please Wait message • Success Message • Finished Message

Printer settings for guest badges

In Guest Manager, administrative users you designate as sponsors can access guests' account credentials that show the user name, password, and access start time and end time. Sponsors may print the account details, e-mail them or send them via an SMS message directly to guests after account creation.

If sponsors managing guest kiosks or conferences need to print badges, contact your IT Manager to assure that printer settings are optimized for badge creation:

Make sure the label printer is the default printer for kiosks.

- In the Printer Properties, Paper Options settings, set the paper label size to a minimum of 2” x 2-3/4” (5.1 cm x 7 cm).
- In the Page Handling Settings, make sure that Auto-Rotate is enabled to automatically adjust the orientation to fit the label’s orientation on the sheet.
- Test to make sure that text is centered and fits on each label.

Events and alarms

Certain actions within Guest Manager generate events that appear in the Event Log. Examples of Guest Manager events are listed in the following table.

Event	Definition
Conference Created	Using Guest/Contractor Accounts you can create a batch of conference user accounts. This event is generated when those accounts are created and indicates the number of accounts created.

Event	Definition
Guest Account Created	New guest account is created.
Guest Account Deleted	Guest account is deleted.

If certain event conditions occur, you are immediately informed of the condition through the alarm notification system. You can define and map additional events to alarms.

For more information on events and alarms, e-mail notifications, and how to map events to alarms see Map events to alarms on page 888.

Sponsors

As a Guest Manager sponsor, you must log into FortiNAC to create guest or contractor accounts. Once logged in, the permissions defined by your administrator in your sponsor's Admin Profile are applied. Depending on the permissions, you could be presented with a Locate tab, a Guest/Contractor Accounts tab, a View Reports tab, or all three.

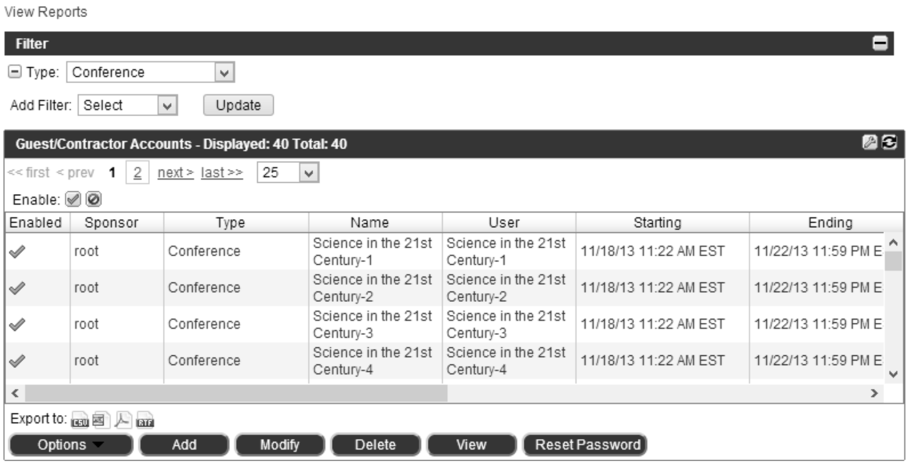
Log in as a sponsor

You can access the sponsor privileges assigned to you only when you log into your account. As a sponsor, you can:

- Create and manage Guest, Contractor, and Conference accounts.
- Locate guests, contractors, and other sponsors.
- Sign-in to the kiosk you are in charge of to allow guests to create their own accounts for network access.

Guest Sponsor users who sign in to the kiosk to prepare it for arriving guests have very limited permissions. If you are responsible for both the kiosk and managing Guest, Contractor and Conference accounts, you will need to have separate logins for each responsibility.

1. To log into Guest Manager, bring up a web browser and the following type in the URL:
   `http://<Hostname>:8080`
   This opens the Administrative User login screen.
2. Enter the username and password that was given to you by the administrator.
3. A screen with the end-user license agreement opens. To access your sponsor account, read the agreement and press **Accept**.
4. Based on your privileges, this screen will show a **Bookmarks** drop-down menu. From this menu you can select **Guest/Contractor Accounts** or **Locate** to locate hosts and users.



Enabled	Sponsor	Type	Name	User	Starting	Ending
✓	root	Conference	Science in the 21st Century-1	Science in the 21st Century-1	11/18/13 11:22 AM EST	11/22/13 11:59 PM E
✓	root	Conference	Science in the 21st Century-2	Science in the 21st Century-2	11/18/13 11:22 AM EST	11/22/13 11:59 PM E
✓	root	Conference	Science in the 21st Century-3	Science in the 21st Century-3	11/18/13 11:22 AM EST	11/22/13 11:59 PM E
✓	root	Conference	Science in the 21st Century-4	Science in the 21st Century-4	11/18/13 11:22 AM EST	11/22/13 11:59 PM E

- To search for host or user records, click the **Locate** tab to open the **Locate** screen. See Locate on page 58.
- As a sponsor you will typically want to create accounts for guest, contractors, and conference members before they arrive. To create and manage accounts, click **Bookmarks > Guest/Contractor** to open the **Create** screen. See Guest or contractor accounts on page 592, Create bulk or multiple accounts on page 598, or Conference accounts on page 602.
- To view reports of guest or contractor accounts and registrations, click the **View Reports** link at the top of the Guest/Contractor Accounts view.

In addition to these privileges, Guest Manager Sponsor users may also have permission to manage a self-serve kiosk or to manage guest self-registration. The kiosk allows guests to create their own accounts for network access. The guest self-registration option allows guests to send a request for network access which can be approved or denied by the Sponsor. A Sponsor with permissions to manage a self-serve kiosk or guest self-registration, does not have permission to manage Guest, Contractor and Conference accounts. A user who is responsible for all of these types of guest account creation, must have a separate login for the Kiosk.

A kiosk is unique within Guest Manager. Once the sponsor's credentials for the kiosk have been entered, guests use the kiosk computer to create their own accounts. Network access is limited and there are generally time constraints. For more information on a self serve kiosk see Using a kiosk on page 606.

Guest or contractor accounts

Guest Accounts allows you to create and manage guest or contractor accounts. To initially set up the accounts, access the Add Guest option and select a template set up by your administrator. Include the e-mail addresses of the guests or contractors as you create their accounts. You can then notify them of start times, required class materials, or other relevant information.

You may enter data specified as *Required* in the guest or contractor registration form, or you can let the guests and contractors enter the data themselves when they log into the portal. At that time, the required fields must be completed in order for the guest or contractor to log into the system.

Passwords are automatically generated when guest or contractor accounts are created. Generated passwords do not include characters that could be difficult to identify, including: the number one, the letter l (ell), the upper case letter I (eye), zero, upper or lowercase letter O. For Conference Accounts with shared passwords you have the option of creating your own password or generating one.

FortiNAC does not recognize or restrict system-generated passwords that may be offensive.

If you have account management privileges in your Sponsor Admin Profile, you may change or remove information in an account. Depending on your privileges, you may be allowed to manage all created accounts or only your own accounts.

Guests also display on the User View. See User view on page 637 and Guest account details on page 605.

Guest/Contractor Accounts can be accessed from **Users > Guest/Contractor Accounts** or from **System > Quick Start > Authentication Settings**, however configuration steps point you to **Users > Guest/Contractor Accounts**.

See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.

Settings

Fields used in filters are also defined in this table.

Field	Definition
View Reports	Opens the Guest Accounts Report view. This option displays only when Guest/Contractor accounts is accessed from the Users menu.
Table columns	
Enabled	Indicates Guest account status. The account is either enabled (green check mark) or disabled (red x).
Sponsor	User name of the Administrator or Sponsor that created the guest account.
Account Type	Guest account type. Types include: • **Guest**—A visitor to your facility with limited or Internet-only network access. • **Conference**—A group of short- or long-term visitors to your organization who require identical but limited access to your network for typically one to five days. • **Contractor**—A temporary employee of your organization who may be granted all or limited network access for a specific time period generally defined in weeks or months.
Name	Guest's first and last name.
User	Guest's email account which is used as the User ID at login.
Starting Start Date	Date and time (using a 24-hour clock format) the account will become active for the guest or contractor.
Ending End Date	Date and time the account will expire.
Login Availability	Times during which the guest is permitted to access the network.
Role	Role is an attribute of a user or a host. It is used in User/Host Profiles as a filter when assigning Network Access Policies, Endpoint Compliance Policies and Supplicant EasyConnect Policies.

Field	Definition
Authentication	Indicates type of authentication used. Options include: Local, LDAP. Guests typically use Local authentication.
Security & Access Value	Attribute assigned to a guest that can be used as a filter. Common values are Guest, Contractor or Visitor.
Account Duration	There are two methods that work together for determining the length of time a guest account is active. The shortest duration of the two is the one that is used to remove a guest account from the database. • **Account Duration (Hours)**— Option included in the Guest Template to limit the time a guest account created with this template remains in the database. If this is blank, the guest account end date is used. The Account Duration starts only when the guest user first logs in. For example, you could create a guest account with a date range that spans one week and if the account duration was 24 hours, they would be able to log in for one 24 hour period any time during that week • **Account End Date**— Option included on the Add Guest Account dialog to determine the date on which the guest account expires. This field is required when a guest account is created.
Reauth Period	Number of hours the guest or contractor can access the network before reauthentication is required.
Last Modified By	User name of the last user to modify the guest account.
Last Modified Date	Date and time of the last modification to this guest account.
Right click menu options	
Delete	To delete an account, select the account and click **Delete**. The account is deleted and will no longer show up in the created accounts window.
Modify	Change information in an existing guest or contractor account. This option also allows you to reset the information and reenter it. To modify an account select the account you want to change and click **Modify**. Conference accounts cannot be modified.
Reset Password	To reset an account password select the account and click **Reset Password**. The account password is automatically changed.
View	View additional account information such as passwords and guest or contractor phone numbers. Select an account and click **View**. This displays the Print, Send e-mail and Send SMS options for the selected account(s).
Send Email	Sends email to the selected guests containing their login information.
Send SMS	Sends a text message to the selected guests' mobile telephone containing their login information.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847.

Field	Definition
	You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.
Select All	Selects all guest accounts displayed in the table.
Enable/Disable	Select the account and click **Enable/Disable**. The account status is changed. This is used to enable a Guest account if a guest were to arrive earlier than expected.
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. This option displays only when Guest/Contractor accounts is accessed from the Users menu.

Create guest/contractor accounts

Guest Manager allows Administrative Users with Sponsor Admin Profiles to create and manage guest or contractor accounts. This helps to:

- Free IT staff from the daily burden of creating accounts for visiting users.
- Ensure that guest and contractor accounts get created ahead of time so they do not have to wait for their accounts to be created when they arrive.

To set up accounts for guests or contractors before they arrive at your organization:

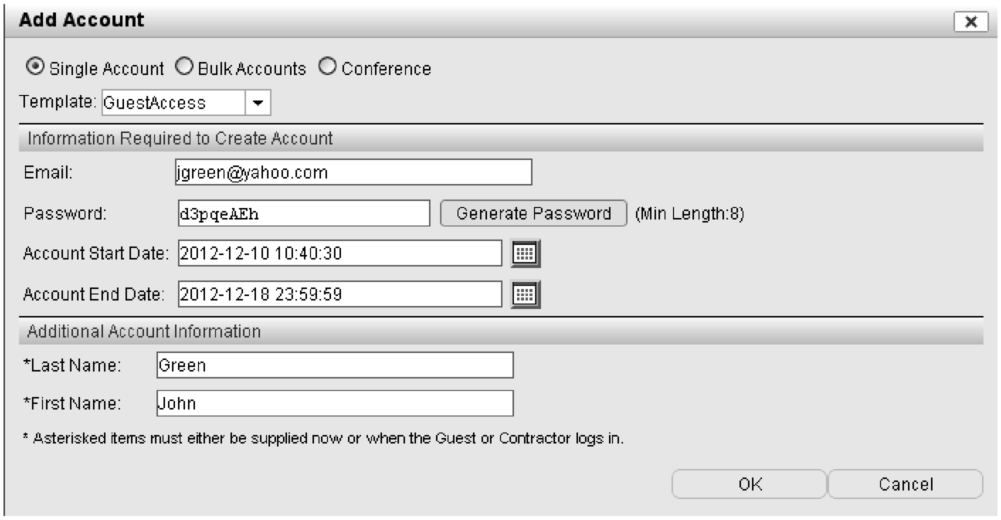
1. Log into your Sponsor account.
2. The Guest/Contractor Accounts window is displayed. Admin users select **Users > Guest/Contractor Accounts**.
3. Click **Add** to open a new screen.
4. Click **Single Account**. Enter the information described below in Settings on page 596.

   E-mail address,start and end dates are required. Additional personal information about the guest or contractor is optional. If the additional personal information is blank, the guest or contractor is prompted to fill in those fields before logging into the network.

   If Send SMS is enabled in the template, then Mobile Number and Mobile Provider are also required to allow you to send a message to the guest's mobile telephone.

5. Click **OK**. The View Accounts screen opens with the account information in it. See Provide login information on page 601.
6. Click **Print** or **Send e-mail** or **Send SMS** to provide account information and password to the guest or contractor, or **Close**. These options are visible to you depending on the privileges you have in your profile. Additional text can be added to the printout or email by typing the text into the Notes tab on the Guest/Contractor template before creating the account. See Create templates on page 569.

Guests also display on the User View. See User view on page 637.



Add Account

● Single Account ○ Bulk Accounts ○ Conference

Template: GuestAccess

Information Required to Create Account

Email: jgreen@yahoo.com

Password: d3pqeAEh Generate Password (Min Length:8)

Account Start Date: 2012-12-10 10:40:30

Account End Date: 2012-12-18 23:59:59

Additional Account Information

*Last Name: Green

*First Name: John

* Asterisked items must either be supplied now or when the Guest or Contractor logs in.

OK Cancel

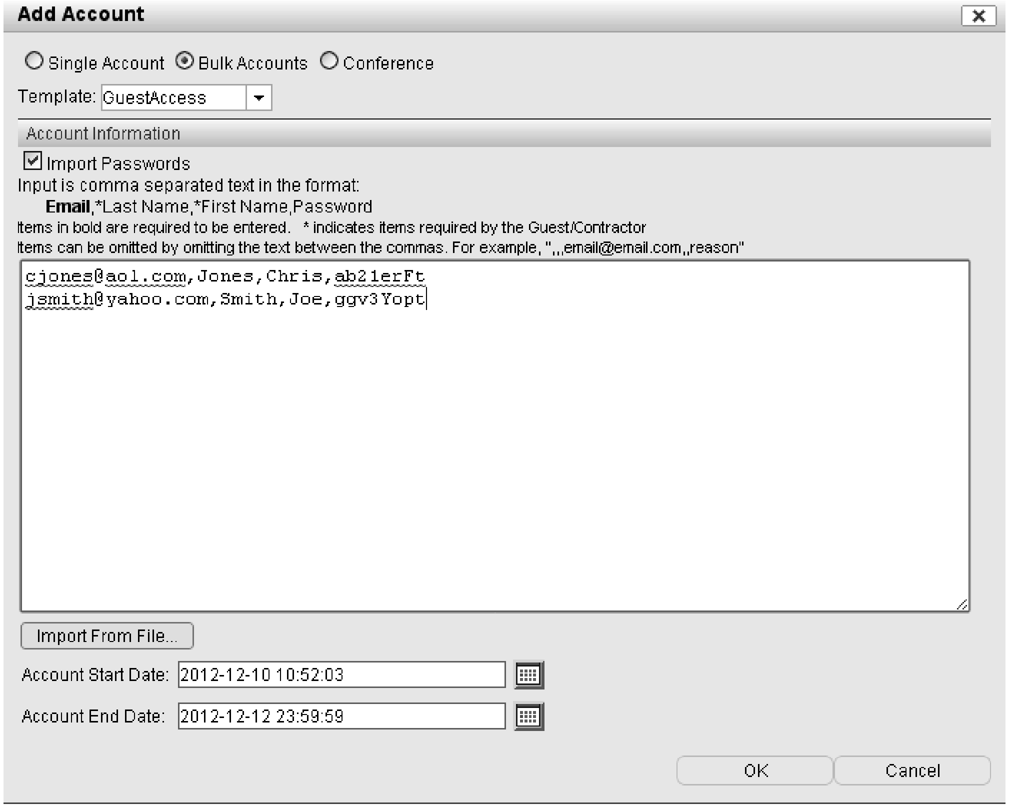
Settings

Field	Definition
Template	Click the down arrow on the Template box and select the type of template you want to use for the account.
Information required to create account	
E-mail	Enter the E-mail address of the guest or contractor. This is the only personal information you are required to enter.
Password	A password is automatically generated for this guest. Click Generate Password to generate a new password if necessary or enter a password manually. Password must meet the minimum length designated in the selected Guest Template. FortiNAC does not recognize or restrict system-generated passwords that may be offensive. If LDAP is specified as the authentication method in the selected Guest Template, the Password field is not displayed.
Account Start Date	Click the calendar icon to the right to select a date or enter the date and time (using a 24-hour clock format) the account will become active for the guest or contractor.
Account End Date	Click the calendar icon to the right to select a date or enter the date and time (using a 24-hour clock format) the account will expire. At that time, the guest or contractor will no longer be able to access the network.

Field	Definition
	This defaults to the date and time calculated based on the number of hours entered in the Account Duration field in the guest template. If this field is empty, no account duration has been entered in the guest template. Admin Users that have an admin profile with custom Guest/Contractor Account permissions will be restricted to choosing an end date that is within the bounds of the "Create accounts active for days (maximum)" setting as defined in the admin profile. For example, if your admin profile has a "Create accounts active for days" set to 20, you will not be able to choose an end date that is more than 20 days ahead of the chosen start date. This date sets the user expiration date for the guest. The host registered to this guest inherits the setting for registered hosts in Global Aging. When the user expires, both the user and host are removed from the database. If the host expires first, then only the host is removed from the database. There are two methods that work together for determining the length of time a guest account is active. The shortest duration of the two is the one that is used to remove a guest account from the database. **Account Duration (Hours)**— Option included in the Guest Template to limit the time a guest account created with this template remains in the database. If this is blank, the guest account end date is used. The Account Duration starts only when the guest user first logs in. For example, you could create a guest account with a date range that spans one week and if the account duration was 24 hours, they would be able to log in for one 24 hour period any time during that week **Account End Date**— Option included on the Add Guest Account dialog to determine the date on which the guest account expires. This field is required when a guest account is created.
Additional account information	
First Name	The guest or contractor's required personal data and the fields below may be entered by the sponsor before the arrival of the guests, or may be left for the individual guests to fill out themselves.
Last Name	
Address	
City	The Required Fields under the Additional Account Information heading are designated with an asterisk (*). These fields must be filled in before the guest or contractor will be granted network access.
State	
Country	
Zip/Postal Code	
Phone	
Asset	The computer serial number, manufacturer's name, and model number, or any other asset identifier of the guest or contractor's computing platform. There may be other Administrator-defined fields here as well, such as license plate. This field has a maximum length of 80.
Reporting To	In this example, these fields were added when the template was created and marked as Required.
Department	

Create bulk or multiple accounts

Depending on permissions, as a Guest Manager Sponsor you may be able to create and manage multiple guest or contractor accounts at one time. The process for creating bulk accounts is similar to that for creating single accounts.



Add Account

○ Single Account ● Bulk Accounts ○ Conference

Template: GuestAccess

Account Information

☑ Import Passwords

Input is comma separated text in the format:

Email,*Last Name,*First Name,Password

Items in bold are required to be entered. * indicates items required by the Guest/Contractor

Items can be omitted by omitting the text between the commas. For example, ",,,email@email.com,,reason"

```
cjones@aol.com,Jones,Chris,ab21erFt
jsmith@yahoo.com,Smith,Joe,ggv3Yopt
```

Account Start Date: 2012-12-10 10:52:03

Account End Date: 2012-12-12 23:59:59

1. Log into your Sponsor account.
2. The **Guest/Contractor Accounts** window is displayed. Admin users select **Users > Guest/Contractor Accounts**.
3. Click **Add**.
4. In the **Add Account** screen, click **Bulk Accounts**.
5. Use the table below to fill in settings.

Field	Definition
Template	Choose either a Guest or Contractor Template.
Import Passwords	Enable this check box if you want to manually specify a password for each guest. the Password must be the last field in each record. If enabled you must specify a password for every guest account being imported. If the check box is disabled, FortiNAC generates a password for each guest account as it is imported.

Field	Definition
	FortiNAC does not recognize or restrict system-generated passwords that may be offensive.
Account Information	You must create a separate record for each account you are creating. Type field place holders for data that you would like the guest to enter. Press **Enter** after each record to indicate that a new record has been started. You also have the option of importing from a text file. Required information for account creation. Use a comma to separate each field. You may choose to enter additional user information if it is available, but it is not required at this time. The guest or contractor will be prompted to fill in the missing fields before they can log into the network. If there is missing information, enter a comma in its place. If you intend to provide login credentials to guests via SMS messages sent to their mobile telephones, you must include mobile number and mobile provider name in the account list of fields. See Mobile providers on page 175 for instructions on accessing the list of names.
Import File From	If you have a CSV or text file of the user record information, click **Import From File** to import the text into the Account Information window. See Bulk guest import on page 599 for more information.
Account Start Date	The day the account becomes active. You can start the account only on one of the days defined in your profile.
Account End Date	The date the accounts become inactive. This date sets the User Expiration date for each Guest. A host registered to a guest inherits the setting for registered hosts in Global Aging. When the User expires, both the User and the Host are removed from the database. If the Host expires first, then only the Host is removed from the database.

6. Click OK. The View Accounts screen opens with the account information in it. See Provide login information on page 601.
7. Click Print or Send e-mail or Send SMS to provide account information and password to the guest or contractor, or Close. These options are visible to you depending on the privileges you have in your profile. Additional text can be added to the printout or email by typing the text into the Notes tab on the Guest/Contractor template before creating the account. See Create templates on page 569.

Guests also display on the User View. See User view on page 637.

Bulk guest import

If you need to create many guest accounts simultaneously, you can create Conference accounts or Bulk accounts. Conference accounts are generated by the system and don't allow you to provide any additional guest information, thus preventing you from e-mailing credentials to attendees. Bulk accounts use data that you supply either by typing it into the Bulk Account screen or by importing it from a CSV or text file.

The fields used in the file vary depending on the template selected to create the accounts. When a Guest Account Template is created you indicate the fields that will be required, optional or ignored for guests. E-mail address is the only field that is absolutely required for all guests and must be included in the file. Other fields, such as first name or last name, may be required but this does not mean that they have to be in the import file. It means that the guest cannot log onto the network unless this information is supplied, either by you in the import file or by the guest when they fill out a web form during the login process.

Using a CSV or text file

Requirements:

- Do not include a header row
- You must have a comma for each possible field
- You must have a carriage return at the end of each record.
- E-mail is mandatory because you must have a way to forward credentials to your guests
- If Import Passwords is enabled the password is mandatory and it must be the last field in the row of data
- If the template is set to send SMS messages to guests, you must include Mobile Number and Mobile Provider
- Other fields may be required for the guest to enter but are optional for the CSV file

1. Log into FortiNAC.
2. The **Guest/Contractor Accounts** window is displayed. Admin users select **Users > Guest/Contractor Accounts**.
3. Click **Add**.
4. In the **Add Account** screen, click **Bulk Accounts**.
5. Select the template that will be used to create these bulk accounts.
6. To manually enter passwords as part of the import file, enable **Import Passwords**. If you prefer that the system generate the passwords, disable this option. If Import Passwords is enabled, it is a required field for each guest. Without this data you cannot import the file.
7. Once the template has been selected you can see the fields that can be imported in a list across the screen. E-mail is bolded indicating that it is required for import. Fields that are preceded by an asterisk are required prior to login but are not necessarily required for import. Therefore, including them in your CSV or text file is optional. Note that if you intend to send login information to guests via SMS, Mobile Provider and Mobile Number fields must be included both in the template and in the import file.
8. For this example, assume that the list of fields on the Bulk Account window is as follows: First Name, Last Name, Address, City, State, Zip, Email, Phone

   Based on the list of fields shown above, the CSV file could look like this:

   ```
   Ana,Bahr,44 Bow St,Pittsfield,NH,03263,asbahr@yahoo.com,603-523-7676
   ,,,,,,jjones@yahoo.com,
   James,Smith,,,,,,jsmith@aol.com,
   ```
9. Save the file as .csv or .txt and make note of its location on your hard drive.
10. On the Bulk Accounts window, click **Import From File**.
11. On the Import From File window, click Choose File. Browse to your CSV file, select it and click **Open**.
12. The contents of the file display in the Bulk Accounts window. Click **OK**.
13. The View Accounts screen opens with the account information in it. See Provide login information on page 601.
14. Click **Print** or **Send e-mail** or **Send SMS** to provide account information and password to the guest or contractor, or Close. These options are visible to you depending on the privileges you have in your profile. Additional text can

be added to the printout or email by typing the text into the Notes tab on the Guest/Contractor template before creating the account. See Create templates on page 569.

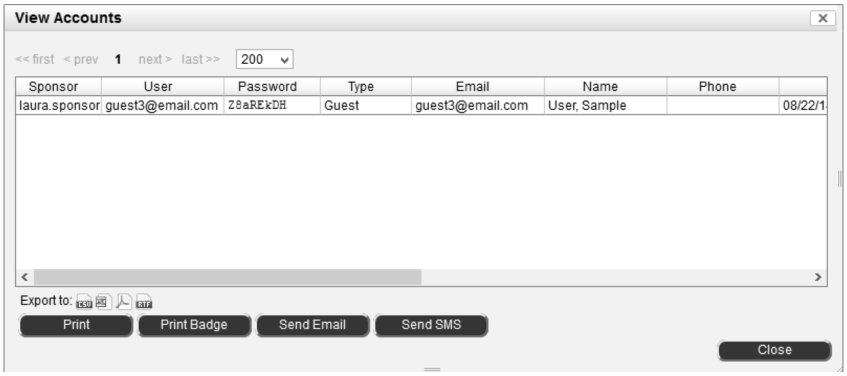
Provide login information

After you have created a Guest or Contractor account, you may want to provide that user with his login information. This information can be printed, viewed on the screen, included in an e-mail or sent to a mobile phone via an SMS message. To include additional text with the account information sent to the guest, you must add the text to the Guest Account template under the Note tab prior to creating the account. See the Guest Template Note section in Create templates on page 569.

Guests who use the self-registration option in the portal receive their credentials automatically. You do not need to send account information to those guests unless they lose the information.

For information on printer settings for guest badges, see Printer settings for guest badges on page 590.

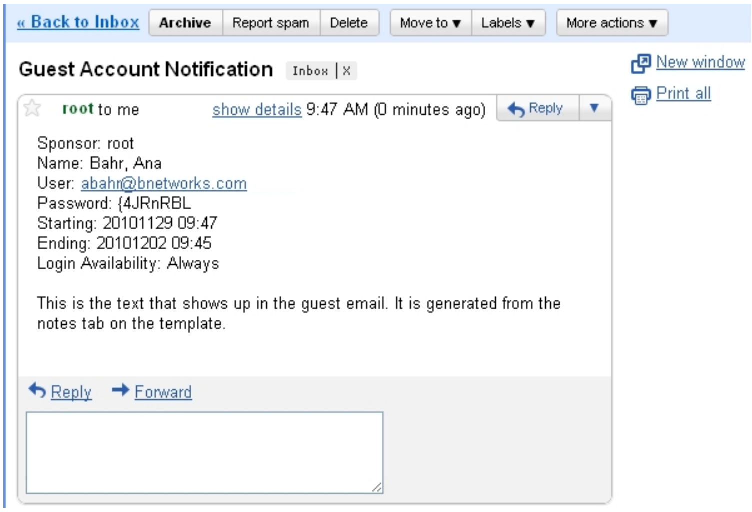
1. Make sure you are on the **Guest/Contractor Accounts** view. Admin users select **Users > Guest/Contractor Accounts**.
2. The list of Guest/Contractor Accounts is displayed.
3. Select one or more accounts for which you wish to view additional information.
4. Click the **View** button.



View Accounts

Sponsor	User	Password	Type	Email	Name	Phone	
laura.sponsor	guest3@email.com	Z8aREkDH	Guest	guest3@email.com	User, Sample		08/22/1

5. Do the following:
   - Click **Print** to print the guest/contractor account information on a full (8.5 X 11) page.
   - Click **Print Badge** to print out the badge containing the guest/contractor account information.
6. Click **Send Email** to send account information to the e-mail account listed.



Guest Account Notification

root to me show details 9:47 AM (0 minutes ago)

Sponsor: root
Name: Bahr, Ana
User: abahr@bnetworks.com
Password: {4JRnRBL
Starting: 20101129 09:47
Ending: 20101202 09:45
Login Availability: Always

This is the text that shows up in the guest email. It is generated from the notes tab on the template.

7. Click S**end SMS** to send account information to the mobile phone number listed in the guest's account.
8. Click **Close** to close the window.

Conference accounts

As a Sponsor, if you have been granted permission in your Admin Profile, you may create Conference accounts, which are bulk accounts in which the account information may be the same for all attendees, or unique to each conference attendee. Conference accounts ensure that attendees have the information they need to access the conference account ahead of time.

Before you create the conference account, determine how you want to manage attendee names and passwords. You may specify:

- Individual names and passwords
- The same name and password for all attendees (for example Seminar1, seminar123)
- Individual attendee names and the same password for all.

If you select Individual Passwords, they will be generated by Guest Manager. Generated passwords do not include characters that could be difficult to identify, including: the number one, the letter l (ell), the uppercase letter I (eye), zero, upper or lowercase letter O. In addition, the template used to create the Conference accounts may have specific characters to be excluded from passwords.

Create accounts

Conference Accounts cannot be modified. The only change that can be made is to Reset Passwords. To modify Conference Accounts you must delete the accounts and create new ones.

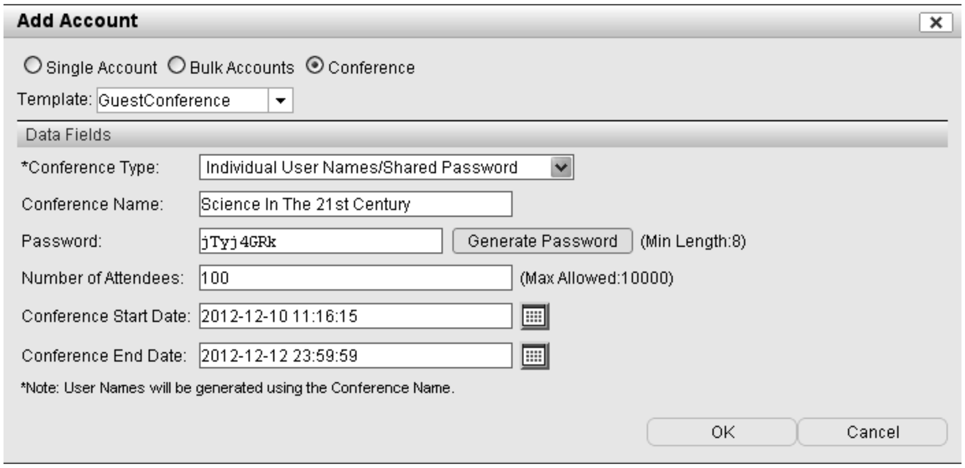
1. Log into your Sponsor account.
2. The Guest/Contractor Accounts window is displayed. Admin users select **Users > Guest/Contractor Accounts**.
3. Click **Add**.
4. On the Add Account screen click **Conference** .
5. Fill in the fields as needed.

6. Click **OK**. The View Accounts screen opens with the account information in it. See Provide login information on page 601.
7. Click **Print** to print out account and password information, or **Close**. These options are visible to you depending on the privileges you have in your profile.

E-mail cannot be sent to these conference attendees unless you enter an e-mail address for each attendee to whom you would like to send e-mail using the Modify User option on the User View.

SMS messages cannot be sent to these conference attendees unless you enter a mobile number and mobile provider using the Modify User option on the User View.

Guests also display on the User View. See User view on page 637.



Add Account

○ Single Account ○ Bulk Accounts ● Conference

Template: GuestConference

Data Fields

*Conference Type: Individual User Names/Shared Password

Conference Name: Science In The 21st Century

Password: jTyj4GRk (Min Length:8)

Number of Attendees: 100 (Max Allowed:10000)

Conference Start Date: 2012-12-10 11:16:15

Conference End Date: 2012-12-12 23:59:59

*Note: User Names will be generated using the Conference Name.

Settings

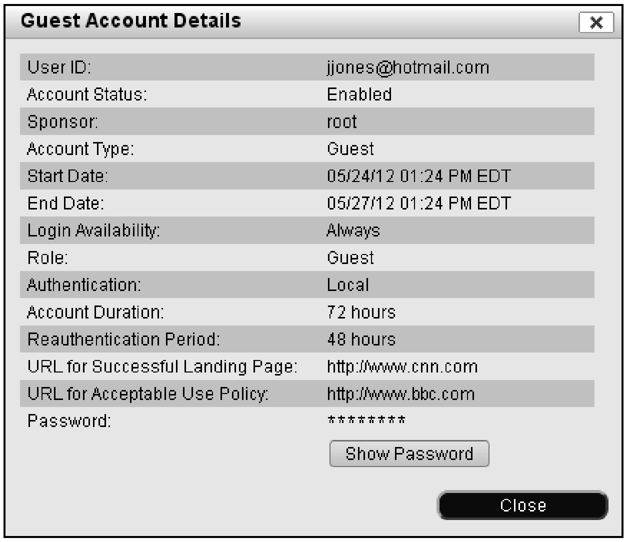
Field	Definition
Template	Select a conference template.
Conference Type	The selection you make from the pull-down menu determines how user names and passwords are managed for the conference. If you click the **Generate Password** button, the Password field is automatically populated. The length of the password is determined by the length requirement specified in the Conference template. The available options are: • **Individual User Names/Individual Passwords**: Individual passwords are generated for each attendee. Conference members are required to enter their name and unique password. • **Individual User Names/Shared Password**: Enter a password in the Password field, or click **Generate Password**. Conference members are required to enter their name and the password that is shared among all conference attendees. • **Shared User Name/Shared Passwords**: Enter a password in the Password field, or click **Generate Password**. All conference attendees are required to enter

Field	Definition
	the shared name and password. FortiNAC does not recognize or restrict system-generated passwords that may be offensive.
Conference Name	Enter the name of the conference. Note that the name of the conference appears as the User Name (conference attendee name) in the list of attendees created when you click Apply on this window. This cannot be modified after the account is created. You must delete the account and create new conference accounts with a new name.
Password	Click Generate Password to generate a password or enter a password manually. Password must meet the minimum length designated in the selected Guest template. See the Conference Types listed above for additional details on generating Passwords.
Number of Attendees	Enter the maximum number of attendees who need network access.
Conference Start Date	Enter a date and time or click the Calendar icon.
Conference End Date	Enter date and time that attendees will no longer need network access. This defaults to the date and time calculated based on the number of hours entered in the Account Duration field in the template. For example, if the template Account Duration is set to 72 hours, the end date can be less than three days but it cannot be more than three days. If this field is empty, no Account Duration has been entered in the template and you can choose any end date. This date sets the User Expiration date for the Guest. A host registered to a guest inherits the setting for registered hosts in Global Aging. When the User expires, both the User and the Host are removed from the database. If the Host expires first, then only the Host is removed from the database. There are two methods that work together for determining the length of time a guest account is active. The shortest duration of the two is the one that is used to remove a guest account from the database. **Account Duration (Hours)**— Option included in the Guest Template to limit the time a guest account created with this template remains in the database. If this is blank, the guest account end date is used. The Account Duration starts only when the guest user first logs in. For example, you could create a guest account with a date range that spans one week and if the account duration was 24 hours, they would be able to log in for one 24 hour period any time during that week **Account End Date**— Option included on the Add Guest Account dialog to determine the date on which the guest account expires. This field is required when a guest account is created.

Guest account details

Guest User records created when Guest accounts are generated are displayed in the Users View with network and administrator users. The Guest Account Details window displays data from the Guest Template used to create the Guest User.

1. Select **Users > User View**.
2. Search for the appropriate user.
3. Select the user and either right-click or click the **Options** button.
4. Select **Guest Account Details**.



Guest Account Details

User ID:	jjones@hotmail.com
Account Status:	Enabled
Sponsor:	root
Account Type:	Guest
Start Date:	05/24/12 01:24 PM EDT
End Date:	05/27/12 01:24 PM EDT
Login Availability:	Always
Role:	Guest
Authentication:	Local
Account Duration:	72 hours
Reauthentication Period:	48 hours
URL for Successful Landing Page:	http://www.cnn.com
URL for Acceptable Use Policy:	http://www.bbc.com
Password:	********

Setting

Field	Description
User ID	Guest's email account which is used as the User ID at login.
Account Status	Indicates whether the guest account is enabled or disabled.
Sponsor	The administrator who created the guest account.
Account Type	Guest account type. Types include: **Guest**—A visitor to your facility with limited or Internet-only network access. **Conference**—A group of short- or long-term visitors to your organization who require identical but limited access to your network for typically one to five days. **Contractor**—A temporary employee of your organization who may be granted all or limited network access for a specific time period generally defined in weeks or months.
Start Date	Date and time (using a 24-hour clock format) the account will become active for the guest or contractor.
End Date	Date and time the account will expire.
Login Availability	Times during which the guest is permitted to access the network.

Field	Description
Role	Role is an attribute of a user or a host. It is used in User/Host Profiles as a filter when assigning Network Access Policies, Endpoint Compliance Policies and Supplicant EasyConnect Policies.
Authentication	Indicates type of authentication used. Options include: Local, LDAP or RADIUS. Guests typically use Local authentication.
Account Duration	Amount of time this account will remain valid and usable.
Reauthentication Period	Number of hours the guest or contractor can access the network before reauthentication is required.
URL for Successful Landing Page	Directs the guest or contractor to a specific web page when they have successfully logged into the network and passed the scan in an Endpoint Compliance Policy. This field is optional and is used only if you have Portal V1 enabled in Portal Configuration.
URL for Acceptable Use Policy	Directs the guest or contractor to a specific web page that details the acceptable use policy for the network.
Password	The Guest's assigned password. Passwords are usually generated by the system unless the guests were bulk imported. Toggle the **Show Password/Hide Password** button to alternately display the password in plain text or as asterisks.

Guest/contractor login

The portal defaults to a guest or contractor login link which opens the default guest authentication page. To log into the network, guests and contractors must enter the required data fields on their account.

1. From the Guest or Contractor Login page, the guest clicks the **Start** link to open the Welcome screen.
2. Guests enter the Username and the Password that was provided to them by a printout, e-mail or SMS message.
3. Guests click **Download** or **Register** to open the Registration screen.
4. The fields that appear in the Registration screen are those that were defined in the Guest/Contractor template. Fields with an asterisk indicate to the guest that this information must be entered in order to register.
5. The guest clicks **Acceptable Use Policy** to read, accept, and exit the Acceptable Use Policy page.
6. The guest clicks **Continue** button. If the host passes the Endpoint Compliance Policy requirements, the successful landing page is displayed.
7. If the host does not pass the Endpoint Compliance Policy requirements, a remediation web page appears and directs the guest to correct the problems that inhibited opening his account.

Using a kiosk

A sponsor is an individual who is granted permission by an administrator to create accounts for guests or contractors. If you are a kiosk sponsor, you log in to a self-serve kiosk with your credentials and display the self-serve web page.

Depending on the parameters defined in the Kiosk Admin Profile by the administrator, the kiosk may only be available on specified days of the week during certain times of the day. As long as you, the kiosk sponsor, remain logged onto the kiosk, guests can create their own accounts. It is strongly recommended that you use a kiosk browser. Kiosk browsers block users from accessing other programs on the host or other web sites.

The required data for guest accounts is pre-defined by the administrator in the Guest template. The required data may include a guest’s name, e-mail, and address. Once guests have created their accounts they can go anywhere within the facility to access the network.

A self serve kiosk:

- Reduces a sponsor’s workload because guests create their own accounts.
- Frees up IT staff from having to create accounts.
- Makes it easier for guests visiting short-term to have network access.
- Allows guests immediate network access without depending on someone to do it for them.

To set up your kiosk:

1. Install a Kiosk browser on the computer being used as the kiosk. See Kiosk browser on page 607.
2. If you plan to have guests print out their credentials, make sure that printer settings are correct for printing guest badges with login information. See Printer settings for guest badges on page 590.
3. If you plan to allow guests to send credentials to a mobile telephone using an SMS message the following requirements must be met:
    - The guest template associated with the Kiosk administrator profile must have Send SMS enabled and Mobile Number and Mobile Provider must be included in the data fields required for the guest account.
    - Enable the Mobile Providers that guests might be using in the Mobile Provider view. See Mobile providers on page 175.
4. Create a guest template that will be used in the Kiosk. The settings in this template control all aspects of the guest account created through the kiosk. See Create templates on page 569.
5. Create an Admin Profile that permits only kiosk access and associate the kiosk guest template. See Add a guest kiosk profile on page 581 .
6. Create a new administrative user and apply the Kiosk Admin Profile to that user.
7. When the Kiosk user has been created, have the that user log into the computer being used as the kiosk. See Log into a kiosk on page 608.

You are now ready to allow guests to create their own accounts.

Kiosk browser

Many browsers can be set to Kiosk mode to prevent access to everything on the computer on which the browser is running. If your guests will be creating their own network accounts on a publicly available computer, it is recommended that you install a browser that can run as a Kiosk browser. The example and instructions show below are for Firefox. Many other browsers have similar capabilities.

1. Download and install Firefox.
2. Download and install the Real Kiosk add-on.

Once the Real Kiosk add-on is installed, this browser will always run in Kiosk mode.

3. To close Firefox once it is in Kiosk mode type **Alt+F4**.
4. To go to the homepage type **Alt+Home**.

5. To temporarily access Firefox in normal mode, right-click on the Firefox icon and select Properties. In the **Target** field go to the end of the path, add `safe-mode` and click **OK**.
6. Launch Firefox.

Log into a kiosk

As an Administrative user, your administrator has enabled Kiosk Mode in your Admin Profile. This means that once you have logged into a self-serve kiosk, guests can create their own accounts. Guests have access to the network according to the parameters defined by your administrator in the Guest template.

The use of a kiosk browser is recommended to prevent the guests or contractors from logging out and to provide more security.

1. Bring up a web browser and type in the URL: `http://<Hostname>:8080`
2. This brings you to the Administrative User login screen.
3. Enter the Username and Password given to you by your Administrator. The Kiosk Welcome Message Screen appears. Guests also see this Welcome screen.
4. A screen appears with **Information Required to Create an Account**.
5. From this screen, guests can create their own accounts.

Account creation

1. A guest sees a welcome screen with instructions supplied by the administrator.
2. The guest clicks the **Start** button in the welcome screen.
3. A screen opens with a form. Guests must enter their e-mail address, but the other information may be entered upon their arrival or later, when they activate their account.

Parameter	Description
E-mail	The guest’s e-mail address. This becomes the guest's user name for logging on to the network. It is also used to email credentials if desired. Required.
Account Start Date	In Kiosk mode, the date and time cannot be changed. The account end date is determined by the duration entered in the kiosk template specified in the kiosk admin profile. Accounts will never remain active beyond 11:59 PM each day. If no duration is specified in the template of if the duration extends beyond midnight, the account will expire at 11:59 PM on the current day. If the duration ends before midnight, the account will expire at the specified time.
Account End Date	
Additional Account Information	Guests enter Additional Account Information to create an account. The asterisk (*) indicates required fields. Note that the fields that appear in this screen were predefined in the template.
Mobile Number Mobile Provider	If you intend to allow guests to send themselves an SMS message with their login credentials, these two fields must appear on the Kiosk window.

4. The guest clicks Apply, which opens an account details screen containing the guest's e-mail and a generated password. Depending on the configuration of the template used to create the account, guests can print out their credentials so they have password available when they log in later, they can email credentials to themselves or they

can send an SMS message to their mobile telephones.

5. Click **Finish**.

Account activation

The following procedure describes the steps guests follow to activate their temporary account on their own regardless of how it was created. Guest accounts can be created either by an Administrator, an administrative user with a Sponsor profile or the guest themselves using a Kiosk. Once the guest has received his login credentials through one of these account creation methods, the activation process is as follows:

1. Guests type in their e-mail address and the password that was generated when the account was created.
2. Guests click **Register** or **Download**.
3. The Welcome screen opens.
4. The account information in this screen may be filled in if guests entered the data when they arrived. If they did not, they need to do so at this time to create their account. The fields denoted with an asterisk (*) are the pre-defined required fields.
5. Guests click **Continue**. After a few moments, a pop-up screen appears with the Dissolvable Agent.exe file. Guests save this file on their computer.
6. Once guests are at the location in the facility where they will use their computer, they must run the .exe file, which scans their computer. The guest receives a pass or fail message.
7. If the host does not pass the policy requirements, a remediation web page appears and directs the guest to correct the problems that inhibited opening his account.
8. If the computer passes, the .exe file is automatically removed. Now the guest can go anywhere in the facility and connect to the network.

Kiosk shut down

A self-serve kiosk is shut down when the specified login period for the kiosk sponsor has elapsed. Guests will no longer be able to create their own accounts until the kiosk sponsor logs back into the kiosk. During the period that the kiosk is shut down, guests should be directed to contact the help desk for account creation.

Guest self-registration

Use the Self-Registration feature to allow a guest to create a request for access to your network from their own device. When the guest opens a browser he is redirected to the registration page in the captive portal. From that page he can either login with previously assigned credentials or request access. Requests are forwarded to a Sponsor or to a request pool to be approved or denied. When a request is approved, the guest receives his credentials in the browser on the login page, in an email or in an SMS message sent to his mobile telephone. All guest accounts are configured to expire after a user specified amount of time based on the template with which they are created.

Implementation

It is recommended that you review the Implementation process for Guest Manager for general setup details. This section covers only those configuration details that are specifically required for Guest Self-Registration.

- All guest accounts are created based on a template. For Guest Self-Registration you must create a template with Visitor Type set to Self-Registered Guest and it must have an Account Duration to indicate when the account should expire. There is a default template, GuestSelfRegistration, that can be used or you can create a new one. All Self-Registered guests are configured with the same template. The template used is selected in the Portal Content Editor under **Registration > Self-Registration Login**.
- Create an Admin Profile specifically for Administrative users that will respond to Guest Self-Registration requests these users could also have permission for Guest/Contractor Accounts or other parts of FortiNAC that you deem appropriate for their job. See Add a guest self registration profile on page 582.
- Create one or more Administrative users that will be responsible for processing Guest Self-Registration requests and apply the Guest Self-Registration profile. Administrative users must have an e-mail address if they are to receive and respond to requests for guest accounts. Note that Admin users can be created based on groups in your Directory and permissions or profiles can be automatically assigned based on those groups. This can be useful if many people in your organization will be responsible for processing Guest Self-Registration requests. See Set admin privileges based on directory groups on page 692.
- Configure your portal pages for Guest Self-Registration in the Portal Content Editor. See Portal page setup for version 2 on page 588 and .
  - Within the Portal you can specify the sponsor or sponsors to which the request should go or you can enable the Sponsor field for the guest to fill in when creating the request. The guest must enter the sponsor's email address.
  - If you do not enable the Require Sponsor Approval option for guest accounts, guests simply create their own accounts using the template specified in the portal.
- If you require Sponsors and other Admin Users to connect to the Admin UI using https or if you are in a High Availability environment where redundant servers do not share an IP address because those servers are on different subnets you must configure settings to generate the correct links in the emails sent to Sponsors. See Configure the email link on page 611.

Requesting an account

1. Connect to the network.
2. Open a browser. The Isolation message is displayed briefly.
3. The browser is redirected to the Registration page.
4. On the Registration page, click the **Self Registration** option. A request form is displayed.
5. Fill in the form and click **Request Guest Access**. Depending on the configuration of the web page, you may be required to enter the email address of a Sponsor. A Sponsor is a person who has access to the FortiNAC administration program and can approve or deny your access request.
6. The browser displays a welcome message and asks you to wait. You can click **Cancel** if you wish to cancel the request.
7. The request expires if it is not responded to within the number of minutes configured in the portal. The default is 20 minutes.
8. When the Sponsor approves the request, you are taken to the **Login** screen. Depending on the portal configuration, credentials are filled in automatically, they are sent to the guest via email and in an SMS message.
9. Click **Login** on the Welcome page. The the Success page is displayed.
10. A message is displayed indicating that your network is being reconfigured and to close and reopen the browser. Close the browser and reopen it. You are now on the Production network and should be able to access the internet freely.
11. If you shut down your computer and access the network again later, you must open a browser and login again. If cookies are enabled on your computer, the login screen is displayed and the User Name and Password fields may be pre-populated.

Approve or deny a request

When a guest connects to your network and selects Self-Registration from the Registration page in the portal, a request for an account is sent to FortiNAC. The request is sent via email to a Sponsor for approval, however an Administrator can go to the Self-Registration Requests View and approve or deny any pending requests.

1. A guest connects to the network, opens a browser and is taken to the Registration page. The guest submits a request for access.
2. The Sponsor receives an email indicating that a guest has requested an account. Within the email there is either a Login link or Approve and Deny links depending on the configuration of the Self-Registration page in the portal.
3. If the email contains Approve or Deny links, the sponsor clicks the appropriate link. The Guest receives a message indicating that he has been approved or denied. If the request is approved, the guest can login and use the network.
4. If the email contains a Login link, the sponsor clicks **Login** and is taken to a login window for the FortiNAC Admin UI.
5. The Sponsor logs in and the Self-Registration Requests view is displayed with the appropriate request record opened.
6. The Sponsor can add a message indicating what the Guest should do or the reason for a denied request. This message is displayed to the guest in the browser.
7. The Sponsor clicks **Approve** or **Deny** and the response is sent to the Guest.
8. If approved, the Guest can access the network.

Configure the email link

In Guest Manager when Self Registration Requests are sent to sponsors, the email messages contain links for the sponsor to either automatically accept or deny the request, or to login to the Admin UI to do this. In both cases, the default links provided use non-secure HTTP access. If you are using an SSL certificate to secure the FortiNAC Admin UI and you block access to HTTP for Admin Users, the links used in emails to Sponsors for guest self-registration must use https.

The link contained in the email is composed by FortiNAC. The link contains the URL of the FortiNAC server or Control server. In a High Availability environment with an L3 configuration where redundant FortiNAC servers are on different subnets and do not use a shared IP address the URL should contain the FQDN of the correct FortiNAC server or control server.

To configure FortiNAC to use https and the FQDN of the server in the email links you must modify a property file on the FortiNAC server. There are two options that can be set in several different ways. See the table below:

Property	Definition
com.bsc.plugin.guest.SelfRegRequestServer.EmailLinkHost=	Embeds the FQDN of the FortiNAC Server or Control Server in the URL used in the email link. Typically FortiNAC can determine the FQDN, however if there is an issue the FQDN can be configured here. If this property is configured the EmailLinkUseHttps property shown below is ignored. Therefore, if https and port 8443 are required, they must also be configured here.

Property	Definition
com.bsc.plugin.guest.SelfRegRequestServer.EmailLinkUseHttps=	Indicates whether to use HTTPS and port 8443 or HTTP and port 8080 in embedded email links. If this is blank or false, HTTP and port 8080 are used. If this is set to true, HTTPS and port 8443 are used.

Modify the property file as follows:

1. Log into the CLI as root on your FortiNAC Server or Control Server.
2. Navigate to the following directory: `/bsc/campusMgr/master_loader/`
3. Using vi or another editor, open the `.masterPropertyFile` file.
4. At the top of the file there is a sample entry that is commented out. Follow the syntax of the sample entry to create your own changes using one of the following examples:

   Example 1

   To configure email links to use https and port 8443 set EmailLinkUseHttps to true:

   ```
   FILE_NAME=./properties_plugin/selfRegRequest.properties
   {
   com.bsc.plugin.guest.SelfRegRequestServer.EmailLinkHost=
   com.bsc.plugin.guest.SelfRegRequestServer.EmailLinkUseHttps=true
   }
   ```

   Example 2

   To configure email links to use the FQDN of the FortiNAC Server or Control Server add the information to the EmailLinkHost property.

   ```
   FILE_NAME=./properties_plugin/selfRegRequest.properties
   {
   com.bsc.plugin.guest.SelfRegRequestServer.EmailLinkHost=http://<FQDN>:8080
   com.bsc.plugin.guest.SelfRegRequestServer.EmailLinkUseHttps=
   }
   ```

   Example 3

   To configure email links to use the FQDN of the FortiNAC Server or Control Server and use https and port 8443 add the information to the EmailLink Host property.

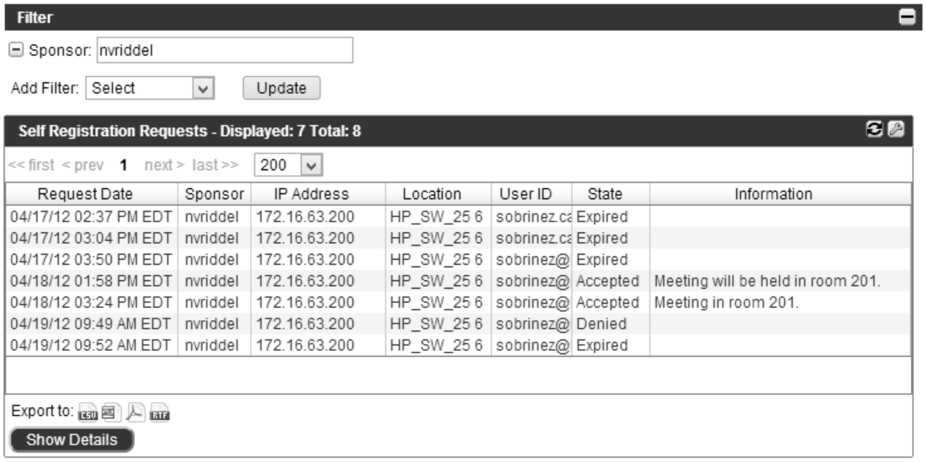
   ```
   FILE_NAME=./properties_plugin/selfRegRequest.properties
   {
   com.bsc.plugin.guest.SelfRegRequestServer.EmailLinkHost=https://<FQDN>:8443
   com.bsc.plugin.guest.SelfRegRequestServer.EmailLinkUseHttps=true
   }
   ```
5. Save the changes to the file.
6. Restart the FortiNAC Server. When the server restarts the changes listed in the `.masterPropertyFile` are written to the `selfRegRequest.properties` file.
7. Log into the CLI of the FortiNAC Server or Control Server and navigate to the following directory: `/bsc/campusMgr/master_loader/properties_plugin/`

8. View the contents of selfRegRequest.properties and verify that the changes have been written to the file. At the prompt type: `cat selfRegRequest.properties`

Self-registration requests

Use the Self-Registration Requests view to manage requests for network access submitted by Guests from the captive portal. The table shows requests based on the search parameters entered, including pending requests that have yet to be processed. Pending requests are approved or denied from this view and a message can be included for the Guest.

To access the view select **Users > Self-Registration Requests**. See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.



Filter

⊟ Sponsor: nvriddel

Add Filter: Select

Update

Self Registration Requests - Displayed: 7 Total: 8

<< first < prev 1 next > last >> 200

Request Date	Sponsor	IP Address	Location	User ID	State	Information
04/17/12 02:37 PM EDT	nvriddel	172.16.63.200	HP_SW_25 6	sobrinez.ca	Expired	
04/17/12 03:04 PM EDT	nvriddel	172.16.63.200	HP_SW_25 6	sobrinez.ca	Expired	
04/17/12 03:50 PM EDT	nvriddel	172.16.63.200	HP_SW_25 6	sobrinez@	Expired	
04/18/12 01:58 PM EDT	nvriddel	172.16.63.200	HP_SW_25 6	sobrinez@	Accepted	Meeting will be held in room 201.
04/18/12 03:24 PM EDT	nvriddel	172.16.63.200	HP_SW_25 6	sobrinez@	Accepted	Meeting in room 201.
04/19/12 09:49 AM EDT	nvriddel	172.16.63.200	HP_SW_25 6	sobrinez@	Denied	
04/19/12 09:52 AM EDT	nvriddel	172.16.63.200	HP_SW_25 6	sobrinez@	Expired	

Settings

Fields used in filters are also defined in this table.

Field	Definition
Request Date	Date and time the request was received.
Response Date	Date and time that either the sponsor or the server responded to the request. For example, if the request expires, the server sends a message to the guest advising that the request expired.
Response Expiration	Date and time that the request expires. This is calculated based on the expiration settings in the Portal Contents Editor under **Registration > Self Registration Login**.
Sponsor	User name of the sponsor or the administrator who processed the request. For pending requests it is the user name of the sponsor to whom the request was sent.
IP address	IP address of the host associated with the guest who sent the request.
Physical Address	MAC address of the interface with which the host connected to the network.
Location	The name of the device and port where the guest is connected to the network.
User ID	User name of the guest requesting network access.

Field	Definition
State	State of the request. Includes: Accepted, Canceled, Denied, Error, Expired or Pending.
Information	Contains text such as messages sent by the sponsor to the guest or the reason for an error state.
Buttons	
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.
Show Details	Displays the Details Panel for the selected request. If the request is pending, allows you to approve or deny the request.

Details

The Details dialog displays information about a request for access sent by a guest user from the Self-Registration page in the portal. If the request is still pending, the details window is used to approve or deny the request. If the request has been processed or has expired, the details window shows the history of the request.

View or process a request

1. From the menu bar select **Users > Self Registration Requests**.
2. Use the Filters to locate the request you want to view or process.
3. Select the appropriate request from the list and click **Show Details**.
4. If this is a pending request, include a message for the guest in the Information field and click **Approve** or **Deny** to process it.
5. If this is a request that has already been processed, view the details and then click **Hide Details** to close the window.

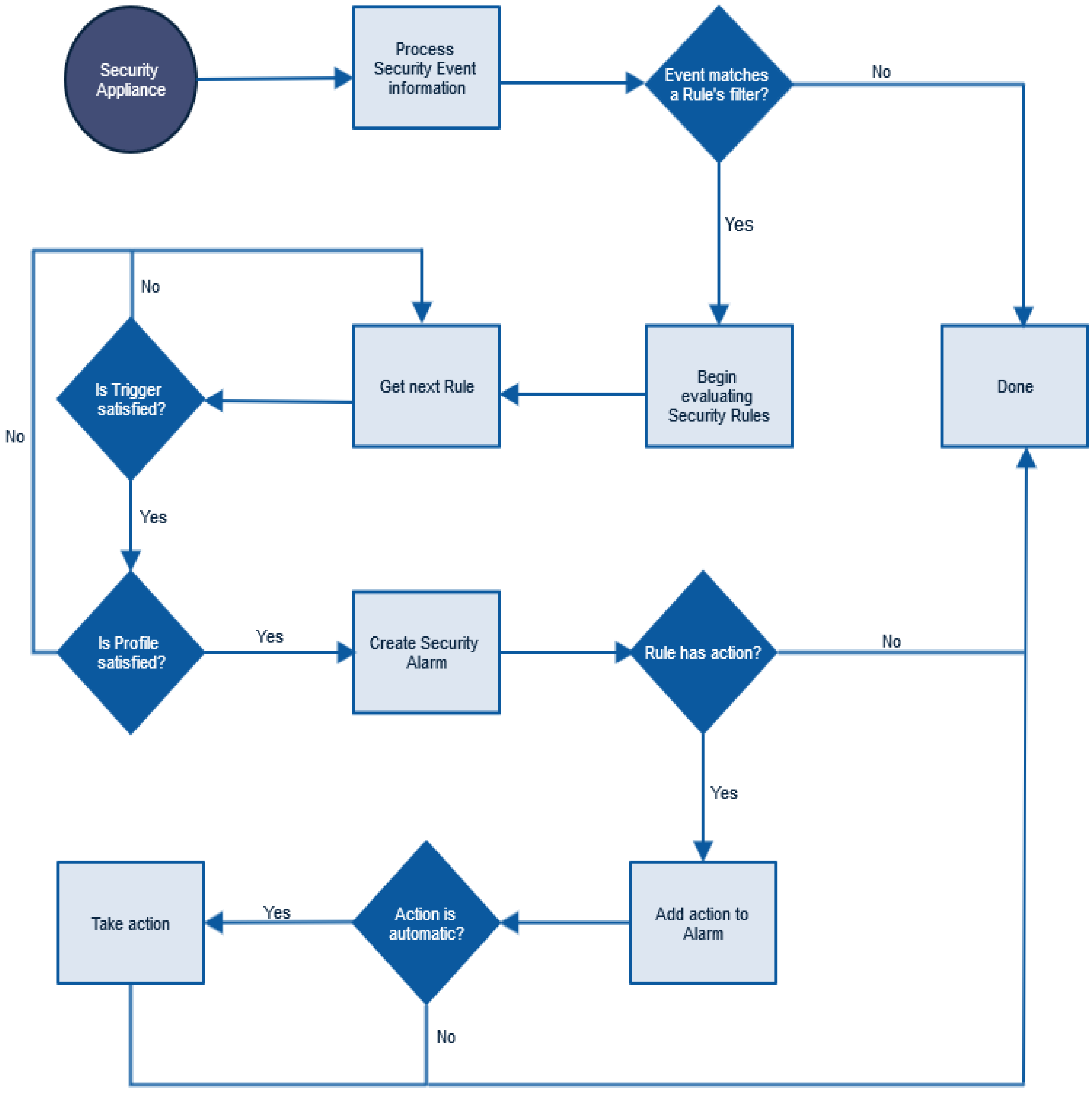
Automated Threat Response (ATR)

Automated Threat Response (ATR) integrates with security solutions such as FireEye, Fortinet, and Palo Alto Networks to correlate security alerts. Incoming information is normalized into a consistent Security Event format and provide additional information about the source hosts.

ATR isolates restricts, or blocks compromised endpoints and reduces threat containment time by:

- Automating actions on an event based on policies
- Providing information in security alerts
- Prioritizing security events
- Tracing a threat across IT domains and automating an action to minimize the threat containment time

If you have not purchased the ATR license you will not be able to access the ATR features.



Implementation

Automated Threat Response (ATR) allows you to build Security Rules to trigger on administrator defined-patterns of Security Events to generate Security Alarms. Security Rules can be targeted to only generate alarms for specific hosts, users, and locations. Actions can be taken on Security Alarms to isolate or block compromised hosts automatically.

This section of the documentation discusses the implementation in the order in which it should be done. As the options are discussed, links to additional information are provided.

Network devices

Find or create devices

You will need to find or create the network devices wish to configure. See Find containers or devices on page 22or Add or modify a pingable device on page 725. For pingable devices, ATR provides the Security Events option. This allows you to select a security appliance from which events may be accepted in order to create a security event when an event rule is matched.

Threat analysis engines

When you have configured the security devices, you can create threat analysis engines, which will scan applications on the host to determine the threat level, and provide a threat score.

Security policies

Security rules

Once you have configured your network devices, you must create security rules. Security Rules contain triggers that correlate incoming events from the network devices and create an alarm. Defined in the host profile, security rules determine which actions to take based on the alarm that is triggered by the host. See Security rules on page 620.

Creating a security rule to catch all incoming events enables you to analyze traffic and identify patterns in order to create rules based on this information. Add a trigger with a single filter, with a minimum severity of 0 and a maximum severity of 10. This will ensure that incoming events of all severity levels are captured by the system.

After you create the trigger, add a security rule using the trigger and set both the User/Host Profile and Action to None.

This Security Rule will catch all incoming events. To ensure that it does not interfere with normal system operation, it should be the lowest ranked rule.

Because this Security Rule will produce a large number of security events, it will affect system performance. The Security Rule should only be enabled in production during specific times, such as off hours.

Once all incoming Security Events are captured, you can create Security Rules directly from the Security Events view based on various types of Security Events. See

Permissions

You must provide permissions for users to view security alarms that are created when a security rule is matched. Users can may then take action on a security alarm if it was not done automatically. You can allow the user to take any action on an alarm, or specify the actions the user is allowed to take. See Add an admin profile on page 671.

Monitor the system

You can monitor and take actions on alarms created from incoming events that satisfy triggers established by security rules that are defined for the host. See Security events on page 634.

A security rule with a trigger satisfied and a matching User/Host profile creates a security alarm. The rule may then take an action automatically. The action for a higher-ranked rule takes precedence over the action for a lower-ranked rule. The lower-ranked rule is not implemented automatically, but can still be done manually. However, the action for a higher-ranked security rule will override a lower-ranked rule that was previously implemented.

You can configure the application settings when creating the security rule in Policy Configuration. See Add or modify a rule on page 622. As hosts are scanned by the agent, the applications are updated. The security rule includes the applications as part of the trigger that will create an alarm when the rule is satisfied. See Application view on page 825.

Security event severity level mappings

Each vendor defines its own severity levels for syslog messages. These severity levels are normalized within FortiNAC to provide additional filtering options for incoming security events. The following table provides severity level mappings between the vendor and FortiNAC.

CheckPoint

Vendor Severity Level	FortiNAC Severity Level
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	10

Stonegate

Vendor Severity Level	FortiNAC Severity Level
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8
8	9
9	10

TippingPoint SMS

Vendor Severity Level	FortiNAC Severity Level
0	1
1	3
2	5
3	7
4	9

FireEye

Vendor Severity Level	FortiNAC Severity Level
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8
8	9

Vendor Severity Level	FortiNAC Severity Level
9	10

FortiOS

Vendor Severity Level	FortiNAC Severity Level
INFORMATION	1
NOTICE	3
WARNING	5
ALERT	7
CRITICAL	8
ERROR	9
EMERGENCY	10

PaloAlto

Vendor Severity Level	FortiNAC Severity Level
INFORMATIONAL	1
LOW	3
MEDIUM	5
HIGH	7
CRITICAL	9

Security rules

Create and manage Security Rules based on triggers that correlate incoming events from network devices. When a security event is received, the highest ranked security rule with a trigger satisfied and a matching User/Host profile creates a security alarm. The rule may then take an action automatically.

See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.

Settings

An empty field in a column indicates that the option has not been set.

Field	Definition
Rank Buttons	Moves the selected rule up or down in the list. Incoming events are compared to rules in order by rank.
Set Rank Button	Allows you to type a different rank number for a selected rules and immediately move the rule to that position. In an environment with a large number of rules this process is faster than using the up and down Rank buttons.
Table columns	
Rank	Rule's rank in the list of rules. Rank controls the order in which incoming events are compared to Security Rules.
Name	User defined name for the security rule.
Enabled	Indicates whether the rule has been enabled.
Trigger	The set of events that will activate the rule if the rule is enabled.
Host Profile	The host profile to which the security rule applies. The = sign indicates the host must match the user host profile. The ≠ indicates the host must not match the user host profile. An alarm is triggered when the security rule is satisfied.
Action	The action that will be associated or automatically taken when the security rule is activated.
Rule Match Email Group	If enabled in the security rule, the Admin Group that will receive an email when the rule creates an alarm.
Action Taken Email Group	If enabled in the security rule, the Admin Group that will receive an email when an action is taken on the created alarm.
Last Modified By	User name of the last user to modify the security rule.
Last Modified Date	Date and time of the last modification to this security rule.
Right click options	
Delete	Deletes the selected security rule.
Modify	Opens the Modify Security Rule window for the selected security rule.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671
Buttons	
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.

Add or modify a rule

1. Select **Policy > Policy Configuration**.
2. In the menu on the left select **Security Rules**.
3. Click the **Add** button or select an existing security rule and click **Modify**.
4. Click in the **Name** field and enter a name for this security rule.
5. Use the table below to enter the security rule information.
6. Click **OK** to save your security rule.

Settings

Field	Definition
Rule Enabled	Select this check box to activate the security rule.
Name	A unique name for this security rule.
Trigger	The trigger that will activate the rule. You can use the icons next to the Trigger field to add a new trigger or modify the trigger shown in the drop-down menu. When you modify this trigger, it is modified for all security rules that make use of the trigger.
User/Host Profile	Indicates whether the rule must match or not match the host profile selected from the drop-down menu. You can use the icons next to the Host Profile field to add a new host profile or modify the profile shown in the drop-down menu. A host profile is not applied to the trigger when **None** is selected.
Action	The action assigned to the security rule. You can select whether the action should be manual or automatic. You can use the icons next to the Action field to add a new action or modify the action shown in the drop-down menu. Note that by selecting **None**, an action is not assigned to the trigger.
Send Email when Rule is Matched	Select this check box to automatically send an email to the selected Admin Group when the security rule creates an alarm.
Admin Group drop-down menu	Select the Admin Group list that will receive the email when an alarm is created.
Send Email when Action is Taken	Select this check box to automatically send an email to the selected Admin Group when the action associated with the security rule is taken.
Admin Group drop-down menu	Select the Admin Group to be notified when the action associated with the security rule is taken.

Field	Definition

Admin Group Email Content	When you select Send Email when Rule is Matched and/or Send Email when Action is Taken, the email message that is sent to the selected Admin group contains information such as the security rule that was matched, the date and time of the alarm, the host and MAC address information, severity, and location of the host.
	The following is an example of the content included in the email:
	`Security Rule Matched = PA_test`
	`Alarm Date/Time = 2015-09-28 17:04:36.0`
	`User ID = testuser`
	`No owner`
	`Host Name = testuser-PC`
	`Host OS = Windows 7 Professional 6.1 Service Pack 1`
	`Host Hardware =`
	`Host MAC Addresses =`
	`     5C:26:0A:44:53:1D,00:24:D7:A2:24:5C,00:50:56:C0:00:01,00:50:56:C0:00:08`
	`Host IP addresses = 192.168.10.139,192.168.4.169,192.168.204.1,192.168.74.1`
	`Host Locations = Concord-3750 Fa3/0/6,Concord_Cisco_1131.example.com VLAN 4`
	`Date = 2015-09-28 17:04:35.0`
	`Alert Type = THREAT`
	`Severity = null`
	`ThreatID = null`
	`Description = HTTP OPTIONS Method(30520)`
	`Source IP = 192.168.10.139`
	`Source MAC = 5C:26:0A:44:53:1D`
	`Destination IP = 23.96.61.106`
	`Location = Concord-3750 Fa3/0/6`
	`Vendor = PaloAlto`

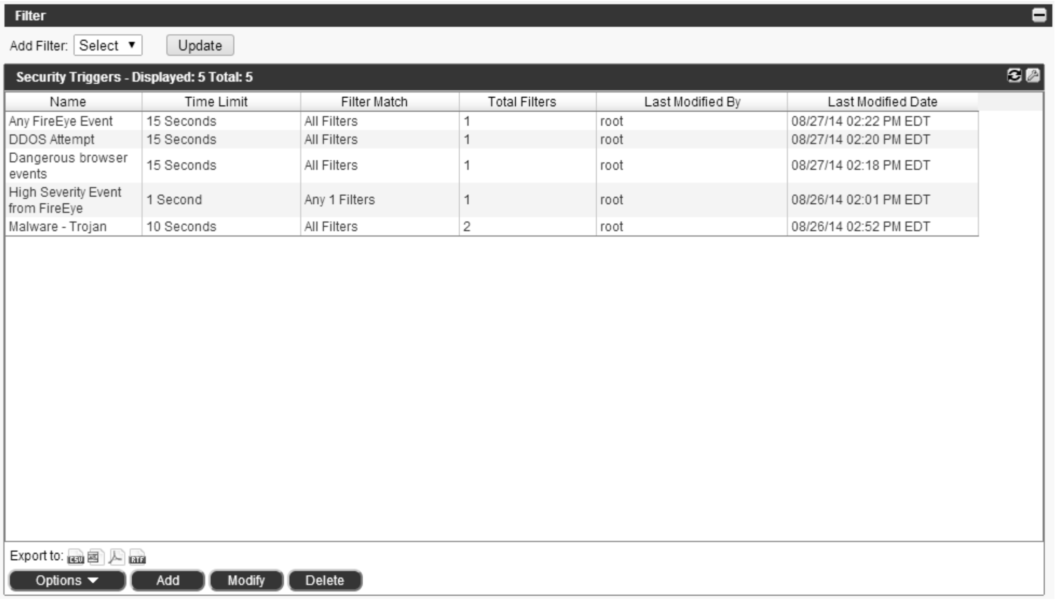
Delete a rule

1. Select **Policy > Policy Configuration**.
2. In the menu on the left select **Security Rules**.
3. Select a rule and click **Delete**.
4. A confirmation message is displayed. Click **Yes** to continue.

Triggers

Create triggers for security rules to correlate incoming security events from network devices. When an incoming security event satisfies a trigger, all security rules using the trigger are evaluated in order of their rank. A security alarm is created based on the first security rule which also matches its optional User/Host Profile. If no security rules are matched, an alarm is not created. An optional security action will be associated to the alarm and, if selected, will be executed automatically.

See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.



Security Triggers - Displayed: 5 Total: 5

Name	Time Limit	Filter Match	Total Filters	Last Modified By	Last Modified Date
Any FireEye Event	15 Seconds	All Filters	1	root	08/27/14 02:22 PM EDT
DDOS Attempt	15 Seconds	All Filters	1	root	08/27/14 02:20 PM EDT
Dangerous browser events	15 Seconds	All Filters	1	root	08/27/14 02:18 PM EDT
High Severity Event from FireEye	1 Second	Any 1 Filters	1	root	08/26/14 02:01 PM EDT
Malware - Trojan	10 Seconds	All Filters	2	root	08/26/14 02:52 PM EDT

Settings

Field	Definition
Add Filter drop-down list	Allows you to select a field from the current view to filter information. Select the field from the drop-down list, and then enter the information you wish to filter.
Update Button	Displays the filtered data in the table.
Table columns	
Name	User defined name for the trigger. The type of event that will activate the rule if the rule is enabled.
Time Limit	The time span to satisfy all required filters for the trigger to be satisfied.
Filter Match	The number of filters that must be matched by security events for the trigger to be satisfied. Select **Any** to set the minimum number of filters that must be matched. Select **All** to specify that all filters must be matched.
Total Filters	The number of security filters associated with the security trigger.
Last Modified By	User name of the last user to modify the security trigger.
Last Modified Date	Date and time of the last modification to this security trigger.
Right click options	
Delete	Deletes the selected trigger.
Modify	Opens the Modify Security Trigger window for the selected trigger.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847.

Field	Definition
	You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671
Buttons	
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.

Add a trigger

To verify that events are being captured, create a “Catch All” rule to log the security events.

1. Select **Policy > Policy Configuration**.
2. In the menu on the left expand **Security Rules**.
3. Click **Triggers**.
4. Click the **Add** button or select an existing security trigger and click **Modify**.
5. Click in the **Name** field and enter a name for this security trigger.
6. Use the table below to enter the security trigger information.
7. Click **OK** to save your security rule trigger.

Settings

Field	Definition
Name	A name for this security trigger.
Time Limit	The amount of time within which the incoming events must occur before satisfying the trigger.
Filter Match	Select whether any size subset of the security filters must be matched in order to satisfy the trigger.
Not currently in use/In use by	Indicates whether the trigger is in use, and the number of rules currently associated with the trigger.
Security filters	
Frequency	The number of times the security event must occur from the vendor in order to satisfy the trigger.
Vendor	The name of the vendor that is sending the security event.
Type	Specifies the type of security event.
Sub Type	Specifies the subtype of security event.

Field	Definition
Threat ID	A unique identifying code supplied by the vendor for the specific type of threat or event that occurred.
Description	A textual description supplied by the security appliance of the event.
Severity	The range within which the threat level must be defined in order to satisfy the trigger.
Number of Custom Fields	The number of custom fields that were added to the filter.
Add button	Click to add a filter.
Modify button	Click to modify a selected filter.
Delete button	Click to delete a selected filter.
Not currently in use/In use by	Indicates whether the action is in use, and the number of rules currently associated with the action.

Delete a trigger

1. Select **Policy > Policy Configuration**.
2. In the menu on the left expand **Security Rules**.
3. Click **Triggers**.
4. Select a trigger and click **Delete**.
5. A confirmation message is displayed. Click **Yes** to continue.

Add or modify filters

1. Select **Policy > Policy Configuration**.
2. In the menu on the left expand **Security Rules**.
3. Click **Triggers**.
4. Click the **Add** button or select a security trigger and click **Modify**.
5. Under **Security Filters**, click the **Add** button, or select a filter and click **Modify**.
6. Use the table below to enter the security filter information.
7. Click **OK** to save your security filter.

Settings

Field	Definition
Frequency	The number of times the security event must occur from the vendor in order to satisfy the trigger.
Vendor	The name of the vendor that is sending the security event.
Type	Specifies the type of security event.
Sub Type	Specifies the subtype of security event.
Threat ID	The code generated by the vendor for the security event threat level.

Field	Definition
Description	Additional details about the security event.
Severity Range	The range within which the threat level must be defined in order to satisfy the trigger.
Custom Fields	The custom fields that were added to the filter. Click **Add** to add a custom field. Click **Modify** to modify a selected field. Click **Delete** to delete a selected field.

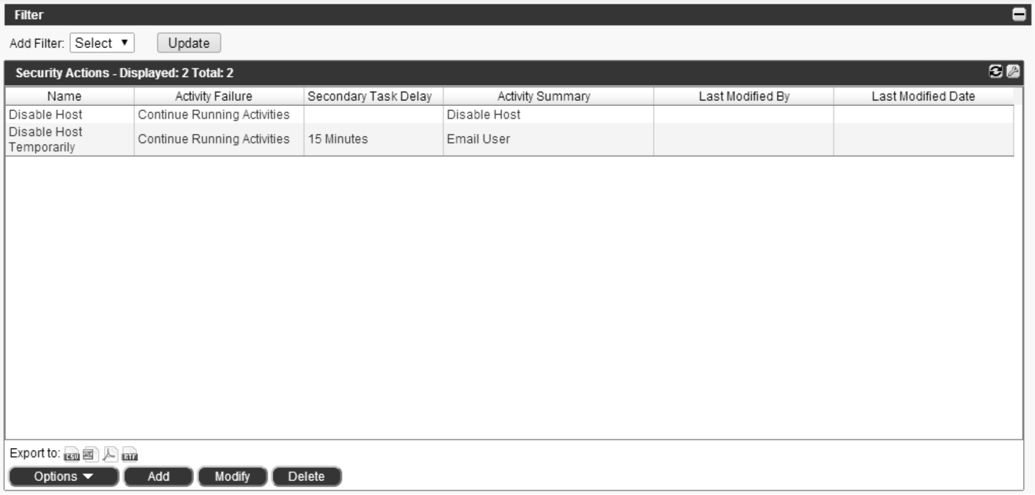
Delete a filter

1. Select **Policy > Policy Configuration**.
2. In the menu on the left expand **Security Rules**.
3. Click **Triggers**.
4. Select a trigger and click **Modify**.
5. Select a security filter and click **Delete**. The filter is deleted.
6. Click **OK**.

Security actions

The Security Actions view allows you to add, modify, and delete actions that can be associated to an alarm. If the action is selected, it can be executed automatically or manually, depending on the security rule configuration.

See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.



Security Actions - Displayed: 2 Total: 2

Name	Activity Failure	Secondary Task Delay	Activity Summary	Last Modified By	Last Modified Date
Disable Host	Continue Running Activities		Disable Host		
Disable Host Temporarily	Continue Running Activities	15 Minutes	Email User		

Settings

Field	Definition
Add Filter drop-down list	Allows you to select a field from the current view to filter information. Select the field from the drop-down list, and then enter the information you wish to filter. See Filters on page 15.
Update Button	Displays the filtered data in the table.

Field	Definition
Table columns	
Name	User defined name for the action. The type of action that will occur if the rule is enabled.
Activity Failure	Indicates whether the system will continue to perform activities for the action if a higher-ranked activity fails. When **Continue Running Activities** is selected, the next ranked activity in the list is performed after a higher-ranked activity fails. When **Stop Running Activities** is selected, no lower-ranked activities are executed when a higher-ranked activity fails.
Secondary Task Delay	The amount of time that will pass before the enabled secondary activity is executed for an activity. For example, the user may wish to enable the host 15 minutes after the host was initially disabled.
Activity Summary	A description of the activity that will occur.
Last Modified By	User name of the last user to modify the action.
Last Modified Date	Date and time of the last modification to this action.
Right click options	
Delete	Deletes the selected action.
Modify	Opens the Modify Security Action window for the selected action.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671
Buttons	
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.

Add or modify an action

1. Select **Policy > Policy Configuration**.
2. In the menu on the left expand **Security Rules**.
3. Click **Actions**.
4. Click the **Add** button or select an existing security action and click **Modify**.
5. Click in the **Name** field and enter a name for this security action.
6. Use the table below to enter the security action information.
7. Click **OK** to save your security rule action.

Settings

Field	Definition
Name	A name for this security action.
On Activity Failure	User indicates whether the system will continue to perform activities for the action if a higher- ranked activity fails. When **Continue Running Activities** is selected, the next ranked activity in the list is performed after a higher-ranked activity fails. When **Stop Running Activities** is selected, no lower-ranked activities are executed when a higher-ranked activity fails.
Perform Secondary Tasks After check box	When selected, if a secondary task is enabled for an activity, the secondary task is automatically executed to undo the action. The user may enter the amount of time that will pass between the primary and secondary tasks. If the check box is not selected, the user may manually undo the action in the Security Alarms view.
Not currently in use/In use by	Indicates whether the action is in use, and the number of rules currently associated with the action.
Activities	
Rank Buttons	Moves the selected action up or down in the list. Activities are performed in order by rank.
Rank	The activity's rank in the list of activities. Rank controls the order in which activities are performed.
Activity	Specifies the activity that will be performed.
Add button	Click to add an activity.
Modify button	Click to modify a selected activity.
Delete button	Click to delete a selected activity.

Delete an action

1. Select **Policy > Policy Configuration**.
2. In the menu on the left expand **Security Rules**.
3. Click **Actions**.
4. Select an action and click **Delete**.
5. A confirmation message is displayed. Click **Yes** to continue.

Add or modify activities

1. Select **Policy > Policy Configuration**.
2. In the menu on the left expand **Security Rules**.
3. Click **Actions**.
4. Click the **Add** button or select an action and click **Modify**.
5. Under **Activities**, click the **Add** button, or select an activity and click **Modify**.

6. Select the activity from the **Activity** drop-down menu.
7. Enter the information associated with the activity.

Some options include the **Secondary Task** check box. Selecting this check box enables the secondary task to occur after the time period specified in the action has passed.

8. Use the table below for information about each activity option.
9. Click **OK** to save your activity.

Settings

Field	Definition
Command Line Script Action	Lets you specify a particular command line script to be executed as an alarm action.
Send Alarm to Custom Script	Lets you send an alarm to a custom command line script located in /home/cm/scripts when the trigger event occurs.
Send Alarm to External Log Hosts	Sends an alarm to an external log host when the trigger event occurs.
Email User Action	Sends an email to the logged on user or owner, only the logged on user, or only the owner when the action is taken. See Host view on page 793 for more information about adding or modifying the host's owner. Enter the message for the user in the **Email Message** box. Select the fields to display information you wish to append to the email. You can update the text to be displayed for each field. Users can add or modify custom fields that are appended to the email. Custom fields include information about a security event that is stored under **Full Event Attributes** in the **Security Events View > Event Details** window. For example, enter a label for the field and the "CS4" key to display the CS4 information in the custom field. See Security events on page 634
Email Group Action	Sends an email to the selected Administrative group.
SMS User Action	Sends an SMS message to the host's owner when the action is taken. See Host view on page 793 for more information about adding or modifying the host's owner. Enter the message for the user in the **SMS Message** box.
Host Role Action	Lets you set the host role to any configured role. You can select the **Secondary Task** check box to enable a secondary task to change the role when the action is undone.
Disable Host	Disconnects the host from the network. You can select the **Secondary Task** check box to enable the host after a specified time period if the **Perform Secondary Task(s)** check box is enabled for the action.
Disable Port	Disconnects the port. You can select the **Secondary Task** check box to enable the port after a specified time period if the **Perform Secondary Task(s)** check box is enabled for the action.

Field	Definition
Run Endpoint Compliance Configuration	When selected, allows you to run additional Endpoint Compliance configurations based on security actions mapped to a scan's results. See Chaining configuration scans on page 424.
Mark Host At Risk	Automatically fails the scan selected in the **Mark Host At Risk For** drop-down list, and places the host in a state of remediation the next time the host connects. You can select the **Secondary Task** check box to mark the host safe after a specified time period if the **Perform Secondary Task(s)** check box is enabled for the action.
Mark Host Safe	Automatically marks the host as safe for the scan selected in the **Mark Host Safe** For drop-down list, and passes the scan. You can select the **Secondary Task** check box to mark the host at risk after a specified time period if the **Perform Secondary Task(s)** check box is enabled for the action.
Send Message to Desktop	Lets you send a message to the desktop of a host running the Persistent Agent.

Delete activities

1. Select **Policy > Policy Configuration**.
2. In the menu on the left expand **Security Rules**.
3. Click **Actions**.
4. Select an action and click **Modify**.
5. Select an activity and click **Delete**. The activity is deleted.
6. Click **OK**.

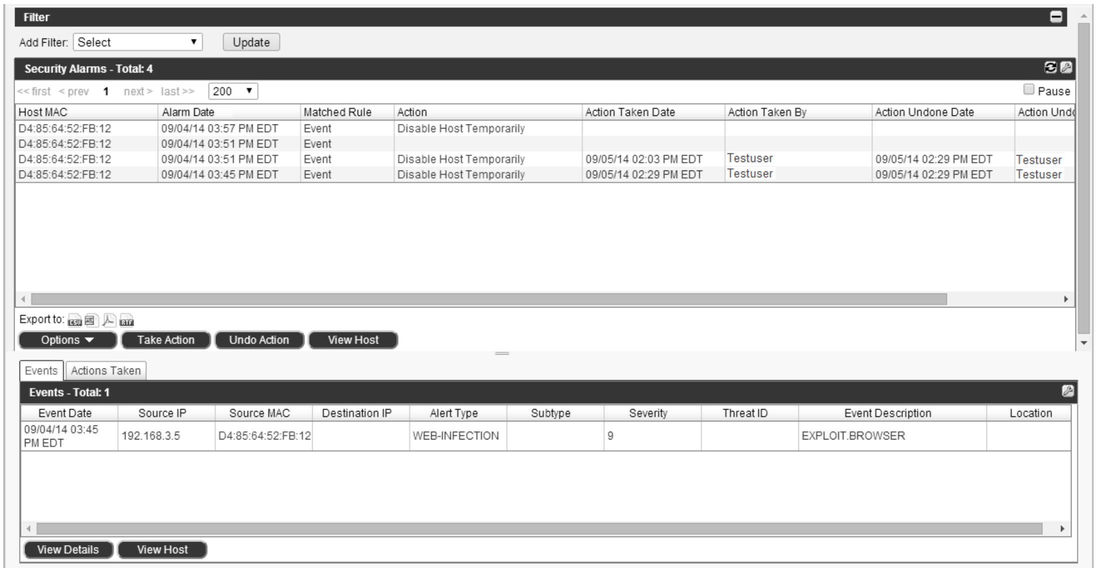
Security alarms

The Security Alarms view displays alarms that are created when an incoming security event satisfies a trigger and activates a rule. The list is updated as alarms are created. Alarms may be created with an associated action from the matched rule. The action may have been taken automatically, or can be taken manually from the view. A user with the correct permissions may override the associated action when taking action manually. Actions may only be taken on an alarm once. You also have the ability to undo the associated action once it's been taken.

When you click a specific alarm, the details of the events that triggered the alarm appear in the Events tab. You can also create a new event rule based on the events in the list. The Actions Taken tab displays the actions that were taken for the alarm, the completion status, and whether they were successfully (if applicable).

Click Logs > Security Alarms. The Security Alarms view appears.

See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.



Filter
Add Filter: Select ▾
Update
Security Alarms - Total: 4
<< first < prev 1 next > last >> 200 ▾
□ Pause

Host MAC	Alarm Date	Matched Rule	Action	Action Taken Date	Action Taken By	Action Undone Date	Action Undo
D4:85:64:52:FB:12	09/04/14 03:57 PM EDT	Event	Disable Host Temporarily				
D4:85:64:52:FB:12	09/04/14 03:51 PM EDT	Event					
D4:85:64:52:FB:12	09/04/14 03:51 PM EDT	Event	Disable Host Temporarily	09/05/14 02:03 PM EDT	Testuser	09/05/14 02:29 PM EDT	Testuser
D4:85:64:52:FB:12	09/04/14 03:45 PM EDT	Event	Disable Host Temporarily	09/05/14 02:29 PM EDT	Testuser	09/05/14 02:29 PM EDT	Testuser

Event Date	Source IP	Source MAC	Destination IP	Alert Type	Subtype	Severity	Threat ID	Event Description	Location
09/04/14 03:45 PM EDT	192.168.3.5	D4:85:64:52:FB:12		WEB-INFECTION		9		EXPLOIT.BROWSER	

Settings

The fields listed in the table below are displayed in columns on the Security Alarms View based on the selections you make in the Settings window.

Field	Definition
Add Filter drop-down list	Allows you to select a field from the current view to filter information. Select the field from the drop-down list, and then enter the information you wish to filter. See Filters on page 15.
Update button	Displays the filtered data in the table.
Pause	Allows user to pause the Security Alarm view from updating with new alarms so specific alarms can be viewed more easily.
Security alarms	
Host MAC	The MAC address for the host that triggered the alarm. Click the MAC address to open the Modify Host window where you can register the host and modify host details. See Add or modify a host on page 807.
Alarm Date	The date when the alarm was created.
Matched Rule	The name of the rule that created the alarm.
Action	The associated action from the rule when the alarm was created or the action was taken on the alarm. Users can click the action to open the Modify Security Action dialog window and modify the action. See Add or modify an action on page 628. If an action is associated to an alarm but was not taken, and the action is then deleted from the Security Actions view, the action is disassociated from the alarm and users may take a new action on the alarm. If an action was taken on an alarm, and the action is then deleted from the Security Actions view, the action remains visible but is not editable.

Field	Definition
Action Taken Date	If an action was taken, shows the date when the action was taken.
Action Taken By	The user who manually took the action on the alarm.
Action Undone Date	If the action was undone, shows the date when the action was undone.
Action Undone By	The user who manually undid the action.
Buttons	
Export	Use the Export option to export a list of selected hosts to CSV, Excel, PDF or RTF formats.
Options	The Options button displays the same series of menu picks displayed when the right-mouse button is clicked on a selected alarm.
Take Action	User can manually take action on the selected alarm, if action has not already been taken.
Undo Action	User can undo an action if the action has been taken on the selected alarm, but has not been undone.
View Host	Opens the Modify Host window to view and update the details of the host that triggered the alarm. See Add or modify a host on page 807.
Right click options	
Take Action	User can manually take action on the selected alarm, if action has not already been taken.
Undo Action	User can undo an action if the action has been taken on the selected alarm. When the action is undone, the secondary task is performed on the host if enabled.
View Host	Opens the Modify Host window to view and update the details of the host associated with the selected security event. See Add or modify a host on page 807.
View in Host View	Opens the host in Host View. See Host view on page 793.
Events tab	
Event Date	The date when the event that triggered the alarm occurred.
Source IP	The IP address for the host that triggered the event.
Source MAC	The MAC address of the host that triggered the event.
Destination IP	The IP address of the host or device the source host was communicating with.
Alert Type	The type of security event that triggered the alarm.
Subtype	The subtype of the security event.
Severity	The severity of the event reported by the security appliance.
Threat ID	A unique identifying code supplied by the vendor for the specific type of threat or event that occurred.

Field	Definition
Event Description	A description supplied by the security appliance of the event.
Location	The location of the source host is on the network. For example, this could be the SSID the host is connected to wirelessly, or the port the host is plugged into on a switch.
Right click options	
View Details	Displays the details of the security event that triggered the alarm.
View Host	Opens the Modify Host window to view and update the details of the host associated with the selected security event. See Add or modify a host on page 807.
View in Host View	Opens the host in Host View. See Host view on page 793.
Create Event Rule	Allows user to create a rule based on the selected events.
Actions taken tab	
Action	The action that was taken on the alarm.
Completed	Indicates whether the action was completed.

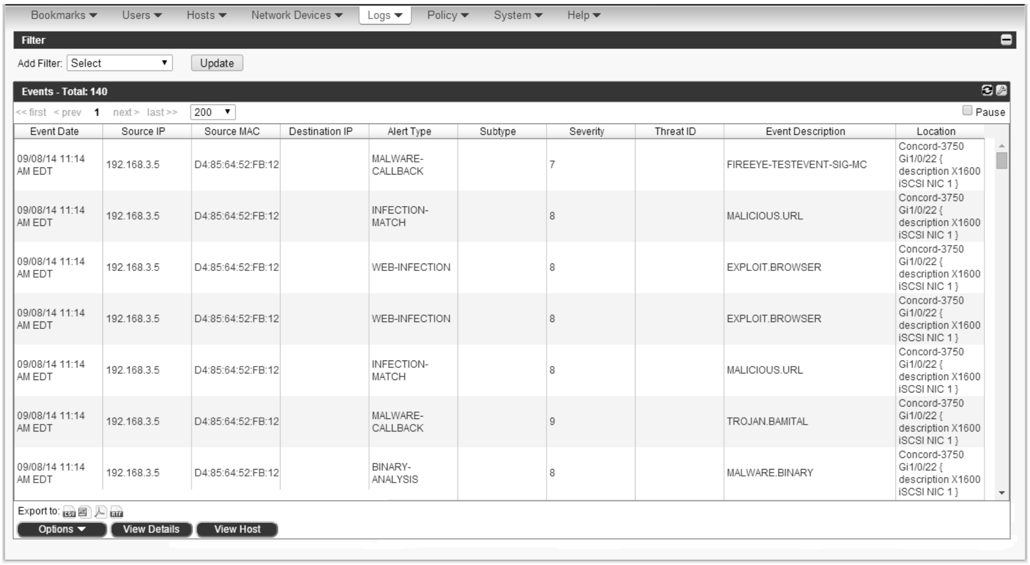
Security events

The Security Events view displays all incoming security events to FortiNAC that satisfy a security trigger. FortiNAC automatically reviews all security rules for each event. When an event satisfies a trigger associated with a rule, an alarm is created.

You can also create an event rule based on one or more security events in the list.

Click **Logs > Security Events**. The **Security Events** view appears.

See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.



Add Filter: Select

Events - Total: 140

200

Event Date	Source IP	Source MAC	Destination IP	Alert Type	Subtype	Severity	Threat ID	Event Description	Location
09/08/14 11:14 AM EDT	192.168.3.5	D4:85:64:52:FB:12		MALWARE-CALLBACK		7		FIREEYE-TESTEVENT-SIG-MC	Concord-3750 Gi1/0/22 { description X1600 iSCSI NIC 1 }
09/08/14 11:14 AM EDT	192.168.3.5	D4:85:64:52:FB:12		INFECTION-MATCH		8		MALICIOUS.URL	Concord-3750 Gi1/0/22 { description X1600 iSCSI NIC 1 }
09/08/14 11:14 AM EDT	192.168.3.5	D4:85:64:52:FB:12		WEB-INFECTION		8		EXPLOIT.BROWSER	Concord-3750 Gi1/0/22 { description X1600 iSCSI NIC 1 }
09/08/14 11:14 AM EDT	192.168.3.5	D4:85:64:52:FB:12		WEB-INFECTION		8		EXPLOIT.BROWSER	Concord-3750 Gi1/0/22 { description X1600 iSCSI NIC 1 }
09/08/14 11:14 AM EDT	192.168.3.5	D4:85:64:52:FB:12		INFECTION-MATCH		8		MALICIOUS.URL	Concord-3750 Gi1/0/22 { description X1600 iSCSI NIC 1 }
09/08/14 11:14 AM EDT	192.168.3.5	D4:85:64:52:FB:12		MALWARE-CALLBACK		9		TROJAN.BAMITAL	Concord-3750 Gi1/0/22 { description X1600 iSCSI NIC 1 }
09/08/14 11:14 AM EDT	192.168.3.5	D4:85:64:52:FB:12		BINARY-ANALYSIS		8		MALWARE.BINARY	Concord-3750 Gi1/0/22 { description X1600 iSCSI NIC 1 }

Settings

The fields listed in the table below are displayed in columns on the Security Events View based on the selections you make in the Settings window.

Field	Definition
Add Filter drop-down list	Allows you to select a field from the current view to filter information. Select the field from the drop-down list, and then enter the information you wish to filter. See Filters on page 15.
Update button	Displays the filtered data in the table.
Pause	Allows user to pause the Security Event view from updating with new events so specific events can be viewed more easily.
Events	
Event Date	The date when the event was received.
Source IP	The IP address for the host that triggered the event.
Source MAC	The MAC address of the host that triggered the event.
Destination IP	The IP address of the host or device the source host was communicating with.
Alert Type	The type of security event was received.
Subtype	The subtype of the security event.
Severity	The severity of the event reported by the security appliance.
Threat ID	A unique identifying code supplied by the vendor for the specific type of threat or event that occurred.
Event Description	A description supplied by the security appliance of the event.
Location	The location of the source host is on the network. For example, this could be the SSID the host is connected to wirelessly, or the port the host is plugged into on a switch.
Buttons	
Export	Use the Export option to export a list of selected hosts to CSV, Excel, PDF or RTF formats.
Options	The Options button displays the same series of menu picks displayed when the right-mouse button is clicked on a selected alarm.
View Details	Displays the details of the security event.
View Host	Opens the Modify Host window to view and update the details of the host associated with the selected security event.
Right click options	
View Details	Displays the details of the security event.
View Host	Opens the Modify Host window to view and update the details of the host associated with the selected security event.

Field	Definition
View in Host View	Opens the host in Host View.
Create Event Rule	Allows user to create a rule based on the selected events.

Add an event rule from security events

You can create security event rules directly from the Security Event view. This enables you to create security rules directly from security events as the events occur.

1. Click **Logs > Security Events**. The Security Events view appears.
2. Use the Filters to locate the appropriate event. Refer to Security events on page 634 for Filter Settings.
3. Select the event(s) you wish to use to create the rule. You can select multiple events at a time.
4. Right-click and select **Create Event Rule**.
5. Select the field(s) from the Available Fields column, and then click the right-arrow to add the fields to the Selected Fields column.
6. Click **OK**.
7. The Add Security Trigger window appears. The selected fields populate the trigger filter fields.
8. Add the details of the trigger. See Add a trigger on page 625.
9. Click **OK**.
10. The Add Security Rule window appears.
11. Add the details of the security rule. See Add or modify a rule on page 622.

The security rule is added to the list of rules in the Security Rules View.

User view

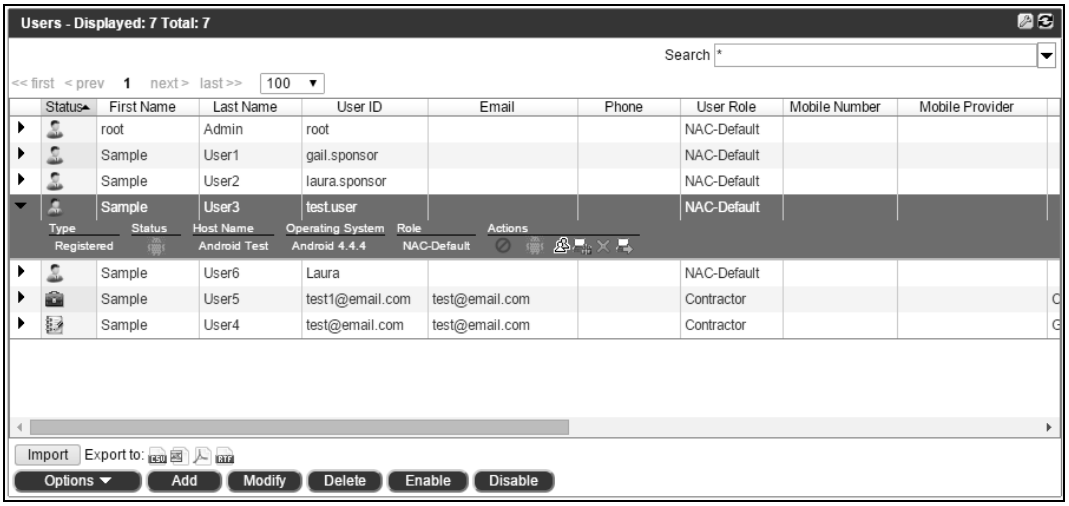
The User View is part of a four tabbed window that includes Adapters, Hosts, Users, and Applications. Use the User View to add, delete, modify, locate and manage users on your network. Users include network users, guest or contractor users and Administrator Users. Administrator users can also be managed from the Admin Users View. Administrator users are also network users, therefore, they are included in the Users View with a slightly different icon. See the Icons on page 30 for information on each icon.

If you have an LDAP or Active Directory configured, user information is added from the directory as users register on the network. The FortiNAC database is periodically synchronized with the directory to make sure that data is the same in both places. User information from the directory is matched to user information in the FortiNAC database based on User ID. If you manually create a user with an ID that is the same as a user in the directory, then directory data will overwrite your manually entered data.

The relationship between Users, Hosts and Adapters is hierarchical. Users own or are associated with one or more hosts. Hosts contain one or more Adapters or network interfaces that connect to the network. By displaying User, Host and Adapter data in a tabbed window, the relationships are maintained. For example, if you search for a host with IP address 192.168.5.105, you are in fact searching for the IP address of the adapter on that host. When the search displays the host, you can click on the Adapters tab, the search is automatically re-run and you see the adapter itself. If there is an associated user, you can click on the Users tab to re-run the search and see the associated user.

Click on the arrow in the left column to drill-down and display the hosts associated with the selected user. Hover over the icon in the Status column to display a tooltip with detailed information about this user. For Settings see Search settings on page 646.

See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.


Users - Displayed: 7 Total: 7
Search *
<< first < prev 1 next > last >> 100 ▼

	Status	First Name	Last Name	User ID	Email	Phone	User Role	Mobile Number	Mobile Provider
▶		root	Admin	root			NAC-Default		
▶		Sample	User1	gail.sponsor			NAC-Default		
▶		Sample	User2	laura.sponsor			NAC-Default		
▼		Sample	User3	test.user			NAC-Default		
▶		Sample	User6	Laura			NAC-Default		
▶		Sample	User5	test1@email.com	test@email.com		Contractor		
▶		Sample	User4	test@email.com	test@email.com		Contractor		

Type	Status	Host Name	Operating System	Role	Actions
Registered		Android Test	Android 4.4.4	NAC-Default	

Settings

Field	Definition
Address	Users's street address.
Allowed Hosts	The number of hosts that can be associated with or registered to this user and connect to the network. There are two ways to reach this total. If the host is scanned by an agent or if adapters have been manually associated with hosts, then a single host with up to five adapters counts as one host. If the host is not scanned by an agent or if the adapters have not been associated with specific hosts, then each adapter is counted individually as a host. In this scenario one host with two network adapters would be counted as two hosts. Numbers entered in this field override the default setting in **System > Settings > Network Device**. Blank indicates that the default is used. See Network device on page 130. If an administrator exceeds the number of hosts when registering a host to a user, a warning message is displayed indicating that the number of Allowed Hosts has been incremented and the additional hosts are registered to the user.
City	User's city of residence.
Created Date	Date the user record was created in the database. Options include Before, After, and Between.
Delete Hosts When User Expires	Indicates whether hosts registered to this user should be deleted from the database when the user's record ages out of the database.
Email	User's email address.
Expiration Date	Controls the number of days a user is authorized on the network. Options include Before, After, Between, Never, and None. The user is deleted from the database when the date specified here has passed. The date is automatically calculated based on the information entered when Aging is configured. See Aging out host or user records on page 823.
Delete Hosts When User Expires	Indicates whether hosts owned by this user should be deleted when the user ages out of the database. It is recommended that you set this to Yes.
Inactivity Date	Controls the number of days a User is authorized on the network. Options include Before, After, Between, Never, and None. User is deleted from the database when the date specified here has passed. The date is continuously recalculated based on the information entered in the Days Inactive field. See Aging out host or user records on page 823 or Set user expiration date on page 655.
Inactivity Limit	Number of days the user must remain continuously inactive on the network to be removed from the database. See Aging out host or user records on page 823 or Set user expiration date on page 655.
Last Login/Logout	Date of the last time the user logged into or out of the network or the FortiNAC Admin UI. This date is used to count the number of days of inactivity. Options include Before, After, Between, and Never.
Last Name	User's last name.

Field	Definition
Mobile Number	User's mobile phone number. Can be used to send SMS messages based on alarms. Requires the Mobile Provider to send SMS messages.
Mobile Provider	Provider or carrier for user's mobile phone.
Notes	Notes about this user.
Phone	User's telephone number.
User Role	Role assigned to the user. Roles are attributes of users and are used as filters for User/Host Profiles. See Role management on page 553.
User Security & Access Value	Value that typically comes from a field in the directory, but can be added manually. This value groups users and can be used to determine which role to apply to a user or which policy to use when scanning a user's computer. The data in this field could be a department name, a type of user, a graduation class, a location or anything that distinguishes a group of users.
State	User's state of residence.
Status	Current or last known status is indicated by an icon. See Icons on page 30. Hover over the icon to display additional details about this User in a tool tip. **Access** — Indicates whether user is enabled or disabled.
Title	User's title, this could be a form of address or their title within the organization.
Type	Type of user. Allows you to differentiate between network users and guest/contractor users.
User ID	Unique alphanumeric ID. If you are using a directory for authentication, this should match an entry in the directory. If it does not, FortiNAC assumes that this user is authenticating locally and asks you for a password. When using a directory for authentication, fields such as name, address, email, are updated from the directory based on the User ID when the database synchronizes with the directory. This is true regardless of how the user is created and whether the user is locally authenticated or authenticated through the directory. If the User ID matches a User ID in the directory, the FortiNAC database is updated with the directory data.
Postal Code	User's zip code based on their state of residence.
Last Modified By	User name of the last user to modify the user.
Last Modified Date	Date and time of the last modification to this user.

Navigation, menus, options, and buttons

For information on selecting columns displayed in the User View see Configure table columns and tooltips on page 641. Some menu options are not available for all Users. Options may vary depending on user state.

Field	Definition
Quick Search	Enter a single piece of data to quickly display a list of users. Search options include: IP address, MAC address, Host Name, User Name and User ID. Drop-down arrow on the right is used to create and use Custom Filters. If you are doing a wild card search for a MAC address you must include colons as separators, such as, 00:B6:5*. Without the separators the search option cannot distinguish that it is a MAC address. When Quick Search is enabled, the word Search appears before the search field. When a custom filter is enabled, Edit appears before the search field.
Right click options	
User Properties	Opens the Properties window for the selected user. See User properties on page 649.
Add Users To Groups	Add the selected user(s) to one or more group(s). See Add users to groups on page 653.
Delete Users	Deletes the selected user(s) from the database. See Delete a user on page 652.
Disable Users	Disables the selected user (s) preventing them from accessing the network regardless of the host they are using.
Enable Users	Enables the selected user(s) if they were previously disabled. Restores network access.
Group Membership	Displays groups in which the selected user is a member. Note: If the User is also an Admin User, separate options are displayed for Admin User Groups and User Groups. Options are labeled Group Membership (User) and Group Membership (Administrator).
Guest Account Details	Displays account details for the selected guest record, such as User ID, Account Status, Sponsor, Account Type, Start and End dates, Availability, Role, Authentication, Security Policy, Account Duration, Reauthentication Period, Success URL and the guest's password. See Guest account details on page 654.
Modify User	Opens the Modify User window. See Add or modify a user on page 651.
Policy Details	Opens the Policy Details window and displays the policies that would apply to the selected user at this time, such as Endpoint Compliance Policies, Network Access Policies or Supplicant Policies. See Policy details on page 381.
Set Expiration	Launches a tool to set the date and time for the user to age out of the database. See Set user expiration date on page 655.
Set Role	Assigns a role to the selected user. See Role management on page 553.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.

Field	Definition
Show Events	Displays all events for the selected user.
Collapse All	Collapses all records that have been expanded.
Expand Selected	Expands selected user records to display host information.
Buttons	
Import/Export	Import and Export options allow you to import users into the database from a CSV file or export a list of selected hosts to CSV, Excel, PDF or RTF formats. See Import hosts, users or devices on page 696 or Export data on page 710.
Options	The Options button displays the same series of menu picks displayed when the right-mouse button is clicked on a selected user.

Configure table columns and tooltips

Use the configuration button 🔧 on the User View, Adapter View, Host View, and Applications View to open the Settings window. The Settings window controls the columns displayed in each view and the details displayed in tooltips when you hover over an icon.

Table columns

1. Click the **Configuration** button at the top of the window.
2. When the Settings window displays, select the **Table Columns** tab.
3. Mark the columns to be displayed in the table on the User, Adapter or Host View with a check mark and click **OK**.
4. These settings are saved for the logged in user.

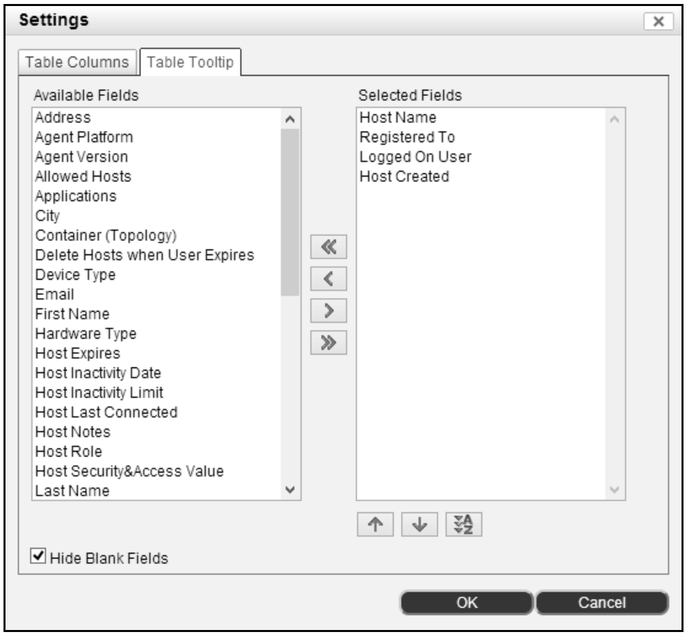
Tooltips

Select the fields to be displayed in the tooltip when you hover the mouse over the status icon of either a User, an Adapter, or a Host. Available fields vary depending on which item you are configuring.

1. Click the **Configuration** button at the top of the window.
2. When the Settings window displays, select the **Table Tooltip** tab.
3. The **Available Fields** column displays fields that can be displayed, but have not yet been selected. The Selected Fields column displays fields that will display in the tooltip.
4. Use the arrows in the center of the window to move fields from one column to the other until the appropriate set of fields is displayed in the **Selected Fields** column.
5. Select a field in the Selected Fields column and use the up and down arrow buttons to change the order of display. Use the AZ button to sort fields alphabetically.
6. The **Hide Blank Fields** option is enabled by default. It reduces the size of the tooltip when selected fields are blank for a particular item. For example, if you have selected Host Expires and the selected Host does not have an

expiration date, then when the tooltip for that host is displayed, the Host Expires field is hidden.

7. Click **OK** to save your changes. These settings are saved for the logged in user.



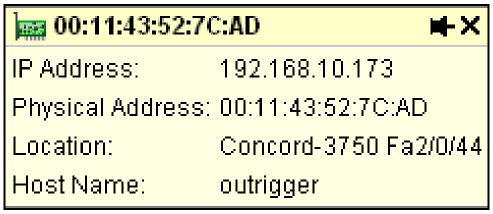
Available Fields
Address
Agent Platform
Agent Version
Allowed Hosts
Applications
City
Container (Topology)
Delete Hosts when User Expires
Device Type
Email
First Name
Hardware Type
Host Expires
Host Inactivity Date
Host Inactivity Limit
Host Last Connected
Host Notes
Host Role
Host Security&Access Value
Last Name

Selected Fields
Host Name
Registered To
Logged On User
Host Created

☑ Hide Blank Fields

Using tooltips

Tooltips are displayed when you hover the mouse over a status icon in the User, Adapter, or Host views. Tooltip details are configured using the Settings window shown in the previous section.



00:11:43:52:7C:AD

IP Address:	192.168.10.173
Physical Address:	00:11:43:52:7C:AD
Location:	Concord-3750 Fa2/0/44
Host Name:	outrigger

- When a tooltip is displayed, click the Push Pin icon to anchor it to the screen. Now you can move the tooltip around your desktop without it closing.
- High-light text in a tooltip and press Ctrl-C to copy it. Press Ctrl-V to paste the text in a field.
- Open and anchor multiple tooltips to quickly compare data.
- Hover over the status icon in the top left corner for text based status information.

Search and filter options

There are several search and filter mechanisms used to locate Hosts, Adapters, Users or Applications. These four tabs share a single view and search mechanism. Options include: Quick Search and Custom Filters, which can be used once or saved for reuse.

When a search or filter is run, the search data or the name of the filter remains in the search field at the top of the window. If you then click on a different tab, that search is rerun in the context of the new tab.

Wild cards

When searching using a text field in a Custom Filter or the Quick Search field you must enter specific search data, such as 192.168.10.5. Wild cards can be used in these fields. Possible wild cards include the following:

Option	Example
*	192.* in the IP address field searches for all IP addresses that begin with 192.
[...]	[192.168.10.10,172.168.5.22,192.168.5.10] Searches for each IP address in the series and returns multiple records. Any search field that starts and ends with square brackets "[]" and has one or more commas "," is treated as a list of values.
!	!192. in the IP address field searches for all IP addresses that do not contain 192.
![...]	![John, Frank, Bob] in the First Name field returns all records that do not contain John, Frank or Bob in the First Name field.
<esc>!	<esc>!John in the First Name field returns records that match !John. The "<esc>" allows you to search for data that contains an exclamation point (!).

Quick search

The Quick Search field at the top of the window allows you to search based on a single piece of data, such as IP address, and display all matching records. The following fields are included in the Quick Search: IP address, MAC Address, Host Name, User First Name, User Last Name, Registered User, Logged On User, and User ID. To search by MAC Address you must use one of the following formats:

```
xx:xx:xx:xx:xx:xx
xxxxxxxxxxxx
xx.xx.xx.xx.xx.xx
xx-xx-xx-xx-xx-xx
xxxx.xxxx.xxxx
```

Wild card searches can also be done. If you are doing a wild card search for a MAC address you must include colons as separators, such as, 00:B6:5*. Without the separators the search option cannot distinguish that it is a MAC address.

If you are searching by IP address, you enter 192.168.5.1* and all records for IP addresses beginning with 192.168.5.1 are returned. See Wild cards on page 643.

The information displayed varies depending on the tab that is selected. As you click from tab to tab the search in the Quick Search field is applied automatically.

- Hosts Tab — Displays all hosts with an adapter that matches the IP range.
- Adapters Tab — Displays all adapters that match the IP range

To broaden the search, enter less information, such as *11*. This returns any IP, MAC, or Host Name containing 11 depending on the tab you have selected.

To use the Quick Search option:

1. Select **Hosts > Host View**.
2. Select either the Adapters, Hosts or Users Tab.
3. Enter a single piece data in the search field and press **Enter**. Wild card searches can be done.

Custom filter

The Custom Filter is the equivalent to an advanced search feature. It provides many fields that can be used in combination to narrow the list of Adapters or Hosts displayed. A Custom Filter can be created and used just once or can be saved under a filter name. The file can be Private, only the current user can see them or shared with all administrators. The new filter then displays in the drop-down menu and separated into two sections, a Private and Shared. They can be accessed by clicking the arrow on the Quick Search field at the top of the window. Custom Filters can be modified, copied or deleted as needed. You can also export Custom Filters to a .txt file which allows Custom Filters to be imported and used by other Admin users.

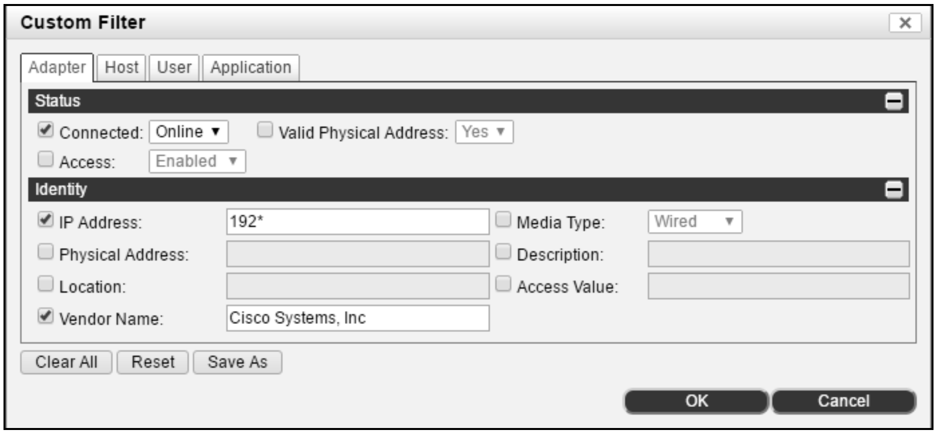
Use your mouse to hover over a saved filter in the drop-down menu and display a tooltip with details about that filter. There is currently only one default Custom Filter, Online Hosts, that displays a list of hosts that are connected to the network.

Create and save a custom filter

1. Click the arrow on the right side of the Quick Search field at the top of the window.
2. From the drop-down menu select **New Filter**.
3. Enter the name of the new filter and click **OK**.

Filter names do not support more than 20 characters.

Configure a custom filter



Status

☑ Connected: Online ▾ ☐ Valid Physical Address: Yes ▾

☐ Access: Enabled ▾

Identity

☑ IP Address: 192* ☐ Media Type: Wired ▾

☐ Physical Address: ☐ Description:

☐ Location: ☐ Access Value:

☑ Vendor Name: Cisco Systems, Inc

This window is used in two ways. First if you have selected New Filter from the menu off of the Quick Search drop-down, you can configure the filter and FortiNAC saves it for future use. Second, if you have selected Custom Filter from the menu off of the Quick Search, you can configure this filter and use it just one time.

This dialog box is common to the Adapter, Host and User Views. Custom filter entries on any of these tabs will persist if you navigate between these views.

1. Once you have the Filter window displayed, enable the fields to be included in the filter by marking them with a check mark.
2. For each enabled field you must provide additional information. For example, if you select the Connected field, you must choose either On Line or Off Line.
3. For text fields, such as the IP address field, you must enter the search data, such as 192.168.10.5. Wild cards can be used in these fields. See Wild cards on page 643.
4. To erase all selections, click the **Clear All** button.
5. If you have opened a saved filter and started to modify it, use the **Reset** button to return the filter to its original settings.
6. Click **OK** to run the configured filter. If this filter was assigned a name, the settings will be saved.
7. Immediately after the filter is run, the filter name displays at the top of the view in the Quick Search field. To modify the filter, click the Edit link to the left of the Quick Search field. This modifies the filter whether it was saved or just configured and run one time.

Edit a custom filter

1. Select **Hosts > Host View**.
2. Select either the Adapters, Hosts, Users, or Applications Tab.
3. Click the arrow on the right side of the Quick Search field at the top of the window.
4. On the drop-down menu locate the custom filter to be edited and click the pencil or edit icon to the right of the filter name.
5. When the Filter window displays, modify the filter as needed.
6. Click **OK** to save your changes.

Delete a custom filter

1. Click the arrow on the right side of the Quick Search field at the top of the window.
2. On the drop-down menu locate the custom filter to be deleted and click the red X to the right of the filter name.
3. When the confirmation message displays, click **Yes**.

Export a custom filter

1. Click the arrow on the right side of the Quick Search field at the top of the window.
2. On the drop-down menu select **Import/Export**, and then click **Export**.
3. In the Export Filters dialog, select the filters you want to export. Use Ctrl or Shift to select multiple filters.
4. Click **OK**. The filters are downloaded to a .txt file to your default download directory.

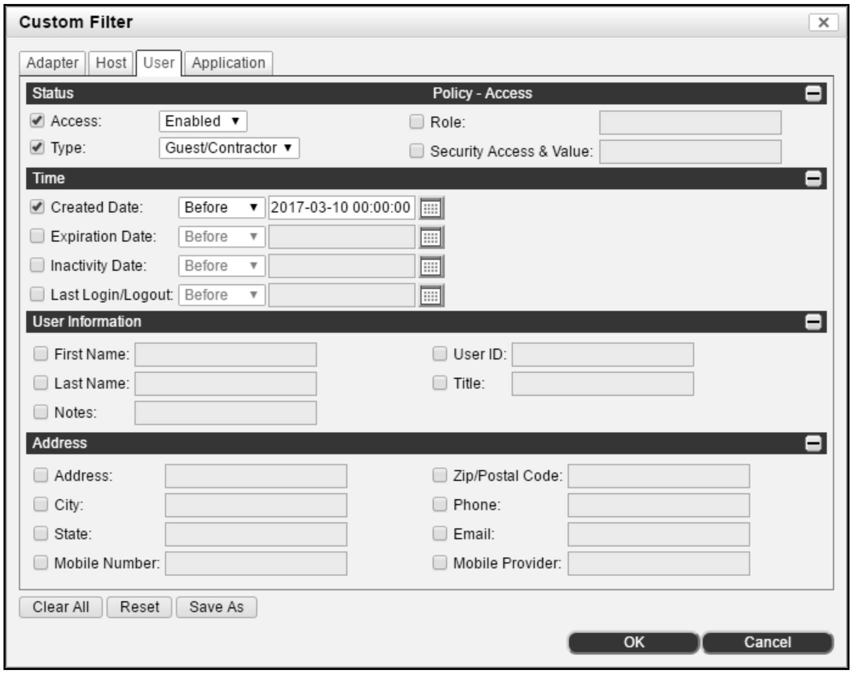
Import a custom filter

1. Click the arrow on the right side of the Quick Search field at the top of the window.
2. On the drop-down menu select **Import/Export**, and then click **Import**.
3. Click Choose File to find and select the .txt file containing the filters.
4. Click **OK** to import the filters. The filters appears in the list.

Search settings

The fields listed in the table below are displayed in columns on the User View based on the selections you make in the Settings window, see Configure table columns and tooltips on page 641. Most of these fields are also used in Custom Filters to search for hosts, see Search and filter options on page 642. Additional fields that can be displayed on the User View are fields for the host associated with the selected user, see Settings on page 795.

You may not have access to all of the fields listed in this table. Access depends on the type of license key installed and which features are enabled in that license.



Custom Filter

Adapter | Host | User | Application

Status

☑ Access: Enabled ▼

☑ Type: Guest/Contractor ▼

Policy - Access

□ Role:

□ Security Access & Value:

Time

☑ Created Date: Before ▼ 2017-03-10 00:00:00

□ Expiration Date: Before ▼

□ Inactivity Date: Before ▼

□ Last Login/Logout: Before ▼

User Information

□ First Name:

□ Last Name:

□ Notes:

□ User ID:

□ Title:

Address

□ Address:

□ City:

□ State:

□ Mobile Number:

□ Zip/Postal Code:

□ Phone:

□ Email:

□ Mobile Provider:

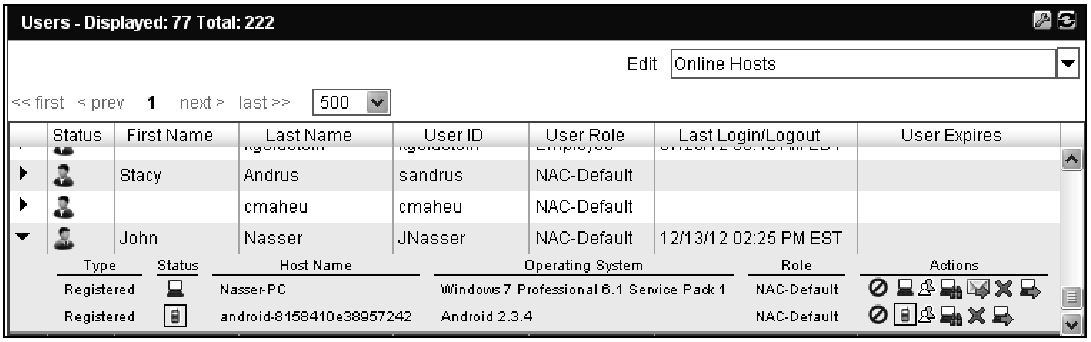
Field	Definition
Access	Indicates whether host is enabled or disabled
Address	Users's street address.
City	User's city of residence.
Created Date	Date the user record was created in the database. Options include Last, Between, Before, and After.
Email	User's email address.

Field	Definition
Expiration Date	Controls the number of days a user is authorized on the network. Options include Next, Before, After, Between, Never, and None. The user is deleted from the database when the date specified here has passed. The date is automatically calculated based on the information entered when Aging is configured. See Aging out host or user records on page 823.
First Name	User's first name.
Inactivity Date	Controls the number of days a User is authorized on the network. Options include Next, Before, After, Between, Never, and None. User is deleted from the database when the date specified here has passed. The date is continuously recalculated based on the information entered in the Days Inactive field. See Aging out host or user records on page 823 or Set user expiration date on page 655.
Inactivity Limit	Number of days the user must remain continuously inactive on the network to be removed from the database.
Last Login/Logout	Date of the last time the user logged into or out of the network or the FortiNAC Admin UI. This date is used to count the number of days of inactivity. Options include Last, Before, After, Between, and Never.
Last Name	User's last name.
Mobile Number	User's mobile phone number. Can be used to send SMS messages based on alarms. Requires the Mobile Provider to send SMS messages.
Mobile Provider	Provider or carrier for user's mobile phone.
Notes	Notes about this user.
Phone	User's telephone number.
Role	Role assigned to the user. Roles are attributes of users and are used as filters for User/Host Profiles. See Role management on page 553.
Security & Access Value	Value that typically comes from a field in the directory, but can be added manually. This value groups users and can be used to determine which role to apply to a user or which policy to use when scanning a user's computer. The data in this field could be a department name, a type of user, a graduation class, a location or anything that distinguishes a group of users.
State	User's state of residence.
Title	User's title, this could be a form of address or their title within the organization.
Type	Type of user. Allows you to differentiate between network users and guest/contractor users.

Field	Definition
User ID	Unique alphanumeric ID. If you are using a directory for authentication, this should match an entry in the directory. If it does not, FortiNAC assumes that this user is authenticating locally and asks you for a password. When using a directory for authentication, fields such as name, address, email, are updated from the directory based on the User ID when the database synchronizes with the directory. This is true regardless of how the user is created and whether the user is locally authenticated or authenticated through the directory. If the User ID matches a User ID in the directory, the FortiNAC database is updated with the directory data.
Postal Code	User's zip code based on their state of residence.

User drill-down

Use the arrow in the far left column to expand a user and view host details. Expand or collapse multiple users by selecting them and using the right - mouse button or Options button. All hosts associated with a user are contained within the expanded section of the window.



Users - Displayed: 77 Total: 222

Edit Online Hosts

	Status	First Name	Last Name	User ID	User Role	Last Login/Logout	User Expires
▶	👤	Stacy	Andrus	sandrus	NAC-Default		
▶	👤		cmaheu	cmaheu	NAC-Default		
▼	👤	John	Nasser	JNasser	NAC-Default	12/13/12 02:25 PM EST	

Type	Status	Host Name	Operating System	Role	Actions
Registered	💻	Nasser-PC	Windows 7 Professional 6.1 Service Pack 1	NAC-Default	⊘ 💻 ✕
Registered	📱	android-8158410e38957242	Android 2.3.4	NAC-Default	⊘ 📱 ✕

Settings

Field	Definition
Type	Type of host associated with this user. Types include: Registered
Status	Status of the host. See the Icons on page 30 for status information.
Operating System	Operating system installed on the host.
Role	Role assigned to the host. Roles are attributes of hosts that can be used as filters in User/Host Profiles. See Role management on page 553.
Actions	Use the action icons to do the following: • Enable/Disable a host. • Access Host Properties • View/Modify group membership • Scan the host • Send a message to the host (only hosts with the Persistent Agent installed)

Field	Definition
	• Delete host • Go to host in the Host View

User properties

The User Properties view provides access to detailed information about a single user. From this view you can access the associated host by clicking on the adapter's physical address displayed in the Registered Hosts tab at the bottom of the window.

Access user properties

1. Select **Users > User View**.
2. Search for the appropriate user.
3. Select the user and either right-click or click the **Options** button.
4. From the menu, select **User Properties**.

Settings

Field	Description
General	
First Name	User's first name.
Last Name	User's last name.
ID	Unique alphanumeric ID for this user. Typically comes from the directory but if you are not using a directory, this field can be created manually. This field cannot be modified. When using a directory for authentication, fields such as name, address, and email, are updated from the directory based on the User ID when the database synchronizes with the directory. This is true regardless of how the user is created and whether the user is locally authenticated or authenticated through the directory. If the User ID matches a User ID in the directory, the FortiNAC database is updated with the directory data.
Title	User's title, this could be a form of address or their title within the organization.
Role	Role assigned to the user. Roles are attributes of users that can be used as filters in User/Host Profiles. See Role management on page 553.
Security And Access Attribute Value	Value that typically comes from a field in the directory, but can be added manually. This value can be used as a filter to determine which policy to use when scanning a user's computer. The data in this field could be a department name, a type of user, a graduation class, a location or anything that distinguishes a group of users.
User Status	Radio buttons indicating whether the user is Enabled or Disabled. To enable or disable the user, click the appropriate button and then click Apply.
Allowed Hosts	The number of hosts that can be associated with or registered to this user and connect to the network. There are two ways to reach this total.

Field	Description
	If the host is scanned by an agent or if adapters have been manually associated with hosts, then a single host with up to five adapters counts as one host. If the host is not scanned by an agent or if the adapters have not been associated with specific hosts, then each adapter is counted individually as a host. In this scenario one host with two network adapters would be counted as two hosts. Numbers entered in this field override the default setting in **System > Settings > Network Device**. Blank indicates that the default is used. See Network device on page 130. If an administrator exceeds the number of hosts when registering a host to a user, a warning message is displayed indicating that the number of Allowed Hosts has been incremented and the additional hosts are registered to the user.
Time	
Expiration Date	Controls the number of days a user is authorized on the network. User is deleted from the database when the date specified here has passed. The date is automatically calculated based on the information entered in the Set User Expiration date window. To modify click **Set**. See Set user expiration date on page 655 for additional information.
Inactivity Date	Controls the number of days a user is authorized on the network. User is deleted from the database when the date specified here has passed. The date is continuously recalculated based on the number of days entered for Inactivity Limit. For example, if the user logs off the network on August 1st and Inactivity Limit is set to 2 days, the Inactivity Date becomes August 3rd. If on August 2nd the user logs back in again, the Inactivity Date is blank until the next time he logs out. Then the value is recalculated again. To modify click Set.
Inactivity Limit	Number of days the user must remain continuously inactive to be removed from the database. See Aging out host or user records on page 823.
Last Login/Logout	Date of the last time the user logged into or out of the network or the FortiNAC Admin UI. This date is used to count the number of days of inactivity.
Delete Hosts Upon Expiration	If set to Yes, hosts registered to the user are deleted when the user ages out of the database. To modify click **Set**.
Created	Indicates when this record was created in the database.
Tabs	
Registered Hosts	Displays a list of hosts, by the MAC address of their adapters, registered to this user. Click on a MAC address to open the Host Properties.
Logged In Hosts	List of hosts by host name registered to this user that are currently logged onto the network.
Notes	Notes entered by the administrator. If this user registered as a guest, this section also contains information gathered at registration that does not have designated database fields, such as Person Visiting or Reason for Visit.

Field	Description
Buttons	
Apply	Saves changes to the User Properties.
Reset	Resets the values in the User Properties window to their previous settings. This option is only available if you have not clicked Apply.

Add or modify a user

User records are created as users connect to the network and register. Users can be added by importing them in a file or by entering the data manually. See Import and export data on page 695. The Add or Modify User feature allows you to create new users or edit existing ones.

1. Select **Users > User View**.
2. Click the **Add** button.
3. In the **Enter User ID** window type a unique alphanumeric ID for this user. If you are using a directory for authentication, enter the user ID from the directory. This allows FortiNAC to synchronize its database with the directory and update user data.
4. Click **OK**. FortiNAC verifies that the user ID is in the directory and populates fields that have existing data in the directory, such as First and Last Name.
5. If the user is not in the directory, you can still add the user, but FortiNAC assumes that this user will authenticate locally and asks you for a password for the user.
6. To modify an existing user, use the search or filter mechanisms on the **User View** to locate the appropriate user.
7. Click on the user to select it.
8. Click the **Modify** button.
9. See the **t**able below for detailed information on each field.
10. Click **OK** to save your data.

Settings

Field	**Definitions**
Required fields	
User ID	
Change Password	Allows you to change the password for this user. Users who authenticate through the directory will not have a Change Password button. Only users who are locally authenticated by FortiNAC have a change password option.
First Name Last Name	User's name as it is retrieved from the directory. If you are using a directory, these fields are updated every time the directory is re-synchronized with the database. If you are not using a directory, enter the user's first and last name.
Role	Roles are attributes of users and can be used as filters in User/Host Profiles. These profiles are used to determine which Network Access Policy, Endpoint Compliance Policy or Supplicant EasyConnect Policy is applied.

Field	Definitions
Additional info	
Address	User's address of residence.
City	User's city of residence.
State	Two letter abbreviation for state of residence.
Zip/Postal Code	Postal code for the user's city and state of residence.
Email	User's email address. For multiple e-mail addresses, enter addresses separated by commas or semi-colons. Messages are sent to all e-mail addresses provided.
Title	This can be a form of address, such a as Mr., or a title within the organization.
Mobile Number	Mobile Phone number used for sending SMS messages to guests and administrators.
Mobile Provider	Mobile provider for the mobile phone number entered in the previous field. Used to send SMS messages to guests and administrators. This field also displays the format of the SMS address that will be used to send the message. For example, if the provider is US Cellular, the format is xxxxxxxxxx@emai.uscc.net, where the x's represent the user's mobile phone number. The number is followed by the email domain of the provider's message server.
Allowed Hosts	The number of hosts that can be associated with or registered to this user and connect to the network. There are two ways to reach this total. If the host is scanned by an agent or if adapters have been manually associated with hosts, then a single host with up to five adapters counts as one host. If the host is not scanned by an agent or if the adapters have not been associated with specific hosts, then each adapter is counted individually as a host. In this scenario one host with two network adapters would be counted as two hosts. Numbers entered in this field override the default setting in **System > Settings > Network Device**. Blank indicates that the default is used. See Network device on page 130. If an administrator exceeds the number of hosts when registering a host to a user, a warning message is displayed indicating that the number of Allowed Hosts has been incremented and the additional hosts are registered to the user.
Global Default	Default number of Allowed Hosts used if the Allowed Hosts field is empty. The default is set in **System > Settings > User/Host Management > Allowed Hosts**.
Notes	Free form notes entered by the Administrator.
Security and Access Attribute Value	This value is an attribute of users and can be used as a filter in User/Host Profiles. These profiles are used to determine which Network Access Policy, Endpoint Compliance Policy or Supplicant EasyConnect Policy is applied. If a directory is in use, the Security and Access Attribute value comes from the directory when it is synchronized with the database. Otherwise the value can be entered manually.

Delete a user

When you delete a user, you have the option to delete hosts registered to this user or leave them in the database. It is recommended that you delete the registered hosts. If they are not deleted, registered hosts associated with a deleted user become registered devices. If a user connects to the network with one of these devices, there is nothing to prevent network access because the device is known in the database.

1. Select **Users > User View**.
2. Use the **Quick Search** or **Custom Filter** to locate the appropriate user.
3. Select the user and click the **Delete** button.
4. A warning message is displayed asking if you would like to delete registered hosts associated with this user.
5. To delete hosts, enable the check box labeled **Delete Hosts Registered to User** and click **Yes**.
6. To convert hosts to registered devices, disable the check box labeled **Delete Hosts Registered to User** and click **Yes**.

Add users to groups

You can add selected users to groups you have created. See Groups view on page 838 for detailed information on Groups and how they are used in FortiNAC.

1. Select **Users > User View**.
2. Use the **Quick Search** or **Custom Filter** to locate the appropriate user(s).
3. Use Ctrl-click or Shift-click to select the records you wish to add to the group.
4. Right-click or click the **Options** button and select **Add Users To Groups**. The **Add Users to Groups** view lists the available user groups and sub-groups. Sub-groups are displayed under their parent group or groups.
5. To add the users to a group, click the box next to the group name and then click **OK**.
6. To create a missing group:
   a. Click the **Create Group** button.
   b. Enter a group name.
   c. If the new group should be a sub-group of an existing group, enable the **Parent Group** option and select the appropriate group from the list.
   d. **Description** is optional.
   e. Click **OK** to save the new group.
7. Click **OK**.

Group membership

From the User View window you can view or modify the group membership of an individual user. Use this option to open a window that displays a list of all groups to which the selected user belongs.

1. Select **Users > User View**.
2. Use the **Quick Search** or **Custom Filter** to locate the appropriate user(s).
3. Click on a user to select it.
4. Right-click or click the **Options** button and select **Group Membership**.
5. The **Group Membership** view lists the available user groups and sub-groups. Sub-groups are displayed under their parent group or groups. A check next to a group name indicates that this user is contained in that group.
6. To add the user to a group, click the box next to the group name and then click **OK**.
7. To remove the user from a group, click to uncheck the box next to the group name and then click **OK**.

8. To create a missing group:
   a. Click the **Create Group** button.
   b. Enter a group name.
   c. If the new group should be a sub-group of an existing group, enable the **Parent Group** option and select the appropriate group from the list.
   d. **Description** is optional.
   e. Click **OK** to save the new group.
9. Click **OK**.

Guest account details

Guest User records created when Guest accounts are generated are displayed in the Users View with network and administrator users. The Guest Account Details window displays data from the Guest Template used to create the Guest User. To access Guest Account Details:

1. Select **Users > User View**.
2. Search for the appropriate user.
3. Select the user and either right-click or click the **Options** button.
4. From the menu select **Guest Account Details**.

Settings

Field	Description
User ID	Guest's email account which is used as the User ID at login.
Account Status	Indicates whether the guest account is enabled or disabled.
Sponsor	The administrator who created the guest account.
Account Type	Guest account type. Types include: • **Guest**—A visitor to your facility with limited or Internet-only network access. • **Conference**—A group of short- or long-term visitors to your organization who require identical but limited access to your network for typically one to five days. • **Contractor**—A temporary employee of your organization who may be granted all or limited network access for a specific time period generally defined in weeks or months.
Start Date	Date and time (using a 24-hour clock format) the account will become active for the guest or contractor.
End Date	Date and time the account will expire.
Login Availability	Times during which the guest is permitted to access the network.
Role	Role is an attribute of a user or a host. It is used in User/Host Profiles as a filter when assigning Network Access Policies, Endpoint Compliance Policies and Supplicant EasyConnect Policies.
Authentication	Indicates type of authentication used. Options include: Local, LDAP or RADIUS. Guests typically use Local authentication.

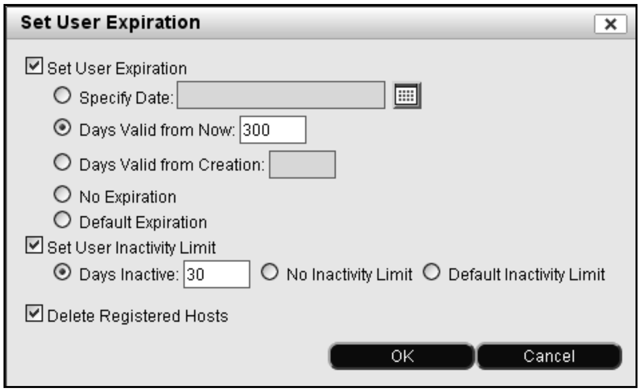
Field	Description
Account Duration	Amount of time this account will remain valid and usable.
Reauthentication Period	Number of hours the guest or contractor can access the network before reauthentication is required.
URL for Successful Landing Page	Directs the guest or contractor to a specific web page when they have successfully logged into the network and passed the scan in an Endpoint Compliance Policy. This field is optional and is used only if you have Portal V1 enabled in Portal Configuration.
URL for Acceptable Use Policy	Directs the guest or contractor to a specific web page that details the acceptable use policy for the network.
Password	The Guest's assigned password. Passwords are usually generated by the system unless the guests were bulk imported. Toggle the **Show Password/Hide Password** button to alternately display the password in plain text or as asterisks.

Set user expiration date

The expiration date on a user determines when the user record is automatically deleted or aged out of the database. Administrator Users default to No Expiration. See Aging out host or user records on page 823 for information on other methods.

The user inactivity timer is started when all hosts registered to a user are seen as offline. When a host is seen as connected, the timer is cleared. The timer is also cleared when the user logs into FortiNAC.

Admin Users assigned the Administrator Profile cannot be aged out.



Set User Expiration

☑ Set User Expiration

○ Specify Date:

● Days Valid from Now: 300

○ Days Valid from Creation:

○ No Expiration

○ Default Expiration

☑ Set User Inactivity Limit

● Days Inactive: 30 ○ No Inactivity Limit ○ Default Inactivity Limit

☑ Delete Registered Hosts

The Set User Expiration Date feature can be accessed either from the User View or the Host View.

1. Select **Users > User View**.
2. Use the **Quick Search** or **Custom Filter** to locate the appropriate user(s).
3. Select the users to be modified.
4. Right-click or click **Options** and select **Set User Expiration**.

5. Use the table below to enter expiration criteria.
6. Click **OK** to set the expiration dates.

Settings

Field	Definition
Specify Date	Allows you to select a specific date that the user will be aged out of the database.
Days Valid From Now	Enter the number of days from today that you would like the user to expire. The expiration date is calculated based on this number.
Days Valid From Creation	This is the number of days from the date the user record was created. The expiration date is calculated based on this number.
No Expiration	This user is never deleted from the database even if global or group aging options are added or modified.
Default Expiration	Defaults to the global aging settings configured in **System > Settings > User/Host Management > Aging**.
Set User Inactivity Limit	Enables the option to delete a user based on the number of days that the user did not log onto the network or into the Admin UI.
Days Inactive	Number of consecutive days the user must be inactive to be aged out of the database. For example, if this is set to 4 days, and after 2 days the user connects to the network again, the counter is restarted.
No Inactivity Limit	With this option enabled, the user is never deleted from the database due to inactivity even if global or group aging options are added or modified.
Default Inactivity Limit	Defaults to the global aging settings configured in **System > Settings > User/Host Management > Aging**.
Delete Registered Hosts	If enabled, hosts registered to the selected user are deleted when the user ages out of the database. It is recommended that you delete hosts with the user or they become registered devices when the user ages out of the database.

Admin profiles and permissions

Admin profiles are templates assigned to administrative users to define what a user can do in FortiNAC. Every administrative user is required to have an admin profile. An admin profile can be assigned to more than one Administrative User.

Each admin profile contains a list of permissions that are inherited by the associated Administrative Users. Permissions configured in Admin Profiles control the views in FortiNAC that can be accessed. If permission for access is given, in most cases, the Administrative User can Add/Modify and Delete data.

If an Admin Profile that is in use is changed, the changes do not take effect until the associated Administrative Users log out of FortiNAC and log in again.

Custom setting

For special functions such as Guest Manager or Device Profiler there are Advanced permissions. Advanced permissions control items such as the Guest Account templates that can be used by someone with permission for Guest/Contractor Accounts.

Landing page

Admin Profiles also designate the first screen or landing page displayed when the Administrative User logs into FortiNAC, days and times that users can log in and the number of minutes of inactivity that trigger an automatic logout. Due to the complexity of the permissions structure, it is recommended that you define the job functions of your Administrative Users to ensure that you have considered the permissions required for each Admin Profile.

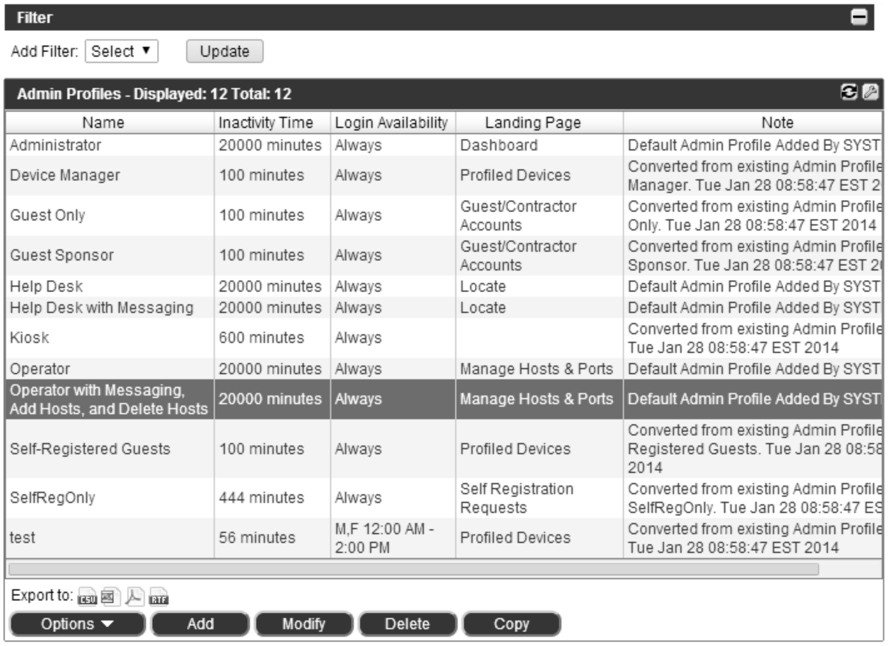
Profile mapping

Admin Profiles can be mapped to Groups to automatically assign a profile to Administrative Users as they are added to selected groups. Note that if Admin Profile Mapping is configured, moving an Administrative User to a group that is mapped changes their profile to the profile for the group. See Mappings process on page 678 for additional information.

Administrator profile

The Administrator profile is a default system profile that cannot be copied, deleted or renamed. This is the only profile that has access to every view in FortiNAC including: Admin Users, Admin Profiles and the Quick Start wizard. See Default administrator profiles on page 659.

See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.



Admin Profiles - Displayed: 12 Total: 12

Name	Inactivity Time	Login Availability	Landing Page	Note
Administrator	20000 minutes	Always	Dashboard	Default Admin Profile Added By SYST
Device Manager	100 minutes	Always	Profiled Devices	Converted from existing Admin Profile Manager. Tue Jan 28 08:58:47 EST 2
Guest Only	100 minutes	Always	Guest/Contractor Accounts	Converted from existing Admin Profile Only. Tue Jan 28 08:58:47 EST 2014
Guest Sponsor	100 minutes	Always	Guest/Contractor Accounts	Converted from existing Admin Profile Sponsor. Tue Jan 28 08:58:47 EST 2
Help Desk	20000 minutes	Always	Locate	Default Admin Profile Added By SYST
Help Desk with Messaging	20000 minutes	Always	Locate	Default Admin Profile Added By SYST
Kiosk	600 minutes	Always		Converted from existing Admin Profile Tue Jan 28 08:58:47 EST 2014
Operator	20000 minutes	Always	Manage Hosts & Ports	Default Admin Profile Added By SYST
Operator with Messaging, Add Hosts, and Delete Hosts	20000 minutes	Always	Manage Hosts & Ports	Default Admin Profile Added By SYST
Self-Registered Guests	100 minutes	Always	Profiled Devices	Converted from existing Admin Profile Registered Guests. Tue Jan 28 08:58 2014
SelfRegOnly	444 minutes	Always	Self Registration Requests	Converted from existing Admin Profile SelfRegOnly. Tue Jan 28 08:58:47 ES
test	56 minutes	M,F 12:00 AM - 2:00 PM	Profiled Devices	Converted from existing Admin Profile Tue Jan 28 08:58:47 EST 2014

Settings

Field	Definition
Name	User specified name for the profile. This name is displayed in the Admin User window when you are attaching the profile to an Administrative User.
Inactivity Time	User is logged out after this amount of time has elapsed without any activity.
Login Availability	Indicates when users with this profile can log in to FortiNAC. Options include: Always or Specify Time. If you choose Specify Time, the user is limited to certain times of day and days of the week.
Landing Page	Indicates the first view displayed when an Admin User with this profile logs into FortiNAC.
Note	User specified note field. This field may contain notes regarding the data conversion from a previous version of FortiNAC
Last Modified By	User name of the last user to modify the profile.
Last Modified Date	Date and time of the last modification to this profile.
Right click options & buttons	
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.
Copy	Copy the selected Profile to create a new record. The Administrator Profile cannot be copied.
Delete	Deletes the selected Profile. Profiles cannot be deleted if they are in use. The Administrator Profile can never be deleted.

Field	Definition
Modify	Opens the Modify Admin Profile window for the selected profile. On the Administrator Profile only the Inactivity Time can be modified.
In Use	Opens a list of Administrative Users that have the selected profile attached.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.

Default administrator profiles

FortiNAC has some default profiles that can be used to control system access. These profiles are always included in the database. With the exception of the Administrator Profile, they can be modified, deleted or copied.

Default Profiles - New Database

The table below describes the profiles that are in any new FortiNAC database and the default settings for each profile.

View	Access	Permissions Enabled
Administrator		
All	This profile cannot be deleted or copied. The only attribute of this profile that can be modified is the Inactivity Time. The Administrator profile has access to every part of FortiNAC.	All
Help desk		
Group Membership	User can access the Group Membership dialogs for Hosts and add or modify the selected host's membership in groups.	Access
Guest/Contractor Accounts	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
Locate Hosts & Users	User can search for Hosts and Users but cannot modify data. This is the default landing page when a user with this profile logs into FortiNAC.	Access
Self-Registration Requests	User can view Self-Registration Requests and allow or deny those requests.	Access Add/Modify
Operator		
Group Membership	User can access the Group Membership dialogs for Hosts and add or modify the selected host's membership in groups.	Access Add/Modify

View	Access	Permissions Enabled
	Operators are restricted to the host and user groups they are configured to manage. They do not have access to all hosts and users	
Locate Hosts & Users	User can view Adapter, Host, User and Device Identity. User can modify Host information but cannot delete any records.	Access
Manage Hosts & Ports	• Adapter List - Disable adapters. • Adapter Properties- View only. • Host Properties-View and modify access, but cannot send a message. • User Properties - View Only. • Device Identity - View and export data. This is the default landing page when a user with this profile logs into FortiNAC.	Access
Guest/Contractor Accounts	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
Self-Registration Requests	User can view Self-Registration Requests and allow or deny those requests.	Access Add/Modify
Profile_Sample		
Group Membership	User can access the Group Membership dialogs for Hosts and add or modify the selected host's membership in groups.	Access Add/Modify
Guest/Contractor Accounts	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials. User is limited to the GuestAccess_Sample template, can create accounts 45 days in advance and can create accounts with a maximum duration of 15 days.	Access, Add/Modify Custom Settings
Self-Registration Requests	User can view Self-Registration Requests and allow or deny those requests.	Access Add/Modify
Security analyst		
Dashboard	User can access and view the Dashboard	Access
Network Devices	User can view, add, modify, or delete network devices in the following views: • CLI Configuration • Device Profiling Rules • L2 Polling • L3 Polling • Locate • Port Changes • Topology	Access Add/Modify Delete
Users/Hosts/ Adapters	User can access, add, modify, or delete users, hosts, and adapters in the following views: • Adapters View	Access Add/Modify Delete

View	Access	Permissions Enabled
	- Connections - Device Identity - Hosts View - Scan Results - Users View	

Possible Profiles - Upgraded Database

Prior versions of FortiNAC contained several user types with varying permissions. From Version 7.0 forward there is only one type of user, Administrative, and access is controlled based on the settings of the Admin Profile associated with each user. During the upgrade process any existing Admin User types and their corresponding permissions are converted to Admin Profiles and assigned to Admin Users. There may be many as two Help Desk profiles and eight Operator profiles created during the upgrade. The table below contains the full list of Admin Profiles that could be created.

View	Access	Permissions Enabled
Administrator		
All	This profile cannot be deleted or copied. The only attribute of this profile that can be modified is the Inactivity Time. The Administrator profile has access to every part of FortiNAC.	All
Help desk		
Group Membership	User can access the Group Membership dialogs for Hosts and add or modify the selected host's membership in groups.	Access
Guest/Contractor Accounts	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
Locate Hosts & Users	User can search for Hosts and Users but cannot modify data. This is the default landing page when a user with this profile logs into FortiNAC.	Access
Self-Registration Requests	User can view Self-Registration Requests and allow or deny those requests.	Access Add/Modify
Help desk with messaging		
Group Membership	User can access the Group Membership dialogs for Hosts and add or modify the selected host's membership in groups.	Access
Guest/Contractor Accounts	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
Locate Hosts & Users	User can search for Hosts and Users but cannot modify data. This is the default landing page when a user with this profile logs into FortiNAC.	Access

View	Access	Permissions Enabled
Send Message	User can send messages to hosts with the Persistent Agent or Mobile Agent installed.	Access
Self-Registration Requests	User can view Self-Registration Requests and allow or deny those requests.	Access Add/Modify
Operator		
Group Membership	User can access the Group Membership dialogs for Hosts and add or modify the selected host's membership in groups. Operators are restricted to the host and user groups they are configured to manage. They do not have access to all hosts and users	Access Add/Modify
Locate Hosts & Users	User can view Adapter, Host, User and Device Identity. User can modify Host information but cannot delete any records.	Access
Manage Hosts & Ports	Adapter List - Disable adapters. Adapter Properties- View only. Host Properties-View and modify access, but cannot send a message. User Properties - View Only. Device Identity - View and export data. This is the default landing page when a user with this profile logs into FortiNAC.	Access
Guest/Contractor Accounts	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
Self-Registration Requests	User can view Self-Registration Requests and allow or deny those requests.	Access Add/Modify
Operator with messaging		
Group Membership	User can access the Group Membership dialogs for Hosts and add or modify the selected host's membership in groups.	Access Add/Modify
Locate Hosts & Users	User can view Adapter, Host, User and Device Identity. User can modify Host information but cannot delete any records.	Access
Manage Hosts & Ports	• Adapter List - Disable adapters. • Adapter Properties- View only. • Host Properties-View and modify access, and can send a message. • User Properties-View Only. • Device Identity - View and export data. This is the default landing page when a user with this profile logs into FortiNAC.	Access
Guest/Contractor Accounts	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete

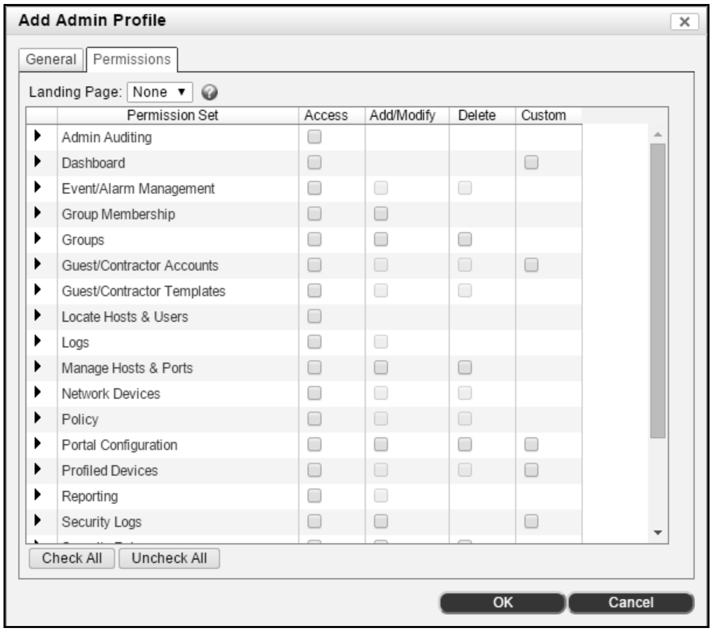
View	Access	Permissions Enabled
Self-Registration Requests	User can view Self-Registration Requests and allow or deny those requests.	Access Add/Modify
Send Message	User can send messages to hosts with the Persistent Agent installed.	Access
Operator with add hosts		
Group Membership	User can access the Group Membership dialogs for Hosts and add or modify the selected host's membership in groups.	Access Add/Modify
Locate Hosts & Users	User can view Adapter, Host, User and Device Identity. User can modify Host information but cannot delete any records.	Access
Manage Hosts & Ports	• Adapter List - Disable adapters. • Adapter Properties- View only. • Host Properties-View and modify access, but cannot send a message. • User Properties-View only. • Device Identity - View and export data. • User can add hosts. This is the default landing page when a user with this profile logs into FortiNAC.	Access Add/Modify
Guest/Contractor Accounts	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
Self-Registration Requests	User can view Self-Registration Requests and allow or deny those requests.	Access Add/Modify
Operator with delete hosts		
Group Membership	User can access the Group Membership dialogs for Hosts and add or modify the selected host's membership in groups.	Access Add/Modify
Locate Hosts & Users	User can view Adapter, Host, User and Device Identity. User can modify Host information and delete host and adapter records.	Access
Manage Hosts & Ports	• Adapter List - Disable adapters. • Adapter Properties- View only. • Host Properties-View and modify access, but cannot send a message. • User Properties-View only. • Device Identity - View and export data. This is the default landing page when a user with this profile logs into FortiNAC.	Access Delete
Guest/Contractor Accounts	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
Self-Registration Requests	User can view Self-Registration Requests and allow or deny those requests.	Access Add/Modify

View	Access	Permissions Enabled
Operator with add hosts and messaging		
Group Membership	User can access the Group Membership dialogs for Hosts and add or modify the selected host's membership in groups.	Access Add/Modify
Locate Hosts & Users	User can view Adapter, Host, User and Device Identity. User can modify Host information but cannot delete any records.	Access
Manage Hosts & Ports	• Adapter List - Disable adapters. • Adapter Properties- View only. • Host Properties-View and modify access, and can send a message. • User Properties-View only. • Device Identity - View and export data. • User can add hosts. This is the default landing page when a user with this profile logs into FortiNAC.	Access Add/Modify
Guest/Contractor Accounts	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
Self-Registration Requests	User can view Self-Registration Requests and allow or deny those requests.	Access Add/Modify
Send Message	User can send messages to hosts with the Persistent Agent installed.	Access
Operator with delete hosts and messaging		
Group Membership	User can access the Group Membership dialogs for Hosts and add or modify the selected host's membership in groups.	Access Add/Modify
Locate Hosts & Users	User can view Adapter, Host, User and Device Identity. User can modify Host information and delete host and adapter records.	Access
Manage Hosts & Ports	• Adapter List - Disable adapters. • Adapter Properties- View only. • Host Properties-View and modify access, and can send a message. • User Properties-View only. • Device Identity - View and export data. This is the default landing page when a user with this profile logs into FortiNAC.	Access Delete
Guest/Contractor Accounts	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
Self-Registration Requests	User can view Self-Registration Requests and allow or deny those requests.	Access Add/Modify
Send Message	User can send messages to hosts with the Persistent Agent installed.	Access

View	Access	Permissions Enabled
Operator with delete hosts, add hosts, and messaging		
Group Membership	User can access the Group Membership dialogs for Hosts and add or modify the selected host's membership in groups.	Access Add/Modify
Locate Hosts & Users	User can view Adapter, Host, User and Device Identity. User can modify Host information and delete host and adapter records.	Access
Manage Hosts & Ports	• Adapter List - Disable adapters. • Adapter Properties- View only. • Host Properties-View and modify access, and can send a message. • User Properties-View only. • Device Identity - View and export data. • User can add hosts. This is the default landing page when a user with this profile logs into FortiNAC.	Access Add/Modify Delete
Guest/Contractor Accounts	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
Self-Registration Requests	User can view Self-Registration Requests and allow or deny those requests.	Access Add/Modify
Send Message	User can send messages to hosts with the Persistent Agent installed.	Access
Profile_Sample		
Group Membership	User can access the Group Membership dialogs for Hosts and add or modify the selected host's membership in groups.	Access Add/Modify
Guest/Contractor Accounts	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials. User is limited to the GuestAccess_Sample template, can create accounts 45 days in advance and can create accounts with a maximum duration of 15 days.	Access, Add/Modify Custom Settings
Self-Registration Requests	User can view Self-Registration Requests and allow or deny those requests.	Access Add/Modify
Security analyst		
Dashboard	User can access and view the Dashboard	Access
Network Devices	User can view, add, modify, or delete network devices in the following views: • CLI Configuration • Device Profiling Rules • L2 Polling • L3 Polling • Locate • Port Changes • Topology	Access Add/Modify Delete

Permissions list

Admin Profiles contain permissions settings. An Administrative User inherits permissions from the Admin Profile applied to his user account. The table below contains a list of the permissions that can be set in an Admin Profile and any special information about each setting.



Landing Page: None ▾

Permission Set	Access	Add/Modify	Delete	Custom
Admin Auditing	□			
Dashboard	□			□
Event/Alarm Management	□	□	□	
Group Membership	□	□		
Groups	□	□	□	
Guest/Contractor Accounts	□	□	□	□
Guest/Contractor Templates	□	□	□	
Locate Hosts & Users	□			
Logs	□	□		
Manage Hosts & Ports	□	□	□	
Network Devices	□	□	□	
Policy	□	□	□	
Portal Configuration	□	□	□	□
Profiled Devices	□	□	□	□
Reporting	□	□		
Security Logs	□	□		□

Access levels

Level	Definition
Access	If enabled, the user will be able to see data in the views shown in the Permission Set, but not add, modify or delete. There are some exceptions to this that are noted in the table of permissions. In some cases, by enabling Access, other permissions are automatically enabled. For example, if you enable Access for Guest/Contractor Accounts, Add/Modify and Delete are automatically enabled and cannot be disabled.
Add/Modify	If enabled, the user can add or modify data in the views shown in the Permission Set.
Delete	If enabled, the user can delete data in the views shown in the Permission Set.
Custom	If enabled, an additional tab is shown that contains advanced settings for the Permission Set. For example, if Access to Guest/Contractor Accounts is enabled and Custom is enabled, advanced options can be set on the Manage Guests tab.

Permissions list

Where applicable, this table assumes that Access, Add/Modify, Delete and Custom options are enabled.

Views	Permissions	Notes
Admin auditing		
Admin Auditing	Provides access to the Admin Auditing Log.	
Dashboard		
Dashboard	Provides access to the Dashboard Tiles. Tiles require additional permissions as follows: • **Alarms Panel**—Requires access to Event/Alarm, links and buttons are enabled if Add/Modify is enabled. • **Summary Panel**—Requires access to System Settings. • **Network Device Summary Panel**—Requires access to Devices, links are enabled if Add/Modify or Delete are enabled for Devices. • **Host Summary Panel**—Requires access to Users/Hosts/Adapters. • **Scans Panel**—Requires access to Policy. • **User Summary Panel**—Requires access to Users/Hosts/Adapters. • **License Information Panel**—Requires access to System Settings. • **Persistent Agent Summary Panel**—Requires access to Policy. • **Performance Summary Panel**—Requires access to Event/Alarm.	Requires that other permissions be selected to display associated tiles.
Event/alarm		
Event to Alarm Mappings Event Management	If enabled, the views shown in the left column can be accessed.	Reports can be accessed but not all options can be used without access to User/Host/Adapter being enabled.
Group membership		
Group Membership	Allows access to Host, User, Device or Port group membership. Requires that one of the following additional permissions be enabled: • Devices • Locate Hosts & Users • Manage Hosts & Ports • Users/Hosts/Adapters	
Groups		
Groups	If enabled, allows access to the Groups View where you can view, add, modify or delete a group.	
Guest/Contractor Accounts		

Views	Permissions	Notes
Guest/Contractor Accounts	If enabled, allows access to the Guest Contractor Accounts View where you can view, add, modify or delete a guest account.	Has a Custom option that enables the Manage Guests Tab.
Custom/Manage Guests	This tab displays when the Custom permission is enabled. Custom Options include: • **Guest Account Access**—Indicates whether user can access All, Own or No guest accounts after they have been created. • **Account Types**—Allows user to create Individual, Bulk and or Contractor accounts • **Create Accounts Days in Advance (Maximum)**—Number of days before guest registers that the account can be created. • **Create Accounts Active For Days (Maximum)**—Maximum number of days that accounts created by this user are allowed to be active. • **Allowed Templates**—Templates that can be used to create Guest Accounts Refer to Add a guest manager profile on page 578 for detailed information.	
Locate hosts & users		
Locate Hosts & Users	If enabled, the views shown in the column on the left can be accessed. • User can view Adapter, Host, User and Device Identity. • User can view Group Membership for Hosts and Users. • User can modify Host information including registering a host. • User can modify User properties for network users and Admin users. • User can delete Host and Adapter records.	
Logs		
Alarms Connections Events Scan Results	If enabled, the views shown in the column on the left can be accessed. Users can view information about events within the system and on the network.	
Manage hosts & ports		
Manage Hosts & Ports	If enabled, the views shown in the column on the left can be accessed. Access is limited to users, hosts and adapters in groups for which user has permission. See Limit user access with groups on page 841.	

Views	Permissions	Notes
	User can view Adapter, Host, User and Device Identity. User can modify Host information including registering a host. User can modify User properties for network user. User can enable or disable an adapter. User can view Port properties for the ports where an adapter is connected.	
Network devices		
Network Device Summary Dashboard Tile CLI Configuration Device Profiling Rules L2 Polling L3 Poling Locate Port Changes Topology	If enabled, the views shown in the left column can be accessed.	To see Profiled Devices that option must be enabled separately.
Policy		
Control Access Network Device Roles Passive Agent Configuration Persistent Agent Properties Policy Configuration Remediation Configuration Roles	If enabled, the views shown in the left column can be accessed. The Passive Agent Registration View requires access to Groups to add or modify Passive Agent Configurations.	
Portal configuration		
Portal Configuration	If enabled, allows the user to view and edit settings for portals. Users with the Policies permission set enabled will also have this permission set enabled. Custom options include: • **Access** — Allows the user to view the portal settings. • **Add/Modify** — Allows the user to view the settings, add new portal settings, and delete existing portal configurations. Requires that Access permissions be enabled. Permissions can be further modified to prevent the user from adding new portal configurations or modifying the Default Portal Configuration. • **Delete** — Allows the user to view portal settings, add new ones, and modify and delete existing portal configurations. Requires that Add/Modify permissions be enabled.	
Profiled devices		

Views	Permissions	Notes
Profiled Devices	If enabled, allows the user to view the list of profiled devices. User can also Export devices, register a device, enable or disable a device, delete the device from the list and view details and notes for a selected device. The Views column on the Profiled Devices View contains icons that provide access to details about the selected device. these icons only display if additional permissions are enabled for the Administrative User. Possible views include: Adapter Properties, Group Membership, Port Properties and Device Properties. **Adapter Properties**—Requires permission for Users, Hosts and Adapters. **Group Membership**—Requires permission for Group Membership. **Port Properties**—Requires permission for Devices. **Device Properties**—Requires permission for Users, Hosts and Adapters or Devices.	Has a Custom option that enables the Profile Devices Tab.
Custom/Profile Devices	This tab displays when the Custom permission is enabled. Custom Options include: • **Register, Delete, and Disable Profiled Devices**—If enabled, the user can register, delete and disable devices that have been profiled by Device Profiler. • **Modify Device Rule Confirmation Settings**—If enabled, the user can change rule confirmation settings on devices that have been profiled by Device Profiler. Rule confirmation settings control whether or not Device Profiler checks a previously profiled device to determine if it still meets the criteria of the rule that categorized the device. • **Manage Profiled Devices Using These Rules**: • **All Rules**—includes current rules and any rules created in the future. • **Specify Rules**—you must choose the rules from the Available Rules field and manually move them to the Specify Rules field. • **Available Rules**—Shows the existing rules you can select for this profile. Select the rule and click the right arrow to move it to the Selected Rules pane. • **Selected Rules**—Shows the rules you selected	

Views	Permissions	Notes
	from the Available Rules section. The user can only access the devices associated with the rules in this list. Refer to for detailed information.	
Reporting		
Analytics Reports	If enabled, the views shown in the left column can be accessed.	
Security logs		
Security Alarms Security Events	If enabled, the views shown in the left column can be accessed. User has access to view security alarms created when a security rule is matched. Users can take action on a security alarm if it was not done automatically. The user's Admin Profile settings determine the actions they are allowed to complete.	This permission set is only available when Automated Threat Response (ATR) is enabled within your current license package. Has a Custom option that enables the Security Events tab.
Security rules		
Security Actions Security Rules Security Triggers	If enabled, the views shown in the left column can be accessed. User can create security devices, and security event rules. Users will establish and maintain all rules and the default actions associated with each rule.	This permission set is only available when ATR is enabled within your current license package.
Self registration requests		
Self Registration Requests	If enabled, user can manage requests for network access submitted by Guests from the captive portal.	
Send message		
Send Message	User can send messages to hosts with the Persistent Agent or Mobile Agent installed.	
System settings		
Scheduler Settings	If enabled, the views shown in the left column can be accessed.	All settings can be accessed when this permission is enabled. Refer to Settings on page 71 for a complete list.
Users/hosts/adapters		
Adapters View Device Identity Hosts View Users View	If enabled, the views shown in the left column can be accessed.	

Add an admin profile

Admin Profiles control permissions for Administrative Users.

1. Click **Users > Admin Profiles**.
2. Click **Add**. The **Add Admin Profile** screen appears with the **General** tab highlighted.

3. Enter a name for the profile.
4. Use the table below to configure the new admin profile.
5. On the **Permissions** tab note that some permissions are dependent on each other. Refer to the Permissions list on page 666 for additional information.
6. Click **OK** to save.

General tab settings

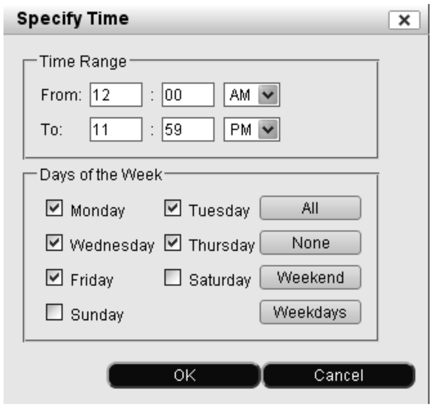
Field	Definition
Name	Enter a name that describes the profile, such as Librarian or IT Staff.
Logout After ... Minutes of Inactivity	User is logged out after this amount of time has elapsed without any activity in the user interface.
Login Availability	Indicates when users with this profile can log in to FortiNAC. Options include: **Always** or **Specify Time**. If you choose Specify Time, user access to FortiNAC is limited to certain times of day and days of the week.
Manage Hosts And Ports	Restricts an Administrative User to a specific set of hosts or ports. The set is defined by host and port groups that are assigned to be managed by a specific group of Administrative Users. Any Administrative User that has a profile with this option enabled can only view and or modify a subset of the data in FortiNAC. Typically, this type of user would ONLY have the Manage Hosts & Ports permission set on the Permissions tab, therefore, this setting is not used frequently. Default = All. **All**—All groups containing hosts and ports can be accessed. **Restrict By Groups**—Enables the restriction of Administrative Users to specific hosts and ports. For an overview and additional setup information see Limit admin access with groups on page 691.
Note	User specified note field. This field may contain notes regarding the data conversion from a previous version of FortiNAC for an existing Admin Profile record.
Enable Guest Kiosk	If you enable this mode, the ONLY thing that the Administrative User can access is the self-service Kiosk. Everything else in FortiNAC is disabled. The Administrative User can log into FortiNAC to provide visitors self-serve account creation through a kiosk. For added security, use a kiosk browser. See to read the Administrative User's procedure.
Kiosk Template	Field displays only if Enable Guest Kiosk is selected. Select a Kiosk template for this Admin Profile. All visitors who use the self-service Kiosk when this Administrative User is logged in are assigned this guest template.
Kiosk Welcome Message	Field displays only if Enable Guest Kiosk is selected. Enter the message that will appear when the kiosk user creates a guest account.

Permissions tab settings

Field	Definition
Landing Page	Indicates the first view displayed when an Admin User with this profile logs into FortiNAC. There are no options displayed in this field until permissions are selected.
Permission Set	Click the arrow next to a permission set to see the Views that can be accessed when this permission set is enabled. For example, if Devices is selected, this profile provides access to the following: CLI Configuration, Device Profiling Rules, L2 Polling, L3 Polling, Locate, Port Changes and Topology
Access	Indicates that the user will have view access to the permission set in the left column. Depending on the permission set, enabling Access automatically enables Add/Modify and/or Delete.
Add/Modify	Indicates that the user will be able to add or modify records in the permission set in the left column.
Delete	Indicates that the user will be able to delete records in the permission set in the left column.
Custom	When Custom is enabled for a permission set an addition tab is displayed. For example, if Custom is enabled for Guest Contractor Accounts a Manage Guests tab is displayed allowing you to configure additional controls for guest account creation. See Add a guest manager profile on page 578 for information on the Manage Guest tab. See Administrative user profiles for device managers on page 363for information on the Profile Devices tab.
Check All Uncheck All Buttons	Checks or unchecks all permissions.

Specify login availability time

This option allows you to limit access to FortiNAC for an Administrative User based on the time of day and the day of the week. Any Administrative User associated with this profile can only access FortiNAC as specified in the Login Availability field for the Admin Profile.


Specify Time

Time Range

From: 12 : 00 AM

To: 11 : 59 PM

Days of the Week

☑ Monday ☑ Tuesday

☑ Wednesday ☑ Thursday

☑ Friday □ Saturday

□ Sunday

1. Click **Users > Admin Profiles**.
2. Click select an admin profile and click **Modify**.
3. In the **Login Availability** field, select **Specify Time**.
4. In the **Time Range** section of the **Specify Time** dialog, enter the **From** and **To** times for the time of day that administrative users should be able to access the network.
5. In the **Days of the Week** section, select the days during which these users should be allowed to access the network.
6. Click **OK**.

Manage guests tab settings

Field	Definition
Guest Account Access	You can give Administrative Users with this profile privileges that allow them to manage all guest contractor accounts, regardless of who created them, only their own accounts, or no accounts. The privileges include whether the sponsors can add or modify accounts, locate guests or contractors, and view reports. **No**—Users can only see guest accounts they create and send credentials to those guests. Users cannot modify or delete any guest accounts. **Own Accounts**—Users can see guest accounts they create, send credentials to those guests, and modify or delete their own guest accounts. **All Accounts**—User can see all Guest accounts in the database, send credentials to guests and modify or delete any guest accounts.
Account Types	**Individual**—Sponsor can create single guest accounts. Within the constraints of the template, the sponsor may specify account start and end date. Each account has a unique name and password associated with it. **Bulk**—Sponsors may create multiple accounts with unique passwords by importing a bulk account file. **Conference**—Sponsors may create any number of conference accounts, or the number may be limited by a template. Conference accounts may be named identically but have a unique password for each attendee, have the same name and password, or have unique names and passwords.
Create Accounts Days in Advance (Maximum)	The maximum number of days in advance this sponsor is allowed to create accounts.
Create Accounts Active For Days (Maximum)	Determines the length of time the guest account remains active in the database.
Allowed Templates	Indicates whether the Administrative User can use all guest templates or only those in the Specify Templates > Selected Templates field. Default = All. Options include: **All Templates**—Profile gives the Administrative User access to all templates in the database when creating guest accounts. **Specify Templates**—Profile gives the Administrative User access to the templates listed in Selected Templates.

Field	Definition
Specify Templates	Allows you to select guest/contractor templates available for Administrative Users with this Admin User Profile. Use the arrows to place the templates needed in the Selected Templates column and the unwanted templates in the Available Templates column. If All Templates is selected in the Allowed Templates field, all templates are moved to the Selected Templates column and the arrows are hidden.
Available Templates	Shows the templates that have not been selected to be included in this Admin User Profile.
Selected Templates	Shows the templates selected to be included in this Admin User Profile.
Add Icon	Click this button to create a new Guest/Contractor template. For information on templates,
Modify Icon	Click this button to modify the selected Guest/Contractor template. For information on templates,

Profile devices tab settings

Field	Definition
Register, Delete, and Disable Profiled Devices	If enabled, the user can register, delete and disable devices that have been profiled by Device Profiler.
Modify Device Rule Confirmation Settings	If enabled, the user can change rule confirmation settings on devices that have been profiled by Device Profiler. Rule confirmation settings control whether or not Device Profiler checks a previously profiled device to determine if it still meets the criteria of the rule that categorized the device.
Manage Profiled Devices Using These Rules	**All Rules**—includes current rules and any rules created in the future. **Specify Rules**—you must choose the rules from the Available Rules field and manually move them to the Specify Rules field.
Available Rules	Shows the existing rules you can select for this profile. Select the rule and click the right arrow to move it to the Selected Rules pane.
Selected Rules	Shows the rules you selected from the Available Rules section. The user can only access the devices associated with the rules in this list.
Add Icon	Click this button to create a new Device Profiling Rule. For information on rules, see Add or modify rules on page 355.
Modify Icon	Click this button to modify the selected Device Profiling Rule. For information on rules, see Add or modify rules on page 355.

Security events tab settings

The Security Events tab is only available when ATR is enabled within your current license package.

Field	Definition
Allow Overriding of Recommended Actions	If enabled, the user can override the associated action when taking action on the alarm.
Allowed Actions for Security Events	**All Actions**—includes current actions and any actions created in the future. **Specify Actions**—you must choose the rules from the Available Actions field and manually move them to the Selected field.
Available Actions	Shows the existing actions you can select for this profile. Select the action and click the right arrow to move it to the Selected Actions pane.
Selected Actions	Shows the actions you selected from the Available Actions section. The user can only complete the actions in this list.

Modify admin profiles

1. Log into your administrator account.
2. Click **Users > Admin Profiles**.
3. A list of existing profiles is displayed.
4. Select a profile and click **Modify**. Refer to Add an admin profile on page 671 for settings.
5. Change the information and click **OK** to save.

If you modify an Admin Profile, the changes apply to all administrative accounts it is attached to, including those created before you modified the profile. Changes do not take effect until the associated Administrative Users log out of FortiNAC and log in again

The Modify Admin Profile window can also be accessed from the Admin Users View by clicking on the profile link associated with each Admin user.

Modify admin profiles for administrator users

1. Log into your administrator account.
2. Click **Users > Admin Profiles**.
3. Select the administrator profile and click **Modify**.
4. Enter the amount of time needed to elapse without any activity in the user interface before the user is logged out.
5. Select the **Landing Page** for the administrator user from the drop-down list.
6. Click **OK** to save.

If you modify an Admin Profile, the changes apply to all administrative accounts it is attached to, including those created before you modified the profile. Changes do not take effect until the associated Administrative Users log out of FortiNAC and log in again.

Delete an admin profile

You can not delete an Admin Profile if it is in use.

1. Log into your administrator account.
2. Click **Users > Admin Profiles**.
3. Select an admin profile and click **Delete**.
4. A message displays asking if you are sure. Click **Yes** to continue.

Copy an admin profile

You can create a copy of an existing Admin Profile and save it with a different name. This saves time when you create Admin Profiles if you are only changing a few fields.

1. Log into your administrator account.
2. Click **Users > Admin Profiles**.
3. The **Admin Profiles** option opens a window containing existing profiles.
4. To copy an admin profile, select the profile and click **Copy**.
5. Modify information as needed.
6. Click **OK**.

Admin profile mappings

Admin Profile Mappings allow you to apply an Admin Profile to an Administrative User when the user is added to an Administrator Group. An Admin Profile Mapping consists of a Administrative Profile that is linked to an Administrator Group.

Admin Profiles can be assigned to Administrative Users based on the users' group membership. Admin Profile Mappings Policies are ranked in priority starting with number 1. When an Administrative User is added to an Administrator Group the group name is compared to the group in each Admin Profile Mapping starting with the first mapping (Rank 1) in the list. If the group does not match in the first mapping, the next one is checked until a match is found.

When groups are nested within a parent group, admin profiles must be mapped to the groups that contain the users, and not the parent group only.

There may be more than one Administrator Group that is match for this Administrative User, however, the first match found is the one that is used.

Admin Profile assignments are not permanent. The Administrative User is reevaluated each time that user is added to or deleted from an Administrator Group.

Settings

Field	Definition
Rank Buttons	Moves the selected mapping up or down in the list. Administrative Users are compared to Admin Profile Mappings in order by rank.
Table columns	
Rank	Mapping's rank in the list of mappings. Rank controls the order in which Administrative Users are compared to mappings.
Admin Profile	Name of the profile that is assigned when an Administrative User becomes a member of the associated group. See Admin profiles and permissions on page 657.
Group	Contains the required group for an Administrative User.
Last Modified By	User name of the last user to modify the mapping.
Last Modified Date	Date and time of the last modification to this mapping.
Right click options & buttons	
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.
Copy	Copies the selected mapping.
Delete	Deletes the selected mapping.
Modify	Opens the Modify Mapping window for the selected mapping.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.

Mappings process

Admin Profile Mappings establishes a profile for Administrative Users who are members of a particular Administrator Group. Admin Profile Mappings are ranked so that if an Administrative User is a member of more than one group, FortiNAC can determine which Admin Profile should be applied to the user.

Example:

1. Administrative User John is in Group A and Group B.
2. Group A is mapped to a Guest Sponsor Profile and Ranked #5.
3. Group B is mapped to a Device Manager Profile and Ranked #2.
4. FortiNAC associates John with the Device Manager Profile because that mapping is higher in Rank and is the first match for John.

Adding an Administrative User to a Group that has an Admin Profile mapped can change the Admin Profile applied to that user.

Admin Profiles are only applied to members of an Administrator Group when the Administrative User is added to the group or deleted from a higher ranking group. The Administrative User could be added to the group manually or on directory resynchronization. Review the scenarios below for information on the behavior of Admin Profile Mappings.

Administrative user added to a group manually

- An existing Administrative User is added to Administrator Group A that is mapped to Admin Profile C. The user is not in any other Administrator groups. The Administrative User's profile is updated to Profile C because it is mapped to Group A.
- An existing Administrative User is added manually to Administrator Group A that is mapped to Admin Profile C. The user is also in Administrator Groups B and C, but the new group A is ranked higher in the Admin Profile Mappings list and the new Admin Profile C is assigned.

Administrative user added to a group based on directory group membership

- Admin Users are created automatically in FortiNAC when users authenticate to the Directory and then access FortiNAC through the Admin UI or by registering a host. The users are then assigned group membership according to their Directory groups.

  Possible scenarios that create Admin Users automatically are:
  - If a user exists in the directory, for example jdoe, but the user is not a user of any kind in FortiNAC, when jdoe logs into the FortiNAC User Interface using a directory user id and password, a user "jdoe" is created in FortiNAC as an Administrator user.
  - If a user exists in the directory, for example asmith, but the user is not a user of any kind in FortiNAC, when asmith registers a host via FortiNAC, a user for asmith, of type "user" is created. Then, when the Directory Synchronization task runs, asmith becomes an administrator user in FortiNAC.
  - If a user exists in the directory, for example tjones, but the user is not a user of any kind in FortiNAC, when tjones registers a host via FortiNAC, a user for tjones, of type "user" is created. If, before the Directory Synchronization task runs, the user logs into the FortiNAC Admin UI, the tjones user will transition to be an Administrator user at that time (i.e., not waiting for the Directory Sync.)
- When the Directory Synchronization is run, users are added to FortiNAC Administrator Groups that match the groups in the Directory. Adding Admin Users to a group triggers an evaluation of Admin Profile Mappings. If the Admin User is in multiple Directory groups, the user will be assigned to multiple groups in FortiNAC, and the Admin Profile will be assigned according to the Admin Profile ranking.

When an Admin Group is created in FortiNAC with the same name as a group being synchronized from a Directory, the Admin Group members will remain the same as the Directory group members. Therefore, if you add a non-Directory user to the Admin Group and then synchronize the Directory, the non-Directory user is removed from the Admin Group because the user is not a member of the Directory group.

Modify ranks of admin profile mappings

- The order of the Admin Profile Mapping records is changed modifying the ranking. A scheduled directory synchronization runs. Administrative Users' groups are updated each time the synchronization is run causing the Admin Profile Mappings to be analyzed again. Since the ranking has changed, some Administrative Users that are members of more than one group are assigned different Admin Profiles based on the new ranking.
- The order of the Admin Profile Mapping records is changed modifying the ranking. No directory is being used. Administrative Users continue to have the same Admin User Profiles because there is no mechanism to trigger a re-evaluation of group membership.

Administrative user deleted from a group manually

- An existing Administrative User is deleted from Administrator Group A that is mapped to Admin Profile C. The user is a member of Groups B and C mapped to Profiles D and F. A new profile is assigned based on one of the other groups used in the Admin Profile Mapping with the highest rank.

  Administrator Group B is mapped to Admin Profile D. Administrator Group C is mapped to Admin Profile F. The mapping for Group B has the highest rank, therefore the Administrative User's profile us updated to Admin Profile D.
- An existing Administrative User is deleted from Group A that is mapped to an Admin Profile C. The user is not a member of any other group mapped to a profile. The user's Admin Profile C is completely removed. The user loses his Admin User status and becomes only a regular network user under **Users > Users View**. To restore the user to an Admin User you must add the Admin User again with the same user ID and assign an Admin Profile.

Administrative user deleted from a group in the directory

- An existing Administrative User is deleted from Administrator Group A in the Directory. The directory resynchronizes with FortiNAC which deletes the Administrative user from Group A that is mapped to Admin Profile C. The user is a member of Groups B and C mapped to Profiles D and F. A new profile is assigned based on one of the other groups used in the Admin Profile Mapping with the highest rank.

  Administrator Group B is mapped to Admin Profile D. Administrator Group C is mapped to Admin Profile F. The mapping for Group B has the highest rank, therefore the Administrative User's profile us updated to Admin Profile D.
- An existing Administrative User is deleted from Administrator Group A in the Directory. The directory resynchronizes with FortiNAC which deletes the Administrative user from Group A that is mapped to Admin Profile C. The user is not a member of any other group mapped to a profile. The user's Admin Profile C is completely removed. The user loses his Admin User status and becomes only a regular network user under Users > Users View. To restore the user to an Admin User you must add the Admin User again with the same user ID and assign an Admin Profile.

Administrator group is deleted from FortiNAC

- An existing Administrative User is in Group A that is mapped to Admin Profile C. The user is not a member of any other group mapped to a profile. Group A is deleted from the Groups View. The user's Admin Profile C is completely removed. The user loses his Admin User status and becomes only a regular network user under Users > Users View. To restore the user to an Admin User you must add the Admin User again with the same user ID and assign an Admin Profile.

Admin profile mapping is deleted from FortiNAC

- Administrative Users are not affected when an Admin Profile Mapping is deleted from the data base until a user is added to or deleted from a Group. If the group is no longer mapped their profile is not updated. If the group continues to be mapped, their profile is updated as described in the previous scenarios.

When groups are nested within a parent group, admin profiles must be mapped to the groups that contain the users, and not the parent group only.

Changing the Ranking on existing Admin Profile Mapping records does not change profiles on Administrative Users unless those users are in the directory and the directory is resynchronized.

Adding a new Admin Profile Mapping does not affect existing Administrative Users until the directory is resynchronized or a user's membership in a mapped group changes.

If you are not using a directory there is no mechanism for Administrative Users to be reevaluated.

Add or modify a mapping

1. Click **Users > Admin Profiles**.
2. Select **Admin Profile Mappings** from the menu on the left.
3. Select an existing mapping and click **Modify** or click **Add**.
4. In the **Admin Profile** drop-down select a profile. If the profile you need is not in the list, use the **New** button to create it. See Add an admin profile on page 671 for instructions.
5. In **the** Group drop-down select an administrator group. If the group you need is not in the list, use the **New** button to create it. See Add groups on page 839 for instructions.
6. Click **OK** to save.

Delete a mapping

Deleting an Admin Profile Mapping does not affect profiles assigned to Administrative Users. They continue to have the same Admin Profile until something triggers a re-evaluation such as a directory synchronization.

1. Click **Users > Admin Profiles**.
2. Select **Admin Profile Mappings** from the menu on the left.
3. Select an existing mapping and click **Delete**.
4. Confirm that you want to delete the mapping.

Admin users

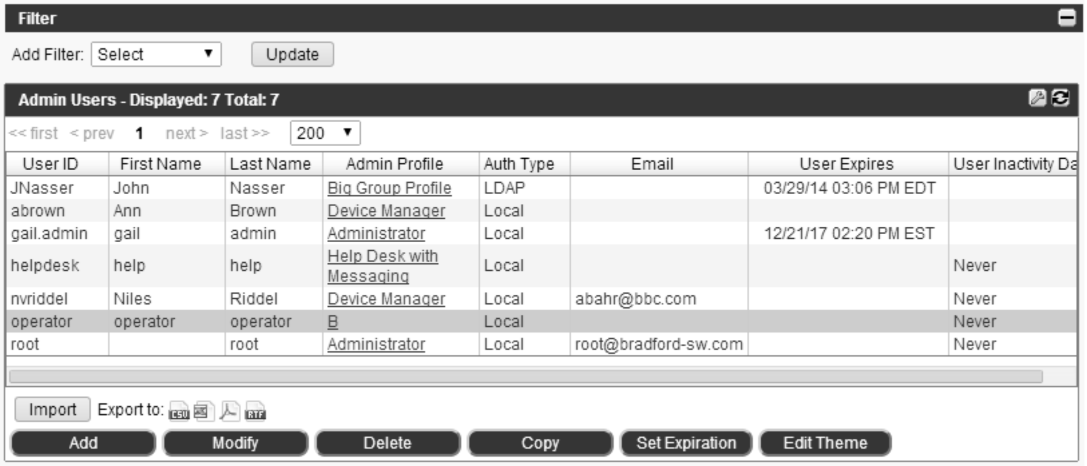
The Admin users view displays a list of existing system users. Use this window to add, modify or delete FortiNAC users. Admin users are also network users, therefore, FortiNAC also displays them in the Users View. If you are logged in as an Admin user, you cannot delete the Admin user account that you are using.

Administrator users cannot select a different admin profile for their own account. Use a second administrator account to access the administrator user and select a different admin profile.

If there are more than 1000 admin users in the database, the users are not automatically displayed. Instead, a confirmation dialog is shown asking if you would like to continue. Note that large numbers of records may load very slowly if not filtered. Choose **Yes** to display all admin users or **No** to reduce the number displayed by using the filters.

Admin Users can be accessed from **Users > Admin Users** or from **System > Quick Start > Authentication Settings**, however configuration steps point you to **Users > Admin Users**.

See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.


Filter
Add Filter: Select ▼
Update
Admin Users - Displayed: 7 Total: 7
<< first < prev 1 next > last >>
200 ▼

User ID	First Name	Last Name	Admin Profile	Auth Type	Email	User Expires	User Inactivity Da
JNasser	John	Nasser	Big Group Profile	LDAP		03/29/14 03:06 PM EDT	
abrown	Ann	Brown	Device Manager	Local			
gail.admin	gail	admin	Administrator	Local		12/21/17 02:20 PM EST	
helpdesk	help	help	Help Desk with Messaging	Local			Never
nvriddel	Niles	Riddel	Device Manager	Local	abahr@bbc.com		Never
operator	operator	operator	B	Local			Never
root		root	Administrator	Local	root@bradford-sw.com		Never

Settings

Fields used in filters are also defined in this table.

Field	Definition
Add Filter drop-down list	Allows you to select a field from the current view to filter information. Select the field from the drop-down list, and then enter the information you wish to filter. See Filters on page 15.
Update button	Displays the filtered data in the table.
Admin users	
User ID	Unique alphanumeric ID for this user. Required.

Field	Definition
First Name	User's first name.
Last Name	User's last name. Required.
Type	Indicates the type of Admin user being created. Types include Administrator and Administrative.
Admin Profile	Admin Users must have an associated Admin Profile that provides them with permissions for features in FortiNAC. Click the link in the Admin Users table for the selected user to go to the profile displayed. See Admin profiles on page 578.
Auth Type	Authentication method used for this Admin user. Types include: • **Local** — Validates the user to a database on the local FortiNAC appliance. • **LDAP** — Validates the user to a directory database. FortiNAC uses the LDAP protocol to communicate to an organization’s directory. • **RADIUS** — Validates the user to a RADIUS server.
E-mail	E-mail address used to send system notifications associated with features such as alarms or profiled devices.
Phone	Optional demographic information.
Address	
City	
State	
Postal Code	
Title	
Mobile Number	Mobile Phone number used for sending SMS messages to administrators.
Mobile Provider	Mobile provider for the mobile phone number entered in the previous field. Used to send SMS messages to administrators. This field also displays the format of the SMS address that will be used to send the message. For example, if the provider is US Cellular, the format is xxxxxxxxxx@emai.uscc.net, where the x's represent the user's mobile phone number. The number is followed by the email domain of the provider's message server.
User Expires	The user is deleted from the database when the date specified here has passed. The date is automatically calculated based on the information entered when Aging is configured. The default setting for Administrator users is blank or Never Expire. Administrative Users may or may not have an expiration date depending on how the account was created. See Aging out host or user records on page 823. To configure aging see, Set user expiration date on page 655. Admin Users assigned the Administrator Profile cannot be aged out.

Field	Definition
User Inactivity Date	Controls the number of days a User is authorized on the network. User is deleted from the database when the date specified here has passed. The date is continuously recalculated based on the information entered in the Days Inactive field. See Aging out host or user records on page 823.
User Inactivity Limit	Number of days the user must remain continuously inactive on the network to be removed from the database. See Aging out host or user records on page 823.
Last Login/Logout	Date of the last time the user logged into or out of the network or the FortiNAC Admin UI. This date is used to count the number of days of inactivity.
Last Modified By	User name of the last user to modify the admin user.
Last Modified Date	Date and time of the last modification to this admin user.
Right click menu options	
Copy	Copy the selected User to create a new record.
Delete	Deletes the selected User.
Group Membership	Displays groups in which the selected user is a member. Admin Users are also regular Users, therefore, separate options are displayed for Admin User Groups and User Groups. Options are labeled Group Membership (User) and Group Membership (Administrator).
Groups	Displays groups in which the selected user is a member. See Group membership on page 694.
Modify	Opens the Modify User window for the selected profile.
Set Admin Profile	Allows you to modify the Admin Profile for one or more users. This also allows you to remove the "Administrator" Profile for a user without the need to first delete and then recreate the user. See Modify a user's admin profile on page 689
Set Expiration	Launches a tool to set the date and time for the user to age out of the database. See Set user expiration date on page 655.
Edit Theme	Opens the User Theme dialog and allows you to modify the look and feel of the user interface for each Admin User.
Import/Export	Import and Export options allow you to import users into the database from a CSV file or export a list of selected hosts to CSV, Excel, PDF or RTF formats. See Import admin users on page 704 and Export data on page 710.

Add an admin user

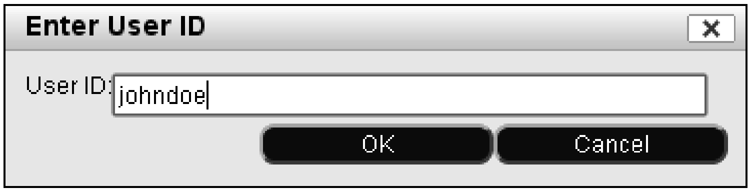
This option can be accessed from **Users > Admin Users**.

If you are creating Admin Users to manage guests or devices, you must create an Administrative User who has the appropriate Admin User Profile associated. See Admin profiles and permissions on page 657.

1. Select **Users > Admin Users**.
2. Click the **Add** button.

3. In the User ID window displayed, enter an alphanumeric **User ID** for the new Admin user and click **OK**. As you enter the User ID, the network user database is checked to see if there is a current user with the same ID and a drop-down list of matching users is displayed. If you enter an ID that already exists as a regular network user, the network user and the Admin user become the same person with a single account.

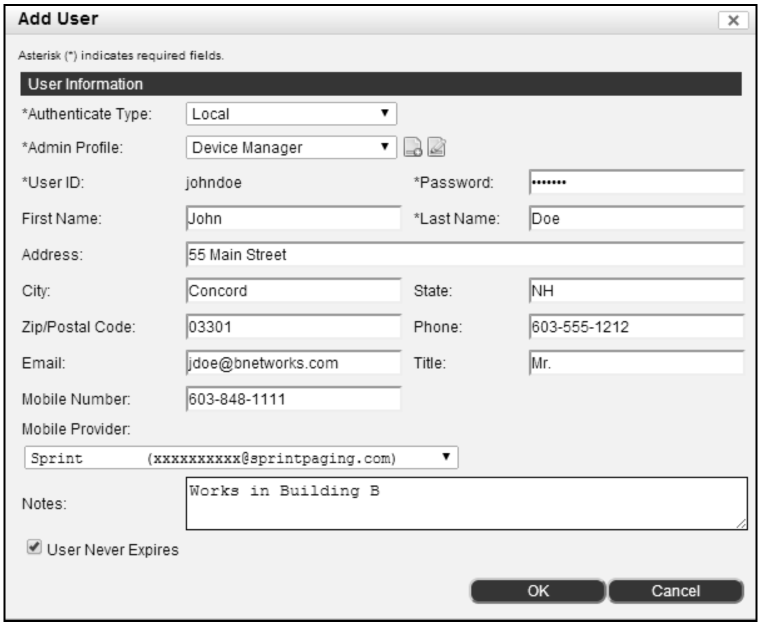
   This allows you to give a network user administrator privileges to help with some administrative tasks.



Enter User ID

User ID: johndoe

4. Use the table of Settings below to complete the information in the Add User dialog.
5. Click **OK** to save the new user.



Add User

Asterisk (*) indicates required fields.

User Information

*Authenticate Type:	Local		
*Admin Profile:	Device Manager		
*User ID:	johndoe	*Password:	•••••••
First Name:	John	*Last Name:	Doe
Address:	55 Main Street		
City:	Concord	State:	NH
Zip/Postal Code:	03301	Phone:	603-555-1212
Email:	jdoe@bnetworks.com	Title:	Mr.
Mobile Number:	603-848-1111		
Mobile Provider:	Sprint (xxxxxxxxxx@sprintpaging.com)		
Notes:	Works in Building B		

☑ User Never Expires

Settings

Field	Definition
Authentication Type	Authentication method used for this Admin user. Types include: • **Local** — Validates the user to a database on the local FortiNAC appliance. • **LDAP** — Validates the user to a directory database. FortiNAC uses the LDAP protocol to communicate to an organization's directory. • **RADIUS** — Validates the user to a RADIUS server.
Admin Profile	Profiles control permissions for administrative users. See Admin profiles and permissions on page 657. **Add** — Opens the Admin Profiles window allowing you to create a new profile without exiting the Add User window.

Field	Definition
	Modify — Allows you to modify the selected Admin Profile. Note that modifications to the profile affect all Administrative Users that have been assigned that profile.
User ID	Unique alphanumeric ID for this user.
Password	Password used for local authentication. If you authenticate users through LDAP or RADIUS, the password field is disabled and the user must log in with his LDAP or RADIUS password.
First Name	User's first name.
Last Name	User's last name.
Address	Optional demographic information.
City	
State	
Zip/Postal Code	
Phone	
E-mail	E-mail address used to send system notifications associated with features such as alarms or profiled devices. Also used to send Guest Self-Registration Requests from guests requesting an account. For multiple e-mail addresses, enter addresses separated by commas or semi-colons. Messages are sent to all e-mail addresses provided.
Title	User's title, such as Mr. or Ms.
Mobile Number	Mobile Phone number used for sending SMS messages to administrators.
Mobile Provider	Mobile provider for the mobile phone number entered in the previous field. Used to send SMS messages to administrators. This field also displays the format of the SMS address that will be used to send the message. For example, if the provider is US Cellular, the format is xxxxxxxxxx@email.uscc.net, where the x's represent the user's mobile phone number. The number is followed by the email domain of the provider's message server.
Notes	Free form notes field for additional information.
User Never Expires	If enabled, Admin users are never aged out of the database. The default is enabled. Admin Users assigned the Administrator Profile cannot be aged out.
Propagate Hosts	The Propagate Hosts setting controls whether or not the record for the host owned by the user is copied to all managed FortiNAC appliances. This field is only displayed if the FortiNAC server is managed by a FortiNAC Control Manager.

Modify an admin user

Administrator Users cannot select a different Admin Profile for their own account. Use a second Administrator account to access the Administrator User and select a different Admin Profile.

1. Select **Users > Admin Users**.
2. Select a user from the list.
3. Click the **Modify** button.
4. On the **Modify User** window, edit your data as needed.
5. Click the **Change Password** button to modify this user's password. This button is only available if the user is set for Local authentication. Users who authenticate through the directory or a RADIUS server must change their passwords in the directory or RADIUS server directly.
6. Click **OK** to save your changes.

For information on individual fields, see Settings on page 686.

Delete an admin user

1. Select **Users > Admin Users**.
2. Select a user from the list.
3. Click the **Delete** button.
4. A message is displayed asking if you are sure. Click **OK** to continue.

You are asked if you would like to delete registered hosts. If the Admin User is also the owner of any registered hosts, it is recommended that you delete the registered hosts. If they are not deleted, registered hosts associated with a deleted user become registered devices. If a user connects to the network with one of these devices, there is nothing to prevent network access because the device is known in the database.

Copy an admin user

You may copy a user, save it under another name, and use it as the basis for a new user.

1. Log into your administrator account.
2. Click **Users > Admin Users**.
3. The **Admin Users** window opens with a list of current users.
4. Select the user and click, **Copy**.
5. In the **User ID** window displayed, enter an alphanumeric ID for the new Admin user and click **OK**. As you enter the User ID, the network user database is checked to see if there is a current user with the same ID and a drop-down list of matching users is displayed. If you enter an ID that already exists as a regular network user, the network user and the Admin user become the same person with a single account.

   This allows you to give administrator privileges to a network user to help with some administrative tasks.
6. Change the name of the user, or other information and parameters.
7. Click **OK**.

Modify a user's admin profile

You can modify the Admin Profile for one or multiple users at a time. This also allows you to remove the "Administrator" Profile for a user without the need to first delete and then recreate the user.

1. Select **Users > Admin Users**.
2. Select one or more users from the list.
3. Right-click and select **Set Admin Profile**.
4. Select the **Admin Profile** from the drop-down list.
5. Click the **Add** button to add a new profile, or the **Edit** button to modify the selected profile.
6. Click **OK**.

User theme

Themes control the look and feel of the FortiNAC user interface for each individual user.

Set theme

1. Select **Users > Admin Users**.
2. The **Admin Users** window opens with a list of users.
3. Select the user to be modified.
4. Select **Edit Theme**.
5. Use the table below to enter settings.
6. Select the **Switch User(s) to Custom Theme Automatically** check box to automatically apply the custom theme to the selected user(s).
7. Selecting the **Switch User(s) to Custom Theme Automatically** check box allows an administrator to apply the custom theme to the selected user(s) without the need for the user to log in and change the theme manually.
8. Click **Apply To** to enable this theme for more users.
9. Click **OK** to set the theme.

Enable theme

After a theme is set for a specific user, that user must log into FortiNAC and enable the new theme as follows:

1. Navigate to **Help > Preferences** to display the **Admin User Preferences** dialog.
2. From the **Theme** drop-down, select **Custom**.
3. Click **OK**.

Settings

Field	Definition
Header	
Header	Controls the colors and text in the banner at the top of the window.

Field	Definition
Product Title	Removes the logo displayed in the banner and adds the text included in the Product Title field.
Text Color	Controls the color of any text displayed in the banner at the top of the window.
Primary Color	Controls the background color of the banner. Depending on the Blend Direction setting this is the first color starting from the top down or from left to right.
Secondary Color	Controls the background color of the banner. Depending on the Blend Direction setting this is the second color starting from the top down or from left to right.
Blend Direction	Controls how the Primary and Secondary colors are blended in the banner. Vertical blends from top to bottom with the Primary at the top. Horizontal blends from left to right with the Primary on the left.
Navigation	
Navigation	Controls the text and background colors of the menu bar.
Navigation Style	Controls the navigation method of the menu bar. Navigation bar is a plain menu bar in which the menu options are links and the menu with focus is underlined. Gradient with Tabs is a menu bar where the selected background color becomes lighter from top to bottom, and the menu with focus looks like a tab with a different background color. In this case, the color of the tab is controlled by the Detail Color option.
Text Color	Controls the color of the text on the menu bar.
Background Color	Controls the background color of the menu bar.
Detail Color	Controls the background color of a selected menu item when Navigation Style is set to Gradient With Tabs.
Selection Color	Color of the underline that indicates that a menu has focus when Navigation Style is set to Navigation Bar.
Panels	
Panels	Controls the colors and text in the title bars of panels such as tables of data.
Text Color	Controls the color of the text in the title bars of panels and dialog boxes.
Header Background	Controls the background color of the title bars of panels and dialog boxes.
Buttons	
Buttons	Controls the text and background colors of buttons.
Primary Color	Controls the background color of primary buttons throughout the system.
Primary Text Color	Controls the color of the text in primary buttons throughout the system.
Secondary Color	Controls the background color of secondary buttons throughout the system.
Secondary Text Color	Controls the color of the text in secondary buttons throughout the system.
Side bar	

Field	Definition
Side Bar	Controls the colors and text in side menus displayed on the left.
Text Color	Controls the color of the text in the side menus displayed on the left.
Background Color	Controls the background color of the side menus displayed on the left.
Hover Text Color	Controls the color of the text when the mouse hovers over a menu item in the side menus displayed on the left.
Hover Background Color	Controls the background color of a menu option when the mouse hovers over it in the side menus displayed on the left.
Dialog buttons	
Preview	Displays selected theme settings in the User Interface.
Remove Customizations	Returns the settings to the factory defaults for the selected user.
Switch User(s) to Custom Theme Automatically	Applies the theme to selected user(s) automatically without the need for the user(s) to manually change it.
Apply To	Allows you to select a list of users to whom this theme should apply.

Limit admin access with groups

To control which hosts and ports Admin users can access you can place those Admin users in special groups. Then designate those special Admin groups to manage groups of hosts or ports.

Example:

Assume you have two Administrative Users that are responsible for monitoring medical devices and nurses in a hospital. They should not see any other data. To accomplish this you must configure the following:

- Place the nurses' workstations into a host group.
- Place the medical devices to be monitored into a host group.
- Place the ports where the medical devices connect into a port group.
- Place these two Administrative Users in a special Administrator Group.
- Assign these two Administrative User to a profile with permissions for Manage Hosts & Ports. Make sure the Manage Hosts & Ports setting on the General Tab of the profile is set to Restrict by Groups.
- Set the Administrator group to manage the nurses group, the medical device group and the port group.
- Remove these two Administrative Users from the All Management Group or they will have access to all hosts and ports.

When those Administrative Users log into the Admin user interface, they can only see data associated with the nurses, medical devices or the ports in the groups they manage.

Make sure to remove affected Administrative Users from the All Management group or they will continue to have access to all hosts and ports.

Administrative Users can still view all hosts and users from the Locate View if their Admin Profile gives them permission for that view, but they can only modify those that are in the group they are managing.

1. Create the group of hosts or ports. See Add groups on page 839 for instructions.
2. Create an admin profile for with permissions for manage hosts & ports. Make sure the **Manage Hosts & Ports** setting on the **General Tab** of the profile is set to **Restrict by Groups**. See Add an admin profile on page 671
3. Create an administrator group that contains the administrative users responsible for the devices or ports.
4. Remove the administrative users from the **All Management** group. See Modify a group on page 841 for instructions.
5. Right-click on the administrator group and select **Manages**.
6. On the **Manages** window select the group(s) to be managed by marking them with a check mark.
7. Click **OK**.

Set admin privileges based on directory groups

To provide access to the FortiNAC user interface you can place Administrative Users in special groups that set the appropriate privileges. Typically this is done for users in your Directory, by placing them in special groups within the directory that correspond to matching groups in FortiNAC. When the Directory is synchronized with FortiNAC, users in the appropriate groups will be given Administrator or Administrative privileges based on their group settings and the Admin Profile Mapping that matches the user's group.

The Domain Users Group cannot be used to set Admin privileges because user details for users in that group are not populated in FortiNAC when a directory synchronization is done.

When an Admin Group is created in FortiNAC with the same name as a group being synchronized from a Directory, the Admin Group members will remain the same as the Directory group members. Therefore, if you add a non-Directory user to the Admin Group and then synchronize the Directory, the non-Directory user is removed from the Admin Group because the user is not a member of the Directory group.

Implementation

Directory

- Integrate your Directory with FortiNAC. See Directories on page 79 for configuration and integration information.
- Temporarily disable the Directory Synchronization task in the FortiNAC Scheduler to prevent the synchronization from pulling directory information before the setup is complete. See Scheduler view on page 849.
- If you want to send e-mail to Admin users, make sure to map the e-mail field in your directory to the e-mail field in FortiNAC. To set up this mapping go to **System > Settings > Authentication > LDAP**. Select the directory and click Modify. Select the Attribute Mappings tab and make sure that the e-mail field is configured. This setting allows

users to receive e-mails based on Device Profiling settings, Guest Manager settings, and event to alarm mappings based on group membership.

- Create groups in the directory for each set of administrator privileges you wish to grant. For example, if you want to have Administrative Users with full rights to FortiNAC and Administrative Users who are just Sponsors for guest access, create two groups in the directory, one for each type of Administrative Users. Add the appropriate Administrative Users to the new groups.
- Make sure the new groups are selected to be included when the directory and FortiNAC are synchronized. To select the groups go to **System > Settings > Authentication > LDAP**. Select the directory and click Modify. Click the Select groups tab and review the selected groups

FortiNAC

- All Administrative Users require an Admin Profile that provides permissions. Create the appropriate Admin User Profiles first. See Admin profiles and permissions on page 657.
- Go to the Groups View and create Administrator groups to contain the users who will be given access to FortiNAC. The group name must be absolutely identical to the name of the group in the directory.
- Since groups automatically brought over from the directory are typically Host groups, you must create the Administrator groups manually. If a group already exists with the name of one of the Administrator groups, you must delete that group and add it again as an Administrator group.
- Map Administrator Groups to Admin Profiles. These mappings allow FortiNAC to determine the Admin Profile that should be associated with an Administrative User based on the group that contains that user. Mappings are ranked and Administrative Users are associated with the first mapping they match. See Admin profile mappings on page 677.

  Example:

  - Administrative User John is in Group A and Group B.
  - Group A is mapped to a Guest Sponsor Profile and Ranked #5.
  - Group B is mapped to a Device Manager Profile and Ranked #2.
  - FortiNAC associates John with the Device Manager Profile because that mapping has a higher Rank and is the first match for John.
- Go to the Scheduler View in FortiNAC and enable the Directory Synchronization task. Run the task to update the groups. Users that have already registered in FortiNAC are updated immediately. New users that are not in the FortiNAC database but do exist in the Directory are added to FortiNACgroups when they log into the Admin User Interface the first time.
- Go to the Groups View and verify that the correct users have been placed in each group. See Groups view on page 838.
- Go to the Admin Users View and verify that the Admin User Profile is correct for each user. See Admin users on page 683.

If the root account for FortiNAC is placed in a group with an Admin User Profile other than the Administrator Profile, the Admin Profile of this account will change. This could potentially leave you without a root or admin login that provides access to the entire FortiNAC product.

Aging for new Administrative Users created by being added to a directory group is determined by Global Aging settings. See Aging on page 242 and Aging out host or user records on page 823.

Add admin users to groups

You can add selected Admin Users to groups you have created. See Groups view on page 838 for detailed information on Groups and how they are used in FortiNAC.

1. Select **Users > Admin User View**.
2. Use the filters to locate the appropriate Admin User(s).
3. Use Ctrl-click or Shift-click to select the records you wish to add to the group.
4. Right-click or click the **Options** button and select **Add Admin Users To Groups**.
5. The **Group Membership** view lists the available groups and sub-groups. Sub-groups are displayed under their parent group or groups.
6. To add the users to a group, click the box next to the group name and then click **OK**.
7. To create a missing group:
   a. Click the **Create Group** button.
   b. Enter a group name.
   c. If the new group should be a sub-group of an existing group, enable the **Parent Group** option and select the appropriate group from the list.
   d. **Description** is optional.
   e. Click **OK** to save the new group.
8. Click **OK**.

Group membership

From the Admin Users View you can view or modify the group membership of an individual User.

1. Select **Users > Admin Users**.
2. Select the user and click the **Groups** button.
3. The **Group Membership** view lists the available administrator groups. A check next to a group name indicates that this user is contained in that group.
4. To add the user to a group, click the box next to the group name and then click **OK**.
5. To remove the user from a group, click to uncheck the box next to the group name and then click **OK**.

Configure secure mode

Secure SSL Mode can be used for Administrative User access. Unique security certificates for the appliances are required to use secure mode. Secure certificates in a High Availability configuration may be used on both the primary and secondary appliances if the certificate provider licensing allows them to be transferred to their counterpart in the configuration.

FortiNAC appliances are pre-configured with a self-signed security certificate. The administrative user logs in at the following URL, which provides secure access:

```
https://<host name_or_IP>:8443
```

See SSL certificates on page 523.

Import and export data

Importing and exporting data allows you to leverage information across products, manipulate data outside your software or restore archived data. Import and export methods vary greatly depending on the type and location of the data. Review the tables below for information on import and export types and links to corresponding instructions.

Import types

Type	Definition
Import archived data on page 696	FortiNAC periodically archives and purges data from the database. Use this import to retrieve archived data for review.
Import hosts, users or devices on page 696	Allows you to import hosts, users with associated hardware, devices and IP Phones.
Import admin users on page 704	Allows you to import data for Admin users.
CLI import tool on page 706	A command line tool that allows you to import lists of devices by type into a selected container in the Topology View.
Import port descriptions on page 709	Allows you to import port descriptions into the Topology View from a .csv file.
Import IP ranges on page 706	Allows you to import ranges of IP addresses into the Access Point Management configuration view.
Import portal content on page 253	Allows you to import previously exported portal pages.
Bulk guest import on page 599	Allows you to import guest data from a text file to be used when creating bulk accounts.

Export types

Type	Definitions
Export data on page 710	Allows you to export data from table views in FortiNAC.
Add a custom report on page 904	After generating a custom report, you can export the data it contains.
Device identity on page 828	Allows you to export the results of a Device Identity search.
Conference accounts on page 602	Guest/Contractor Account views that allow you to export the data displayed.
Create bulk or multiple accounts on page 598	
Create guest/contractor accounts on page 595	

Type	Definitions
Export portal content on page 253	Allows you to export portal pages configured with the Portal Configuration Content Editor.
License information on page 42	Allows you to export data from the License Usage dialog. Click on the number in the In Use column on the License Information panel to open License Usage dialog. Export options are displayed at the bottom of the window.

Import archived data

When the Purge Events task runs, FortiNAC creates an archive of several different types of records. You can reimport this data if necessary. Importing archived data does not overwrite existing data it adds the archived records back into the database. Records that are archived and can be re-imported include the following:

- Alarms view on page 887
- Events view on page 867

1. Navigate to one of the views listed above.
2. Click the Import button at the bottom of the view to display the Import window.
3. Select the archive from the drop-down list. The archives are listed by date with the name of the view at the beginning. For example, for the Connections View the archive would have the following format: `DYNAMICLOG_Archive_YY_MM_DD.bua.gz`
4. Click OK.

Some archive files can be quite large and make take several minutes to import. A progress dialog is displayed as the import is taking place. A message is displayed when the import is complete.

Import hosts, users or devices

Hosts, users or devices can be imported into the database from a .csv (comma separated value) file. Devices imported through the Host View are displayed in the Host View.

Create an import file

To add Hosts, users, devices or IP Phones create a comma separated value (.csv) file using any text editor or spreadsheet tool. If you are using a text editor to create the file, use commas to separate the fields when you enter the data. Use carriage returns to separate records. You can mix the types of records you are importing. For example, you can import hosts, users and IP Phones in the same file as long as you have all of the appropriate fields in the header row.

To add Hosts or Devices create a comma separated value (.csv) file using any text editor or spreadsheet tool. If you are using a text editor to create the file, use commas to separate the fields when you enter the data. Use carriage returns to separate records.

The first row in the file is a header row and must contain a comma separated list of the database field names that are included in the import file. The order of the fields does not matter. For example, to import hosts and their corresponding adapters the header row could have the following fields: `adap.mac,adap.ip,host.owner,host.host,siblings`

Unless otherwise specified, data type is a string with no size limitations. Fields are case sensitive. For example, if you have User IDs SMITH123 and Smith123, the database treats these as two separate user records.

If you import something that already exists in the database, the existing record is updated with the new data from the import. For example, assume the database contains a host record with MAC address A0:11:22:BE:44:2C, IP address 192.168.10.102 and host name Taylor1 and you import a record that has MAC address A0:11:22:BE:44:2C, IP address 192.168.5.10 and host name Jones1. The MAC address remains the same since that is the key, but the other fields are updated. The database now contains a host record with MAC address A0:11:22:BE:44:2C, IP address 192.168.5.10 and host name Jones1.

Imported data is displayed on multiple views. Adapter data is displayed on the Adapter View and in Adapter Properties. Host data is displayed in the Host View, in Host Properties, and Topology View if Container is used in the import file. User data is displayed in the User View and User Properties.

The table below lists all of the possible import data fields by the name that should be used in the header row, indicates which fields are required and provides a definition for each field.

Fields

Header Field	Required For	Properties Field — Definition
Adapter		
adap.ip		**IP address** — IP address of the adapter. Use a valid IP format, such as, 127.0.0.1.
adap.mac	host	**Physical Address** — MAC address of the adapter. Use a valid MAC format, such as 00:19:D1:94:5C:06.
adap.loc		**Location** — The switch and port where the adapter is connected to the network.
adap.media		**Media Type** — Network interface type (wired or wireless).
adap.accessVal		**Access Value** — VLAN to which the adapter is assigned.
adap.descr		**Description** — Description of the adapter, such as, Intel(R) 82566DM Gigabit Network Connection.
adap.venName		**Vendor Name** — Name of the vendor for the adapter based on the first three octets of the MAC address, such as, Intel Corporation. Vendor OUIs are stored in the database and can be viewed through the Vendor OUI screen. See Vendor OUIs on page 127.
Host		
host.host		**Host Name** — Name of the host.

Header Field	Required For	Properties Field — Definition
host.role		**Role** — Roles are attributes on hosts that can be used as filters by FortiNAC when selecting a Network Access Policy, an Endpoint Compliance Policy or a Supplicant EasyConnect Policy. The role must be defined in FortiNAC and must be the same spelling and case. If the role field is blank or is not included in the import the host is assigned to the NAC-Default role.
host.owner		**Registered User** — User ID of the host's owner. On import FortiNAC checks for the user in its own database and in the LDAP directory. If the user does not exist a new user record is created. If the user does exist the user is connected to the host.
host.expireDate		**Expiration Date** — Date that the host is aged out of the database. Date format is MM/dd/yy HH:mm AM/PM Timezone or 04/07/10 08:11 AM EST. If not included in the import, the global setting in FortiNAC Properties is used. See Aging on page 242. The value "**Never**" can be used to prevent a host from ever being removed from the database by the aging process. Host age times are evaluated every ten minutes. If you specify a date and time, the host may not be removed from the database for up to ten minutes after the time selected.
host.inact		**Days Inactive** — the host can be inactive before being aged out. This number is used to calculate the date to age the host out of the database. If not included in the import, the global setting in FortiNAC Properties is used. See Aging on page 242. To avoid using the default settings you must enter a number in this field. You can use a very large number to ensure that the host is not deleted, such as 1825 Days (equals five years). Make sure that there is a space between the number and the word Days. The format for the value must be as follows: xxx Days 1825 Days
host.sn		**Serial Number** — Serial number of the host.
host.hwType		Hardware Type
host.os		**Operating System** — Host's operating system such as Windows XP or macOS. Only hosts that have an operating system listed in Host Properties are rescanned at the scheduled rescan time. Valid operating systems include: Windows or Mac.

Header Field	Required For	Properties Field — Definition
host.agentTag		**Asset Tag** — Arbitrary value assigned in the BIOS by the owner or manufacturer.
host.agentVer		**Agent Version** — Version number of the Persistent Agent installed on the host.
host.hasAgent		**Persistent Agent** — Indicates whether or not the host has an agent installed. Use true or false. If the field is left blank, the default is false.
host.notes		**Notes** — Data is imported into the Notes field in Host Properties.
host.topo	host - if importing into Topology	**Topology** — Container in Topology where this host should be placed on import. This field is required if importing into Topology. Host is managed by the Host View but displays in both the Host View and the Topology View.
host.dirPolVal		**Security And Access Value** — Security and Access Value is an attribute used as a filter for User/Host Profiles. Typically this is a value that comes from the user record in the directory. However, if you are not authenticating through a directory or if this host does not have an owner, the Security and Access Value can be entered manually.
host.devType		**Device Type** — Must be one of the following device types or blank: • Alarm System • Android • Apple iOS • Camera • Card Reader • Cash Register • Dialup Server • Environmental Control • Gaming Device • Generic Monitoring System • Health Care Device • Hub • IP Phone • Linux • macOS • Mobile Device • Network • PBX • Pingable • Printer • Registered Host • Server • StealthWatch

Header Field	Required For	Properties Field — Definition
		• Top Layer IPS • Unix • UPS • Vending Machine • Windows • Wireless Access Point • VPN • IPS / IDS
siblings		**Siblings** — Adapters that are on the same host are siblings. For example, if a PC has a wireless adapter and a wired adapter, those adapters are siblings. Enter the MAC addresses of all of the adapters for this host separated by semi-colons (;). See the example below: 00:15:70:CA:7D:01**;**00:15:70:CA:7D:00 Each adapter must have a separate record in the .csv file, with a siblings field listing all of the adapters on the host. Some device types may have only one adapter, such as IP Phones. To import those devices, include the MAC Address of the single adapter in the siblings field with no semi-colon.
User		
authType		**Local**- local user **Radius**- radius user **LDAP**- ldap user If "authType" is set to "LDAP" the user record will sync with the directory
user.fn		User's first name.
user.ln		User's last name.
user.uid	user	**ID** — Unique alpha numeric User ID. If a directory is used for authentication, when the FortiNAC database is synchronized with the directory, data for users with matching IDs is overwritten with data from the directory. For example, if you import a user with ID AB118 named Ann Brown and the directory contains a record of AB118 as Andrew Bowman, then your database shows AB118 Andrew Bowman.
user.email		User's e-mail address. For multiple e-mail addresses, enter addresses separated by commas or semi-colons. Messages are sent to all e-mail addresses provided.

Header Field	Required For	Properties Field — Definition
user.addr		User's mailing address.
user.city		User's city.
user.st		User's state.
user.zip		User's postal code.
user.ph		User's telephone number.
user.title		User's title.
user.role		**Role** — Roles are attributes on users that can be used as filters by FortiNAC when selecting a Network Access Policy, an Endpoint Compliance Policy or a Supplicant EasyConnect Policy. The role must be defined in FortiNAC and must be the same spelling and case. If the role field is blank or is not included in the import the host is assigned to the NAC-Default role.
user.notes		**Notes** — Data is imported into the Notes field in User Properties.
user.pw		**Password** — Password for this user.
user.dirPolVal		**Security And Access Value** — Security and Access Value is an attribute of a user that can be used as a filter for User/Host Profiles. Typically this is a value that comes from the user record in the directory. However, if you are not authenticating through a directory the Security and Access Value can be entered manually.
user.expireDate		**Expiration Date** — Date that the user is aged out of the database. Date format is MM/dd/yy HH:mm AM/PM Timezone or 04/07/10 08:11 AM EST.
user.maxHosts		**Allowed Hosts** — Maximum number of hosts that can be associated with or registered to this user and connect to the network.
user.delHosts		**Delete Associated Hosts** — Indicates whether or not hosts registered to this user should be deleted when the user is aged out of the database. Enter either Yes or No. This data displays on the User Properties window in the Time section and is set when the expiration date is set. Importing this field requires that you also include **user.expireDate** in your import file. If you do not include **user.expireDate**, the **user.delHosts** field data is not imported.
user.smsNum		**Mobile Number** — User's mobile phone number. This can be used to send SMS Messages based on events and alarms.
user.smsPro		**Mobile Provider** — The carrier or provider for the user's mobile phone. This must match the name of one of the providers in the Mobile Providers list in the database. See Mobile providers on page 175.

Sample import files

Hosts, Adapters, Users or Devices can be imported through the Hosts View using a .csv file. All of these items can be included in the same import file as long as the header row contains the appropriate database field names. Below are sample import files for each type as well as an import file containing records of all types.

Host import

The `adap.mac` field is required for this import.

```
adap.mac,siblings,adap.ip,host.owner,host.devType

00:13:CE:6C:56:75,00:13:CE:6C:56:75,192.168.20.45,Smith2010,Windows

00:15:70:D9:46:B0,00:15:70:D9:46:B0;00:15:70:D9:46:B1,,Orr2010,Linux

00:15:70:D9:46:B1,00:15:70:D9:46:B0;00:15:70:D9:46:B1,,Orr2010,Linux
```

Pingable device import

The `adap.mac` field is required for this import. The `host.devType` field is recommended to ensure that the correct icon displays. Use the `host.topo` field to display this device both in the Host View and the Topology View. Entering the name of the Topology Container in the host.topo field triggers FortiNAC to display the device in the Topology View. The device is automatically displayed in the Host View.

```
adap.mac,siblings,adap.ip,host.topo,host.devType

00:13:CE:6C:56:75,00:13:CE:6C:56:75,192.168.20.45,Blding_B,PBX

00:15:70:D9:46:B0,00:15:70:D9:46:B0,192.168.20.10,Blding_A,Camera

00:15:70:D9:46:B2,00:15:70:D9:46:B2,192.168.20.12,Blding_A,Printer
```

IP phone import

The `adap.mac` field is required for this import. The host.devType field is not required, however, since IP Phones are treated differently to prevent dropped calls, it is recommended that you include this field.

```
adap.mac,host.devType

00:12:C2:6C:56:74,IP Phone

00:12:C2:D9:46:B0,IP Phone
```

User import

The `user.uid` field is required for this import.

```
user.uid,user.fn,user.ln

Hebert2010,Frank,Hebert

Miller2009,Tammy,Miller
```

Mixed record types import

When combining different record types into a single import file, all of the fields for each record type must exist in the header row. For fields that do not apply to a particular record type, you must still include commas. Required fields for each type must be included.

```
adap.mac,siblings,host.owner,host.devType,user.uid,user.fn,user.ln
,,,,Hebert2010,Frank,Hebert
00:12:C2:6C:56:74,,,IP Phone,,,
00:13:CE:6C:56:75,00:13:CE:6C:56:75,Smith2010,Windows,,,
```

Import from a .csv file

To import from a .csv file created in V4.1.1 or higher, see Import from a previous version on page 703 for file format information.

1. Click **Hosts > Hosts View**.
2. At the bottom of the **Host View**, click **Import**.
3. Browse to the .csv file containing the items to be imported.
4. Select the file and click **Open**.
5. Click **OK** on the Import window.
6. FortiNAC processes the import file and displays a list of records in the Import Results window. Verify that the data is displaying in the correct columns.
7. Click **OK** to continue the import.

If the required columns are missing or data is not in the correct format, an error message is displayed and the import will not proceed.

If there are no issues with the data, a message is displayed indicating that the import is complete.

Import from a previous version

If you have a .csv file created for or exported from version 4.1.1 or higher, you can import that data into the current version of FortiNAC. You must modify the .csv file so that it conforms to the new import format.

The first row in the .csv file must be a header row and must contain a comma separated list of the database field names that are included in the import file. The order of the fields does not matter, but the order in the header row must match the order of the data contained in the file.

For the names and definitions of the fields that should be used in the header row see Fields on page 697.

Once your .csv file is formatted correctly, see Import from a .csv file on page 703 for import instructions.

Import admin users

Admin users can be imported into the database from a .csv (comma separated value) file through the Admin Users View.

Create an import file

To import Admin users create a comma separated value (.csv) file using any text editor or spreadsheet tool. If you are using a text editor to create the file, use commas to separate the fields when you enter the data. Use carriage returns to separate records.

The first row in the file is a header row and must contain a comma separated list of the database field names that are included in the import file. The order of the fields does not matter. For example, to import admin users the header row could have the following fields: `profileName,uid,authType,fn,ln`

Unless otherwise specified, data type is a string with no size limitations. Fields are case sensitive. For example, if you have User IDs SMITH123 and Smith123, the database treats these as two separate user records. If you import something that already exists in the database, the existing record is updated with the new data from the import.

If you import an existing Admin user, all fields will be replaced by those in the import file.

When you select the Make Importable check box while exporting users, any user with an authentication type of "LDAP" is imported as a local user.

Imported data is displayed on both the Admin User view and the User View. The table below lists all of the possible import data fields by the name that should be used in the header row, indicates which fields are required and provides a definition for each field.

Fields

Field	Required	Definition
profileName	Yes	**Admin Profile** — Administrative Users must have an associated Admin Profile that provides them with permissions for features in FortiNAC. Enter the name of the Admin Profile that matches an existing Profile in the database.
uid	Yes	**User ID** — Unique alpha numeric User ID. If a directory is used for authentically the FortiNAC database is synchronized with the directory, data for users with matching IDs is overwritten with data from the directory. For example, if you import a user with ID AB118 named Ann Brown and the directory contains a record of AB118 as Andrew Bowman, then your database shows AB118 Andrew Bowman.

Field	Required	Definition
authType		Authentication method used for this Admin user. Types include: • **CM** — Validates the user to a database on the local FortiNAC appliance. • **LDAP** — Validates the user to a directory database. FortiNAC uses the LDAP protocol to communicate to an organization's directory. • **RADIUS** — Validates the user to a RADIUS server.
fn		User's first name.
ln		User's last name.
email		User's e-mail address. For multiple e-mail addresses, enter addresses separated by commas or semi-colons. Messages are sent to all e-mail addresses provided.
addr		User's mailing address.
city		User's city.
st		User's state.
zip		User's postal code.
ph		User's telephone number.
title		User's title.
notes		Notes about this user.
expireDate		**Expiration Date** — Date that the user is aged out of the database. Date format is MM/dd/yy HH:mm AM/PM Timezone or 04/07/10 08:11 AM EST.
createDate		**Creation Date** — Date that the user record was created. Date format is MM/dd/yy HH:mm AM/PM Timezone or 04/07/10 08:11 AM EST.
smsNum		**Mobile Number** — User's mobile phone number. This can be used to send SMS Messages based on events and alarms.
smsPro		**Mobile Provider** — The carrier or provider for the user's mobile phone. This must match the name of one of the providers in the Mobile Providers list in the database. See Mobile providers on page 175.

Sample import file

Below is a sample .csv file for importing Admin users. the profileName and uid fields are required.

```
profileName,uid,authType,fn,ln

Administrator,ajones111,LDAP,,Jones

Administrator,admin111,CM,Admin,User111
```

```
Conference Accounts,dpcuser,CM,Elaine,White

Conference Accounts,ajames,CM,james,james
```

Import IP ranges

Some views in FortiNAC require lists of IP address ranges. An import mechanism is provided to speed up the process of entering this data.

1. Click **System > Settings**.
2. Navigate to the view where you would like to import IP address ranges.
3. Click **Import** at the bottom of the screen.
4. In the **Import** window type the first and last IP address of each range separated by a comma. Press Enter to start a new line. You should not have overlapping ranges or ranges that cross subnets such as 192.168.5.100-192.168.6.150.
5. Click **OK** to import the IP address range.
6. Click **Save Settings** to save your changes.

CLI import tool

If you need to add a set of devices to your FortiNAC database, those devices can be imported from a .csv file using a CLI device import tool. When importing a device, the import tool first checks the database to see if a device with the same IP already exists. If the device exists, then it is removed from the database before the new device is created.

For an SNMP device, the device discovery process determines the device class based on the SNMP MIBs supported by the device. For other device types, the class is based on the import type entered on the CLI command line. You must create a separate .csv file for each device type. For example, if you are importing printers and hubs, the list of printers must be contained within one .csv file and the list of hubs must be contained within another .csv file.

The latest device import tool is located in the `/bsc/campusMgr/bin` directory on the FortiNAC Server (Control Server in an Application/Control server pair).

Device types that can be imported include:

- SNMP
- hub
- WAP
- printer
- server
- pingable
- healthcare
- IPS
- DialUpServer
- StealthWatch
- gaming
- camera
- UPS
- cardReader

- cashRegister
- hvac
- vending
- PBX
- generic
- security
- VPN
- IP phone
- mobile
- network
- toplayer
- Linux
- Unix
- Windows
- macOS

iOS and Android devices cannot be imported with this tool. Use the import options on the Host View instead. See Import hosts, users or devices on page 696.

Create .csv files for device import

Create the CSV file with a text editor, or by exporting the device information from an application that can generate the CSV file format. The file should be formatted as follows for SNMP and non-SNMP devices.

Each device type must be contained within its own .csv file. For example, if you are importing printers and hubs, you must have a .csv file for printers and a separate file for hubs.

SNMP devices

For SNMP devices, format each line in the CSV file as follows:

```
CONTAINER,IP,USER,TELNET,ENABLE,RWCOMM,ROCOMM,ROLE
```

There must be a carriage return at the end of the each line in the file. The final line in the CSV file must also end in a carriage return or the last line will not be imported. Also, if a field is null, you must still include the field delimiter (comma).

If multiple SNMP devices with the same name are imported, the first device has the correct name. All subsequent devices are named with a combination of the name and IP address, such as Camera[192.168.5.86].

Settings

Field	Definition
CONTAINER	Folder model in the topology view. Containers are used to group devices (**required**). If the Container field is blank, the IP address is used as the Container name and a localhost IP is entered (127.0.0.1).
IP	IP address of the new device (**required**). If the IP address field is blank, a localhost IP is entered (127.0.0.1).
USER	User name used to telnet into the device.
TELNET	Password used to telnet into the device.
ENABLE	Enable password.
RWCOMM	Read/Write Community Name. This must come first, before the Read Only community name.
ROCOMM	Read Only Community Name.
ROLE	Role for the device.

Example:

```
test,192.168.5.32,admin,net123,,private,public,NAC_Default,
test,192.168.5.35,admin,net456,bscen1,private,public,NAC_Default
```

Non-SNMP devices

For non-SNMP devices, format each line in the CSV file as follows: `CONTAINER,IP,NAME,MAC,na,na,na,Role`

There must be a carriage return at the end of the each line in the file. The final line in the CSV file must also end in a carriage return or the last line will not be imported. Also, if a field is null, you must still include the field delimiter (comma).

Settings

Field	Definition
CONTAINER	Folder model in the topology view. Containers are used to group devices (**required**). If the Container field is blank, the IP address is used as the Container name and a localhost IP is entered (127.0.0.1).
IP	IP address of the new device (**required**). If the IP address field is blank, a localhost IP is entered (127.0.0.1).
NAME	Name of the device.

Field	Definition
	If multiple non-SNMP devices with the same name are in the import file, the first device has the correct name. All subsequent devices are not imported.
MAC	MAC address of the device (optional).
NA	blank
NA	blank
NA	blank
ROLE	Role for the device.

Import devices with the CLI tool

If you are importing different types of devices, each type must be contained within its own CSV file. For example, to import five printers and two vending machines, you must have a CSV file for the printers and a separate CSV file for the vending machines.

1. Use a secure copy tool to copy the CSV file from your local PC to the FortiNAC appliance (e.g., use Winscp).
2. Back up the current FortiNAC database before proceeding.
3. From the FortiNAC appliance CLI, navigate to the following directory: `cd /bsc/campusMgr/bin`
4. Run the DeviceImport tool as follows:

   ```
   RunClient DeviceImport <absolutePathToImportFile> -type <t>
   ```

   Where:

   <absolutePathToImportFile> = The absolute path to the CSV file.

   <t> = snmp |hub |wap |printer |server |PINGABLE |healthCare |IPS |Nessus |DialUpServer |StealthWatch |gaming |camera |UPS |cardReader |cashRegister |hvac |vending |pbx |generic |security |vpn |ipPhone |mobile |network |toplayer |linux |unix |windows |macosx

   Examples:

   ```
   RunClient DeviceImport server.csv -type server
   RunClient DeviceImport switches.csv -type snmp
   ```
5. Log into the FortiNAC.
6. Go to **Topology** view, and verify that the devices have been imported. If necessary, modify the device properties.

Import port descriptions

From within the Topology View you can import port descriptions into the FortiNAC Server and FortiNAC Control Server appliances from a .csv text file containing the comma separated values.

Use only letters, numbers and hyphens (-) when creating port descriptions. Other characters, such as #, may prevent FortiNAC from communicating properly with the device.

1. Create the .csv file with any text editor or spreadsheet tool.

   Use commas to separate the data fields if you are using a text editor to create the file. The data you enter into the record for each port must contain all the fields.

   Example:

   "IPAddress","InterfaceID","Floor","Room","Jack"

   Settings

Field	Description
IPAddress	IP address of the switch.
InterfaceID	ID of the interface. This ID is displayed in the Port Properties window for the selected port.
Floor	Optional field. If not used, type open and closed quotation marks: “”.
Room	Optional field. If not used, type open and closed quotation marks: “”.
Jack	Optional field. If not used, type open and closed quotation marks: “”.

2. Save the file with the .csv extension in the filename.
3. Click **Network Devices > Topology**.
4. Right-click the **Customer Container** and select **Import Port Desc**.
5. Navigate to the directory where the .csv file containing the port descriptions is located. Click to select the file, then click **Open**.

The port description data is imported into FortiNAC.

Export data

Export data to a CSV file, an Excel spreadsheet, a PDF document or an RTF document. Select from a list of possible fields and control the order of the data in the export. If you plan to re-import the same file after editing it, you must use a CSV file. See Import hosts, users or devices on page 696 for a list of fields that can be exported or imported and their definitions.

1. Navigate to a View with export options at the bottom, such as the Host View.
2. Use the Search or Filters to display a list of records.
3. Use Ctrl-click or Shift-click to select the records you wish to export. If you do not select specific records, all displayed records are exported. When the Export dialog is displayed, check the Selected Rows check box to export only selected records.
4. At the bottom of the window, click the icon for the type of export file needed, such as PDF.

5. In the File Name field, enter a name for the export file. Do not add an extension. It is added when you click OK based on the file type you selected in the previous step.
6. The fields contained in the Export Dialog vary based on the View from which you are exporting.
7. Select the field(s) you want to export and click the right-arrow to move the field to the Show As Columns list. Ctrl-click to select more than one field at a time.
8. Click the double-arrows to move all of the fields from one column to the other.
9. To remove fields from the export, select them in the Show As Columns list and click the left-arrow.
10. To reorder the fields in the **Show As Columns** list, click the field and then click the Up or Down arrows. The order displayed from top to bottom corresponds to the columns in the export from left to right. For example, if the first field at the top of the list is Last Name, that is the left most column in the export.
11. To sort fields alphabetically, click the **Sort** button labeled AZ.
12. Check the **Selected Rows** check box to export only the records selected in the View. If you leave this box unchecked, all the records in the View are exported.
13. A Header line consisting of the field names is inserted in the .csv file if you check either or both of the **Make Importable** check boxes. In addition, the fields required for import are automatically added to your export.

> When you select the **Make Importable** check box while exporting users, any user with an authentication type of "LDAP" is imported as a local user.

> Only the Export Dialog accessed from Users, Hosts or Adapters views includes two Make Importable check boxes because of the relationship between Users and their corresponding Hosts. The Export Dialog accessed from other views may have one Make Importable check box, such as, Admin Users, or no Make Importable check boxes, such as Connections.

14. Click **OK**.
15. Depending on your browser, the file is either generated and saved to a downloads location or you may need to navigate to the location where the file is to be placed.

Topology view

The Topology view provides an overview of the managed network. To access the Topology view select **Network Devices > Topology**.

The topology tree is displayed in the left frame. It consists of FortiNAC and user-created containers. User-created containers contain managed network devices. Device icons displayed in the tree change to red if contact is lost. See Topology tree contact status on page 714. See the Icons on page 30 for a description of the icons.

The right pane displays a tabbed view with tabs for Containers, Devices, Ports and SSIDs, depending on the selection in the tree. For example, if a Container is selected, tabs for Devices, Ports and SSIDs are displayed.

Options

The right-click menu contains the following options based on the selected icon. When you select an item in the tree, the menu shows options specific to the selection.

Icon	Definition	Right-Click Options
🔍 Find	Opens a search field above the Topology Tree. Search for containers or devices by name, IP address or Physical address. See Find containers or devices on page 22.	
⚑ Customer	Represents the organization. When selected, a tabbed view is displayed in the right pane with tabs for Containers, Devices, Ports and SSIDs. Pingable devices are not displayed in the tabs on the right only in the tree.	• **Add Container**—Create a new container • **Control Access**—Select devices and containers to be isolated • **Control Access Network Summary**—Status of the access control groups for containers and devices • **Import Port Descriptions**—Import Port descriptions • **Rename**—Modify customer name
⚑ Container	Containers allow logical grouping of network devices. When selected, a tabbed view is displayed in the right pane with tabs for Devices, Ports and SSIDs.	• **Add Device**—Add an SNMP enabled device to the selected container. • **Add Pingable Device**—Add a pingable device to the selected container. • **Control Access**—Enable/disable access control groups on the selected container • **Convert Pingables To Hosts**—Convert all Non-SNMP devices in the container to Hosts. • **Delete**—Deletes the selected item • **Start Discovery**—Discovers SNMP enabled devices on your network and adds them to the selected container

Icon	Definition	Right-Click Options
		• **Modify**—Modify the container name
Device	Represents individual network devices. When selected, a tabbed View is displayed in the right pane with tabs for Ports, Element, System, Polling, Credentials and, if applicable, SSIDs. If the device is a pingable, device properties are displayed in the right pane. Hosts that are displayed in Host View and Topology View are not shown in the right pane on the Devices tab because they are managed in Host View. You can display these hosts by clicking the View in Host View link.	• **Control Access**—Enable/disable access control groups on the selected device • **Convert To Host**—Convert a Non-SNMP device to a host. • **Delete**—Deletes the selected item • **Group Membership**—View Groups associated with this device • **Local Mgmt (HTTP)**—Open an HTTP interface for local management of the device. Device must support local management. • **Move To Container**—Move selected device to a different container. • **Network Access/VLANs**—Modify Device Values, Summary, and Update Current & Default Values • **Poll For Contact Status**—Poll the device immediately instead of waiting for scheduled Poll. • **Poll for L2 (Hosts) Info**—Read the host information on the selected device and update the Ports tab. • **Ports and Hosts**—Display VLAN (Current and Default) and Host (Name and IP) information for each port on the device. • **Properties**—Provide detailed information about the device and allow some configuration. • **Show Audit Log** —Opens the Admin Auditing Log showing all changes made to the selected item. • **Modify**—Edit contact and communication settings for the device. • **Resync Interfaces**—Update interface information for the device. • **Role Membership**—View associated roles. • **Update Device Mappings**—Assign a device type to an unknown SNMP device, allowing it to be managed. • **Device Specific**—Global Model Configuration, Model Configuration, Running Configuration, and Secure

Icon	Definition	Right-Click Options
		/Static Ports - **Select Device In Tree**—Highlights the non-SNMP device in the Topology Tree and displays device properties in the right pane. Device Specific options vary depending on the device type.
Port	Ports cannot be selected in the tree, only from the Ports tab in the right pane.	- **Connection Details**—Opens a new view with information about hosts or users connected to the selected port - **Group Membership**—View or modify port groups containing selected port - **Port Changes**—Opens Port Changes View detailing changes to the selected port such as VLAN changes or CLI Configurations applied. - **Port Properties**—Opens Port Properties dialog with current port settings and status - **Role Membership**—Displays list of roles that contain the selected port - **Select Device In Tree**—Highlights the device associated with the selected port in the Topology Tree.
SSID	SSIDs cannot be selected in the tree, only from the SSIDs tab in the right pane.	- **Properties**—Opens the SSID Properties dialog with current settings - **Group Membership**—Displays list of groups that contain the selected SSID - **Select Device In Tree**—Highlights the device associated with the selected SSID in the Topology Tree

Topology tree contact status

The tree in the left hand frame of the Topology View displays a list of network devices that are managed by FortiNAC, such as switches or routers. In addition to devices that provide network services, FortiNAC can manage pingable devices, such as alarm systems or printers. If FortiNAC cannot contact a device, a red box is displayed around the icon for the device and also around the icon for the Container used to group devices. The red icons in the Topology tree indicate that the device has not responded to periodic pings sent by FortiNAC. However, there are circumstances in which devices are in contact with FortiNAC but due to their configuration, they will not respond to a ping.

If you are using a Directory server, it is communicating with FortiNAC via LDAP. The Topology View may turn the Directory icon red even though the two are communicating. To prevent this, enable ping on the Directory server.

Devices that display in both the Host View and the Topology View are managed by the Host View. The Host View does not use ping as a method to verify the connection between FortiNAC and the device. The Host View relies on the polling interval of the switch to which each device is connected to determine if the device is still connected and in contact with FortiNAC. In the Topology tree the icons for devices managed in Host View will turn red if the device has not had any activity on the port to which it is connected for some time. This would eventually cause the MAC address of the device to be removed from the forwarding table of the switch. Depending on the device, you may want to manage it only in the Topology View. This prevents the icon from turning red indicating that contact with the device has been lost.

See Icons on page 30 for status icon definitions.

Control access

The purpose of the Control Access feature on containers, devices, and ports is to place devices and ports into system groups that control network access for hosts connected to those ports.

The top level Control Access window shows containers and devices. Within this view, you can globally select all containers or manually select individual containers. Uplink ports are exempt from being placed in system access groups.

When the Control Access feature is used, selected ports and devices are placed first into their own groups. Then, those groups are placed into one of the system access groups. For example, if you have a container named Building A that contains devices Cisco Switch 1 and Cisco Switch 2, when the devices are placed under access control FortiNAC creates a device group that contains both switches and a port group that contains all of their corresponding ports. The port and device groups are named using access group, container name and device or port.

In this example the device group would be Registration-Building A-Devices. The port group would be Registration-Building A-Ports.The device group and the port group are then moved into the access group selected in the Type field. If the Type field is set to Registration, the ports go into the Forced Registration group.

You may select and move all the ports or devices to access groups including: Forced Registration, Forced Authentication, Forced Remediation, Dead End and Role-Based Access. Adding devices and ports to a Forced Remediation group enables Quarantine VLAN switching, a FortiNAC feature. Any devices that have been unselected are removed from the access group shown in the Type field.

Each of these groups refers to an underlying port group, with the exception of Dead End. The underlying group for Dead End is a device group (rather than a port group) named Physical Address Filtering.

Devices and ports contained within any of these groups can also be modified from the Groups View. Device and port groups created by this process are treated as system groups and cannot be deleted from the Groups View. They can be deleted from the Container Control Access window.

Removing a device, its ports, or both from all of the access control groups mentioned above ensures that no network access control will occur on those ports. The presence of a device, its ports, or both in any of those groups enables access control for that device, its ports, or both, meaning that FortiNAC will dynamically attempt to change the network access configuration based on the state of the host appropriate to the group. Ports will also be moved into the default network configuration should a connected host not satisfy the related isolation criteria. If an affected port is a member of the Role-Based access group, a network access policy may override the default network configuration.

Control Access can be modified from the Topology View by right-clicking on any of the following:

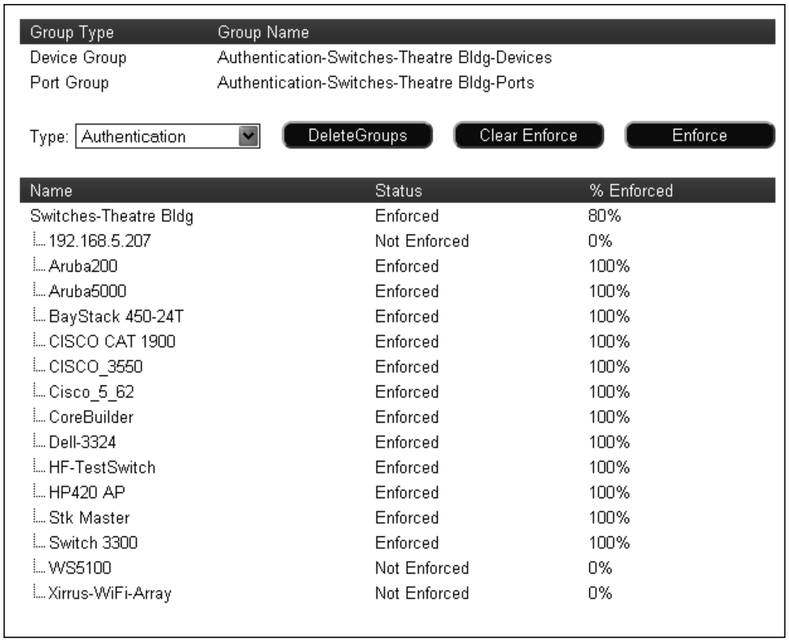
- **Customer Icon**—Set up access control for multiple containers and devices.
- **Container Icon**—Set up access control for all devices within the container.
- **Device**—Set up access control for all ports on a device.

Containers

This option is used to modify membership of devices and ports in the selected container in system access control groups. This information can also be modified in the Groups View.

Percentage Enforced indicates the percentage of ports that are in the selected access control group. For example, if a switch has 10 ports, and % Enforced displays 80%, then 8 of the 10 ports for that switch are an access control group, such as Registration. Unregistered hosts connecting to one of the 8 ports would be forced to register.

If a device group has 5 switches, and % Enforced for the group displays 20%, then one of the 5 switches in the device group has some ports in the access control group selected.



Group Type	Group Name
Device Group	Authentication-Switches-Theatre Bldg-Devices
Port Group	Authentication-Switches-Theatre Bldg-Ports

Type: Authentication

Name	Status	% Enforced
Switches-Theatre Bldg	Enforced	80%
192.168.5.207	Not Enforced	0%
Aruba200	Enforced	100%
Aruba5000	Enforced	100%
BayStack 450-24T	Enforced	100%
CISCO CAT 1900	Enforced	100%
CISCO_3550	Enforced	100%
Cisco_5_62	Enforced	100%
CoreBuilder	Enforced	100%
Dell-3324	Enforced	100%
HF-TestSwitch	Enforced	100%
HP420 AP	Enforced	100%
Stk Master	Enforced	100%
Switch 3300	Enforced	100%
WS5100	Not Enforced	0%
Xirrus-WiFi-Array	Not Enforced	0%

1. Log into your administrator account.
2. Click **Network Devices > Topology**.
3. In the navigation pane, right-click on the container and select **Control Access**.
4. This view shows the device and port groups that have been created and their names. If no device or port groups have been created, NONE is displayed.
5. In the Type field select the system access group to be modified. Options include: Authentication, Registration, Remediation, Dead End and Role-Based access. When a Remediation group is created it enables the Quarantine VLAN switching option under **System > Settings > Control > Quarantine**.
6. The bottom half of the screen allows you to check the status of the container.
7. To create device and port groups for all devices in the container, click **Create Groups**.
8. To add all switches in the container to the system access control group selected in the **Type** field, click **Enforce**. This also creates the necessary device and port groups if they do not exist.
9. To remove all switches in the container from the selected system access group click **Clear Enforce**.

10. To delete the device and port groups, click **Delete Groups**. This also removes all of the devices and ports from the selected system access group.
11. A confirmation screen appears. Click **OK**. The screen refreshes and displays the new settings.

Network summary

Displays the access status of the containers and devices on the network. Enforced indicates that access control is enforced on the container or device. For example, hosts connecting to a device in the registration access control group are forced to register. Not Enforced indicates that no ports on the device or container are in the access control group.

Percentage Enforced indicates the percentage of ports that are in the selected access control group. For example, if a switch has 10 ports, and % Enforced displays 80%, then 8 of the 10 ports for that switch are an access control group, such as Registration. Unregistered hosts connecting to one of the 8 ports would be forced to register.

If a device group has 5 switches, and % Enforced for the group displays 20%, then one of the 5 switches in the device group has some ports in the access control group selected.

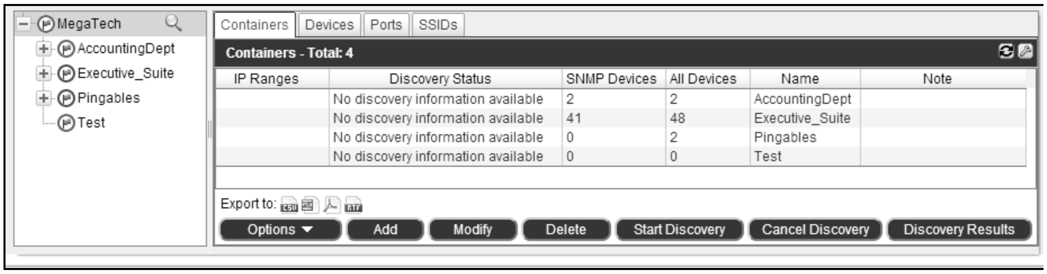
1. Log into your administrator account.
2. Click **Network Devices > Topology**.
3. Right-click the **Customer** icon.
4. In the drop-down list, select **Control Access Network Summary**. This view shows all of the containers and devices on the network and their status for each system access group type.
5. Click in the **Type** field to select a different system access group. Options include: Authentication, Registration, Remediation, Dead End and Role-Based Access.
6. If there is a container, a device within a container, or device whose status is **Not Enforced**, use the **Topology** view and **Control Access** to modify their status.

Customer icon

The Customer Icon in the Topology View represents the organization. Select this icon to display tabs for Containers, Devices, Ports and SSIDs in the right frame. All Containers, Devices, Ports and SSIDs in the database can be accessed from here. Right-click on the Customer Icon to add containers, import port description data, and modify the customer name. Click the Find button to the right of the icon to locate

See Import port descriptions on page 709 and for additional information on those Customer Icon features.

When FortiNAC is installed, the Customer node in the Topology View is listed as Customer. See Rename customer icon on page 721 for instructions on entering a new .



Containers - Total: 4

IP Ranges	Discovery Status	SNMP Devices	All Devices	Name	Note
	No discovery information available	2	2	AccountingDept	
	No discovery information available	41	48	Executive_Suite	
	No discovery information available	0	2	Pingables	
	No discovery information available	0	0	Test	

Settings

Field	Definition
Containers Tab	When the Customer Icon or Node is selected, the Containers tab is displayed with a list of all Containers in the database. Containers are also displayed in the tree under the Customer Icon. See Containers view on page 830. Selecting a container from the Containers tab or from the tree provides you with the same set of right-click options. Add a container by right-clicking the Customer Icon or using the Add button on the Containers tab. See Configure container for devices on page 831.
Devices Tab	When the Customer Icon or Node is selected, the Devices tab is displayed with a list of all Devices in the database. Devices are also displayed in the tree under the Container in which they reside. See Device view on page 739. Hosts that are displayed both in Host View and Topology View are not displayed in the table of devices because they are managed in the Host View. They are displayed in the tree. Selecting a device from the Devices tab or from the tree provides you with the same set of right-click options. Add a device by right-clicking the Container Icon or using the Add button on the Devices tab.
Ports Tab	When the Customer Icon or Node is selected, the Ports tab is displayed with a list of all Ports in the database. Ports are read from devices and cannot be added manually. See Ports view on page 778.
SSIDs Tab	When the Customer Icon or Node is selected, the SSIDs tab is displayed with a list of all SSIDs in the database. SSIDs are read from devices and cannot be added manually. See SSID view on page 786
Right click options	
Add Container	Adds a new container to the database which is displayed in the tree. For additional information see, Configure container for devices on page 831.
Control Access	Place devices and ports into system groups that control network access for hosts connected to those ports. See Control access on page 715.
Control Access Network Summary	Displays the control access enforcement status of all devices on the network. See Network summary on page 717.
Import Port Descriptions	Import port descriptions into the FortiNAC Server and FortiNAC Control Server appliances from a .csv text file containing the comma separated values. See Import port descriptions on page 709.
Rename	Modify the name of the Customer Icon. See Rename customer icon on page 721.

Configure container for devices

Containers are similar to folders and are used to group devices within your FortiNAC database. The Containers view also has a status column. As devices for a container are being discovered by FortiNAC the status of that process is displayed in the Status column. You must click the Refresh button at the top of the window to update the status.

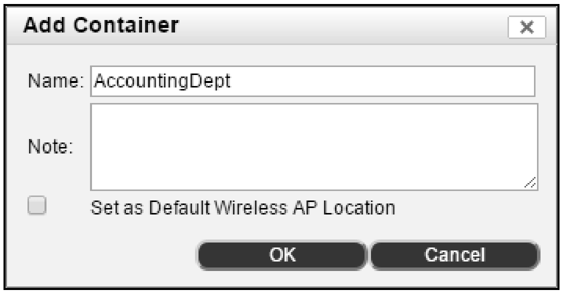
When you delete a container, all associated devices are also deleted. To avoid this issue move your devices to a new container first, then delete the unwanted container.

Access Containers from one of the following locations:

- **System > Quick Start > Network Device Settings**
- **Network Devices > Topology > Customer Icon**

Add a container

1. Select **Containers**.
2. On the Containers panel click **Add**.
3. Enter the Container Name and click **OK**.
4. Select the **Set as Default Wireless AP Location** check box to specify that the container is the default container where Wireless APs will be added. This will occur if there is no alternative AP location specified on the wireless device's model configuration view.



Add Container

Name: AccountingDept

Note:

□ Set as Default Wireless AP Location

Modify a container

1. Select **Containers**.
2. On the Containers panel, select the container to be modified.
3. Click **Modify**.
4. Edit the name and click **OK**.
5. Select the **Set as Default Wireless AP Location** check box to specify that the container is the default container where Wireless APs will be added. This will occur if there is no alternative AP location specified on the wireless device's model configuration view.

Delete a container

1. Select **Containers**.
2. In the Containers panel select the Container to be removed.
3. Click **Delete**.

Forced registration group

This option allows you to place devices and ports into the Forced Registration group. Hosts connecting to ports in this group are forced to register if they have not already done so.

1. Log into your administrator account.
2. Click **Network Devices > Topology**.
3. Right-click the **Customer Icon** and select **Control Access**.
4. The Control Access screen opens with a list of all of the containers and devices. Click **Expand All**.
5. In the **Type** field select the Registration system access group.
6. From the **Containers and Devices** list, select the components for which you want to enforce access control. You can click **Select All** or select individual containers and devices. If you have already configured this group, removing devices here also removes them from the Forced Registration group.
7. Click **Next**.
8. A screen opens that describes what the Control Access function will do, and shows a list of all the selected containers and devices. Note that the view contains helpful general information above the list and in the Group Notes section below the list.
9. The **Known** column indicates the number of connected hosts that are registered. The **Unknown** column indicates the number of rogues connected. Some rogues could be devices such as a gaming device or an IP Phone. Those devices are not capable of registering themselves. You may want to disable them or remove them from the network before placing ports in to Forced Registration. Use the **Manage Hosts** button to open the Host View and see your rogue hosts.
10. Click **Finish**. In the confirmation screen, click **OK**.
11. The **Control Access Network Summary** window displays showing you the access control status of the containers and devices you selected.

Control access

This option allows you to place devices and ports into one of the following system access groups: Forced Registration, Forced Authentication, Forced Remediation, Dead End and Role-Based Access. See Forced registration group on page 720 for instructions on using the Forced Registration groups. For all other groups, continue with this set of instructions.

1. Log into your administrator account.
2. Click **Network Devices > Topology**.
3. Right-click the **Customer Icon** and select **Control Access**.
4. The **Control Access** screen opens with a list of all of the containers and devices. Click **Expand All**.
5. In the **Type** field select the system access group to which you would like to add selected devices and containers. Options include: Authentication, Remediation, Dead End or Role-Based Access. When a Remediation group is created it enables the Quarantine VLAN switching option under **System > Settings > Control > Quarantine**.

6. From the **Containers and Devices** list, select the components for which you want to enforce access control. You can click **Select All** or select individual containers and devices. Click **Next**.
7. The **Control Access Network Summary** window displays showing you the access control status of the containers and devices you selected.

Rename customer icon

1. Click **Network Devices > Topology**.
2. Right-click the **Customer Icon** and select **Rename**.
3. Enter a new name.
4. Click **OK**.

Container icon

Containers are logical groups that are used to organize network devices. See Configure container for devices on page 831 for more information. Click the Container icon to manually add, delete, and automatically discover devices, and to view and edit device properties.

A device must be given a unique name in order to appear in Topology view. You cannot add devices with duplicate names.

Any device you add to a container must be reachable by IP through ICMP/Ping and then with the SNMP v1 or v3 credentials. Check firewall settings to determine whether the device is reachable prior to adding the device to a container. Make sure ICMP is enabled on the network.

Network devices should have static IP addresses or dynamic IP addresses that are reserved. Once a device that provides network services had been identified in FortiNAC there is no mechanism to automatically update the IP address for that device if there is a change. If the IP address on the device itself is changed, the device appears in FortiNAC to be offline or to have a communication error.

See Control access on page 715 for additional information on that Container Icon feature.

When a Container is selected in the Topology View tree, the panel on the right displays Devices, Ports and SSIDs tabs. These contain lists of every device and every port that reside within the selected container. Hosts that display both in Host View and Topology View are not included in the Devices tab because they are managed through the Host View, and are indicated by the number of host devices not shown.

The title bar of the Devices panel shows the number of devices Displayed, Total Devices in the database and Host Devices that are not shown. The View in Host View link allows you to display the hosts that are managed in Host View.

To see host devices, expand the appropriate Container in the tree. Hover over an item in the tree to display the associated tool tip. The tool tip indicates whether the item is a Host or a Network Device.

Settings

Field	Definition
Devices Tab	When the Customer Icon or Node is selected, the Devices tab is displayed with a list of all Devices in the database. Devices are also displayed in the tree under the Container in which they reside. See Device view on page 739. Hosts that are displayed both in Host View and Topology View are not displayed in the table of devices because they are managed in the Host View. They are displayed in the tree. Click the View in Host View link to display the hosts that are managed in Host View. Selecting a device from the Devices tab or from the tree provides you with the same set of right-click options. Add a device by right-clicking the Container Icon or using the Add button on the Devices tab.
Ports Tab	When the Customer Icon or Node is selected, the Ports tab is displayed with a list of all Ports in the database. Ports are read from devices and cannot be added manually. See Ports view on page 778.
SSIDs Tab	When the Customer Icon or Node is selected, the SSIDs tab is displayed with a list of all SSIDs in the database. SSIDs are read from devices and cannot be added manually. See SSID view on page 786
Right click options	
Add Device	Adds an SNMP device to the selected container. See Add or modify a device on page 723
Add Pingable Device	Adds hubs, IPS/IDS, printers, servers, wireless access points and other non-SNMP or pingable devices to a container. See Add or modify a pingable device on page 725.
Control Access	Place devices and ports into system groups that control network access for hosts connected to those ports. See Control access on page 715.
Convert Pingables To Hosts	Converts one or more selected non-SNMP or pingable devices to hosts. After conversion these devices are removed from Network Devices but do display both in the Topology View and the Host View. See Convert all pingables to hosts on page 734. Wireless Access Points added as pingables cannot be converted to hosts.
Start Discovery	Searches the network based on user specified IP ranges and determines what SNMP enabled devices exist on the network. Once a device is discovered, FortiNAC creates a model for the device in the database and places the device in the Network Devices list. See Discover devices on page 735.

Add or modify a device

You can manually add devices to a container. This process adds a single SNMP-enabled device at a time. Devices may be configured for SNMPv1 or SNMPv3 communication.

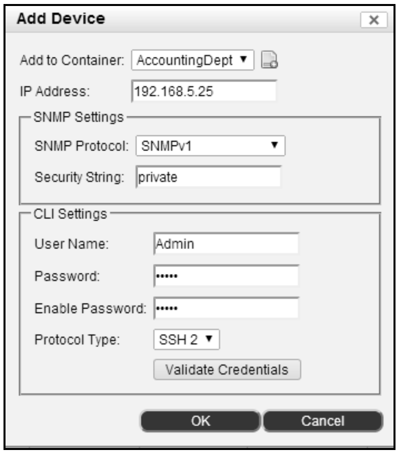
A device must be given a unique name in order to appear in Topology view. You cannot add devices with duplicate names.

For information on the specific devices and support requirements, log into the Customer Portal and search for the device or device family.

If your device has multiple interfaces, each with a different IP address that is configured with its own SNMP settings, multiple representations of the same device will be added to FortiNAC. FortiNAC does not consolidate the duplicates in this case.

1. Click **Network Devices > Topology**.
2. Select the Container icon.
3. Right-click a container and select **Add Device** or right-click on a device in the Devices Tab and select **Modify**.
4. Click in the **Add To Container** field and select a container for this device. If the container you need does not exist, click the **New** icon and add the container first.
5. Enter the **IP address** of the device.
6. Select an **SNMP** protocol.

   For SNMPv1 communication, enter the security string to use when communicating with the device.



Add Device

Add to Container: AccountingDept

IP Address: 192.168.5.25

SNMP Settings

SNMP Protocol: SNMPv1

Security String: private

CLI Settings

User Name: Admin

Password: •••••

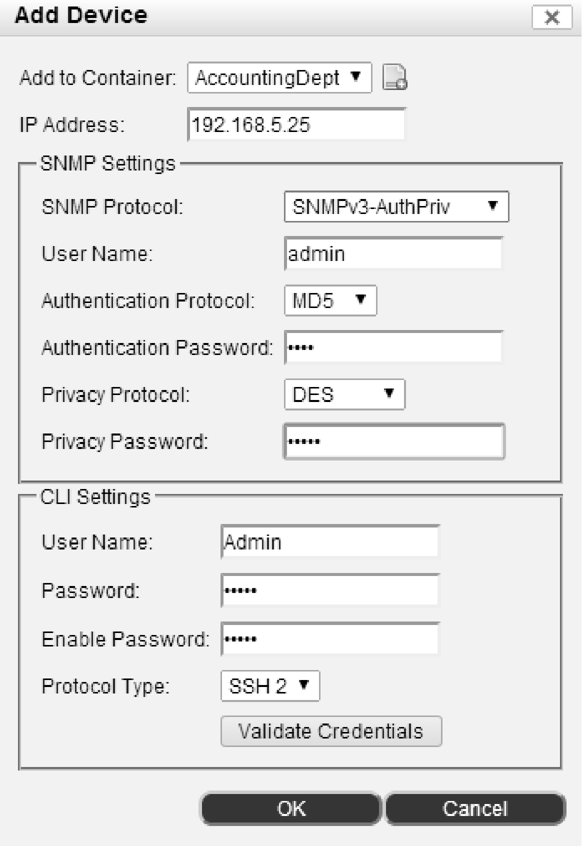
Enable Password: •••••

Protocol Type: SSH 2

If the device has multiple security strings, enter only the Read/Write security string. This is the string that will ensure that FortiNAC has the ability to control the device.

For SNMPv3 communication enter the User Name, select the Authentication Protocol, and then enter the Authentication Password you used when you configured the device. For SNMPv3-AuthPriv, you must enter the

Privacy Protocol and Privacy Password. These settings must match the corresponding settings on the device you are adding.



Add Device

Add to Container: AccountingDept

IP Address: 192.168.5.25

SNMP Settings

SNMP Protocol: SNMPv3-AuthPriv

User Name: admin

Authentication Protocol: MD5

Authentication Password: ••••

Privacy Protocol: DES

Privacy Password: •••••

CLI Settings

User Name: Admin

Password: •••••

Enable Password: •••••

Protocol Type: SSH 2

Settings

Field	Definition
SNMP Protocol	Available options are AuthPriv or AuthNo Priv.
User Name	User Name for access to the device. Recommended but not required.
Authentication Protocol	Available options are: • MD5 • SHA1 (Recommended)
Authentication Password	Specify password to match what the device is using.
Privacy Protocol	Available options are: • DES • AES-128 (Recommended)
Privacy Password	Specify password to match what the device is using.

If the device is configured for AuthPriv, the Authentication password, Privacy Protocol and Privacy password are required. If the device is configured for AuthNoPriv, only the Authentication password is required.

In the CLI Settings section, enter the Username, Passwords and Protocol for CLI access to this device. FortiNAC requires CLI access to manage hosts on the device.

CLI settings

Field	Definition
User Name	User name used to log on to the device for configuration. The user account must have the appropriate permissions configured on the device. For network devices using API credentials, the User Name is the serial number of the appliance.
Password	Password required to configure the device. For network devices using API credentials, the Password is the REST API Key.
Enable Password	Enable password for the device, if applicable.
Protocol Type	Protocol used for communication with the device. Options include: Telnet, SSH1 and SSH2.

7. Click **Validate Credentials** to test the CLI and SNMP credentials entered.
8. Click **OK**.
9. Go to the **Model Configuration** view for this device to complete the configuration. See Model configuration on page 767 for instructions.

Add or modify a pingable device

Use the Add Pingable Device option to add hubs, IPS/IDS, printers, servers, wireless access points and other pingable devices to a container. The Physical Address (MAC) is required when creating pingable devices if the IP to MAC cannot be resolved when the ARP tables are read.

A device must be given a unique name in order to appear in Topology view. You cannot add devices with duplicate names.

1. Click **Network Devices > Topology**.
2. Select the **Container** icon.
3. Right-click a container and select **Add Pingable Device** or right-click on a pingable device in the **Devices** tab and select **Modify**.
4. From the drop-down menu select the **Container** where this device will be stored. You can use the icon next to the **Container** field to add a new container.

5. Use the tables below to create or modify the pingable device.
6. Click **OK**.

Element tab settings

Field	Definition
Container	Container in the Topology View tree where this device is stored.
Name	Name of the device
IP address	IP address of the device
Physical Address	The MAC address of the device. Appears in the view only when the device is a pingable.
Device Type	Select the device type from the drop-down list.
Incoming Events • Not Applicable • Syslog • Security Events *Available when Automated Threat Response (ATR) is configured.*	When Syslog is selected, available syslog files appear that can be used by FortiNAC to parse information received from the external devices and generate an event. When Security Events is selected, available security event parsers appear that can be used by FortiNAC to parse information received from the external devices and generate a security event. See Security event parsers on page 198.
SSO Agent	• Not Applicable • Custom Script • Palo Alto • RADIUS • iboss
Custom Script	Displayed when Custom Script is selected in the SSO Agent field. Allows you to write and select a script that will integrate with a SSO Agent that is not currently supported.
Apply to Group	Select this check box to apply the Custom Script SSO options only to the selected Host group in the drop-down list. If you do not select the check box, the SSO options are applied to all Host groups.
RADIUS Accounting Port	Displayed when RADIUS is selected in the SSO Agent field. Port on the Fortinet Single Sign-On User Agent configured to receive RADIUS Accounting messages from external devices. This port must match the port configured in Fortinet.
RADIUS Secret	Displayed when RADIUS is selected in the SSO Agent field. Must match the RADIUS secret configured for FortiNAC in Fortinet.
Apply to Group	Select this check box to apply the RADIUS SSO options only to the selected Host group in the drop-down list. If you do not select the check box, the SSO options are applied to all Host groups.
XML API Port	Displayed when Palo Alto User Agent is selected in the SSO Agent field. Port on the Palo Alto User Agent configured to receive messages from external devices. This port must match the XML API port configured on the Palo Alto User Agent.

Field	Definition
	See Add or modify the Palo Alto User-ID agent as a pingable on page 728.
Domain Name	Displayed when Palo Alto User Agent is selected in the SSO Agent field. Fully Qualified Domain Name for your network users' domain. This is sent with the logged in User ID to Palo Alto.
Use Integrated Agent	When selected, FortiNAC will integrate with the firewall directly.
API Key	Displayed when the Use Integrated Agent check box is selected. Enter the API Key value. The key can be retrieved manually or via the Retrieve button.
Apply to Group	Select this check box to apply the Palo Alto SSO options only to the selected Host group in the drop-down list. If you do not select the check box, the SSO options are applied to all Host groups.
iboss Port	Displayed when iboss is selected in the SSO Agent field. The IBOSS port is the IBOSS HTTP port that is used to talk to the IBOSS SSO agent. The IBOSS port is defined in the IBOSS SSO GUI.
iboss Key	Displayed when iboss is selected in the SSO Agent field. The IBOSS key is a security key used to talk to the IBOSS SSO agent.The IBOSS key is defined in the IBOSS SSO GUI.
iboss Domain	Displayed when iboss is selected in the SSO Agent field. The iboss Domain is a required field that allows the user to enter their Active Directory Domain Name.
Apply to Group	Select this check box to apply the iboss SSO options only to the selected Host group in the drop-down list. If you do not select the check box, the SSO options are applied to all Host groups.
Role	The Role for this device. Available roles appear in the drop-down list.
Description	Description of the device entered by the Administrator.
Note	User specified notes about the device.
Contact Status Polling	Enable or disable contact status polling for the selected device.
Poll Interval	Determines how often the device should be polled for communication status. Time is stored in minutes.
Poll Now	Polls the device immediately for contact status.
Last Successful Poll	Date and time that the device was last polled successfully.
Last Attempted Poll	Date and time that the device was last polled.

Details tab settings

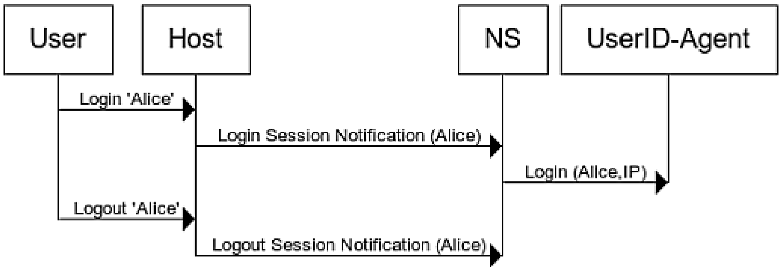
Field	Definition
Host Name	Name of the device.
Department	Name of the department.
Owner	Name of the owner of the device.

Field	Definition
Administrative Contact	Administrative contact person for the device.
Geographical Location	Geographical location of the device (for example, Res Hall A, Equipment Closet 1st Floor, Rack 2, Unit 3).
Business Purpose	Business purpose of the device.
BOOTP Address	IP address for the BOOTP Protocol.
Print Queue	Name of the print queue for the device.

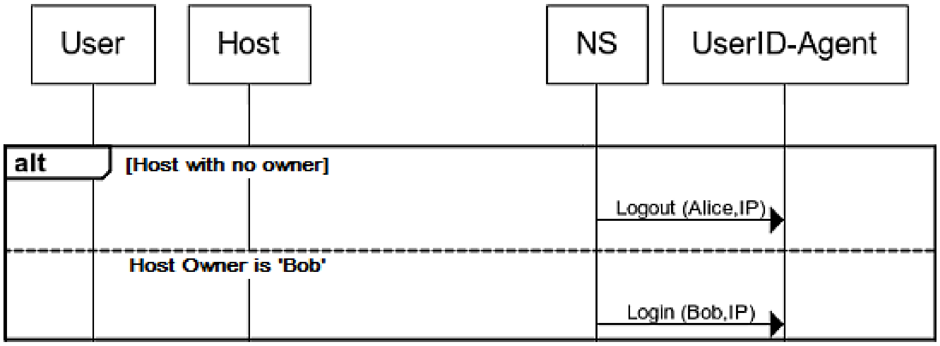
Add or modify the Palo Alto User-ID agent as a pingable

When the Palo Alto Networks User-ID agent is configured in FortiNAC as a pingable device, FortiNAC sends a message to Palo Alto Networks firewall each time a host connects to the network or the host IP address changes, such as when a host is moved from the Registration VLAN to a Production VLAN. A message is also sent when one user logs off a host and a new user logs on to that same host while the host is still on-line. All messages include User ID and IP address. This information identifies the user to Palo Alto Networks allowing it to apply user specific policies. There are several scenarios that generate messages to Palo Alto Networks, as described below and in the flow diagram:

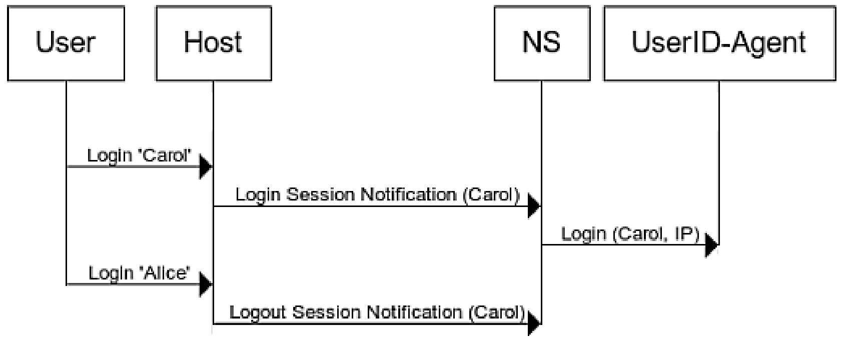
A host is registered to a specific user; the owner logs onto the network with the host. FortiNAC sends User ID and IP address.


User
Host
NS
UserID-Agent
Login 'Alice'
Login Session Notification (Alice)
Login (Alice,IP)
Logout 'Alice'
Logout Session Notification (Alice)

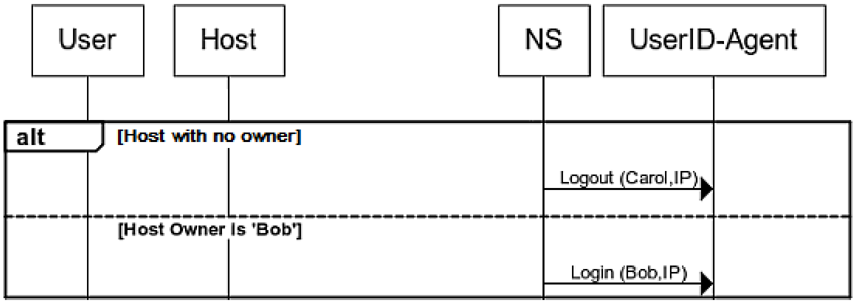
A host has no associated owner and is registered as a device; a user logs onto the network with this host. If this yields a logged on user, FortiNAC sends User ID and IP address.



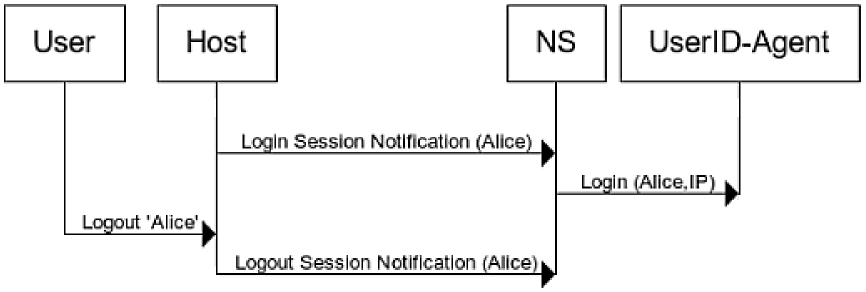
If a host is registered to a specific user, when a different user logs onto the host, that new user's user ID is sent to Palo Alto Networks with the host IP address.


User
Host
NS
UserID-Agent
Login 'Carol'
Login Session Notification (Carol)
Login (Carol, IP)
Login 'Alice'
Logout Session Notification (Carol)

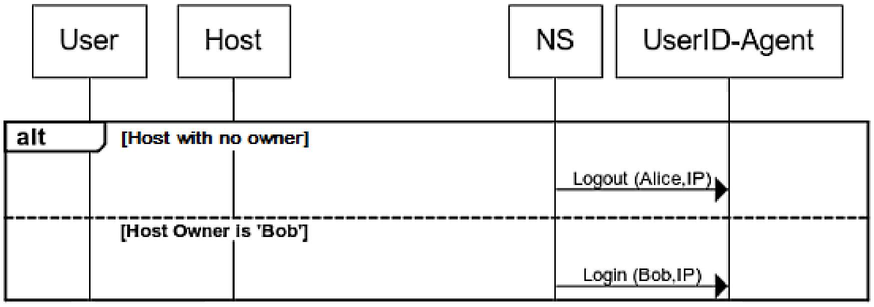
When a user who is not registered as the host's owner logs out of the host, the User ID of the host's owner is sent to Palo Alto Networks with the host IP address, even though the owner did not actually log onto the network.

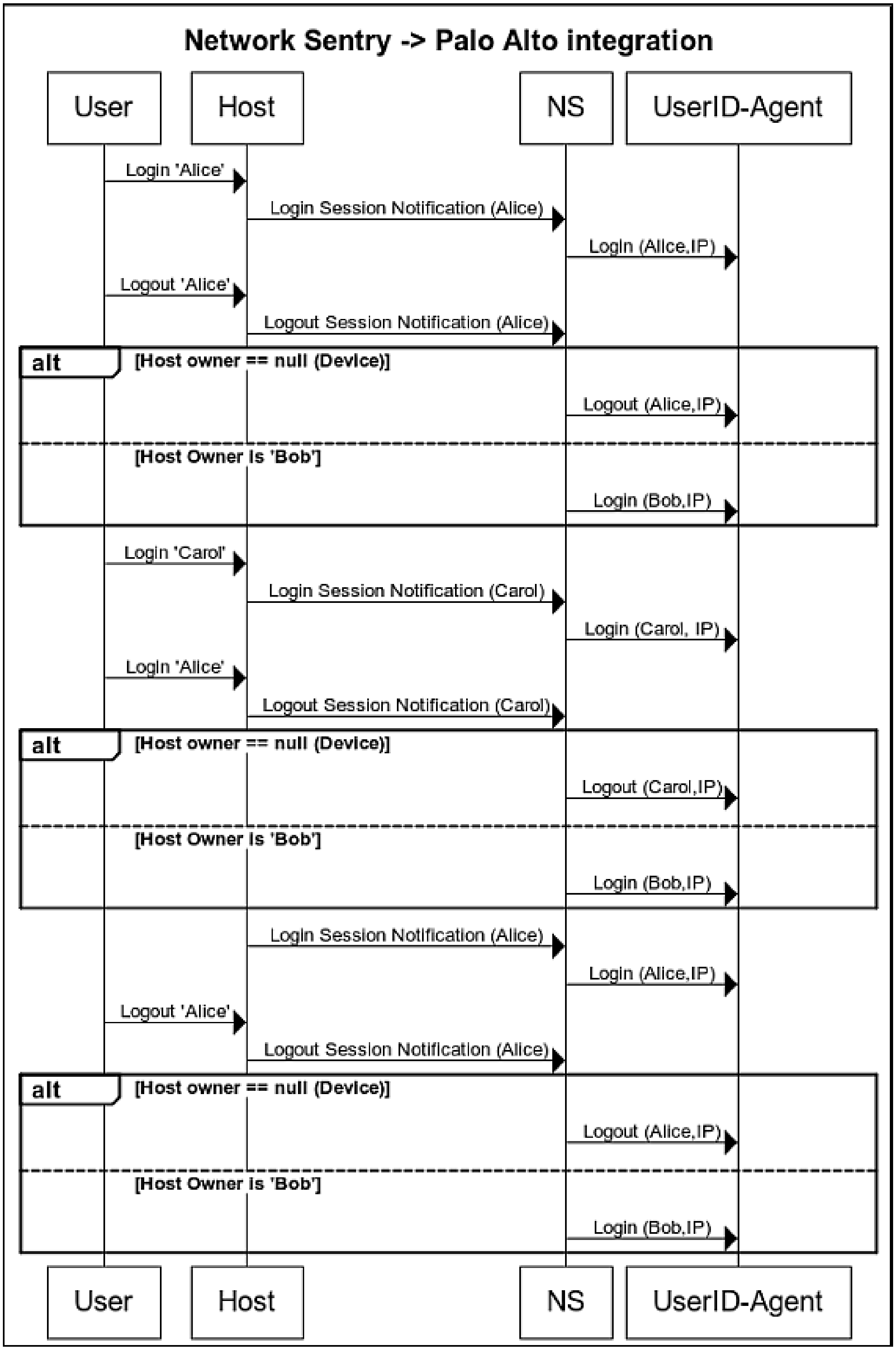


When a user logs out of a host that has no owner, FortiNAC notifies Palo Alto Networks that the user has logged out.


User
Host
NS
UserID-Agent
Login Session Notification (Alice)
Login (Alice,IP)
Logout 'Alice'
Logout Session Notification (Alice)

If a user is logged in remotely, such as through Remote Desktop, and there is no Persistent Agent installed on the host, login and logout information are not provided to Palo Alto Networks.




Network Sentry -> Palo Alto integration
User
Host
NS
UserID-Agent
Login 'Alice'
Login Session Notification (Alice)
Login (Alice,IP)
Logout 'Alice'
Logout Session Notification (Alice)
alt
[Host owner == null (Device)]
Logout (Alice,IP)
[Host Owner is 'Bob']
Login (Bob,IP)
Login 'Carol'
Login Session Notification (Carol)
Login (Carol, IP)
Login 'Alice'
Logout Session Notification (Carol)
alt
[Host owner == null (Device)]
Logout (Carol,IP)
[Host Owner is 'Bob']
Login (Bob,IP)
Login Session Notification (Alice)
Login (Alice,IP)
Logout 'Alice'
Logout Session Notification (Alice)
alt
[Host owner == null (Device)]
Logout (Alice,IP)
[Host Owner is 'Bob']
Login (Bob,IP)
User
Host
NS
UserID-Agent

Implementation

To integrate with the Palo Alto Networks User-ID agent you should be aware of and configure the following items:

Palo Alto Networks

- Palo Alto Networks firewall must be Version 4.0 or higher.
- Palo Alto Networks User-ID agent must be Version 4.0 or higher.
- For Palo Alto Windows User-ID agent versions prior to 7.0.4, the XML API must be enabled to allow communication with FortiNAC. In the Windows User-ID agent under **User Identification > Setup** make sure **Enable User-ID XML API** is set to **Yes**. This option is configured on the **Agent Setup** dialog under the **Agent Service** tab.

FortiNAC cannot integrate with Windows User-ID Agent versions 7.0.4 and higher because the Enable User-ID XML API option is not available.

FortiNAC

- To configure the integration of FortiNAC with the Windows User-ID Agent for Agent Versions prior to 7.0.4, do not select the **Use Integrated Agent** check box. Specify the **XML API Port** value to match the port you have configured the Windows User-ID agent to use. The agent uses port 5007 by default.
- FortiNAC cannot integrate with the Windows User-ID Agent Version 7.0.4 or later. If you cannot use an earlier version of the agent, you can instead configure FortiNAC to integrate with the firewall directly.
- If you are not using the Windows User-ID Agent and your firewall is version 6.0 or later, you must configure FortiNAC to integrate directly with the firewall. Select the **Use Integrated Agent** check box and enter port 443 in the **XML API Port** field. Enter the **API Key** value. The key can be retrieved manually or via the **Retrieve** button.

  Direct integration of FortiNAC with versions of the firewall prior to 6.0 is not supported.

- Hosts that will be affected by or managed by the Palo Alto Networks User-ID agent must have a logged-on User. If no user is associated with the host, only the IP address is sent to the Palo Alto Networks User Agent. The User Agent cannot apply a policy without a User ID. Registration methods such as the Persistent Agent, Device Profiler, or login scripts can be set to register hosts as devices, but then it is the user's login/logout that triggers that messages be sent from FortiNAC to Palo Alto.
- Add the Palo Alto Networks User Agent as a pingable device in FortiNAC. See the instructions below for the steps.
- FortiNAC and the Palo Alto Networks User Agent communicate via SSL. SSL certificates on the Palo Alto Networks User Agent Server are automatically imported into the .keystore file on your FortiNAC Control Server or Server.
- In Event Management, the event Communication Lost With Palo Alto User Agent is automatically enabled. This event is generated when the Palo Alto Networks User Agent cannot be reached. The Palo Alto Networks User Agent is not being notified when hosts connect to the network, therefore, policies may not be applied. See Enable and disable events on page 857 to disable the event if necessary.
- In Event to Alarm Mappings, you can map the Communication Lost With Palo Alto User Agent event to an alarm if you wish to be notified when FortiNAC and the Palo Alto Networks User Agent are no longer communicating. See Add or modify alarm mapping on page 892.

Add pingable

1. Click **Network Devices > Topology**.
2. Select the **Container** icon.
3. Right-click the container and select **Add Pingable Device**.
4. Use the table below to enter the data for the Palo Alto Networks User-ID agent.
5. Click **OK** to save.

Settings

Field	Definition
Element tab	
Container	Container in the Topology View tree where this device is stored.
Name	Name of the device
IP address	IP address of the device
Physical Address	The MAC address of the device. Appears in the view only when the device is a pingable.
Device Type	Lists all available device types. Select Firewall or Server.
Incoming Events	Lists the security appliances available when either Syslog or Security Events is selected. Select Not Applicable.
SSO Agent	The third party agent communicating with the same authenication credentials as FortiNAC, utilizing the ability to unify credentials across multiple products (e.g., Single Sign-On).
XML API Port	Displayed when Palo Alto User Agent is selected in the SSO Agent field. Port on the Palo Alto User Agent configured to receive messages from external devices. This port must match the XML API port configured on the Palo Alto User Agent. See Add or modify the Palo Alto User-ID agent as a pingable on page 728.
Domain Name	Displayed when Palo Alto User Agent is selected in the SSO Agent field. Fully Qualified Domain Name for your network users' domain. This is sent with the logged in User ID to Palo Alto.
Use Integrated Agent	Allows you to integrate directly with the firewall when FortiNACdoes not integrate with the Windows User-ID Agent.
API Key	The authorization key that allows a user to send user mapping data to the firewall. Can be retrieved from the firewall manually, or by providing the credentials for an administrator account on the firewall when prompted via the Retrieve button.
Apply to Group	Select this check box to apply the Palo Alto SSO options only to the selected Host group in the drop-down list. If you do not select the check box, the SSO options are applied to all Host groups.
Role	The Role for this device. Available roles appear in the drop-down list.
Description	Description of the device entered by the Administrator.

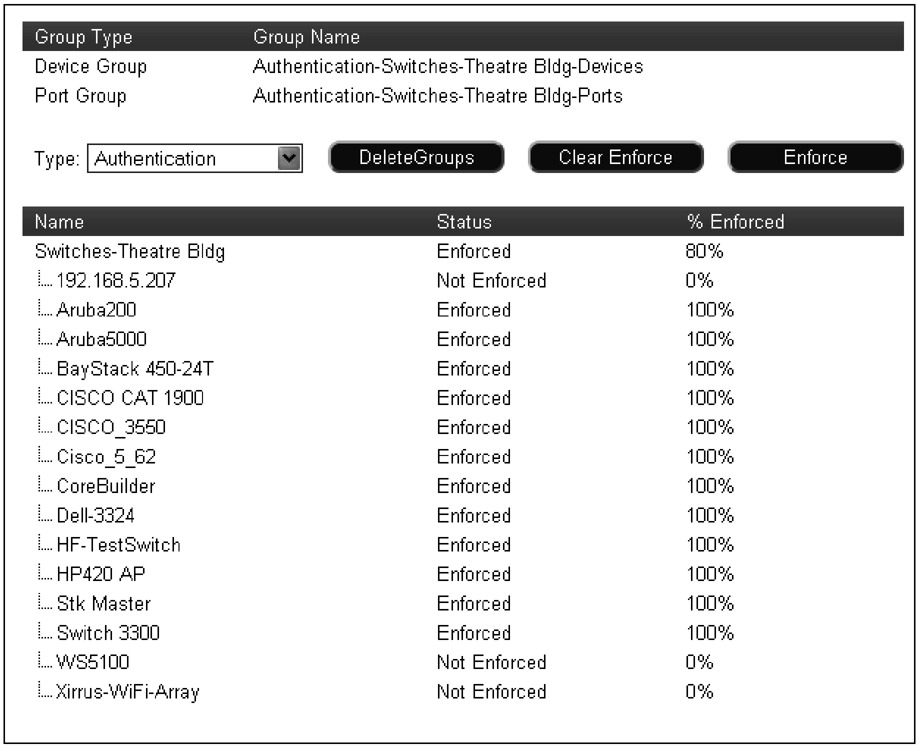
Field	Definition
Note	User specified notes about the device.
Contact Status Polling	Enable or disable contact status polling for the selected device.
Poll Interval	Determines how often the device should be polled for communication status. Time is stored in minutes.
Poll Now	Polls the device immediately for contact status.
Last Successful Poll	Date and time that the device was last polled successfully.
Last Attempted Poll	Date and time that the device was last polled.

Control access on devices in a container

This option is used to modify membership of devices and ports in the selected container in system access control groups. This information can also be modified in the Groups View.

Percentage Enforced indicates the percentage of ports that are in the selected access control group. For example, if a switch has 10 ports, and % Enforced displays 80%, then 8 of the 10 ports for that switch are an access control group, such as Registration. Unregistered hosts connecting to one of the 8 ports would be forced to register.

If a device group has 5 switches, and % Enforced for the group displays 20%, then one of the 5 switches in the device group has some ports in the access control group selected.



Group Type	Group Name
Device Group	Authentication-Switches-Theatre Bldg-Devices
Port Group	Authentication-Switches-Theatre Bldg-Ports

Type: Authentication

Name	Status	% Enforced
Switches-Theatre Bldg	Enforced	80%
192.168.5.207	Not Enforced	0%
Aruba200	Enforced	100%
Aruba5000	Enforced	100%
BayStack 450-24T	Enforced	100%
CISCO CAT 1900	Enforced	100%
CISCO_3550	Enforced	100%
Cisco_5_62	Enforced	100%
CoreBuilder	Enforced	100%
Dell-3324	Enforced	100%
HF-TestSwitch	Enforced	100%
HP420 AP	Enforced	100%
Stk Master	Enforced	100%
Switch 3300	Enforced	100%
WS5100	Not Enforced	0%
Xirrus-WiFi-Array	Not Enforced	0%

1. Log into your administrator account.
2. Click **Network Devices > Topology**.
3. In the navigation pane, right-click on the container and select **Control Access**.

4. This view shows the device and port groups that have been created and their names. If no device or port groups have been created, NONE is displayed.
5. In the Type field select the system access group to be modified. Options include: Authentication, Registration, Remediation, Dead End and Role-Based access. When a Remediation group is created it enables the Quarantine VLAN switching option under **System > Settings > Control > Quarantine**.
6. The bottom half of the screen allows you to check the status of the container.
7. To create device and port groups for all devices in the container, click **Create Groups**.
8. To add all switches in the container to the system access control group selected in the **Type** field click **Enforce**. This also creates the necessary device and port groups if they do not exist.
9. To remove all switches in the container from the selected system access group click **Clear Enforce**.
10. To delete the device and port groups, click **Delete Groups**. This also removes all of the devices and ports from the selected system access group.
11. A confirmation screen appears. Click **OK**. The screen refreshes and displays the new settings.

See Control access on page 715 and Network summary on page 717 for additional information.

Convert all pingables to hosts

Non-SNMP devices displayed in the Topology View can be converted to Hosts. These hosts display both in the Host View and the Topology View. Rogues that display in the Host View can be registered as devices in both Host View and Topology View. See Register a host as a device on page 812.

Devices that are kept in the Host View have a connection history and can be associated with a user. Devices that are placed in the Topology View can be polled for their connection status. Devices that are not connected display in red on the Topology View. If the connection to the device fails, events and alarms can be configured to notify you that the device is no longer communicating.

There are certain repercussions when pingables are converted to hosts that should be taken into consideration:

- Converting a pingable device to a host causes that device to be subject to aging rules configured for hosts. Aging rules control the expiration and inactivity dates used to automatically remove hosts from the database. See Aging out host or user records on page 823.
- When a device is converted to a host the IP address of that device is not propagated to the host record. The next L3 poll will add the IP address to the host record.

Wireless Access Points added as pingable devices cannot be converted to hosts.

Convert all pingables

1. Click **Network Devices > Topology**.
2. Select the **Container** icon.
3. Right-click a container and select **Convert Pingables To Hosts**. This option converts all non-SNMP devices to hosts and displays them both in Host View and Topology View.
4. Click **Yes** on the confirmation window.
5. Select **Hosts > Host View** and verify that the Pingable devices now display in Host View.

Convert one or more pingables from topology view

1. Click **Network Devices > Topology**.
2. Expand the **Container** where the device is located.
3. Select the device to be converted. Hold down the **Ctrl** key to select multiple devices.
4. Right-click a device and select **Convert To Host**. This option converts the non-SNMP devices selected to hosts.
5. Click **Yes** on the confirmation window.
6. Select **Hosts > Host View** and verify that the pingable devices now display.

Convert one or more pingables from network devices view

1. Click **Network Devices > Topology**.
2. Make sure the filter is set to display the devices to be converted.
3. Select the device to be converted. Hold down the **Ctrl** key to select multiple devices.
4. Click the **Convert To Host** button. This option converts the non-SNMP devices selected to hosts.

The conversion skips any selected SNMP devices and warns you of the number of devices that were not converted.

5. Click **Yes** on the confirmation window.
6. The device is removed from the Network Devices window, but will display in Topology View and Host View.
7. Select **Hosts > Host View** and verify that the Pingable devices now display.

Discover devices

FortiNAC can search the network based on IP ranges and determine what SNMP enabled devices exist on the network. Once a device is discovered, FortiNAC creates a model for the device in the database and places the device in the Network Devices list.

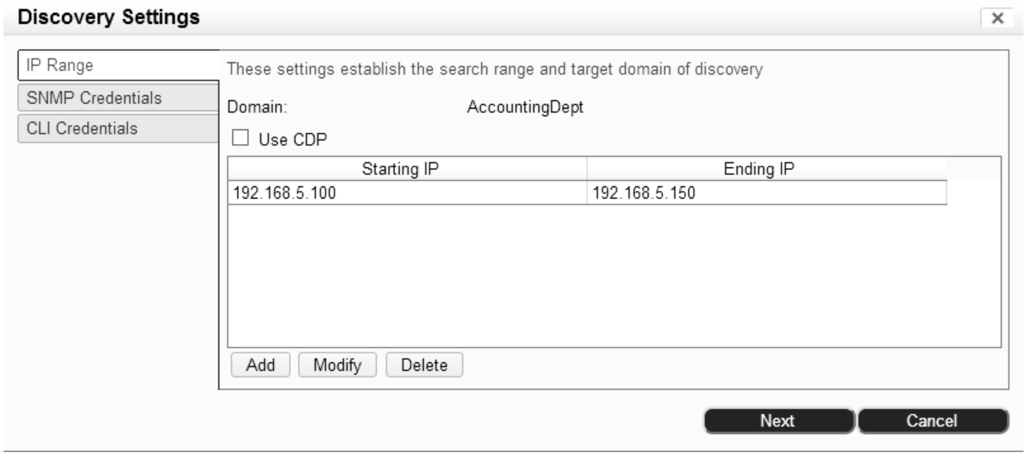
FortiNAC receives traps through SNMPv1 and SNMPv2 communications, but communicates with devices through SNMPv3.

When the **Use CDP** option on the Discovery window is enabled, FortiNAC queries devices about other connected devices on the network. If a device has this discovery protocol enabled it gathers and stores information about devices it manages and devices it can contact on the network. Enabling the Cisco Discovery Protocol (CDP) when adding search criteria for Discovery allows FortiNAC to query devices for information about those secondary devices. For example, FortiNAC can query a device and discover routers and switches connected to the original device. FortiNAC can then query those secondary devices and so on, until the edge of the network is reached. Only devices with CDP enabled will respond to a CDP query.

When a discovery process is started for a particular container, the status of that process is displayed in the Containers view. Click the **Refresh** button on the Containers view to update the status periodically.

If your device has multiple interfaces, each with a different IP address that is configured with its own SNMP settings, multiple representations of the same device will be added to FortiNAC. FortiNAC does not consolidate the duplicates in this case.

When configuring the device itself, use only letters, numbers and hyphens (-) in names for items within the device configuration, in security strings and in SNMP credentials. Other characters may prevent FortiNAC from reading the device configuration. For example, in many cases the # sign is interpreted by FortiNAC as a prompt. Cisco restricts the use of @ and #.


Discovery Settings

These settings establish the search range and target domain of discovery

Domain: AccountingDept

☐ Use CDP

Starting IP	Ending IP
192.168.5.100	192.168.5.150

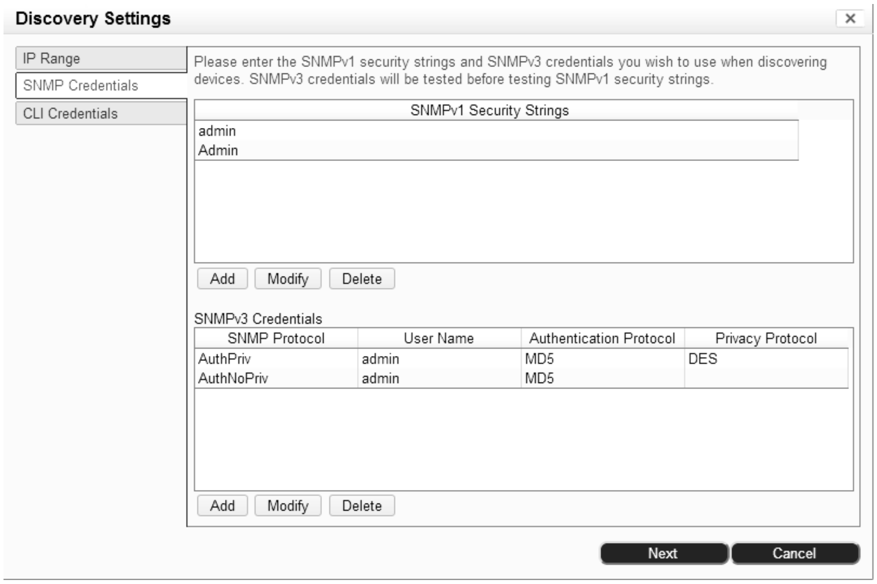
Discovery can be started from either of the following locations:

- **System > Quick Start > Network Device Settings > Containers**
- **Network Devices > Topology > Customer Icon > Containers**

1. Select a Container that will be populated by the discovery process.
2. Click **Start Discovery** in the Containers panel.
3. The Discovery Settings window displays.
4. If you would like to search for devices using the Cisco Discovery Protocol, click the **Use CDP** check box to enable it.
5. On the IP Range tab, click **Add**.
6. Enter the **Starting** and **Ending IP addresses** of the range to be queried for new devices. If you selected **Use CDP**, only the starting IP address is required.

   If you have an extensive network and you plan to enable Use CDP, it is recommended that you limit the number of levels queried beyond the initial device. In large networks, discovery can take an extended amount of time and may cause delays. For information on limiting the depth of the CDP discovery see Network device on page 130.

7. Add all of the IP Ranges required.
8. Click **Next** or click the **SNMP Credentials** tab.



Discovery Settings

Please enter the SNMPv1 security strings and SNMPv3 credentials you wish to use when discovering devices. SNMPv3 credentials will be tested before testing SNMPv1 security strings.

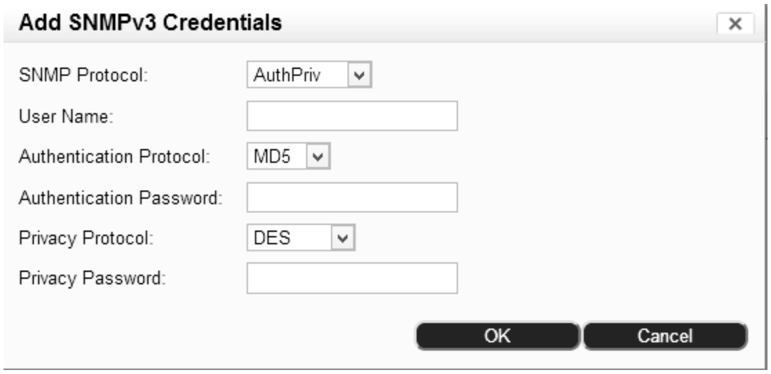
SNMPv1 Security Strings
admin
Admin

SNMPv3 Credentials

SNMP Protocol	User Name	Authentication Protocol	Privacy Protocol
AuthPriv	admin	MD5	DES
AuthNoPriv	admin	MD5	

9. Under **SNMPv1 Security Strings**, enter the read/write security strings to use when communicating with the discovered devices. Click **Add** to add a security string. Select a security string and click **Delete** to remove it from the list.

10. Under SNMPv3 Credentials, click Add to enter the settings to use when communicating with the discovered devices.



Add SNMPv3 Credentials

SNMP Protocol:	AuthPriv
User Name:	
Authentication Protocol:	MD5
Authentication Password:	
Privacy Protocol:	DES
Privacy Password:	

Settings

Field	Definition
SNMP Protocol	Available options are AuthPriv or AuthNo Priv.
User Name	User Name for access to the device. Recommended but not required.
Authentication Protocol	Available options are: MD5 SHA1 (Recommended)
Authentication Password	Specify password to match what the device is using.
Privacy Protocol	Available options are:

Field	Definition
	DES AES-128 (Recommended)
Privacy Password	Specify password to match what the device is using.

If the device is configured for AuthPriv, the Authentication password, Privacy Protocol and Privacy password are required. If the device is configured for AuthNoPriv, only the Authentication password is required.

11. Click **Next** or click the **CLI Credentials** tab.
12. Click **Add** to enter CLI Credentials for managing discovered devices.

The user account must have the appropriate permissions configured on the device.

CLI Settings

Field	Definition
User Name	The user name used to log on to the device for configuration. This is for CLI access. For devices using API credentials, enter the serial number for the appliance.
Password	The password required to configure the device. This is for CLI access. For devices using API credentials, enter the REST API Key.
Protocol Type	Use Telnet, SSH1 or SSH2 to logon to the device for configuration.

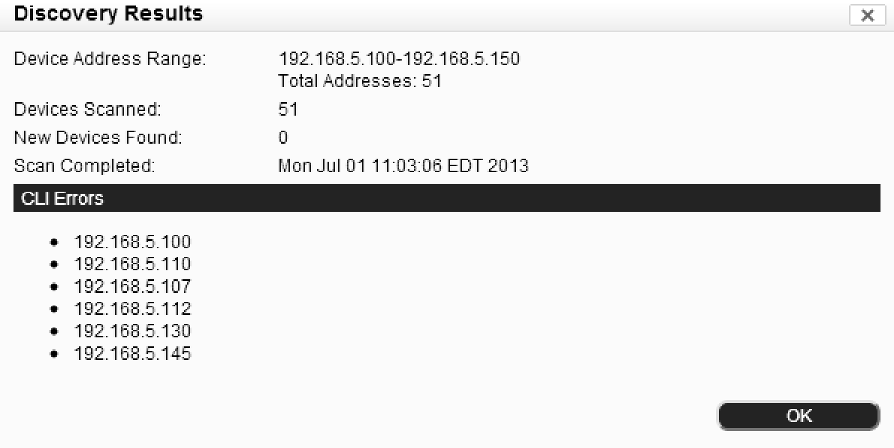
13. Click **OK** to start the discovery process. The process runs in the background.

    The status of a discovery task is displayed in the **Devices** header.
14. Click **Cancel Discovery** to cancel the discovery process.

Discovery results

Discovery Results displays a dialog with detailed information about the discovery process. Access Discovery Results from one of the following locations:

- **System > Quick Start > Network Device Settings > Containers**
- **Network Devices > Topology > Customer Icon > Containers**



Discovery Results

Device Address Range: 192.168.5.100-192.168.5.150
Total Addresses: 51

Devices Scanned: 51

New Devices Found: 0

Scan Completed: Mon Jul 01 11:03:06 EDT 2013

CLI Errors

- 192.168.5.100
- 192.168.5.110
- 192.168.5.107
- 192.168.5.112
- 192.168.5.130
- 192.168.5.145

Settings

Field	Definition
Device Address Range	Range of IP addresses selected and the total number of addresses within the range.
Devices Scanned	Number of devices within the IP address range that were scanned.
New Devices Found	Number of devices in the IP address range that were added to the database.
Scan Completed	Date and time that the discovery process finished scanning the network for devices.
SNMP Errors	List of IP addresses that were scanned but with which FortiNAC could not communicate via SNMP.
CLI Errors	List of IP addresses that were scanned and with which FortiNAC was able to communicate via SNMP, but the CLI Credentials were incorrect.

Device view

When a Container is selected in the tree on the Topology View, the Devices tab is displayed in the panel on the right. Devices can be hubs, pingables, printers, servers, or switches and have various management options, depending on the device type. To view these management options, select a device from the tree or the table and then right-click to view the drop-down menu.

Settings

Field	Definition
Status	Indicates whether or not communication has been established with the device. Displays either Established or Lost.

Field	Definition
Name	Name of the selected device.
IP address	IP address of the selected device. IP addresses or Address Ranges are used to add or discover devices.
Physical Address	MAC Address of the selected device.
Container	Container where the device resides. Containers are used to group devices.
Role	Displays the role assigned to this device. To modify the role go to Device Properties for this device. This field does not list the roles associated with this device through Network Device Roles. To view Role Membership right-click on the device in the Topology View.
Notes	User specified notes about the device that are entered on the Device Properties view.
Raw Type	The OID of the device.
Device Type	Indicates the type of devices, such as switch, printer, router, etc.
Protocol	SNMP version used for the device, options include: SNMPv1, SNMPv3 and Pingable.
CLI Protocol	Communication method used to connect to the CLI of the device, options include: Telnet, SSH1 and SSH2.
Polling	Indicates whether polling is enabled or disabled and displays the polling interval.
Last Polled	Date and time the server last attempted to poll the device.
Last Polled Success	Date and time that the device was last polled successfully.
L2 Polling	Indicates whether L2 polling is enabled or disabled and displays the polling interval.
L2 Last Polled	Date and time the server last attempted a L2 poll of the device.
L2 Last Polled Success	Date and time of the last successful L2 poll.
L3 Polling	Indicates whether L3 polling is enabled or disabled and displays the polling interval.
L3 Last Polled	Date and time the server last attempted a L3 poll of the device.
L3 Last Polled Success	Date and time of the last successful L3 poll.
CDP Polling	Indicates whether CDP polling is enabled or disabled for the device and displays the polling interval. Disabled (unsupported) displayed in this column, indicates that the first CDP poll was unsuccessful because CDP queries are not supported by the device or may not be configured on the device. If the device has ever been successfully polled for CDP, later unsuccessful polls are not interpreted as a problem with CDP on the device.
CDP Last Polled	Date and time the server last attempted a CDP poll of the device.
CDP Last Poll Success	Date and time of the last successful CDP poll.
Group	Filters the list of devices based on the group selected. Only devices that are members of the selected group display in the list.
Last Modified By	User name of the last user to modify the device.

Field	Definition
Last Modified Date	Date and time of the last modification to this device.
Right click options	
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.
Add	Add a SNMP device to the Topology View, such as a switch. See Add or modify a device on page 723.
Add Pingable	Add a pingable device to the Topology View, such as an alarm system. See Add or modify a pingable device on page 725.
Delete	Deletes the selected devices.
Modify Properties	Appears when multiple devices are selected. Allows you to modify device properties for multiple devices simultaneously. See Modify multiple device properties on page 758.
Convert To Host	Converts one or more selected non-SNMP or pingable devices to hosts. After conversion these devices are removed from Network Devices but do display both in the Topology View and the Host View. See Convert all pingables to hosts on page 734. Wireless Access Points added as pingables cannot be converted to hosts.
Group Membership	Displays the Device Group Membership dialog which allows you to view and modify the groups in which this device is a member. See Device group membership on page 744. There is now a search bar and a collapse all tab for Port Groups.
Local Management (HTTP)	Opens a browser to manage the device through the web interface. This option may not be available for all devices.
Move To Container	Moves the selected devices to a different Container. See Move a device to a different container on page 745
Network Access/VLANS	Modify device and model values and display the current and default network access assignments stored in the FortiNAC model of that device. See Network access/VLANs on page 745.
Poll For Contact Status	Polls the selected devices immediately instead of waiting for the next scheduled poll. See Poll for contact status on page 748.
Poll For L2 Hosts Info	Reads the host information on the selected device and updates the Ports tab in Topology View. See Poll for L2 (hosts) information on page 748.

Field	Definition
Ports And Hosts	Displays VLAN (Current and Default) and Host (Name and IP) information for each port on the device. If the Host Name is unknown, the MAC Address is displayed. See Ports and hosts on page 752.
Properties	Displays the Properties View for the selected device. See Device properties on page 753 and Pingable device properties on page 759.
Modify	Modify the selected device. See Add or modify a device on page 723 or Add or modify a pingable device on page 725.
Resync Interfaces	Reads the interface information from a modeled device and updates FortiNAC's representation of that device. This information includes the interface's index, description, name, and status. See Resync interfaces on page 767.
Role Membership	Displays the list of roles in which the device is a member. See View role membership on page 761.
Select Device In Tree	Locates the selected device in the tree on the right and highlights it.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.
Show Events	If the Devices tab is selected, displays events for the selected device. If the Ports tab is selected, displays events for the selected port.
Update Device Mappings	Update device icon for the selected device when the device type is unknown and the icon is a question mark. See Update device mapping on page 763.
Global Model Config	Opens the Global Model Configuration window to configure data for multiple devices of the same brand, such as passwords for communication with the device, VLANs, and RADIUS server information. See Global model configuration on page 772.
Model Config	Opens the Model Configuration window for the selected device to configure data such as passwords for communication with the device, VLANs, and RADIUS server information. See Model configuration on page 767.
Running Configuration	View the configuration running on the selected device (device dependent). This option is only available for some devices.
Static Port Configuration	Allows you to designate a specific port as a Dead-End VLAN and use that port to disable hosts. The MAC address of the disabled host is placed in a list on the device which indicates it only has permission to use the port designated as secure or static. See Secure port/static port overview on page 776.

Control access on a device

1. Log into your administrator account.
2. Click **Network Devices > Topology**.
3. In the navigation pane, Expand the container where the device is located.
4. Right-click on the device for which you want to enforce isolation and select **Control Access**.
5. In the **Control Access** screen check the status of the device.
6. In the **Type** field, select the system access group to be modified. Options include: Authentication, Registration, Remediation, Dead End and Role-Based access. When a Remediation group is created it enables the Quarantine VLAN switching option under **System > Settings > Control > Quarantine**.
7. To add all ports on the device to the system access control group selected in the **Type** field, click **Enforce**. This also creates the necessary device and port groups if they do not exist.
8. To remove all ports on the device from the system access control group selected in the Type field click **Clear Enforce**. Device and port groups are not removed.
9. A confirmation screen appears. Click **OK**.
10. The screen refreshes and displays the new settings.

Percentage Enforced indicates the percentage of ports that are in the selected access control group. For example, if a switch has 10 ports, and % Enforced displays 80%, then 8 of the 10 ports for that switch are an access control group, such as Registration. Unregistered hosts connecting to one of the 8 ports would be forced to register.

See Control access on page 715 and Network summary on page 717 for additional information.

Delete a device

When a device is deleted the associated configuration is also removed.

1. Click **Network Devices > Topology**.
2. Expand the container where the device is located.
3. Select the device to be deleted.
4. Click **Edit > Delete** to remove the device from the container.

Convert devices to hosts

Non-SNMP devices displayed in the Topology View can be converted to Hosts. These hosts display both in the Host View and the Topology View. Rogues that display in the Host View can be registered as devices in both Host View and Topology View. See Register a host as a device on page 812.

Devices that are kept in the Host View have a connection history and can be associated with a user. Devices that are placed in the Topology View can be polled for their connection status. Devices that are not connected display in red on the Topology View. If the connection to the device fails, events and alarms can be configured to notify you that the device is no longer communicating.

There are certain repercussions when pingables are converted to hosts that should be taken into consideration.

- Converting a pingable device to a host causes that device to be subject to aging rules configured for hosts. Aging rules control the expiration and inactivity dates used to automatically remove hosts from the database. See Aging out host or user records on page 823.

- When a device is converted to a host the IP address of that device is not propagated to the host record. The next L3 poll will add the IP address to the host record.

Wireless Access Points added as pingable devices cannot be converted to hosts.

Convert all pingables in a container

1. Click **Network Devices > Topology**.
2. Select the **Container** icon.
3. Right-click a container and select **Convert Pingables To Hosts**. This option converts all non-SNMP devices to hosts and displays them both in **Host** view and **Topology** view.
4. Click **Yes** on the confirmation window.
5. Select **Hosts > Host View** and verify that the pingable devices now display in **Host View**.

Convert from Topology view

1. Click **Network Devices > Topology**.
2. Expand the container where the device is located.
3. Select the device to be converted. Hold down the Ctrl key to select multiple devices.
4. Right-click a device and select **Convert To Host**. This option converts the non-SNMP devices selected to hosts.
5. Click **Yes** on the confirmation window.
6. Select **Hosts > Host View** and verify that the pingable devices now display in **Host View**.

Convert from Network Devices view

1. Click **Network Devices > Topology**.
2. Make sure the filter is set to display the devices to be converted.
3. Select the device to be converted. Hold down the Ctrl key to select multiple devices.
4. Click the **Convert To Host** button. This option converts the non-SNMP devices selected to hosts.
5. Click **Yes** on the confirmation window.
6. The device is removed from the **Network Devices** window, but will display in **Topology View** and **Host View**.
7. Select **Hosts > Host View** and verify that the pingable devices now display in **Host View**.

Device group membership

Devices on your network can belong to groups. Group membership can be viewed from the Groups View window or by selecting the device in the Topology View.

1. Click **Network Devices > Topology**.
2. Expand the **Container** where the device is located.
3. On the Devices panel on the right, right-click on a device and select **Group Membership**.

4. Check marks indicate that the device is a member of the group.
5. To add the device to a group, click the box next to the group name and then click **OK**.
6. To remove the device from a group, click to uncheck the box next to the group name and then click **OK**.
7. Click **OK** to save your group selections.

> If an item is placed in a subgroup, it can only be removed when viewing the membership of that subgroup. It cannot be removed from the parent group containing the subgroup.
>
> For example, the L2 Network Devices Group contains the Wired Devices and Wireless Devices subgroups. The Wired Devices subgroup contains four 3COM switches. The Wireless Devices subgroup contains two Cisco switches. The L2 Network Devices Group membership list shows all six switches, but to remove one of the 3COM switches you must go to the Wired Devices membership list.

Local management (HTTP)

Use the Local Management option to open a browser and manage the device through the web interface. This option may not be available, depending on the device.

1. Click **Network Devices > Topology**.
2. Expand the **Container** where the device is located.
3. Right-click the device and select **Local Management (HTTP)**.
4. A browser window opens and displays the login window for this device.

Move a device to a different container

1. Click **Network Devices > Topology**.
2. Expand the **Container** where the device is located.
3. Right-click on the device to be moved.
4. Select **Move To Container**.
5. Select the container where the device will be located.
6. Click **OK**. The device is now listed in the **Topology View** under container.

Network access/VLANs

Use this option to modify device and model values and to display the current and default network access assignments stored in the FortiNAC model of that device. Network access could be through VLANs/Roles, CLI Configurations, or VPN groups, depending on the device type. In the following discussion, the term *VLANs* refers to any of the Network Access types.

- The current VLANs are read from the device in the following situations:
- When you click Read VLANs in VLAN Summary view of the device.
- When the first trap (link up, link down, or cold start) is received after the device is added to the topology.
- When the first trap (link up, link down or cold start) is received after regaining contact with the device.
- When the first trap (link up, link down, or cold start) is received after starting up FortiNAC.

If you have not yet supplied the telnet or SSH parameters, FortiNAC can not retrieve the VLANs.

The VLANs option allows you to force a read of the current values from the device, edit the model's current values, and modify the default VLAN values.

The modified default values are stored in the FortiNAC database but do not perform a write memory to the boot configuration for switch vendors whose switches support running and boot configurations.

The FortiNAC default VLAN is the VLAN that the port is switched to for normal network access. To set the default VLAN globally for all ports on this device, go to the Model Configuration window. See Model configuration on page 767 for more information. To set different default VLANS for individual ports, use the Edit Default button on this window.

The Network Access Summary window displays the VLAN information for the device. Each port on the device is listed with its current and default VLAN value.

1. Click **Network Devices > Topology**.
2. Expand the **Container** where the device is located.
3. Right-click the device and select **Network Access/VLANs**.
4. Click **Read VLANs** to get the current and default VLAN values on the device.

Modify current device VLANs

Use this feature to set the VLANs for the device through the FortiNAC UI instead of the command line interface.

1. Click **Network Devices > Topology**.
2. Expand the **Container** where the device is located.
3. Right-click on the device and select **Network Access/VLANs**.
4. Click **Edit Current** to modify the values on the device.
5. Enter the **VLAN value** for one or more ports.
6. Click **Apply**.

The values are written to the device as the current value.

Modify default device VLANs

Use this feature to modify the default VLANs for the device model in the FortiNAC database.

1. Click **Network Devices > Topology**.
2. Expand the **Container** where the device is located.
3. Right-click on the device and select **Network Access/VLANs**.
4. Click **Edit Default** to modify the default VLAN values on the device.
5. Enter the **VLAN value** for one or more ports.
6. Click **Apply**.

The values are written to the database model as the default values.

VLAN switching

At times it may be necessary to disable VLAN switching for a specific device until the updated device information is entered/changed in FortiNAC. VLAN usage by the FortiNAC appliance and the device will be out of sync when:

- An administrator discovers/adds a device to the Topology view in the Admin UI but does not perform a model configuration to specify the VLANs to be used.
- After the device has already been added to Topology view and configured with specific VLANs, an administrator changes the VLANs on the device itself and does not change the configuration on the FortiNAC appliance to reflect those changes

Disable VLAN switching

VLAN switching is set to enabled by default. FortiNAC uses the default VLAN information for the device when a host connects. To prevent a host from being automatically switched from the new VLAN to the old VLAN during network upgrades, VLAN switching may be disabled. Once the updated information is entered or changed in FortiNAC and the VLAN information has been verified for the device, enable VLAN switching again.

1. Login as an administrator.
2. Click **Network Devices > Topology**.
3. Expand the container where the device is located.
4. Click on the device to select it.
5. Right-click on the device and select **Properties**.
6. In the **VLAN Switching** field, select the **Disable** radio button.
7. Click **Apply**, then close the **Properties** window.

Verify the default VLAN

1. Click **Network Devices > Topology**.
2. Expand the container where the device is located.
3. Click on the device to select it
4. Right-click on the device and select **Network Access/VLANs**.
5. The **Network Access Summary** window is displayed.
6. Verify that the switch/port has the correct default VLAN information.

> If the default VLAN has been changed on the switch/ports, the VLAN default settings on the Summary window must be changed as well.

7. Make any changes as needed to the default VLAN settings for each port and click **Apply**.
8. Click the **Refresh** button on the browser to refresh the view.
9. Verify that the switch/port has the correct default VLAN information.
10. Close the **Summary** window.

Enable VLAN switching

When all the changes to the device have been completed, enable the VLAN switching on the device.

1. Click **Network Devices > Topology**.
2. Expand the container where the device is located.
3. Click on the device to select it.
4. Right-click on the device and select **Properties**.
5. In the **VLAN Switching** field, select the **Enable** radio button.
6. Click **Apply**, then close the **Properties** window.

Review the model configuration

1. Click **Network Devices > Topology** view.
2. Expand the container where the device is located.
3. Click on the device to select it.
4. Right-click on the device and select the **Device Name > Model Configuration**. This shows the current configuration from within FortiNAC.
5. Compare the VLAN settings to those read from the device. If there is no value for **Default**, hosts get the default specified by the device. In some instances, there may be more than one production default. Also compare the other VLAN settings to the current VLANs read off of the device.
6. Modify the model configuration, as necessary. Set a value for each of the VLANs you want to use. If hosts who are not at risk should get a specific default VLAN, set that value here.
7. Apply your edits and exit the **Model Configuration** window.
8. Select the device, and right-click. Select **Resync Interfaces** to apply the model configuration to the ports on the device.

Poll for contact status

Use the feature to Poll a device immediately rather than waiting for the next scheduled poll.

1. Click **Network Devices > Topology**.
2. Expand the container where the device is located.
3. Right-click on the device and select **Polling > Contact Status**.

Poll for L2 (hosts) information

This option reads the host information on the selected device and updates the Ports tab in Topology View. See Ports view on page 778 for more information. To access this option:

1. Click **Network Devices > Topology**.
2. Expand the container where the device is located.
3. Right-click on the device and select **Polling > L2 (Hosts) Information**.

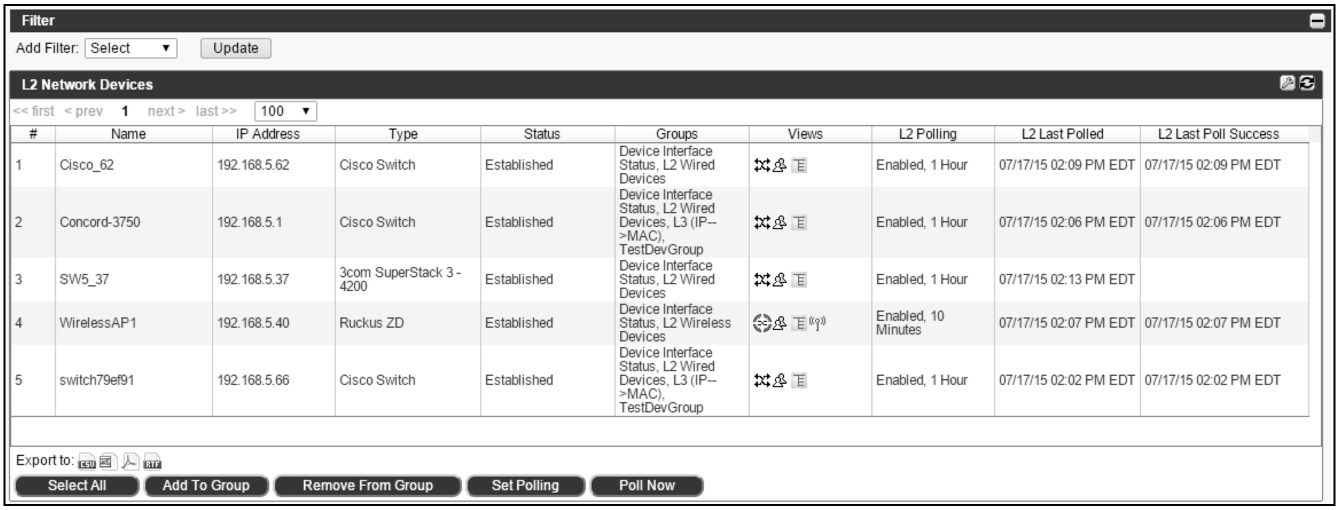
L2 polling (resync hosts)

L2 Polling is one in a series of initial setup windows designed to help you get your FortiNAC program up and running as quickly as possible. Similar functions exist in other parts of the software, but this window provides access to the most essential configuration information.

This window displays devices that were added either manually or through Discovery on the Network Devices window. As devices are added they are evaluated. Any device that is capable of L2 polling (polling hosts) is immediately placed in either the L2 Wired Devices or L2 Wireless Devices sub-group. These are default groups that are created in the database and populated for you. Devices that are not in one of these groups do not display on the L2 Network Devices window.

L2 Network Devices listed here are configured to poll network hosts and discover their IP addresses. The default polling interval is 10 minutes for wireless devices and one hour for wired devices. Devices displayed here can be added to or removed from the L2 Network Device Groups and their polling settings can be modified.

To access click **Network Devices > L2 Polling (Resync Hosts)**. See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.



#	Name	IP Address	Type	Status	Groups	Views	L2 Polling	L2 Last Polled	L2 Last Poll Success
1	Cisco_62	192.168.5.62	Cisco Switch	Established	Device Interface Status, L2 Wired Devices		Enabled, 1 Hour	07/17/15 02:09 PM EDT	07/17/15 02:09 PM EDT
2	Concord-3750	192.168.5.1	Cisco Switch	Established	Device Interface Status, L2 Wired Devices, L3 (IP-->MAC), TestDevGroup		Enabled, 1 Hour	07/17/15 02:06 PM EDT	07/17/15 02:06 PM EDT
3	SW5_37	192.168.5.37	3com SuperStack 3 - 4200	Established	Device Interface Status, L2 Wired Devices		Enabled, 1 Hour	07/17/15 02:13 PM EDT	
4	WirelessAP1	192.168.5.40	Ruckus ZD	Established	Device Interface Status, L2 Wireless Devices		Enabled, 10 Minutes	07/17/15 02:07 PM EDT	07/17/15 02:07 PM EDT
5	switch79ef91	192.168.5.66	Cisco Switch	Established	Device Interface Status, L2 Wired Devices, L3 (IP-->MAC), TestDevGroup		Enabled, 1 Hour	07/17/15 02:02 PM EDT	07/17/15 02:02 PM EDT

Settings

Fields used in filters are also defined in this table.

Field	Definition
Name	Name of the selected device.
#	Indicates the order of display.
Type	Indicates the type of devices, such as, switch, printer, router, etc.
IP address	IP address of the selected device. IP addresses or Address Ranges are used to add or discover devices.
Status	Indicates whether or not communication has been established with the device. Displays either Established or Lost.
Groups	Indicates that the device is a member of the groups listed.
Views	Series of icons that can be clicked to provide additional details about the selected device. Icons provide access to Device Properties, Group Membership and Ports and Hosts. Click an icon to access the view.
L2 Polling	Indicates whether or not L2 polling is enabled and the time interval between polls.

Field	Definition
L2 Last Polled	Date and time of the last polling attempt, regardless of whether it was successful or not.
L2 Last Poll Success	Date and time of the last successful poll.
Container	Container in the Topology View where the device is stored. Containers are a grouping mechanism similar to folders.
Right click options	
Export	Exports data to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.
Add To Group	Adds selected devices to a user specified device group.
Remove From Group	Removes selected devices from a user specified group.
Set Polling	Allows you to enable or disable polling and set the polling time interval for the selected device(s).
Poll Now	Polls selected devices immediately instead of waiting for the next poll interval.

Set L2 polling

1. Click **Network Devices > L2 Polling (Resync Hosts)**.
2. The L2 Network Devices window displays.
3. Select one or more devices from the list. To select all devices click the **Select All** button.
4. Click **Set Polling**.
5. Use the **Enable Polling** check box to enable or disable polling for the selected device.
6. If polling is enabled, select a time interval to control how often polling should occur. The interval can be set in Hours or Minutes.
7. Click **OK**.

L3 polling (IP address to MAC address)

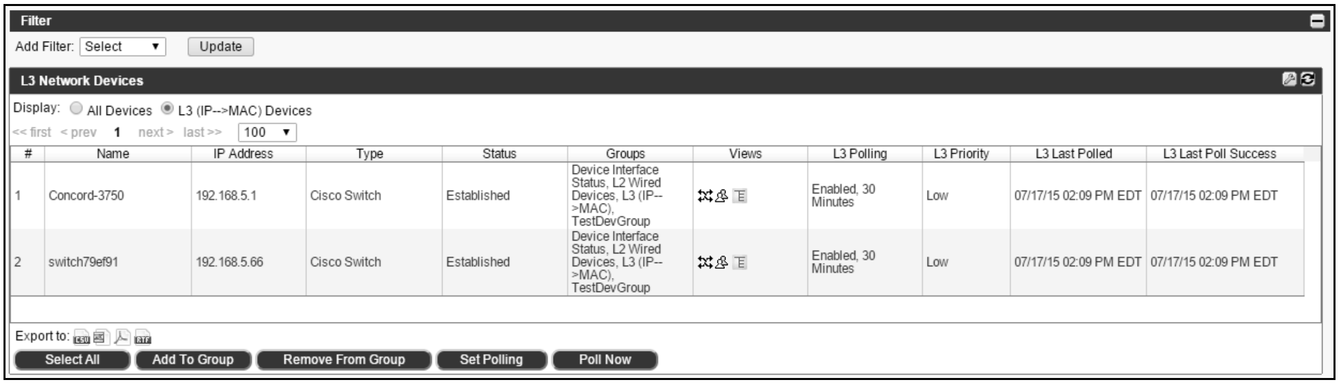
L3 Polling is one in a series of initial setup windows designed to help you get your FortiNAC program up and running as quickly as possible. Similar functions exist in other parts of the software, but this window provides access to the most essential configuration information.

L3 Polling triggers the IP address to MAC address conversion. Use this window to set a polling interval for switches and routers. Based on the information returned FortiNAC resolves the MAC addresses associated with IP addresses for hosts and other devices on the network.

As devices are added or discovered they are automatically added into the L2 Network Devices group and either the L2 Wired Devices or L2 Wireless Devices sub-groups. A default L3 (IP --> MAC) group is created by FortiNAC but is not automatically populated. You must add your L3 devices to this group.

By default this window displays devices that have been manually placed in the L3 (IP --> MAC) group. If you have not placed any devices in this group, the window does not display any devices. Select the All Devices option and click the Refresh button to display all network devices in the window.

To access click **Network Devices > L3 Polling (IP-->MAC)**. See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.



Display: ○ All Devices ● L3 (IP-->MAC) Devices

#	Name	IP Address	Type	Status	Groups	Views	L3 Polling	L3 Priority	L3 Last Polled	L3 Last Poll Success
1	Concord-3750	192.168.5.1	Cisco Switch	Established	Device Interface Status, L2 Wired Devices, L3 (IP-->MAC), TestDevGroup		Enabled, 30 Minutes	Low	07/17/15 02:09 PM EDT	07/17/15 02:09 PM EDT
2	switch79ef91	192.168.5.66	Cisco Switch	Established	Device Interface Status, L2 Wired Devices, L3 (IP-->MAC), TestDevGroup		Enabled, 30 Minutes	Low	07/17/15 02:09 PM EDT	07/17/15 02:09 PM EDT

Settings

Fields used in filters are also defined in this table.

Field	Definition
Display	**All Devices**—Displays all network devices. When Group is selected in the **Filter By** section, all device groups are displayed in the Group drop-down. **L3 (IP --> MAC) Devices**—Displays all devices in the L3 (IP --> MAC) Devices group. When Group is selected in the **Filter By** section, the L3 Devices group and any sub-groups are displayed in the Group drop-down.
#	Indicates the order of display.
Name	Name of the selected device.
IP address	IP address of the selected device. IP addresses or Address Ranges are used to add or discover devices.
Type	Indicate the type of devices, such as, switch, printer, router, etc.
Status	Indicates whether or not communication has been established with the device. Displays either Established or Lost.
Groups	Indicates that the device is a member of the groups listed.
Views	Series of icons that can be clicked to provide additional details about the selected device. Icons provide access to Device Properties, Group Membership and Ports and Hosts. Click an icon to access the view.
L3 Polling	Indicates whether or not L3 polling is enabled and the time interval between polls.
L3 Priority	Indicates high, medium or low priority given to the device when hosts connect to the network. Devices are polled in batches based on priority to retrieve host IP addresses. It is recommended that high traffic routers and switches be given a higher priority to allow hosts on those devices to connect more quickly.
L3 Last Polled	Date and time of the last polling attempt, regardless of whether it was successful or not.

Field	Definition
L3 Last Poll Success	Date and time of the last successful poll.
Container	Container in the Topology View where the device is stored. Containers are a grouping mechanism similar to folders.
Export	Exports data to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.
Right click options	
Add To Group	Adds selected devices to a user specified device group.
Remove From Group	Removes selected devices from a user specified group.
Set Polling	Allows you to enable or disable polling and set the polling time interval for the selected device(s).
Poll Now	Polls selected devices immediately instead of waiting for the next poll interval.

Set L3 polling

L3 devices have a Priority setting that allows you to associate a High, Medium or Low polling priority with each L3 device. When hosts connect to an L3 device the priority setting determines how quickly the device is polled. For example, if you have a high traffic device and a low traffic device and hosts are seen on both, which should be polled first? Typically you would give the high traffic device a high priority and the low traffic device a low or medium priority. When hosts are seen by both devices, the high priority device would be polled first. If you expand this example throughout your network, devices will be polled in groups by their priority with high priority devices being polled first.

1. Click **Network Devices > L3 Polling**.
2. The Devices window displays.
3. Select one or more devices from the list. To select all devices click the **Select All** button.
4. Click **Set Polling**.
5. Use the **Enable Polling** check box to enable or disable polling for the selected device.
6. If polling is enabled, select a time interval to control how often polling should occur. The interval can be set in Hours or Minutes.
7. In the **Priority** field, select the priority given to the device when hosts connect to the network. The higher the priority the more quickly a host connects.
8. Click **OK**.

Ports and hosts

The Ports and Hosts option displays VLAN (Current and Default) and Host (Name and IP) information for each port on the device. If the Host Name is unknown, the MAC Address is displayed.

1. Click **Network Devices > Topology**.
2. Expand the container where the device is located.
3. Right-click on the device and select **Ports and Hosts**.

Device properties

The **Properties** view for devices has Element, System, Polling and Notes tabs. Use these tabs to maintain information about the device and to change settings for the device.

Element view

1. Click **Network Devices > Topology**.
2. Expand the container where the device is located.
3. Right-click on the device and select **Properties**.
4. Click the **Element** tab.
5. Click **OK** to save the changes to this window.

If you have selected a Pingable device instead of a switch or a router, refer to Add or modify a pingable device on page 725 for Settings.

Settings

Field	Definition
Name	Name of the device.
Type	Type of device, such as a switch. May include model information. This information is derived by FortiNAC based on information received from the device.
Physical Address	Only displays for devices that do not have an IP address, such as, some wireless access points that are Layer 2 only.
Has IP address	Only displays for devices that do not have an IP address, such as, some wireless access points that are Layer 2 only. If the check box is enabled, then the IP address field can be edited and validated. For devices that do not have an IP address, this box should remain unchecked and no validation will be done when the record is saved.
IP address	IP address of the device.
Vendor / Version	Vendor / Version specific information. This cannot be edited.
VLAN Switching	Enable or Disable. If Disabled, VLAN switching is not performed on the device.
PA Optimization	If enabled, the Persistent Agent requests the new IP address for its host when the host is moved to a new VLAN. Actions taken by FortiNAC via the switch to request a new IP address for a host, such as blacklisting or shutting down the port, are disabled. Enabling PA Optimization minimizes the amount of time required to renew the host's IP address. This option applies only to hosts with a Persistent Agent. If PA Optimization is disabled, both methods are used to request a new IP address when moving a host to a new VLAN. Hosts with no Persistent Agent are subject to the actions taken by FortiNAC via the switch to supply the host with a new IP address after a VLAN change.
MAC Filtering	Enable or Disable. If Disabled, MAC Filtering is not performed on the device.

Field	Definition
Description	Description of the device.
Role	Role for this device. Select a role from the drop-down list.
Incoming Events • Not Applicable • Syslog • Security Events *Available when Automated Threat Response (ATR) is enabled.*	The availability of this field is dependent upon the type of SNMP device. When **Syslog** is selected, the following security applicances appear: • FireEye IPS • FortiOS 4.0 • FortiOS 5.0 • PaloAlto Firewall • Sourcefire IPS • StoneGate IPS • TippingPoint SMS • TopLayer IPS When **Security Events** is selected, the following security appliances appear: • FireEye • FortiOS 4.0 • FortiOS 5.0 • PaloAlto • Sourcefire • StoneGate • TippingPoint SMS • TopLayer
Advanced	
Manage as a Generic SNMP Device	Allows FortiNAC to manage an unknown SNMP device where no vendor specific information is available.
Use SNMP To Read L2/L3 Data From The Device	This option displays only for Cisco devices. It allows FortiNAC to read L2 and L3 data and the current VLAN from the device via SNMP instead of the CLI. The check box is not selected by default. However, if you create a device without CLI credentials, the management of the device will default to using SNMP. When using SNMP, full read/write privileges are not required to collect read only L2 and L3 information. However, if you enable SNMP to collect ARP information, duplicate ARP entries cannot be differentiated by time, which results in FortiNAC having outdated IP addresses.
Override Network Device Type	When selected, this option allows you to override the current Network Device Type icon with either a Switch or a Router icon. This does not affect the functionality of the device.
Buttons	

Field	Definition
Group Membership button	View Device Groups. Add the device to a group or remove the device from a group by checking or unchecking the box next to the group name.

System view

1. Click **Network Devices > Topology**.
2. Expand the container where the device is located.
3. Right-click on the device and select **Properties**.
4. Click the **System** tab.
5. Click **OK** to save the changes to this window.

If the correct Read/Write SNMP credential is specified in the Element tab, the Name, Contact and Location values will be written to the device when you click the Apply button.

The information in the table below is obtained from the SNMP System MIB:

Settings

Field	Definition	MIB Attribute
Name	The name of the device.	sysName
Contact	The contact person for the device	sysContact
Location	The location of the device (for example, Res Hall A, Equipment Closet 1st Floor, Rack 2, Unit 3)	sysLocation
Uptime	The length of time the device has been running	sysUpTime
Description	Description of the device derived by FortiNAC based on information from the device.	sysDescr

Polling view

The Polling tab is where you configure if/when polling will occur, how often, and what will be polled. You can also manually poll the device.

1. Click **Network Devices > Topology**.
2. Expand the container where the device is located.
3. Right-click on the device and select **Properties**.
4. Click the **Polling** tab.
5. Click **OK** to save the changes to this window.

Settings

Field	Definition
Contact Status	
Polling	Enable or disable contact status polling for the selected device.
Poll Interval	Determines how often the device should be polled for communication status. Time is stored in minutes.
Last Successful Poll	Date and time that the device was last polled successfully.
Last Attempted Poll	Date and time that the device was last polled.
Poll Now	Polls the device immediately for contact status.
L2 (hosts) information	
Polling	Enable or disable polling for hosts connected to the device.
Poll Interval	Determines how often the device should be polled for new host connection information. Time is stored in minutes. Wired device default is 60 minutes. Wireless device default is 10 minutes.
Last Successful Poll	Date and time that the device was last polled successfully.
Last Attempted Poll	Date and time that the device was last polled.
Poll Now	Polls the device immediately for host connections.
L3 (IP-->MAC) information	
Polling	Indicates whether L3 Polling for this device is enabled or disabled.
Poll Interval	Indicates how often the device should be polled for IP information used in IP to MAC Address identification.
Priority	Indicates the priority for polling this device. Devices are polled in batches from High priority to Low priority until the required information is found.
Last Successful Poll	Date and time that the device was last polled successfully.
Last Attempted Poll	Date and time that the device was last polled.
Cisco Discovery information	
Global Polling	Indicates whether the global setting for Cisco Discovery Protocol is enabled or disabled. If the global setting is disabled, the feature is disabled for all devices regardless of the setting in the polling field. To change the global setting see Network device on page 130.
Polling	Indicates whether the Cisco Discovery option for this device is enabled or disabled. Default = Disabled
Poll Interval	Indicates how often the device should be polled for information stored about other connected devices on the network.
Last Successful Poll	Date and time that the device was last polled successfully.
Last Attempted Poll	Date and time that the device was last polled.

If the device you have selected is not capable of L2 polling (polls host connections), L3 polling (polls to do IP to MAC Address conversions) or Cisco Discovery, those options are not displayed.

L2 Polling information can also be configured using the L2 Polling window. To access this window select Network Devices > L2 Polling (Resync Hosts). See L2 polling (resync hosts) on page 748 for additional information.

L3 Polling information is configured using the L3 Polling window. To access this window select Network Devices > L3 Polling (IP --> MAC). See L3 polling (IP address to MAC address) on page 750 for additional information.

Credentials view

Configure or update the credentials to allow FortiNACto talk to the device. Credentials match the settings on the device.

1. Click **Network Devices > Topology**.
2. Expand the container where the device is located.
3. Right-click on the device and select **Properties**.
4. Click the **Credentials** tab.
5. Click **OK** to save the changes to this window.

The options vary depending on the SNMP protocol selected.

Settings

Field	Description
Validate Credentials	Click to test the CLI and SNMP credentials entered.
SNMP Settings	
SNMP Protocol	Select SNMPv1 or SNMPv3. This option is not available for all types of devices.
SNMPv1	
Security Strings	Click **Add** to add a security string for the device into the FortiNAC database. This must be the read/write security string. Click **Remove**. On the window displayed, select and remove security strings for this device from the FortiNAC database. This field displays a list of security strings used during Discovery. The security string most recently used for read/write access is listed first. Also known as the SNMP Community string.
SNMPv3	
User Name	User Name for access to the device. Recommended but not required.
Authentication protocol	
Authentication Password	Enter the password you configured on the device.
Privacy Protocol	Available options are DES and AES-128. Used only for AuthPriv.

Field	Description
Privacy Password	Enter the password you configured on the device. Used only for AuthPriv.
Clear Cached Engine ID	Clears the Engine ID cached for this device and forces the re-establishment of a new Engine ID. If you have replaced one device with another and reused the IP address, you may need to clear this cache. If you have deleted the original device and then try to add a new device with the same IP address you may need to clear this cached ID. Since the device is not successfully added, you cannot access the device properties to use the Clear Cached Engine ID button. Instead, log into the CLI for the FortiNAC Server or Control Server, navigate to the /bin directory and use the ClearEngineID tool as follows: ClearEngineID -ip <device IP address> Example: ClearEngineID -ip 192.168.15.25
CLI settings	
User Name	The user name used to log on to the device for configuration. This is for CLI access. The user account must have the appropriate permissions configured on the device.
Password	The password required to configure the device. This is for CLI access.
Enable Password	The enable password for the device. This is for CLI access.
Protocol Types	Telnet - Use to log on to the device for configuration. SSH1 - Use to log on to the device for configuration. SSH2 - Use to log on to the device for configuration.

Modify multiple device properties

You can modify the properties for multiple devices simultaneously. Properties that appear depend on which type of devices are selected.

Settings that are not supported by a selected device will not appear in the view.

Modifications to properties are only applied to selected devices that support those properties. For example, if you select four devices, but only two devices support L3 Polling, a warning icon and tooltip is displayed next to the L3 Polling setting indicating the number of the selected devices that support L3 Polling.

1. Click **Network Devices > Topology**.
2. Select the container where the devices are located.
3. In the **Devices** view, use Ctrl-click or Shift-click to select the devices you wish to modify.
4. Right-click the devices and click **Modify Properties**.

5. Modify the properties for the devices.
6. Click **OK**.

Pingable device properties

The Properties view for Pingable Devices, such as IPS/IDS system, has Element and Details tabs. Maintain device information and change settings on these tabs.

1. Click **Network Devices > Topology**.
2. Expand the container where the device is located.
3. Click on the device and properties are displayed in the right pane.

Element tab settings

Field	Definition
Container	Container in the Topology View tree where this device is stored.
Name	Name of the device
IP address	IP address of the device
Physical Address	The MAC address of the device. Appears in the view only when the device is a pingable.
Device Type	Select the device type from the drop-down list.
Incoming Events • Not Applicable • Syslog • Security Events *Available when Automated Threat Response (ATR) is configured.*	When Syslog is selected, available syslog files appear that can be used by FortiNAC to parse information received from the external devices and generate an event. See Syslog management on page 190. When Security Events is selected, available security event parsers appear that can be used by FortiNAC to parse information received from the external devices and generate a security event. See Security event parsers on page 198.
SSO Agent	• Not Applicable • Custom Script • Palo Alto • RADIUS • iboss
Custom Script	Displayed when Custom Script is selected in the SSO Agent field. Allows you to write and select a script that will integrate with a SSO Agent that is not currently supported.
Apply to Group	Select this check box to apply the Custom Script SSO options only to the selected Host group in the drop-down list. If you do not select the check box, the SSO options are applied to all Host groups.
RADIUS Accounting Port	Displayed when RADIUS is selected in the SSO Agent field. Port on the Fortinet Single Sign-On User Agent configured to receive RADIUS Accounting messages from external devices. This port must match the port configured in Fortinet.

Field	Definition
RADIUS Secret	Displayed when RADIUS is selected in the SSO Agent field. Must match the RADIUS secret configured for FortiNAC in Fortinet.
Apply to Group	Select this check box to apply the RADIUS SSO options only to the selected Host group in the drop-down list. If you do not select the check box, the SSO options are applied to all Host groups.
XML API Port	Displayed when Palo Alto User Agent is selected in the SSO Agent field. Port on the Palo Alto User Agent configured to receive messages from external devices. This port must match the XML API port configured on the Palo Alto User Agent. See Add or modify the Palo Alto User-ID agent as a pingable on page 728.
Domain Name	Displayed when Palo Alto User Agent is selected in the SSO Agent field. Fully Qualified Domain Name for your network users' domain. This is sent with the logged in User ID to Palo Alto.
Use Integrated Agent	When selected, FortiNAC will integrate with the firewall directly.
API Key	Displayed when the Use Integrated Agent check box is selected. Enter the API Key value. The key can be retrieved manually or via the Retrieve button.
Apply to Group	Select this check box to apply the Palo Alto SSO options only to the selected Host group in the drop-down list. If you do not select the check box, the SSO options are applied to all Host groups.
iboss Port	Displayed when iboss is selected in the SSO Agent field. The IBOSS port is the IBOSS HTTP port that is used to talk to the IBOSS SSO agent. The IBOSS port is defined in the IBOSS SSO GUI.
iboss Key	Displayed when iboss is selected in the SSO Agent field. The IBOSS key is a security key used to talk to the IBOSS SSO agent.The IBOSS key is defined in the IBOSS SSO GUI.
iboss Domain	Displayed when iboss is selected in the SSO Agent field. The iboss Domain is a required field that allows the user to enter their Active Directory Domain Name.
Apply to Group	Select this check box to apply the iboss SSO options only to the selected Host group in the drop-down list. If you do not select the check box, the SSO options are applied to all Host groups.
Role	The Role for this device. Available roles appear in the drop-down list.
Description	Description of the device entered by the Administrator.
Note	User specified notes about the device.
Contact Status Polling	Enable or disable contact status polling for the selected device.
Poll Interval	Determines how often the device should be polled for communication status. Time is stored in minutes.
Poll Now	Polls the device immediately for contact status.
Last Successful Poll	Date and time that the device was last polled successfully.
Last Attempted Poll	Date and time that the device was last polled.

Details tab settings

Field	Definition
Host Name	Name of the device.
Department	Name of the department.
Owner	Name of the owner of the device.
Administrative Contact	Administrative contact person for the device.
Geographical Location	Geographical location of the device (for example, Res Hall A, Equipment Closet 1st Floor, Rack 2, Unit 3).
Business Purpose	Business purpose of the device.
BOOTP Address	IP address for the BOOTP Protocol.
Print Queue	Name of the print queue for the device.

Resync interfaces

This option reads the interface information from a modeled device and updates FortiNAC's representation of that device. This information includes the interface's index, description, name, and status. Ports or interfaces are displayed in the order in which they appear in the interface table on the device. Depending on the device and its configuration, ports may not display in order numerically or alphabetically.

Typically, a device's interfaces remain fairly stable and unchanging. However, devices that reside in a chassis or those that can be stacked share management between separate boards or stacked units. When boards or units are added, removed, or repositioned within the chassis or stack, it is necessary to have FortiNAC re-read the device to learn of the changes and display an accurate representation in the Ports tab in Topology View. See Ports view on page 778 for more information. To access this option:

1. Click **Network Devices > Topology**.
2. Right-click on the device and select **Resync Interfaces**.
3. Click **Yes** on the confirmation dialog to continue.

View role membership

View a list of the role(s) assigned to the selected device or port and the Network Access ID for that role on the device.

1. Click **Network Devices > Topology**.
2. Expand the container where the device is located.
3. Click on the device to select it and display associated ports in the right pane.
4. To view roles for the device: Right-click on the device and select **Role Membership**.
5. To view roles for a port: Right-click on a device port in the right pane and select **Role Membership**.

Settings

Field	Definition
Role	Name of the role.
CLI	Allows you to apply a CLI Configuration to a device or port when this role is used.
Access Value	The Access ID (VLAN ID, VLAN Name, or Role) information associated with this role on the device or port.
Locations	The location defined for the Network Device Role.

Set device mapping for unknown SNMP devices

If an SNMP Device is added to the Topology, but the device could not be identified by the OID, the option will be available to set the device mapping.

1. Select **Network Devices > Topology View**.
2. Right-click on the device marked with a question mark icon.
3. Select the **Set Device Mapping** option from the menu.

Settings

Field	Definition
Name	Name of the selected device.
OID	Detected OID of the selected device.
Description	Description of the device read via SNMP or supplied within the Element details.
Standard Bridge MIB	Whether or not the device appears to support the standard Bridge MIB, 1.3.6.1.2.1.17.
Standard VLAN MIB	Whether or not the device appears to support the standard Switch VLAN MIB, 1.3.6.1.4.1.207.8.9.2.5.2.
Standard IP MIB	Whether or not the device appears to support the standard IP MIB, .1.3.6.1.2.1.4.28.
Current Mapping	The source used for the current Device Mapping for the selected device. If modeled as an existing device mapping, this will list the OID of the device it cloned.
Report Mapping Details to Bradford	If checked, the details of this mapping will be e-mailed using the configured mailer to Fortinet, so we may add them to our product. The e-mail sends only the following information: • Logged On User • Logged On User Email • Appliance Physical Address • Device OID • Device Description • Chosen OID

Field	Definition
Model this Device as a Generic SNMP Device	The device will be managed using the available SNMP MIBs. It may require additional details in the Model Configuration to specify VLANs.
Model this Device as a Device Type	The device is not manageable using standard SNMP MIBs. It may be modeled as an SNMP enabled network device of the type specified in the dropdown.
Model this OID from an Existing Device	All devices with the same OID will be mapped when this is selected, if they have not already been mapped as a Generic SNMP Device or Device Type. This OID will have all properties copied from an existing Device Model. Double click a Device Model to see more information.
Device Model	The name of the Device Model copied to this OID. Typing in this field will search the Device Mappings table based on both OID and Model.

Update device mapping

When new devices are added to the FortiNAC Topology View, recognized device types are displayed with an icon indicating the type of device. The system name (sysName) is used for the name of the device. If the device type is not recognized, a question mark icon is displayed and more information is required to manage the device.

Unrecognized devices which support the IETF standard MIBs listed below can be added as generic SNMP devices. This “Generic SNMP” feature allows hosts to be read, VLANs to be read/switched and IP to MAC address information to be read from the device – without needing a specialized code patch or build. In order to successfully configure a Generic SNMP device, it must fully support the MIB groups as described in the following table.

Devices that appear to support the standard VLAN MIB, may not fully support the standards. The switching of a VLAN on a port may or may not be supported by the device.

Standard	Reference	SNMP MIB Objects/Tasks
RFC1213 – MIB II	Address Translation (AT) MIB	**Read of IP->MAC:** **atTable** - The Address Translation tables contain the NetworkAddress to `physical' address equivalences. SNMP OIDs 1.3.6.1.2.1.3.1.1.2
RFC1158 - MIB II	Address Translation (AT) MIB	**Read of IP -> MAC:** **atTable** - The Address Translation Group contains NetworkAddress to `physical' address equivalences - deprecated by MIB II.

Standard	Reference	SNMP MIB Objects/Tasks
		ipNetToMediaTable - The Address Translation tables contain the NetworkAddress to `physical' address equivalences. SNMP OIDs 1.3.6.1.2.1.3.1.1.2 1.3.6.1.2.1.4.22.1.2
RFC1493 – BRIDGE-MIB	BRIDGE MIB	**Read Hosts:** **dot1dTpFdbTable** - A table that contains information about unicast entries for which the bridge has forwarding and/or filtering information. SNMP OIDs 1.3.6.1.2.1.17.4.3.1.1 1.3.6.1.2.1.17.4.3.1.2 1.3.6.1.2.1.17.4.3.1.3
RFC2674-Q-BRIDGE-MIB	VLAN MIB	**Read / Switch VLANS:** **dot1qPortVlanTable** - A table containing per port control and status information for VLAN configuration in the device. SNMP OIDs 1.3.6.1.2.1.17.7.1.4.5.1.1

Do not change an existing supported device to a generic SNMP device or you will lose the custom options provided in FortiNAC for that device.

If support for a generic SNMP device is added in a later release of FortiNAC, you can either leave the device as generic SNMP device or delete it and re-add it to the Topology View. Deleting the device removes it from all device and port groups. The device and its ports would have to be added to the appropriate groups again manually.

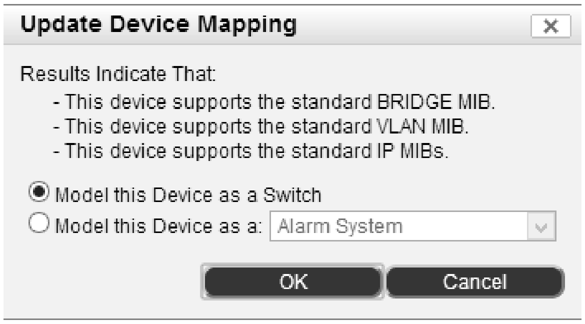
Update unknown SNMP devices

The existence or absence of the SNMP MIB objects determines the type of device to add. Based on the combination of SNMP MIB objects found, options on the Update Image dialog are dynamically adjusted.

If you try to update a device that is no longer in contact with FortiNAC, you will see the following message. “This Device indicates that - Contact is not established with this device.” When that message is displayed you only have the option to select a device type. Update Device Mapping will not be able to determine whether the device is a switch or a router.

1. Select **Network Devices > Topology View**.
2. Right-click on the device marked with a question mark icon.
3. Select the **Update Device Mapping** option from the menu.
4. See the examples listed below for additional information.

Example 1



Update Device Mapping

Results Indicate That:

- This device supports the standard BRIDGE MIB.
- This device supports the standard VLAN MIB.
- This device supports the standard IP MIBs.

● Model this Device as a Switch

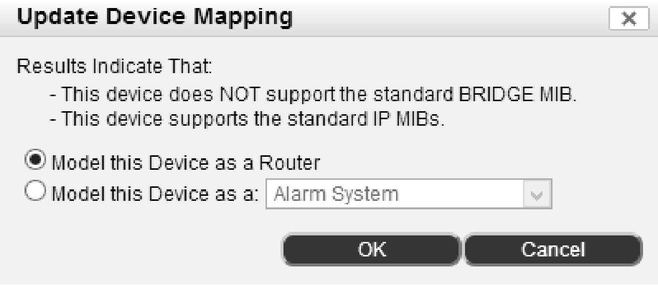
○ Model this Device as a: Alarm System

The following example shows the options for a device that supports both the standard BRIDGE MIB, the standard VLAN MIB and the standard IP MIBs. Therefore, it is likely that this device is a switch. However, if you know this device is not a switch, click the Model this Device as option and select the appropriate device type from the drop-down list.

After updating the image in the Topology View, go to Model Configuration to specify VLANs. See Model configuration on page 767 for additional information.

When testing the device for VLAN switching, check the Events View for a VLAN Switch Failure event. If a VLAN Switch Failure is generated for this device, then the device does not support the standard VLAN MIB. You will not be able to switch VLANs.

Example 2



Update Device Mapping

Results Indicate That:

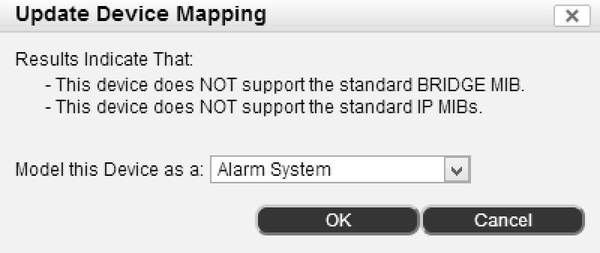
- This device does NOT support the standard BRIDGE MIB.
- This device supports the standard IP MIBs.

● Model this Device as a Router

○ Model this Device as a: Alarm System

The following example shows a device that supports the standard IP MIBs, but does not support the BRIDGE MIB. Therefore, it is likely that this device is a router. However, if you know this device is not a router, click the Model this Device as option and select the appropriate device type from the drop-down list.

Example 3


Update Device Mapping

Results Indicate That:
- This device does NOT support the standard BRIDGE MIB.
- This device does NOT support the standard IP MIBs.

Model this Device as a: Alarm System

The following example shows a SNMP device that does not support the standards. This indicates that the device is neither a switch nor a router. In this example, the device is an alarm system and you can map it as an alarm system with the appropriate icon. You can leave it as an SNMP device and use the Model this Device as option to select the type. When selected the device will display the SNMP interfaces in the panel on the right pane of the Topology View.

If you prefer to see device information instead of the interfaces, go to the Host View, right-click on the device and select Register as Device.

Another option is to delete the device from the Topology View. Right click on the container and use the Add Pingable option from the menu to add the device.

Device configuration

To successfully monitor and configure certain vendor devices, you must set some additional configuration parameters. Access these parameters through the **Model Configuration** view and set them prior to scheduling actions on the device.

1. Click **Network Devices > Topology**.
2. Expand the container where the device is located.
3. Right-click on the device and select one of the options in the table.

Option	Description
Device Name > Global Model Configuration	Configure global database model parameters for all devices of this type across the network.
Device Name > Model Configuration	Configure database model parameters for the selected device.
Device Name > Running Configuration	View the configuration running on the selected device (device dependant). This option is only available for some devices.
Device Name > Static/ Secure Port Configuration	Configure static or secure ports on the selected device (device dependent).

Delete a device

1. Click **Network Devices > Topology**.
2. The Network Devices window displays.

3. Select a device from the list in the Network Devices panel.
4. Click **Delete**.
5. The program asks if you are sure. Click **Yes** to continue.

Resync interfaces

This option reads the interface information from a modeled device and updates FortiNAC's representation of that device. This information includes the interface's index, description, name, and status. Ports or interfaces are displayed in the order in which they appear in the interface table on the device. Depending on the device and its configuration, ports may not display in order numerically or alphabetically.

Typically, a device's interfaces remain fairly stable and unchanging. However, devices that reside in a chassis or those that can be stacked share management between separate boards or stacked units. When boards or units are added, removed, or repositioned within the chassis or stack, it is necessary to have FortiNAC re-read the device to learn of the changes and display an accurate representation in the Ports tab in Topology View. See Ports view on page 778 for more information. To access this option:

1. Click **Network Devices > Topology**.
2. Right-click on the device and select **Resync Interfaces**.
3. Click **Yes** on the confirmation dialog to continue.

Model configuration

The model configuration window allows you to configure devices that are connected to your network so that they can be monitored. Data entered in this window is stored in the FortiNAC database and is used to allow interaction with the device. Data entered on the model configuration window is not sent to the device. This window can be accessed from the Topology View and from the Network Devices window.

When configuring the device itself, use only letters, numbers and hyphens (-) in names for items within the device configuration, in security strings and in SNMP credentials. Other characters may prevent FortiNAC from reading the device configuration. For example, in many cases the # sign is interpreted by FortiNAC as a prompt. Cisco restricts the use of @ and #.

For network devices using API credentials, the User Name is the serial number of the appliance and the Password is the REST API Key.

Access from topology

1. Click **Network Devices > Topology**.
2. Expand the Container icon.
3. Right-click on the device, and then click **Model Configuration**.

Settings

Device configuration information is specific for each device and may include any combination of the fields in the table below:

Settings	Description
General	
User Name	The user name used to log on to the device for configuration. This is for CLI access. The user account must have the appropriate permissions configured on the device. For network devices using API credentials, the User Name is the serial number of the appliance.
Password	The password required to configure the device. This is for CLI access. For network devices using API credentials, the Password is the REST API Key.
Enable Password	The enable password for the device. This is for CLI access.
Super Password	The super password required for access to more features on 3Com devices.
HWC Connect Port	Port for the External Captive Portal that was configured by the user on the device during the initial device setup. This port is required for FortiNAC to send commands to the device. Consult the manufacturer for assistance in locating this port number.
Read Groups From Device	Ports on a device can be placed in to network groups that control access. This option reads the preset groups from the device.
Protocol types	
Telnet	Use Telnet to log on to the device for configuration.
SSH1	Use SSH1 to log on to the device for configuration.
SSH2	Use SSH2 to log on to the device for configuration.
VLAN ID/Network Access	
VLAN Display Format	For some devices, the list of VLANs configured on the device can be read from the device and made available in a drop-down. When this feature is available, the VLAN Display Format option is shown. Choices included: • **VLAN Name** — Displays a drop-down list of VLANs configured on the device by VLAN name for each isolation state. • **VLAN ID** — Displays a drop-down list of possible VLANs configured on the device by VLAN ID or number for each isolation state.

Settings	Description
	- **Manual** — Provides an empty text field to enter the VLAN name or ID. This is used in the event that the VLANS on the device have not been pre-configured
Read VLANs	Click this button to read VLAN configuration from the device and populate the drop-down lists of VLANs for each isolation state.
Default	The Default VLAN value is stored in the FortiNAC database and is used when the VLAN is not determined by another method, such as a Network Access Policy. Typically, if a VLAN is specified as the Default, it is the VLAN used for "normal" or "production" network access. It will be used for all the untagged (non-uplink) ports on the device. If you do not want all ports on the device to use the same "Default" VLAN, you can leave the value blank in Model Configuration and use the Network Access / VLANs feature to customize the Default VLANs for each port. See Network access/VLANs on page 745 for more information.
Dead End	The dead end VLAN for this device. Isolates disabled hosts with limited or no network connectivity from the production network.
Registration	The registration VLAN for this device. Isolates unregistered hosts from the production network during host registration.
Quarantine	The quarantine VLAN for this device. Isolates hosts from the production network who pose a security risk because they failed a policy scan.
Authentication	The authentication VLAN for this device. Isolates registered hosts from the Production network during user authentication.
Voice	The voice VLAN (s) for this device. This field accepts a list of VLANS separated by commas, such as 10, 25,30. This indicates to FortiNAC that these VLANS are excluded from all other uses.
Apply Default VLAN ID To All Non-wireless ports	If a device has both wired and wireless ports, you may choose to assign VLANs to each port individually. You may also choose to assign a single default VLAN to all of the wireless ports for this device, by putting a VLAN ID in the Default field on this window. That number then overrides the individual entries on the wireless ports. The wired ports would continue to have a separate VLAN setting for each port. If you choose to apply the Default VLAN ID to both wireless and wired ports, enabling this feature overrides the original port settings on the wired ports with the setting in the Default field on this window
Manage Captive Portal	Affects only Meru Controllers. If the Captive Portal setting on any Security Profile for any SSID is set to WebAuth indicating that the SSID is being managed by Internal Captive Portal (ICP) on the Meru Controller and this check box is enabled, all SSIDs set to WebAuth will be managed by FortiNAC. If enabled, FortiNAC uses Firewall Rules to treat authenticated and unauthenticated users differently.

Settings	Description
	The treatment selected in the Access Enforcement section of the Model Configuration window is ignored for any SSIDs set to WebAuth. Hosts that are isolated are treated as unauthenticated hosts regardless of the isolation type. Hosts that are not isolated are treated as authenticated.
CLI configurations	
Configurations	This section allows you to associate pre-configured scripts with selected Port states or host states. A default script can also be selected. Scripts are not required. States that can be associated with CLI Configurations include: Default, Registration, Authentication, Dead End and Quarantine. See CLI configuration on page 928 for information on creating scripts.
RADIUS	
Primary RADIUS Server	The RADIUS server used for authenticating users connecting to the network through this device. Select the **Use Default** option from the drop-down list to use the server indicated in parentheses. See RADIUS on page 102 for information on configuring your RADIUS Servers.
Secondary RADIUS Server	If the Primary RADIUS server fails to respond, this RADIUS server is used for authenticating users connecting to the network until the Primary RADIUS Server responds. Select the **Use Default** option from the drop-down list to use the server indicated in parentheses.
RADIUS Secret	The secret used for RADIUS authentication. The RADIUS secret used must be exactly the same on the wireless device, on the RADIUS server and in the FortiNAC software under RADIUS Settings and Model Configuration.
Enable rfc5176 support	Appears for Aruba Controllers. Enables the use of both RADIUS Disconnect and RADIUS Change Of Authorization (CoA) requests depending on the Aruba model being used (L2 Roles with VLANs and L2 Roles only respectively).
Modify Button	Allows you to modify the RADIUS secret.
Restricted access	
Object Group Name	Network List name that is used to contain IPs when the host is marked safe.
Network access - wireless devices	
Read Roles From Device	Retrieves roles that currently exist on the device being configured.
Read Roles	The drop-down next to each type, such as Registration, contains a list of possible roles read from the device. You can select a role for one or more of the types listed below. • Default • Dead End

Settings	Description
	• Registration • Quarantine • Authentication
Host State	Host State is used to determine treatment when the host connects to the network. For each host state select an option in the Access Enforcement column and where applicable in the Access Value column. • Default • Dead End • Registration • Quarantine • Authentication • Roaming Guest Roaming Guest is a special host state detected when a user authenticates using a domain name that is not listed in the local domains list. Users are authenticated via a remote RADIUS Server and are placed on the network immediately unless Deny is selected under Access Enforcement. Roaming Guests bypass the captive portal and Device Profiler. See Roaming guests on page 110.
Access Enforcement	This set of drop-down menus works in conjunction with the Host States listed above to determine treatment for hosts when no VLAN/Role value is supplied or when access control is being enforced. Options include: • **Deny** — Host will be denied access to the network when it is in this state. For example, if the host is not registered and Registration is set to Deny, the host connection will be rejected. Endpoints that have been denied access may continuously request access which can unnecessarily consume system resources. • **Bypass** — Host will be allowed access to the network when it is in this state. The host will be placed on the default VLAN/Role configured on the device for this port or SSID. For example, if Quarantine is set to Bypass, hosts that fail a scan and would normally be placed in Quarantine are placed in the default VLAN/Role on the device. • **Enforce** — Indicates that the host will be placed in the VLAN/Role specified in the Access Value column for this state.
Access Value	VLAN/Role where a host in this state should be placed when it connects to the network. If Enforce is selected in the Access Enforcement field you must enter a value in the Access Value field.
Wireless AP parameters	

Settings	Description
Preferred Container Name	If this device is connected to any Wireless Access Points, they are included in the Topology View. Enter the name of the Container in which these Wireless Access Points should be stored. Containers or folders are created in the Topology view to group devices.
Detail configuration	
Check box	Secure Ports is enabled for ports on this device. When this option is enabled, secure ports allows you to deny access to disabled hosts. See Secure port/static port overview on page 776 for requirements.

Global model configuration

FortiNAC maintains a model of each device it manages in the database. Those database models of physical devices contain information about how to communicate with the device, what VLANs should be used for isolation, which RADIUS server should be used for authentication and what the communication protocol is.

Device-specific information varies by vendor. You can set and store some configuration parameters globally across a specific vendor’s devices by using FortiNAC’s Global Model Configuration option. This window can be accessed from the Topology View and from the Network Devices window.

When configuring the device itself, use only letters, numbers and hyphens (-) in names for items within the device configuration, in security strings and in SNMP credentials. Other characters may prevent FortiNAC from reading the device configuration. For example, in many cases the # sign is interpreted by FortiNAC as a prompt. Cisco restricts the use of @ and #.

Access from topology

1. Click **Network Devices > Topology**.
2. Expand the **Container** icon.
3. Right-click on a device manufactured by the vendor of the group of devices to be configured, select the device name, and then click **Global Model Configuration**.

Configuration

1. On the **Global Model Configuration** window use Ctrl-Click to select one or more devices from the list in the **Select Devices** section.
2. Select one of the Save options:
   - **Save all values for selected device models** saves all data that is displayed on the configuration window to the models in the database for all devices that have been selected. For example, if you have created a model in the database for one device and would like to create the same model for several others, you could go to Network Devices, right-click on the "copy from" device and select Global Model Configuration. The values for the selected device are displayed. Then, select additional devices for which you want to create models. Click the Save All values option and all of the device models will be saved with the same information as the first one.

- **Save only changed values for selected device models** saves only those fields that have been modified to the models in the database for all devices that have been selected. For example, if you have set the user names and passwords on several of your switches to be the same, those modifications must be entered in the model configuration stored in the database to allow FortiNAC to communicate with the devices. Updating the user names and passwords can be done all at once by selecting multiple devices of the same brand, entering the new user name and password and choosing the Save only changed values.

3. The information entered in the configuration is model-specific. See Settings on page 768 for information on each field that you can configure.
4. Click **Apply**.

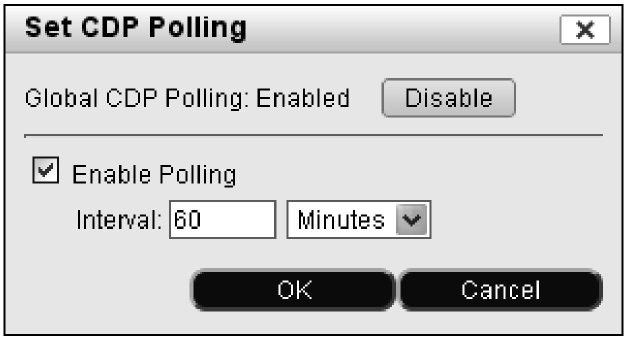
   If you have chosen to Save all values, every field is copied exactly as it displays to the model configuration record of each of the selected devices, including blank fields. A warning is displayed.

   If you have chosen to Save only changed values, only the fields highlighted in orange will be saved to the model configuration record of each of the selected devices. A warning is displayed.

Set CDP polling

Set CDP Polling allows you to enable CDP Polling for one or more devices at the same time by selecting them from the Network Device View. The CDP option leverages the Cisco Discovery Protocol (CDP) feature enabled on some network devices. Network devices that are configured for CDP collect and store information about the network devices they manage or can contact. FortiNAC can gather information about network devices more quickly and efficiently using this mechanism.

The Global CDP setting controls CDP polling system-wide. If this option is disabled, CDP settings on individual devices are ignored.


Set CDP Polling

Global CDP Polling: Enabled

☑ Enable Polling

Interval: 60 Minutes

1. Click **System > Quick Start > Network Device Settings**.
2. Click **Network Devices**.
3. Select one or more devices from the list in the Network Devices View.
4. Click **Set CDP Polling**.
5. To enable or disable Global CDP Polling, toggle the **Enable/Disable** button at the top of the window. If Global CDP Polling is disabled, all CDP settings on individual devices are ignored and CDP Polling is not done. When Global CDP Polling is enabled, individual devices are checked and settings on each device are honored.
6. To enable polling for the selected devices, click **Enable Polling** to mark it with a check mark.
7. In the **Interval** field enter the number of minutes or hours between polls for this set of devices.
8. In the drop-down list, select either **Minutes** or **Hours**.
9. Click **OK** to save.

Wired devices and 802.1X

802.1X authentication, which provides FortiNAC with another means of port-level access control, is supported for a select list of Cisco, Extreme, Juniper and HP switches. Devices include the following:

- Cisco 4500, 3650 and 3750. See Cisco device configuration on page 775.
- HP 2300, 2600, 3500, 5400, and 6400 series
- Juniper EX series switches. Refer to the *Juniper EX Switch: 802.1x / MAC-Auth Configuration* document in the customer portal.
- Extreme 450 XOS

Support for additional devices will be provided based on the number of customer requests and the availability of similar equipment.

Host configuration

Host supplicants should be configured to authenticate using user credentials, not host information, such as hostname. This will give FortiNAC the user information to associate with the host/device allowing for automatic authentication.

HP switches must have a time-window of 0 for the most consistent results.

FortiNAC configuration

- In FortiNAC set up one or more RADIUS servers for authentication. See RADIUS on page 102 for additional information.
- Make sure that the RADIUS secret is the same everywhere, including: the RADIUS server itself, RADIUS server settings configured in FortiNAC, RADIUS settings configured on the Model Configuration window and in the configuration for your device. If the RADIUS secret does not match in all locations, authentication requests will fail.
- Add the Device to FortiNAC using the Discovery process or by adding the device manually. See Discover devices on page 735 or Add or modify a device on page 723.
- After the device is added to FortiNAC you must complete the model for the network device in the database. See Model configuration on page 767.
- If VLAN switching is not enabled, no VLAN will be assigned to an authentication response. Verify that VLAN Switching is enabled under Device Properties.
- Ports on the device that will manage connected hosts should be placed in the appropriate access control groups, such as, Forced Registration, Forced Authentication or Forced Remediation. If ports are not added to these groups, the isolation VLANs associated with those states will not be provided in an authentication response for those ports. See Groups view on page 838.

Device configuration

Define the FortiNAC Server or Control Server as the RADIUS server for the devices you want to manage with FortiNAC as follows:

- Use the management IP address of your FortiNAC Server as the IP of the RADIUS Server.
- Use port 1812 for authentication.
- If you are setting up FortiNAC as the RADIUS server for a device in a Fortinet High Availability environment, you must use the actual IP address of the primary control server, not the Shared IP address. Set up the secondary control server as a secondary RADIUS server using its actual IP address. Regardless of the environment, you may

also want to set up your actual RADIUS server to be used in the event that none of your FortiNAC appliances can be reached. This would allow users to access the network, but they would not be controlled by FortiNAC.

Cisco device configuration

Cisco switches include numerous features with their 802.1x support, many of which are not affected by this integration. Administrators should be familiar with configuring 802.1x port-based authentication on the relevant switches. Many options can be configured that affect the authentication behavior on the device, such as host mode (ie. single-host and multi-host modes) and IP phone support. It is recommended that you have a thorough understanding of these features before deploying 802.1x.

Cisco features that are affected by the integration with FortiNAC include the following:

- Configuring VLANs for the guest, auth and critical values is not supported. FortiNAC does not currently detect how a port has been assigned a VLAN. FortiNAC always assumes it is in control over the VLAN to which a port is assigned. Therefore, if these VLANs are configured, FortiNAC may still attempt to affect a VLAN change on the port based on the connected host state.
- Ensure that RADIUS requests sent by the Cisco router contain the Cisco-NAS-Port vendor specific attribute. FortiNAC uses this attribute to identify the port involved in the authentication.
- MAC-Authentication Bypass is supported, but administrators should be careful to set a reasonable delay. The switch waits for the delay period for the EAPOL message prior to using MAC-Authentication. Connecting hosts will be delayed by at least that amount when no supplicant is present or enabled.

IOS configuration statements relating to 802.1x

The statements listed below represent a minimal configuration to enable 802.1x on a Cisco switch/router running IOS. The commands may vary based on switch model and IOS version. These are taken from a Cisco 3750 -24TS running IOS 12.2(25)SEE3.

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa nas port extended
```

(required to enable Cisco-NAS-Port)

```
!
interface FastEthernet1/0/18
switchport access vlan 163
```

(Port will only be assigned this VLAN if none is assigned or exception condition occurs.)

```
switchport trunk encapsulation dot1q
switchport mode access
dot1x mac-auth-bypass (optional)
dot1x pae authenticator
dot1x port-control auto
dot1x host-mode multi-host
dot1x timeout quiet-period 3
dot1x timeout server-timeout 10
dot1x timeout reauth-period 180
dot1x timeout tx-period 5
dot1x timeout supp-timeout 6
dot1x reauthentication
!
radius-server host 192.168.34.31 auth-port 1812 acct-port 1813 key abc123
```

```
radius-server source-ports 1645-1646
radius-server vsa send authentication
```

Secure port/static port overview

When multiple hosts connect to the same port on a device or you do not have a Dead End VLAN it can be difficult to disable individual hosts. Filtering for a particular physical or MAC address is one option for disabling a host. Options vary depending on the capabilities of the device to which these hosts are connected.

If the device supports either secure ports or static ports, you can designate a secure/static port which becomes the equivalent of a Dead End VLAN. When a host is disabled either manually or by an alarm action, a message is sent to the device indicating that this MAC address has been disabled. The MAC address is placed in a list on the device which indicates it only has permission to use the port designated as secure or static. If the host connects on any other port, it cannot access anything.

Make sure that the port designated as static or secure is not accessible. If a disabled host were to connect to that port, it would have network access.

To use this feature you must configure the following:

FortiNAC

- In the Model Configuration for the device you must enable secure ports. See Model configuration on page 767 for instructions and Settings.
- When secure ports has been enabled, you must designate a port on the device as the secure or static port.
- This device must belong to the Physical Address Filtering group. This group is a default system group and should already exist. See Modify a group on page 841 for instructions on adding the device to the group.
- Membership in the Physical Address Filtering group may cause VLAN switching to occur. See Modify a group on page 841.

Device

The device itself may or may not require any additional configuration.

- **Alcatel**—Alcatel switches do not require any special configuration in order to support Physical Address Filtering.
- **3Com, Cisco, Vertical Horizon**—FortiNAC requires a secure port for each VLAN that is expected to participate in disabling hosts by physical address. Define Cisco and Vertical Horizon secure ports outside of FortiNAC through their respective command line interfaces or local management. Configure secure ports on 3Com switches by selecting Secure Port Management from the device-specific pull-down in the Topology tree.
- **Enterasys**—Enterasys switches do not require any special configuration in order to support Physical Address Filtering.
- **HP**—HP switches currently do not support Physical Address Filtering.
- **Nortel**—Nortel switches do not require any special configuration in order to support Physical Address Filtering.

Disable Hosts

- Hosts can be disabled manually from the Host View. See Enable or disable hosts on page 810.
- Hosts can also be disabled when an event is generated that triggers an alarm. The alarm must be configured to perform an alarm action that disables the host. For more information on alarm actions see Add or modify alarm mapping on page 892.

If you delete a disabled host, the entry for that host's MAC address remains on the switch as disabled. Another user logging in through that host will not be able to access the switch. Be sure to enable the host before you delete it.

Example of host MAC addresses on a secure port

When the secure or static ports feature is used, the MAC addresses of disabled hosts are sent to the device. The device stores these MAC addresses in a list.

The list shown below displays all disabled hosts written to port12 (secure port) on a Cisco 2950 switch.

```
sw_chellis_24#show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation Security Action
(Count)        (Count)      (Count)
--------------------------------------------------------------
Fa0/12          120             3             0              Shutdown
--------------------------------------------------------------
Total Addresses in System : 3
Max Addresses limit in System : 1024

sw_chellis_24#show port-security address
Secure Mac Address Table
---------------------------------------------------------------
Vlan    Mac Address       Type                Ports   Remaining Age
(mins)
----    -----------       ----                -----   -------------
20    0004.2353.2d19    SecureConfigured    Fa0/12      -
20    0009.5b83.e74c    SecureConfigured    Fa0/12      -
20    0009.5b89.0379    SecureConfigured    Fa0/12      -
---------------------------------------------------------------
Total Addresses in System : 3
Max Addresses limit in System : 1024
```

Secure port management

This option is not available for all devices. If the device supports Secure Ports the option appears in the right-click menu for the device.

To define/clear a Secure Port for a device:

1. Click **Network Devices > Topology**.
2. Right-click on the device and click **Secure Port Management**.
3. Click **Add**.
4. Click the port to be set as the secure port on the device.
5. Select the Group of hosts that will be given permission for this port if they are disabled.
6. Click **Add**.
7. The port and group are displayed in the Secure Port Management list.

Static port configuration

This option is not available for all devices. If the device supports Static Ports the option appears in the right-click menu for the device.

To configure a Static Port for a device:

1. Click **Network Devices > Topology**.
2. Right-click on the device and click **Static Port Configuration**.
3. Click the port to be set as the static port on the device.
4. To Add, select **Add Static Port** from the drop-down menu.
5. To Remove, select **Remove Static Port** from the drop-down menu.
6. Click **Apply**.

Ports view

When you select an item from the menu tree in the Topology view, a Ports tab displays in the right pane. This view shows all the ports within the customer, container or device selected and the status of each port. For example, if you select a container, the Ports tab displays all of the ports on all of the devices that reside inside the selected container. If you select a device, all of the ports for that device are displayed.

You can also view the adapters/hosts and port changes for a selected port by clicking Show Details Panel. This panel provides direct access to the information found in the Connection Details and Port Changes Views for the selected port, allowing you to quickly view and modify adapters that are connected to the port. See View connection details on page 781 and Port changes view on page 942 for information about the fields contained in these tabs.

Ports or interfaces are displayed in the order in which they appear in the interface table on a device. Depending on the device and its configuration, ports may not display in order numerically or alphabetically. When hosts are connected to a port, icons are displayed to indicate the type of host that is connected and its status. You can update the Ports view for the selected device.

When you select a supported wireless device from the menu tree, Ports and SSIDs tabs are displayed in the right pane. This view shows all of the SSIDs on the device, however, it does not show when hosts are connected. If an SSID has been removed from the device, it is displayed in red on the SSIDs tab. The configuration information for that SSID remains in the database until it is deleted manually. When FortiNAC resynchronizes with the device, all SSIDs that exist on the device are displayed. If an SSID was deleted from FortiNAC, but still exists on the device, it reappears during resynchronization. See SSID view on page 786.

See Icons on page 30 for additional information.

Settings

Field	Definition
Status	Connection status icons for each port. See Icons on page 30 for additional information on each icon.
Label	Internal ifname of the port.
Name	Default name displayed for the port is comprised of the sysName of the device, the ifName and, in curly braces, the ifAlias or Port Description. All of this information is read from the switch. For example, Cisco_2600 Fa/07 {Library Front Desk}, where Cisco_2600 is the system name of the device, Fa/07 is the ifName and {Library Front Desk} is the Port Description.
IP address	IP address of the device containing the port.
Interface ID	Internal ifIndex of the port.
Default VLAN	Default VLAN for the port read from the device.
Current VLAN	VLAN where the port has been placed based on the Network Access policy for the connected host or device .
Notes	User specified notes about the selected port. Notes are entered on the Port Properties dialog. See Port properties on page 784.
Device	Name of the device containing the port.
Connection State	Defines the state and type of device connected to this port. View the idon in the Status column for additional information. States include: • **All Uplinks**—Displays ports that have a connection status of any uplink type. • **Device**—Device is connected to this port. • **Disabled Phone**—Phone is connected and has been disabled. • **Disabled Registered Host**—Registered host is connected and has been disabled. • **Disabled Rogue Host**—Rogue host is connected and has been disabled. • **Disabled User**—User is connected and has been disabled. • **Learned Uplink**—Uplink mode has been set as Dynamic and a device that is modeled in FortiNAC is connected on the port. See Port uplink types on page 786 • **Multiple Hosts**—More than one host is connected on the port. • **Not Connected**—Nothing is connected to this port. • **Not Uplink**—Port is not an uplink. This is either because the Uplink Mode is dynamic and the conditions for FortiNAC to set it to an uplink have not been met, OR the mode has been set as Never Uplink. See Port uplink types on page 786 • **Phone**—An IP Phone is connected. • **Registered AtRisk Host**—Known host that has failed a scan or has been manually marked AtRisk is connected.

Field	Definition
	- **Registered Host**—Known host is connected. - **Rogue AtRisk Host**—Unregistered host that has failed a scan or has been manually marked AtRisk is connected. - **Rogue Host**—Unknown host is connected. - **Threshold Uplink**—Uplink mode has been set as Dynamic and FortiNAC has determined that the number of MAC addresses on the port exceeds the System Defined Uplink count. See Port uplink types on page 786 - **Unauthenticated Host**—Host that is registered but has not authenticated is connected. - **User**—Authenticated user is connected. - **User Defined Uplink**—Uplink Mode has been configured as Always Uplink. See Port uplink types on page 786 - **WAP Uplink**—Wireless Access Point is connected to the port causing port to be set as an uplink. See Port uplink types on page 786
Current CLI	Name of the CLI Configuration currently applied to the port.
Admin Status	Indicates whether the port has been administratively disabled or enabled.
Operational Status	Indicates whether a port is currently operational and connected to a device or not.
Last Modified By	User name of the last user to modify the port.
Last Modified Date	Date and time of the last modification to this port.
Right click options	
Show/Hide Details Panel	Shows/hides an additional panel showing adapters/hosts and port changes for the selected port. This information can also be found in the Connection Details and Port Changes Views.
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.
Connection Details	Displays connection details for the selected port. See View connection details on page 781.
Group Membership	Displays the Port Group Membership dialog which allows you to view and modify the groups in which this port is a member. See Group membership on page 784.
Port Changes	Opens the Port Changes View. See Port changes view on page 942.
Port Properties	Opens the Port Properties dialog for the selected port. See Port properties on page 784.

Field	Definition
Role Membership	Displays the list of roles in which the port is a member. See View role membership on page 761.
Select Device In Tree	Locates the selected device in the tree on the right and highlights it.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.
Show Events	Displays events for the selected port.

Update ports view

The Ports View for configured devices that have been added to the Topology tree does not initially contain the current host information for each port. FortiNAC must go out to the device and read the current host information. This is typically done automatically based on the polling options configured for the device, but you can also poll the device manually.

1. Click **Network Devices > Topology**.
2. Expand the container where the device is located.
3. Right-click the device and select **Polling > L2 (Hosts) Information**.

   FortiNAC reads the host information from the device and updates the Ports tab in the right pane. The Icons on page 30 contains descriptions of the icons shown in the Ports view.

View connection details

Connection Details displays information about the host connected on the selected port.The description will vary depending on the element connected. Status is represented by an icon. For a legend of status icons, see the Icons on page 30.

1. Click **Network Devices > Topology**.
2. Expand the container where the device is located.
3. Select a device.
4. In the Ports tab on the right, right-click on a port and select **Connection Details**. The connection details are displayed.
5. Click the icon to view the information for the host connected to the port. This takes you to the **Adapter Properties** window for this host. See Properties on page 801 for additional information.

Settings

Field	Description
Name	Name of the switch and port to which the host or device is connected.

Field	Description
Connected Elements	Number of interfaces connected to this port.
Devices	
Status	Displays one of several pingable icons indicating the type of host connected to this port. Pingables in the Devices table are managed only in the Topology View. See the Icons on page 30 for information on each device icon.
Description	A description of the connected device. This field may contain any one of the following: • Vendor Name • Hardware type • IP address
IP address	IP address of the device connected to this port.
Physical Address	MAC address of the device connected to this port.
Vendor Name	Vendor associated with the device's MAC address. Determined based on the Vendor OUI's stored in the FortiNAC database.
Hosts	
Status	Displays the Adapter icon for the selected connection. If the icon is green, the adapter is connected. Click on the icon to go to Adapter Properties. See Properties on page 821.
Host Status	Displays the Host icon for the selected connection. Host state is indicated by the icon displayed. See the Icons on page 30 for information on each state. Click on the icon to go to Host Properties. See Properties on page 801.
IP address	IP address of the adapter connected to this port.
Physical Address	MAC address of the device connected to this port.
Vendor Name	Vendor associated with the host's MAC address. Determined based on the Vendor OUI's stored in the FortiNAC database.
Host Name	Name of the connected host.
Registered To	User ID and name of the user to whom this host is registered. If a host is registered by host name, this field will be blank.
Logged On User	User ID and name of the user that is currently logged onto this host.

Add ports to groups

Ports on your network can belong to groups. Group membership can be viewed from the Groups View window or by selecting the port in the Topology View.

1. Click **Network Devices > Topology**.
2. Expand the container where the device is located.
3. Select a device.
4. In the **Ports** tab on the right, use Ctrl-click or Shift-click to select the records you wish to add to the group.
5. Right-click on the ports and select **Add Ports To Groups**.

6. To add the port to a group, click the box next to the group name and then click **OK**.
7. To create a missing group:
   a. Click the **Create Group** button.
   b. Enter a group name.
   c. If the new group should be a sub-group of an existing group, enable the **Parent Group** option and select the appropriate group from the list.
   d. **Description** is optional.
   e. Click **OK** to save the new group.
8. Click **OK** to save your group selections.

If an item is placed in a subgroup, it can only be removed when viewing the membership of that subgroup. It cannot be removed from the parent group containing the subgroup.

For example, the L2 Network Devices Group contains the Wired Devices and Wireless Devices subgroups. The Wired Devices subgroup contains four 3COM switches. The Wireless Devices subgroup contains two Cisco switches. The L2 Network Devices Group membership list shows all six switches, but to remove one of the 3COM switches you must go to the Wired Devices membership list.

Modify multiple ports

You can modify multiple ports on your network at the same time.

1. Click **Network Devices > Topology**.
2. Expand the container where the device is located.
3. Select a device.
4. In the **Ports** tab on the right, use Ctrl-click or Shift-click to select the records you wish to modify.
5. Right-click on the ports and select **Modify Properties**.
6. Select the **Admin Status** for the ports.
7. Select the **Uplink Mode** for the ports.

Mode	Description
Dynamic	Allows FortiNAC to set the port as an uplink when the threshold for connections is reached. If the MAC address on the port is that of a switch that is modeled in FortiNAC Topology view, the port is set as an Uplink.
Clear	Check this box to clear all dynamic uplink settings for this port. Settings are cleared when you click **Apply**. Once the settings are cleared the check mark is removed from the Clear box by FortiNAC.
Always Uplink	Sets the port to always be an uplink.
Never Uplink	Sets the port to never be an uplink.

8. Select the check boxes next to **Current VLAN** and **Default VLAN** and enter the values.
9. Click **OK**.

Group membership

Ports on your network can belong to groups. Group membership can be viewed from the Groups View window or by selecting the port in the Topology View.

1. Click **Network Devices > Topology**.
2. Expand the container where the device is located.
3. Select a device.
4. In the **Ports** tab on the right, right-click on a port and select **Group Membership**.
5. Check marks indicate that the port is a member of the group.
6. To add the port to a group, click the box next to the group name and then click **OK**.
7. To remove the port from a group, click to uncheck the box next to the group name and then click **OK**.
8. To create a missing group:
   a. Click the **Create Group** button.
   b. Enter a group name.
   c. If the new group should be a sub-group of an existing group, enable the **Parent Group** option and select the appropriate group from the list.
   d. **Description** is optional.
   e. Click **OK** to save the new group.
9. Click **OK** to save your group selections.

Remove ports from multiple groups

1. Click **Network Devices > Topology**.
2. Expand the container where the device is located.
3. Select a device.
4. In the **Ports** tab on the right, use Ctrl-click or Shift-click to select the records you wish to modify.
5. Right-click on the ports and select **Remove Ports from Groups**.
6. Select the check box for each group you wish to remove the ports from.
7. Click **OK**.

Port properties

Use the Port Properties window to view and configure the default Network Access settings for the selected port.

1. Click **Network Devices > Topology**.
2. Expand the container where the device is located.
3. Select a device.
4. In the Ports tab on the right, right-click on a port and select **Port Properties**. The **Port Properties** window displays.
5. The **Port** option is displayed.
6. Items that may be edited are:
   - Port Name
   - Admin Status turned On or Off

- Uplink Mode
- Current VLAN
- Default VLAN
- Notes

7. Modify the **Port Name**. The default name displayed for the port is comprised of the sysName of the device, the ifName and, in curly braces, the ifAlias or Port Description. All of this information is read from the switch. For example, Cisco_2600 Fa/07 {Library Front Desk}, where Cisco_2600 is the system name of the device, Fa/07 is the ifName and {Library Front Desk} is the Port Description.

Use only letters, numbers and hyphens (-) when creating port descriptions. Other characters, such as #, may prevent FortiNAC from communicating properly with the device.

8. To set Admin Status, select **On** or **Off**.
9. The **Connection State** of the port is displayed. See Ports view on page 778 for a list of connection states.
10. Select an **Uplink Mode** for the port.

Mode	Description
Dynamic	Allows FortiNAC to set the port as an uplink when the threshold for connections is reached. If the MAC address on the port is that of a switch that is modeled in FortiNAC Topology view, the port is set as an Uplink.
Clear	Check this box to clear all dynamic uplink settings for this port. Settings are cleared when you click **Apply**. Once the settings are cleared the check mark is removed from the Clear box by FortiNAC.
Always Uplink	Sets the port to always be an uplink.
Never Uplink	Sets the port to never be an uplink.

11. Enter the value for the **Current VLAN**.
12. Enter the value for the **Default VLAN**.
13. The **CLI Configuration** section displays the most recent CLI configuration that has been applied to this port.
14. Click **Port Changes** if you wish to display the **Port Changes View**.
15. Click **Group Membership** if you wish to display the **Port Group Membership** dialog to view and modify the groups in which this port is a member.

The **Group Membership** button only appears if the user has permission to view group membership. If the user has permission to view, but not modify group membership, the button appears but the user cannot save changes to Group Membership.

16. Click **OK** to save.

If you changed the Current VLAN, a warning message appears. Click Yes to confirm that you wish to modify the Current VLAN and save the Port Properties.

Port uplink types

Uplinks disable management of the port, which means access is no longer controlled from the port.

Learned Uplink—The Uplink mode has been set as Dynamic and a device that is modeled in FortiNAC is connected on the port. All hosts read on this port are ignored.

Threshold Uplink—The Uplink mode has been set as Dynamic and FortiNAC has determined that the number of MAC addresses on the port exceeds the System Defined Uplink count. All hosts read on this port are ignored.

User Defined Uplink—The Uplink Mode has been configured as Always Uplink. These are ports the user knows are uplinks, but will not be converted to a Learned or Threshold Uplink. All hosts read on this port are ignored.

WAP Uplink—A Wireless Access Point (WAP) is connected to the port, causing the port to be set as an uplink. These access points represent controller-managed devices.

A WAP Uplink controls access from this port for the AP only. The port is managed based on the physical address of the AP. Port management for all other hosts is disabled.

After an L2 Poll, the Uplink status is removed from all WAP uplinks when the MAC address for the AP is disconnected from the port.

SSID view

When you select a supported wireless device from the menu tree in the Topology View, Ports and SSIDs tabs are displayed in the right pane. This view shows all of the SSIDs on the device, however, it does not show when hosts are connected. If an SSID has been removed from the device, it is displayed in red on the SSIDs tab. The configuration information for that SSID remains in the database until it is deleted manually. When FortiNAC resynchronizes with the device, all SSIDs that exist on the device are displayed. If an SSID was deleted from FortiNAC, but still exists on the device, it reappears during resynchronization.

FortiNAC does not display SSIDs for all wireless devices. Refer to WLAN management on page 973 and for additional information.

See Icons on page 30 for additional information. See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.

Settings

Field	Definition
Add Filter drop-down list	Allows you to select a field from the current view to filter information. Select the field from the drop-down list, and then enter the information you wish to filter.
Update Button	Click to update the data in the table.
Table columns	
Name	The SSID name.

Field	Definition
Container	Container where the device that is broadcasting the SSID resides. Containers are used to group devices.
Device	Name of the device that is broadcasting the SSID.
RADIUS	Indicates whether the SSID inherits the RADIUS server settings from its parent device, or if the settings are customized in the SSID Configuration.
Network Access	Indicates whether the SSID inherits the Network Access or VLAN/Role settings of its parent device, or if the settings are customized in the SSID Configuration.
Primary RADIUS Server	The RADIUS server used for authenticating users connecting to the network through this SSID. See RADIUS on page 102 for information on configuring your RADIUS Servers.
Secondary RADIUS Server	If the Primary RADIUS server fails to respond, this RADIUS server is used for authenticating users connecting to the network until the Primary RADIUS Server responds.
Default	The Default VLAN value is stored in the FortiNAC database and is used when the VLAN is not determined by another method, such as a Network Access Policy. Typically, if a VLAN is specified as the Default, it is the VLAN used for "normal" or "production" network access. It will be used for all the untagged (non-uplink) ports on the device.
Dead End	The dead end VLAN for this SSID. Isolates disabled hosts with limited or no network connectivity from the production network.
Registration	The registration VLAN for this SSID. Isolates unregistered hosts from the production network during host registration.
Quarantine	The quarantine VLAN for this SSID. Isolates hosts from the production network who pose a security risk because they failed a scan defined in an Endpoint Compliance Policy.
Authentication	The authentication VLAN for this device. Isolates registered hosts from the Production network during user authentication.
Right click options	
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.
Delete	Deletes the selected SSID.
Group Membership	Displays the Port Group Membership dialog which allows you to view and modify the groups in which this port is a member. See Group membership on page 784.
SSID Configuration	Opens the SSID configuration on page 788 window. If multiple SSIDs are selected simultaneously, the Modify SSID Configuration window opens.
Select Device In Tree	Locates the selected device in the tree on the right and highlights it.

Field	Definition
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.

SSID configuration

SSIDs on some wireless devices can be configured with VLAN/Role settings that are different than those of the parent device. This option allows you to provide different treatment for each SSID. For example, you can have an SSID that provides only Internet access for guests and a separate more secure SSID that requires authentication for staff.

In an environment where there are multiple SSIDs that have the same name, FortiNAC cannot manage those SSIDs individually. Make sure that SSIDs do not have the same name.

1. Click **Network Devices > Topology**.
2. Expand the container where the wireless device is located.
3. Select a device.
4. In the right pane, select the **SSID tab**.
5. Right-click on the SSID and select **SSID Configuration**. To modify multiple SSIDs simultaneously, see Modify multiple SSIDs on page 790.
6. Use the table below to configure the SSID.
7. Click **OK** to save.

Settings

Settings	Description
RADIUS	
Use Inherited RADIUS Server Definitions from Device	If enabled, the SSID inherits the RADIUS server settings of its parent device.
Use Custom Settings	If enabled, allows you to set the default Primary and Secondary RADIUS servers to the servers indicated in parentheses and set the RADIUS Secret.
Primary RADIUS Server	The RADIUS server used for authenticating users connecting to the network through this SSID. See RADIUS on page 102 for information on configuring your RADIUS Servers.

Settings	Description
Secondary RADIUS Server	If the Primary RADIUS server fails to respond, this RADIUS server is used for authenticating users connecting to the network until the Primary RADIUS Server responds.
RADIUS Secret	The Secret used for RADIUS authentication. Click the field to add or modify the RADIUS Secret. The RADIUS Secret used must be exactly the same on the wireless device, on the RADIUS server and in the FortiNAC software under RADIUS Settings and Model Configuration.
Show/Hide Button	Allows you to display or hide the RADIUS secret.
Network access	
Use Inherited Network Access Policy from Device	If enabled, the SSID inherits the Network Access or VLAN/Role settings of its parent device.
Use Custom Settings	If enabled, allows you to customize the Network Access Policy instead of using the inherited policy from the device.
Access Enforcement	When Use Custom Settings is enabled, this set of drop-down menus works in conjunction with the Host States listed below to determine treatment for hosts when no VLAN/Role value is supplied or when access control is being enforced. Options include: • **Deny** — Host will be denied access to the network when it is in this state. For example, if the host is not registered and Registration is set to Deny, the host connection will be rejected. Endpoints that have been denied access may continuously request access which can unnecessarily consume system resources. • **Bypass** — Host will be allowed access to the network when it is in this state. The host will be placed on the default VLAN/Role configured on the device for this port or SSID. For example, if Quarantine is set to Bypass, hosts that fail a scan and would normally be placed in Quarantine are placed in the default VLAN/Role on the device. • **Enforce** — Indicates that the host will be placed in the VLAN/Role specified in the Access Value column for this state.
Access Value	VLAN/Role where a host in this state should be placed when it connects to the network. If Enforce is selected in the Access Enforcement field you must enter a value in the Access Value field.
Host state	
Default	The Default VLAN value is stored in the FortiNAC database and is used when the VLAN is not determined by another method, such as a Network Access Policy.

Settings	Description
	Typically, if a VLAN is specified as the Default, it is the VLAN used for "normal" or "production" network access. It will be used for all the untagged (non-uplink) ports on the device. Select None to use the default VLAN/Role configured on the device.
Dead End	The dead end VLAN for this SSID. Isolates disabled hosts with limited or no network connectivity from the production network.
Registration	The registration VLAN for this SSID. Isolates unregistered hosts from the production network during host registration.
Quarantine	The quarantine VLAN for this SSID. Isolates hosts from the production network who pose a security risk because they failed a scan defined in an Endpoint Compliance Policy.
Authentication	The authentication VLAN for this device. Isolates registered hosts from the Production network during user authentication.

Modify multiple SSIDs

1. Click **Network Devices > Topology**.
2. Do one of the following:
   - Select the top level container.
   - Select a container where the wireless device is located.
   - Expand the container where the wireless device is located and select a device.
3. In the right pane, select the **SSID** tab.
4. Hold CTRL or SHIFT and click to select multiple SSIDs.
5. Right-click and select **SSID Configuration**.
6. Select **RADIUS**, **Network Access**, or both.
7. See SSID configuration on page 788 for the settings to configure the SSIDs.

   If you select an Access Value that is not supported on all devices associated to the selected SSIDs, a link appears that allows you to view which device or devices do not support the value. Changes to the SSID configuration will only be saved for the devices that support the selected Access Values. The SSID Configuration for the device or devices that do not support the selected Access Values will remain unchanged.

8. Click **OK** to save.

Hosts, adapters, and applications

Hosts are devices that require network services and can be associated with a user, such as a PC or a gaming device. Adapters are the network interfaces on these devices. There are other types of hosts not associated with users, such as IP phones or printers. The Hosts, Adapters, and Users views provide an individual menu option for each, but uses a shared search capability to simplify management of hosts, adapters and their associated users on your network. Regardless of the menu item selected and displayed, the navigation and search or filter options are the same.

Applications that are contained on a host are scanned when the host is connected to the network, and appear in the Applications View. The list of applications is continuously updated as hosts are scanned.

The Quick Search field at the top of the Host View and Adapter View windows allows you to search based on an IP address, MAC Address, User ID, User First and Last Name or Host Name. Wild card searches, such as 192.168.10.1* can be used. The drop-down arrow at the end of the Search field allows you to set up a filter and use it once or save it for future use. See Search and filter options on page 18 for additional information.

The mouse-over feature displays a pop-up window or tool tip when you place the mouse over any icon in the Status column. This tool tip contains detailed data about the user, host or adapter.

Add or remove columns from the table by clicking the Configuration button and selecting your options from the Settings window. The Settings window also controls the data included on in tool tips displayed when you hover over any icon on the left side of the view.

USB/Thunderbolt external Ethernet adapters

The following information explains how FortiNAC manages records of hosts using external Ethernet adapters.

Thunderbolt adapters and docking stations

Thunderbolt Ethernet adapters are similar to USB Ethernet dongle adapters, but use the Thunderbolt connector.

Thunderbolt 2 docking stations have two Thunderbolt ports and one Ethernet port. This allows two computers to connect to the docking station using a Thunderbolt connection, but only one computer is able to have network access. The first computer to connect to the docking station is considered the "root user" and is associated to the Ethernet port. If a second computer connects to the docking station, it will not be able to access the network unless the first computer disconnects from the docking station.

FortiNAC treats the records of hosts connecting to this type of docking station (as well as the adapters) in the same manner as hosts using USB Ethernet dongle adapters.

Host record management when external adapters are moved between hosts

The Persistent Agent provides information regarding adapters enabled on the host. This allows FortiNAC to associate multiple adapters to the host record (not just the one connected during host registration). In conjunction with the

Persistent Agent, FortiNAC is able to identify when an external adapter is moved from one host to another and update host records accordingly.

Hosts must have Persistent Agent 2.2 and above installed and be communicating with FortiNAC before moving the adapter. This will prevent the second host from inheriting the network access of the original host. In this case, the second host would appear as the original host and would not be detected.

If a host record contains only one adapter and the adapter is removed from the host, the host record is removed.

Adapters cannot be successfully moved between hosts using the Dissolvable Agent.

Adapter is moved between registered hosts

Example 1: Registered Host A (with Persistent Agent) to Registered Host B (with Persistent Agent):

Once the adapter is removed from Registered Host A and connected to Registered Host B, the Persistent Agent on Registered Host B will notify FortiNAC of the new adapter. FortiNAC will then remove the adapter from Registered Host A’s record and add it to Registered Host B’s record. All other adapters associated with Registered Host A remain unaffected.

Example 2: Registered Host A (with Persistent Agent) to Registered Host B (without Persistent Agent):

When the adapter is disconnected from Registered Host A, FortiNAC is notified that the adapter is offline with Registered Host A. Since Registered Host B has no way to announce what adapters it owns, the external adapter will remain associated with Host A’s record. If the adapter is then connected to Registered Host B and FortiNAC sees it online, Registered Host B will be assigned whatever network access policy matches for Registered Host A’s record, and the adapter will be shown as online for Registered Host A.

Adapter is moved from a registered host to a rogue

Example 1: Registered Host A (with Persistent Agent) to Rogue Host B (with Persistent Agent):

Once the adapter is removed from Registered Host A and connected to Rogue Host B, the Persistent Agent on Rogue Host B will notify FortiNAC of all adapters (including the new external adapter), and the external adapter will be removed from Host A's host record.

All other adapters associated with Registered Host A remain unaffected.

Example 2: Registered Host A (with Persistent Agent) to Rogue Host B (without Persistent Agent):

When the adapter is disconnected from Registered Host A, FortiNAC is notified that the adapter is offline with Registered Host A. Since Rogue Host B has no way to announce what adapters it owns, the external adapter will remain associated with Registered Host A’s record. If the adapter is then connected to Rogue Host B and FortiNAC sees it online, Rogue Host B will be assigned whatever network access policy matches for Registered Host A's record, and the adapter will be shown as online for Registered Host A.

Host view

The Host View is part of a window that includes menu options for Users, Adapters Hosts, and Applications. Use the Host View to add, delete, modify, locate and manage hosts connected to your network.

The relationship between Users, Hosts and Adapters is hierarchical. Users own or are associated with one or more hosts. Hosts contain one or more Adapters or network interfaces that connect to the network. By displaying User, Host and Adapter data in a group, the relationships are maintained. For example, if you search for a host with IP address 192.168.5.105, you are in fact searching for the IP address of the adapter on that host. When the search displays the host, you can click on the Adapters option, the search is automatically re-run and you see the adapter itself. If there is an associated user, you can click on the Users option to re-run the search and see the associated user.

Click on the arrow in the left column to drill-down and display the adapters and their connection status on this host. Hover over the icon in the Status column to display a tooltip with detailed information about this host. For Settings see Settings on page 795. For information on Status icons see the Icons on page 30.

The Displayed and Total fields in the title bar represent the number of records displayed versus the total number of records in the database.

If a host fails one scan and is denied access to the network, but passes another scan at a different time or location and is allowed access to the network, the host will still be marked At Risk because it failed the first scan. The host will continue to be marked At Risk until actions are taken to pass the failed scan.

Navigation, menus, options, and buttons

For information on selecting columns displayed in the Host View Some menu options are not available for all hosts. Options may vary depending on host state.

Field	Definition
Navigation	Across the top of the Hosts View are navigation tools that allow you to quickly move through large numbers of records. These tools include the following: • **<<first**—Takes you to the first page of records. • **<prev**—Takes you back one page. • **Page Number**—Current page number is displayed. • **next>**—Takes you forward one page. • **last>>**—Takes you to the last page. • **Drop-down Box**—Allows you to select the number of records to be displayed on each page.
Quick Search	Enter a single piece of data to quickly display a list of hosts. Search options include: IP address, MAC address, Host Name, User Name and User ID. Drop-down arrow on the right is used to create and use Custom Filters.

Field	Definition
	If you are doing a wild card search for a MAC address you must include colons as separators, such as, 00:B6:5*. Without the separators the search option cannot distinguish that it is a MAC address. When Quick Search is enabled, the word Search appears before the search field. When a custom filter is enabled, Edit appears before the search field.
Right click options	
Add Hosts To Groups	Add the selected host(s) to one or more group(s). See Add hosts to groups on page 811.
Delete Hosts	Deletes the selected host(s) from the database. Deleting a host from the Host View that is also displayed in the Topology View, removes that host from both views. Deleting a host from the Topology View does not delete it from the Host View. See Delete a host on page 809.
Disable Hosts	Disables the selected host(s) preventing them from accessing the network. See Enable or disable hosts on page 810.
Enable Hosts	Enables the selected host(s) if they were previously disabled. Restores network access.
Group Membership	Displays groups in which the selected host is a member. See Group membership on page 811.
Host Health	Opens a dialog with the contents of the Host Health tab from the Host Properties view. See Host health and scanning on page 803.
Host Applications	Opens the Applications window for the selected host and lists installed applications. See Application inventory on page 805.
Host Properties	Opens the Properties window for the selected host. See Properties on page 801.
Modify Host	Opens the Modify Host window. See Add or modify a host on page 807.
Policy Details	Opens the Policy Details window and displays the policies that would apply to the selected host at this time, such as Endpoint Compliance Policies, Network Access Policies, Portal Policies or Supplicant Policies. See Policy details on page 381.
Register As Device	Changes the selected host to a device in the FortiNAC database. See Register a host as a device on page 812.
Register As Host	Changes the selected Rogue host to a registered host. Displays the Modify Host window. See Add or modify a host on page 807.
Run Agentless Scanner	Manually run an Agentless Scanner for selected hosts. Hosts must be Windows Hosts, members of the domain, have an IP address and be connected to the network.
Scan Hosts	Evaluates the selected host with the scan that applies to the host at that moment. The host must be online and must have a Persistent Agent. If the host is online but does not have a Persistent Agent, it is marked "at risk" for the Scan that most closely matches the host at the moment.

Field	Definition
Send Message	Sends a text box message to the selected host(s). The host must be using the Persistent Agent or Mobile Agent. See Send a message to a host on page 814.
Set Host Expiration	Launches a tool to set the date and time for the selected host(s) to age out of the database. See Set host expiration date on page 813.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.
Set Host Role	Assigns a role to the selected host.
Show Events	Displays the events for the selected host.
Update Persistent Agent	Opens a dialog that allows you to update the Persistent Agent for the selected host.
Go To Logged On User(s)	Opens the Users tab and displays the users currently logged onto the selected hosts. The logged on user may not be the registered user for the selected host.
Set Logged On User Expiration	Launches a tool to set the date and time for the user currently logged on to the selected host to age out of the database. See Set user expiration date on page 655.
Set Logged On User Role	Assigns a role to the user currently logged on to the selected host. See Role management on page 553.
Go To Registered User(s)	Opens the Users tab and displays the registered users for the selected hosts.
Set Registered User Expiration	Launches a tool to set the date and time for the registered user for the selected host to age out of the database. See Set user expiration date on page 655.
Set Registered User Role	Assigns a role to the registered user for the selected host. See Role management on page 553.
Collapse All	Collapses all host records that have been expanded.
Expand Selected	Expands selected host records to display adapter information.
Buttons	
Import/Export	Use Import and Export options to import hosts into the database from a CSV file or export a list of selected hosts to CSV, Excel, PDF or RTF formats. See Import hosts, users or devices on page 696 or Export data on page 710.
Options	The Options button displays the same series of menu picks displayed when the right-mouse button is clicked on a selected host.

Settings

The fields listed in the table below are displayed in columns on the Host View based on the selections you make in the Settings window. These fields are also used in Custom Filters to search for hosts. See Search and filter options on page

18. Additional fields that can be displayed on the Host View are fields for the user associated with the selected host. See Search settings on page 646.

You may not have access to all of the fields listed in this table. Access depends on the type of license key installed and which features are enabled in that license.

Field	Definition
Agent Platform	Distinguishes between Windows, macOS, iOS, and Mobile Agent.
Agent Version	The version number of the Persistent, Mobile or Dissolvable Agent installed on the host. "None" is displayed if the Host has registered or been rescanned with a Dissolvable Agent version that is prior to V 2.1.0.X or if this Host is a type set to by-pass the agent scan in the Endpoint Compliance Configuration.
Allowed Hosts	The number of hosts that can be associated with or registered to this user and connect to the network. There are two ways to reach this total. If the host is scanned by an agent or if adapters have been manually associated with hosts, then a single host with up to five adapters counts as one host. If the host is not scanned by an agent or if the adapters have not been associated with specific hosts, then each adapter is counted individually as a host. In this scenario one host with two network adapters would be counted as two hosts. Numbers entered in this field override the default setting in **System > Settings > Network Device**. Blank indicates that the default is used. See Network device on page 130. If an administrator exceeds the number of hosts when registering a host to a user, a warning message is displayed indicating that the number of Allowed Hosts has been incremented and the additional hosts are registered to the user.
Applications	Applications running on the host. Categories of applications include: Anti-virus, Hotfixes and Operating System.
Asset Tag	The Asset Tag of the host that is populated by the agent when the asset tag is readable by the agent. The asset tag is derived from the System Management BIOS (SMBIOS).
Authenticated	Indicates whether the host is authenticated.
Delete Hosts When User Expires	If set to Yes, hosts registered to the user are deleted when the user ages out of the database. To modify click **Set**.
Device Type	If the Host is a pingable device that is being managed in Hosts view, this field indicates the specific type of device. The list includes: • Alarm System • Android • Apple iOS

Field	Definition
	• Camera • Card Reader • Cash Register • Dialup Server • Environmental Control • Gaming Device • Generic Monitoring System • Health Care Device • Hub • IP Phone • IPS / IDS • Linux • Mobile Device • Network • PBX • Pingable • Printer • Registered Host • Server • StealthWatch • Top Layer IPS • Unix • UPS • Vending Machine • VPN • Windows • Wireless Access Point • macOS
Container (Topology)	Indicates whether this host is also displayed in the Topology View and shows the Container in which it is stored.
First Name	User's first name.
Last Name	User's last name.
Email	User's email address.
Address	User's physical address.
City	User's city.
State	User's state.
Postal Code	User's postal code.
Phone	User's phone number.
Mobile Phone	User's cell phone number.

Field	Definition
Mobile Provider	User's mobile provider.
Notes	Notes entered by the administrator. If this user registered as a guest, this section also contains information gathered at registration that does not have designated database fields, such as Person Visiting or Reason for Visit.
Include IP Phones	Appears when any option except Rogue is in the Host Type drop-down list. When selected, hosts that are IP Phones are included in the Host view.
Hardware Type	Type of Hardware, such as a PC.
Created Date	Date the Host record was created in the database. Options include Last, Between, Before, and After.
Expiration Date	Controls the number of days a Host is authorized on the network. Options include Next, Before, After, Between, Never, and None. Host is deleted from the database when the date specified here has passed. The date is automatically calculated based on the information entered when Aging is configured. See Aging out host or user records on page 823.
Inactivity Date	Controls the number of days a Host is authorized on the network. Options include Next, Before, After, Between, Never, and None. Host is deleted from the database when the date specified here has passed. The date is continuously recalculated based on the information entered in the Days Inactive field. See Aging out host or user records on page 823.
Last Connected	Date and time of the last communication with the Host. Options include Last, Before, After, Between, and Never.
Host Name	Name of the host.
Host Notes	Notes about this host.
Host Role	Role assigned to the Host. Roles are attributes of hosts and can be used as filters in a User/Host Profile. See Role management on page 553.
Host Security & Access Value	Value that typically comes from a field in the directory, but can be added manually. This value groups users and can be used as a filter in a User/Host Profile, which in turn are used to assign Endpoint Compliance Policies, Network Access Policies and Supplicant EasyConnect Policies. The data in this field could be a department name, a type of user, a graduation class, a location or anything that distinguishes a group of users. The access value is inherited from the user associated with this host.
Last Modified By	User name of the last user to modify the host.
Last Modified Date	Date and time of the last modification to this host.
Logged On User	Name of the user currently logged into the Host.
Managed By MDM	Host is managed by a Mobile Device Management system and data was retrieved from that system for registration.

Field	Definition
MDM Compliant	Host is compliant with MDM policies. This data is retrieved directly from the MDM system.
MDM Compromised	MDM system has found this host to be compromised, such as Jailbroken or Rooted.
MDM Data Encryption	MDM system has detected that the host is using data protection.
MDM Passcode	MDM system has detected that the host is locked by a passcode when not in use.
Operating System	Host operating system, such as macOS or Windows XP. This is usually determined based on the DHCP fingerprint of the device or is returned by an agent.
Passed Tests	Shows passed scans.
Persistent Agent	Indicates whether the Persistent Agent has been seen on this Host before.
Persistent Agent Communicating	Indicates whether or not the agent is currently communicating.
Registered To	User ID of the user to which this host is registered.
Serial Number	Serial number on the host.
Status	Current or last known status is indicated by an icon. See Icons on page 30. Hover over the icon to display additional details about this Host in a tool tip. • **Connected** — Indicates whether host is online or offline. • **Access** — Indicates whether host is enabled or disabled. • **Security** — Indicates whether host is safe, at risk or pending at risk. • **Authentication** — Indicates whether or not the user associated with this host has been authenticated. When searching for a host based on Security, search results for Safe include Pending at Risk hosts. Those hosts are a sub-set of Safe hosts. Search results for Pending at Risk do not include Safe hosts.
System UUID	The universal unique identifier used to identify the host.
Title	User's title, this could be a form of address or their title within the organization.
Type	Select the type of host. Host types include: • **Rogue** — Unknown device that has connected to the network. • **Registered Host** — Device that is registered to a known user. • **Registered Device** — Device that is registered by its own Host Name and is not associated with a single user, such as a library computer or a shared workstation. • **Registered Host or Device** — Both devices that are registered to users and devices that are registered by host name. • **Registered Device In Host View** — Pingable device not associated with a user that is managed in the Host View, such as a printer. • **Registered Device In Host and Topology View** — Pingable device not associated with a user that displays in both the Host and Topology Views.
User Created	Indicates when this record was created in the database.

Field	Definition
User Expires	Controls the number of days a user is authorized on the network. User is deleted from the database when the date specified here has passed. The date is automatically calculated based on the information entered in the Set User Expiration date window. To modify click **Set**. See Set user expiration date on page 655 for additional information.
User Inactivity Date	Controls the number of days a user is authorized on the network. User is deleted from the database when the date specified here has passed. The date is continuously recalculated based on the number of days entered for Inactivity Limit. For example, if the user logs off the network on August 1st and Inactivity Limit is set to 2 days, the Inactivity Date becomes August 3rd. If on August 2nd the user logs back in again, the Inactivity Date is blank until the next time he logs out. Then the value is recalculated again. To modify click Set.
User Inactivity Limit	Number of days the user must remain continuously inactive to be removed from the database. See Aging out host or user records on page 823.
User Notes	Notes entered by the administrator. If this user registered as a guest, this section also contains information gathered at registration that does not have designated database fields, such as Person Visiting or Reason for Visit.
User Role	Role assigned to the user. Roles are attributes of users that can be used as filters in User/Host Profiles. See Role management on page 553.
User Security And Access Value	Value that typically comes from a field in the directory, but can be added manually. This value can be used as a filter to determine which policy to use when scanning a user's computer. The data in this field could be a department name, a type of user, a graduation class, a location or anything that distinguishes a group of users.
VPN Client	Indicates whether the host connects to the network using a VPN connection.
Vulnerability Last Scanned	Lets you filter hosts by defining the time/date when Vulnerability scan results were last processed for the host.
Vulnerability Scan Status	Lets you display hosts that passed or failed the Vulnerability Scan, or were not scanned.

Drill-down settings

Use the arrow in the far left column of the Host View to expand a host and view adapter details. Expand or collapse multiple hosts by selecting them and using the right - mouse button or Options button. All adapters associated with a host are contained within the expanded section of the window. Adapters on the same host are considered siblings.

To copy an IP address or Physical Address, click on the address to highlight it. Press Ctrl+C to copy it.

Settings

Field	Definition
Status	Status of the adapter. Options are Online or Offline and Enabled or Disabled. See Icons on page 30.
IP address	IP address assigned to the adapter. If the adapter is offline, this is the last known IP address. Supports both IPv4 and IPv6 addresses.
Physical Address	MAC address of the adapter.
Media Type	Indicates whether the adapter is wired or wireless.
Location	The switch and port where the adapter last connected.
Actions	Use the action icons to do the following: • Enable/Disable adapter • Access Adapter Properties • Access Port Properties for the port where the adapter last connected • Go to the Adapters tab and display the adapter for this host

Properties

The Host Properties view provides access to detailed information about a single host. From this view you can access the associated user's properties by clicking on the User option in the menu on the left or the associated adapter's by clicking on the adapter's physical address displayed in the Adapters tab at the bottom of the window.

1. Select **Hosts > Host View**.
2. Search for the appropriate host.
3. Select the host and either right-click or click the **Options** button.
4. From the menu select **Host Properties**.

Settings

Field	Definition
General	
Host Name	Name of the host.
Hardware Type	Type of host such as workstation.
Operating System	Operating system installed on the host. Only hosts with a valid operating system can be rescanned. Valid operating systems are Windows, Mac, and Linux.
Serial Number	Serial number of the host.
Host Status	Radio buttons indicating whether the host is Enabled or Disabled. To enable or disable the host, click the appropriate button and then click Apply.
Time	

Field	Definition
Created	Indicates when this host record was created in the database. Options include Before, After, and Between.
Expiration Date	Controls the number of days a host is authorized on the network. Host is deleted from the database when the date specified here has passed. Options include Before, After, Between, Never, and None. If Never is displayed, this indicates that the host will not age out of the database. To modify click Set. See Set host expiration date on page 813.
Inactivity Date	Controls the number of days a host is authorized on the network. Host is deleted from the database when the date specified here has passed. Options include Before, After, Between, Never, and None. The date is continuously recalculated based on the number of days entered for Inactivity Limit. For example, if the host logs off the network on August 1st and Inactivity Limit is set to 2 days, the Inactivity Date becomes August 3rd. If on August 2nd the host logs back in again, the Inactivity Date is blank until the next time it logs out. Then the value is recalculated again. To modify click Set.
Inactivity Limit	Number of days the host must remain continuously inactive to be removed from the database. See Aging out host or user records on page 823.
Last Connected	Last time the host was heard on the network. Options include Before, After, Between, and Never.
Policy Agent/access	
Role	Role assigned to the host. Use the drop-down list to select a new role.
Agent Version	The version number of the Persistent or Dissolvable Agent installed on the host. "None" is displayed if the host has registered or been rescanned with a Dissolvable Agent version that is prior to V 2.1.0.X or if this host is part of a group with an Endpoint Compliance Policy set to by-pass the agent scan.
Update Button	Button only displays if the Persistent Agent is installed. Allows you to update this host to a different version of the Persistent Agent.
Security And Access Attribute Value	The **value** of the attribute that can be used as a filter in User/Host Profiles. Data for this field can come from a guest template, can be entered automatically from an LDAP Directory based on attribute mappings or manually by typing a value in this field. If entered from a directory, the data is copied from the user record of the associated user. For example, if you have a policy for staff and a separate policy for executives, you could enter the word **staff** for each staff member and **executive** for each member of the executive group. Enter a matching word on the appropriate User/Host Profile to match the host to an Endpoint Compliance or Network Access Policy. See Policies on page 377.
Tabs	

Field	Definition
Adapters	Displays a list of adapters on this host by MAC address. Click on a MAC address to open the Adapter Properties.
Applications	Displays a list of applications installed on the device. This information is provided by the agent. Typically includes Anti-virus, Hotfixes and operating system. This information is updated with each successful scan.
Notes	Notes entered by the administrator. If this host is the registered host for a guest, this section also contains information gathered at registration that does not have designated database fields, such as Person Visiting or Reason for Visit.
Health	Lists all the Scans and System scripts, and Administrative states for which the host has been scanned or had applied. Each scan the host is eligible for is shown along with the Name, Status, and Action. Click **Show History** for short-term historical data. See Host health and scanning on page 803.
Patch Management	Displays information on patches that have been applied to the host by its associated Patch Management server. The Patch Management Vendor name and the ID number of the most recent patch is displayed.
Logged In Users	User name of the user logged into this host.
Buttons	
Send Message	Opens the Send Message window and allows you to send a message to a host. If the host has the Persistent Agent or Mobile Agent installed, the message can be sent to the host desktop. For more details see Send a message to a host on page 814.
Groups	Displays a list of available host groups. If the host is a member of a group the check box is selected. You may add or remove the host from one or more groups.
Apply	Saves changes to the Host Properties.
Reset	Resets the values in the Host Properties window to their previous settings. This option is only available if you have not clicked Apply.

Host health and scanning

Host health is determined by the Endpoint Compliance Policies, System and Administrative states or scans run on the host. Each time a scan is run a record of that scan is stored in the database and displayed on the Heath tab of the Host Properties window. Each scan and scan type the host is eligible for is shown along with the Name, Status, and Action. The Agent scan shown in bold text and highlighted with a gray bar indicates the scan that is currently applied to the host. Click Show History for short-term historical data.

When multiple scans exist in a host record in Host Health, the combination of the Status fields can affect whether or not the host is allowed on the network or is placed in remediation. In FortiNAC versions lower than Version 6.1, failing any scan would prevent the host from accessing the network, even if that scan no longer applied.

For example, assume an Administrator created an Endpoint Compliance Policy for all Accounting Staff and selected Scan A for that Policy. Accounting Staff would connect to the network, and be scanned using Scan A. Some hosts would fail and others would pass. If the Administrator then changed the scan associated with the Policy to Scan B, hosts that had failed Scan A would never be able to access the network even if they had passed Scan B. The failure of Scan A would prevent network access. In addition, those hosts would not be able to rescan for Scan A and it would remain a Failed scan permanently.

In Versions 6.1 and higher that is no longer true. Using the example above, the results of Scan A would no longer affect the host because the Endpoint Compliance Policy that now applies to the host uses Scan B. However, failing an Admin or System Scan would still prevent network access. Refer to the table below for the effects of the Status fields on network access in Version 6.1 and higher.

		Scan Type/Status		Network Access
Admin	**System**	**Agent Scan A**	**Agent Scan B***	
Initial	Initial	Failure	Initial	No. Must pass scan B.
Initial	Initial	Failure	Success	Yes
Failure	Initial	Failure	Success	No. Must pass Admin Scan.
Success	Failure	Failure	Success	No. Must pass System Scan.
Success	Success	Failure	Success	Yes

*Agent Scan B is the scan that currently applies to the host in the example in the table.

Access the health tab

1. Select **Hosts > Host View**.
2. Search for the appropriate host.
3. Select the host and either right-click or click the **Options** button.
4. From the menu select **Host Properties**.
5. Click on the **Health** tab.

Settings

Option	Description
Type	**Admin** — Indicates the reason why a host was manually marked at risk. They are not actually scanning the host but provide a configuration or profile with which to associate the host state. Admin Scans can be used to mark hosts At Risk or Safe based on an alarm action triggered by an event. These scans can also be used to enable or disable access based on the time of day, for example to limit access for guests after 5:00 pm. **System** — These scans run scripts on the FortiNAC platform.

Option	Description
	Agent — Scans run by an agent installed on the host based on an Endpoint Compliance Policy or set of requirements with which the host must comply. The Agent scan listed in bold and highlighted by a gray bar indicates the scan that is currently applied to the host.
Name	The Name of the scan. There may be more than one scan of a particular type that the host is eligible to be scanned against.
Status	**Initial**—Default setting indicating that the host has not been scanned, therefore it has neither passed nor failed. For Admin scans, manually setting the scan to Initial is the equivalent of Success. For other scan types, setting the status to Initial has no effect. **Failure**—Indicates that the host has failed the scan. This option can also be set manually. When the status is set to Failure the host is marked "At Risk" for the selected scan. **Failure Pending**—The host has been scanned and failed a scan that has the Delayed Remediation option enabled. The host is not placed in remediation and it is marked "Pending At Risk". See Delayed remediation for scanned hosts on page 431 for additional information. **Success**—Indicates that the host has passed the scan. This option can also be set manually. When the status is set to Success the host is marked "Safe" for the selected scan.
Actions	The ReScan button appears in the Actions column for Agent scans. Clicking the ReScan button places the host into the queue to be re-scanned. If FortiNAC cannot contact the host when the ReScan button is clicked, a message is displayed indicating that the host was not rescanned.

View history

1. On the Host Properties Health tab, click **Show History**.
2. View the list of scans, results, and when the scan(s) were performed. Results are sorted with the most recent at the top of the list. Note that if there are no Admin, System, or Endpoint Compliance Policy scan results to display when you click History, the History window opens with the message, "There are no scan results for this host."
3. Inside the History window, click the **Script/Profile** name to view the details of the scan. The details view opens in a new browser window.
4. Close the scan details window.
5. Click **Refresh** on the History view to refresh the list with the most recent data.
6. Close the window when finished.

Application inventory

Application Inventory lists all of the programs found on a selected host either by a FortiNAC Windows, MAC, Linux, or Mobile Agent or an agent from an MDM Service that is integrated with FortiNAC.

Right-click a host in the Host View and select Host Applications.

The application inventory is not populated during the initial scan. Subsequent manual or scheduled scans will perform this function.

FortiNAC agents must be version 3.1 or higher to collect application data.

Settings

Field	Definition
Threat Score	The threat score assigned to the application. This field appears only when the ATR license is enabled.
Operating System	Device operating system, such as iOS.
Operating System Version	The operating system version for the device. (This information may not be available.)
Source	Source of the application data, such as an MDM Service.
Version	Operating system version.
Threat Override	Indicates whether an application as Trusted or Untrusted according to the threat score. This field appears only when the ATR license is enabled.
Package Name	The namespace in which the application is run. (This information may not be available.)
Submit Date	The date when the application was last submitted to a Threat Analysis Engine. This field appears only when the ATR license is enabled.
Host Count	The number of hosts that have the application.
Learned Time	Date and time that FortiNAC first learned about this device.
Last Updated	Date and time of the last update t this device in FortiNAC.
Name	Name of the installed application.
Vendor	Domain name of the application vendor.
Version	Version number of the installed application.
Learned Time	Date and time that FortiNAC first learned about this application.

Field	Definition
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.
Set Threat Override	Marks an application as Trusted or Untrusted, overriding the existing threat score. The original threat score is not changed, and the override may be set back to "none". Users can also right-click in the Applications table to access this option. This field appears only when the ATR license is enabled.

Add or modify a host

Hosts records are created as hosts connect to the network and register. Hosts can be added by importing or by entering the data manually. See Import hosts, users or devices on page 696. Add or Modify Host allows you to create new hosts or edit existing ones. Hosts added through this process are either registered to a user or registered as a device.

Register host to user

A host registered to a user is associated with that user, inherits network access parameters from the user and contributes to the Allowed Hosts count for the user. Each registered device or host consumes one license when it is online. If the host is registered here, the user will not have to go through the registration process elsewhere, such as the captive portal.

Only hosts with a valid operating system can be rescanned. Valid operating systems are Windows or Mac.

Register host as device

A host registered as a device can be displayed in the Host View or both the Host View and Topology View. This type of host consumes license only when it is online. Typically hosts registered as devices are items such as IP phones, security cameras, alarm systems or printers.

Add or modify host

1. Select **Hosts > Host View**.
2. Click the **Add** button.
3. To modify an existing host, use the search or filter mechanisms on the Host View to locate the appropriate host.
4. Click on the host to select it.
5. Click the **Modify** button.
6. See the table below for detailed information on each field.
7. Click **OK** to save your data.

Settings

Field	Definitions
Register host to user	
User ID	ID of the user who owns this host. As you type a list of matching user IDs drops down. For example if you type ab, user IDs that start with ab are displayed. If the user ID does not exist in the database, but does exist in the directory used to authenticate users, the user is created at the same time. If the user does not exist either in the directory or in your database, you cannot save the host. If registering this host to a User exceeds the number of Allowed Hosts for that user, a message is displayed indicating that Allowed Hosts has been automatically incremented and the host is registered to the user.
Register host as device	
Create In	Indicates where the device should be displayed. Options include Host View or Host View And Topology View.
Container	If the host is created in both Host View and Topology View, you must choose a Topology View container to contain the host. Containers in Topology are used to group devices.
General	
Role	Roles are attributes of hosts and users that can be used as filters in User/Host Profiles. If the host is registered to a user, there are two options for selecting the host role. **Use Role From User** — Indicates that the host role is inherited from the registered user associated with the host. **Specify Role** — Indicates that the host role is manually selected. This enables a drop-down list of possible roles from which you can choose. If the host is registered as a device in Topology View only, its role is used to control network access or can be used to apply a CLI configuration. For example, a CLI configuration could be used to reduce the baud rate of a device when it connects to the network.
Host Name	Name of the host being registered.
Hardware Type	Type of hardware such as Printer, Server or Workstation.
Serial Number	Serial number on the device. May be of assistance if the device is ever stolen.
Operating System	Operating system on the host. Only hosts with a valid operating system can be rescanned. Valid operating systems are Windows, Mac, and Linux.
Device Type	Indicates the type of device being registered. When registering a host to a user this field defaults to Registered Host. It could also be set to a gaming or mobile device. When registering as a device, this might be set to devices that are not typically associated with an owner, such as a printer or an alarm system. An icon representing the device selected displays beside the Device Type field.

Field	Definitions
	If the device is an Access Point and you register it in Host View, it is removed from the Host View and moved to Topology View after the first poll. It is also removed from the Concurrent License count once it is recognized as an Access Point.
Notes	Free form notes entered by the Administrator.
Security and Access Attribute Value	This value can be included in a filter when determining the Security Policy that should scan this host when it connects to the network. If a directory is in use and a user is associated with this host, the value comes from the directory when it is synchronized with the database. Otherwise the value can be entered manually.
Adapters	Lists the adapters or network interfaces that exist on this host. By listing all adapter's on the host here, you establish that these adapters are siblings. Number of adapters per host is limited to **five**. See Edit Adapters below. **Physical Address** — MAC Address of the adapter **Media Type** — Indicates whether the adapter is wired or wireless.

Edit adapters

1. Go to the **Adapter** section of the **Add or Modify Host Window**.
2. To add an adapter: Click the **Add** button and provide the **Physical Address** and the **Media Type**, such as wired or wireless.
3. To modify an adapter: Select an **Adapter** and click the **Modify** button. Change the **Media Type** as needed. To change the **Physical Address** you must delete the adapter and add it again.
4. To delete an adapter: Click on the **Adapter** to select it and click **Delete**.
5. Click **OK** to save.

The number of adapters per host is limited to five.

Delete a host

This option deletes the selected host(s) from the Host View.

Deleting a host from the Host View that is also displayed in the Topology View, removes that host from both views. Deleting a host from the Topology View does not delete it from the Host View.

If a device has been detected as a Rogue host and then later manually entered as a device, the Rogue host record remains in the database. It is important to remove the corresponding Rogue host record so there is no conflict between the two records with the same MAC address.

1. Select **Hosts > Host View**.
2. Use the **Quick Search** or **Custom Filter** to locate the appropriate host(s).
3. Select the hosts to be deleted.
4. Click **Delete** at the bottom of the **Host View**.

Enable or disable hosts

Use this option to disable or enable hosts. A message window appears indicating the successful disabling or enabling of the host. When a host is disabled all of its adapters are disabled.

1. Select **Hosts > Host View**.
2. Use the **Quick Search** or **Custom Filter** to locate the appropriate host(s).
3. Select the hosts to be enabled/disabled.
4. Click either **Enable** or **Disable** at the bottom of the **Host View**.

Enabling and disabling hosts can be automated using events and alarm mappings. Specific events, such as, Possible MAC Address Spoof, can be mapped to an alarm that has the action "Disable Hosts" configured. See Add or modify alarm mapping on page 892.

If ATR is enabled

The ATR License must be enabled in order to use the following option.

When enabling a host that was disabled by a security alarm action, a dialog appears that provides the option to:

- Undo the security alarm on the host, which will also undo the associated actions on the host
- Enable the host while leaving the security alarm and its associated actions on the host.

Do one of the following:

- Click **Yes** to undo the security alarm on the host. This will undo the security alarm and the action(s) associated with the security alarm on the host. The number of actions that were undone is displayed. Secondary tasks are performed on the host, if enabled.
- Click **No** to enable the host but maintain the security alarm. All actions associated with the security alarm will remain on the host.

Add IP phones

IP phones can be added using one of the following methods:

- Import IP Phones using a .csv file. See Import hosts, users or devices on page 696.
- Connect your phones to the network and then convert the rogue hosts to IP phones using the Register As Device tool. See Register a host as a device on page 812.
- Connect your phones to the network and use the Device Profiler feature to automatically register them as IP Phones. See Device profiler on page 348.

- Add a new host in the host view and choose Register As A Device in the Add window, then select IP Phone as the device type. See Add or modify a host on page 807.

For more information, see Policy details on page 381.

Add hosts to groups

You can add selected host(s) to groups you have created. See Groups view on page 838 for detailed information on Groups and how they are used in FortiNAC. Only registered hosts can be added to groups.

IP phones have a special group type and can only be added to IP phone groups. If you select IP phones with other registered hosts you will not be allowed to use the **Add Hosts To Groups** option. Select IP phones separately. Only IP phone groups will be displayed.

1. Select **Hosts > Host View**.
2. To select host(s) with specific parameters use the Custom Filter to set the criteria.
3. Use Ctrl-click or Shift-click to select the records you wish to add to the group.
4. Right-click or click the Options button and select **Add Hosts To Groups**.
5. The **Group Membership** view lists the available host groups and sub-groups. Sub-groups are displayed under their parent group or groups.
6. To add the hosts to a group, click the box next to the group name and then click **OK**.
7. To create a missing group:
   a. Click the **Create Group** button.
   b. Enter a group name.
   c. If the new group should be a sub-group of an existing group, enable the **Parent Group** option and select the appropriate group from the list.
   d. **Description** is optional.
   e. Click **OK** to save the new group.
8. Click **OK**.

Group membership

From the Host View window you can view or modify the group membership of an individual host. Use this option to open a window that displays a list of all groups to which the selected host belongs.

IP phones have a special group type and can only be added to IP phone groups. If you select an IP phone only IP Phone groups will be displayed.

1. Select **Hosts > Host View**.
2. To select host(s) with specific parameters use the Custom Filter to set the criteria.
3. Click on a host to select it.
4. Right-click or click the Options button and select **Group Membership**. The **Group Membership** option displays only for registered hosts.
5. The **Group Membership** view lists the available host groups and sub-groups. Sub-groups are displayed under their parent group or groups. A check next to a group name indicates that this host is contained in that group.
6. To add the host to a group, click the box next to the group name and then click **OK**.

7. To remove the host from a group, click to uncheck the box next to the group name and then click **OK**.
8. Click **OK** to save your group selections.

Register a host as a device

Devices such as printers, lab hosts, and servers that have not been placed in the Topology but are connected to managed switches, are created as rogue hosts. If rogue hosts are denied access to the network, they are disabled. Use this option to prevent rogue hosts from being denied access to the network by registering them.

If you select more than one device on the Host View, the IP address and Physical Address fields will not display on the Register As Device window. If multiple devices are selected and those devices do not have IP addresses, you will not be able to place them in the Topology View using the Register As Device option. You can place those devices in the Host View using the Register As Device option.

A host can be registered as a device from the Host View based on the rogue host record or from the Adapter View based on the adapter record.

1. Select **Hosts > Host View** or **Hosts > Adapter View**.
2. Use the **Quick Search** or **Custom Filter** to locate the appropriate record.
3. Click the record to select it. Right-click or click **Options** and select **Register as Device**.
4. Click **Manage In** and select where this device should be placed. Options include:
    - **Device in Host View**—device is kept in Host View allowing you to track connection history and can be associated with a user.
    - **Device in Topology**—device is moved to Topology and removed from Host View. Device can be polled and contact status can be monitored.
    - **Device in Host View and Topology**—device is shown in both the Host View and Topology View. You can track connection history and it can be associated with a user, but it cannot be polled.

    If the device is an Access Point and you register it in Host View, it is removed from the Host View and moved to Topology View after the first poll. It is also removed from the Concurrent License count once it is recognized as an Access Point.

5. Click **Device Type** and select a type from the drop-down list. The icon associated with the selected device type displays to the right of the drop-down list.
6. Click **Role** and select a role from the drop-down list. Roles are configured on the Roles View. You can also click the **Add Role** button to add a role. See Role management on page 553.
7. Select the container for the device from the drop down list. This is where the device will display in the Topology view. This field is disabled if the device is not being managed in the Topology view.
8. Enter the **IP address** for the device. IP address is required for devices being managed in the Topology view.
9. This field does not display if the **Manage In** field is set to something other than **Device In Topology** or if you have selected more than one device. If you have selected more than one device and those devices do not already have IP addresses you cannot add them to the **Topology View**.
10. The **Physical Address** field is read-only and displays only when one of the **Topology View** options is selected in the **Manage In** field.
11. Click **OK**.

Run the agentless scanner

Use the agentless scanner to query individual hosts selected from the host view. Hosts must be Windows hosts that are members of the domain in the agentless scanner configuration and that are connected to the network. Hosts with other operating systems are ignored.

1. Select **Hosts > Host View**.
2. Search for the appropriate host(s).
3. Select one or more hosts and either right-click or click the **Options** button.
4. From the menu, select **Run Agentless Scanner**.

Set host expiration date

The expiration date on a host determines when it is automatically deleted or aged out of the database. Aging out of the database can be triggered by an expiration date, the amount of time the host has been inactive or both. There are many methods for setting an Expiration date. See Aging out host or user records on page 823 for information on other methods.

The Set Host Expiration Date feature is used from the Host View.

1. Select **Hosts > Host View**.
2. Use the **Quick Search** or **Custom Filter** to locate the appropriate host(s).
3. Select the hosts to be modified.
4. Right-click or click **Options** and select **Set Host Expiration**.
5. Use the table below to enter expiration criteria.
6. Click **OK** to set the expiration dates.

Set Host Expiration Settings

Field	Definition
Set Host Expiration	Enables the expiration date option and corresponding calculation methods.
Specify Date	Allows you to select a specific date that the host will be aged out of the database. Host age times are evaluated every ten minutes. If you specify a date and time, the host may not be removed from the database for up to ten minutes after the time selected.
Days Valid From Now	Enter the number of days from today that you would like the host to expire. The expiration date is calculated based on this number.
Days Valid From Creation	This is the number of days from the date the host record was created. The expiration date is calculated based on this number.
No Expiration	This host is never deleted from the database even if global or group aging options are added or modified.
Default Expiration	Defaults to the global aging settings configured in **System > Settings > User/ Host Management > Aging**.

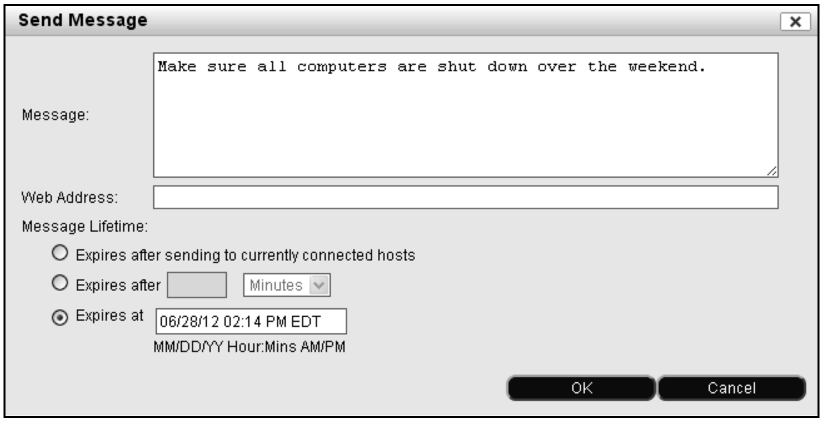
Field	Definition
Set Host Inactivity Limit	Enables the option to delete a host based on the number of days that it did not log onto the network.
Days Inactive	Number of consecutive days the host must be inactive to be aged out of the database. For example, if this is set to 4 days, and after 2 days the host connects to the network again, the counter is restarted.
No Inactivity Limit	With this option enabled, the host is never deleted from the database due to inactivity even if global or group aging options are added or modified.
Default Inactivity Limit	Defaults to the global aging settings configured in **System > Settings > User/ Host Management > Aging**.

Send a message to a host

Use Send Message to send a text message to the selected host from the Host View.

- If the host is online (connected) the message is sent.
- If the host is offline when the message is sent, by default the message expires immediately. If you set a specific expiration time, the message remains active until either the host comes online or the message lifetime is reached.
- If the message is still active when the host comes online, the message is delivered. Otherwise, the host does not receive the message.

See Send a message to group/all hosts on page 551 in the in Security Management section for details on sending a message to all hosts or a group of hosts.



Send Message

Message: Make sure all computers are shut down over the weekend.

Web Address:

Message Lifetime:

○ Expires after sending to currently connected hosts

○ Expires after Minutes

● Expires at 06/28/12 02:14 PM EDT

MM/DD/YY Hour:Mins AM/PM

1. Select **Hosts > Host View**.
2. Use the Quick Search or Custom Filter to locate the appropriate Host(s).
3. Click the host(s) to select it. Right-click or click Options and select **Send Message**.
4. Enter the message in the **Message** block.
5. Optionally, enter a Web Address that will be sent as part of the message.
6. This web address must include the http:// or ftp:// or other information. The page must also be in a location that the host(s) can access from their VLAN such as Remediation, Quarantine, Dead End, or other. For example, if a host is in Remediation, the web page must be accessible from the Remediation VLAN.

7. Click the radio button next to the **Message Lifetime** option and enter the required information.

Options	Description
Expires after sending to currently connected users	The message expires immediately after it has been sent.
Expires after	The message expires after the specified amount of time. Enter a number and select the timeframe of Minutes, Days, or Hours. The message remains active on the server for the selected timeframe. The server sends the message the next time it communicates with a host as long as communication occurs before the message expires.
Expires at	The message expires on the specified date and time. The format is MM/DD/YY hh:mm AM/PM. The message remains active on the server until the specified date and time. The server sends the message the next time it communicates with a host as long as communication occurs before the message expires.

The server can only send messages to hosts with which it is communicating that have Persistent Agent or are registered with Mobile Agent.

8. Click **OK**.

Host registration and user authentication

A registered host is a device requiring network services that is displayed in the Host View and has an ID. Registered hosts have a record in the FortiNAC database and are known entities. There are several methods for registering hosts depending on the type of host.

- Users connecting to the network with their computers or with a gaming device, such as an XBox, typically register their equipment through a web page. See
- Rogue hosts connecting directly to the network, such as an alarm system or a security camera, can be registered automatically using Device Profiler or manually using the Register as Host or Register as Device options in the Host View. See Device profiler on page 348, Add or modify a host on page 807 and Register a host as a device on page 812.
- Hosts can be registered by importing their records from a .csv file into the database. See Import hosts, users or devices on page 696 for more information.

Registered hosts have specific icons that represent the type of device or host that has been registered and their last known state. See the Icons on page 30 for a list of icons and their definitions.

If gaming devices are registered, they are automatically placed in the Forced Scan Exceptions and Forced Authentication Exceptions groups. This prevents them from being scanned or forced to authenticate when they are on the network.

An authenticated user is a network user that has entered a user name and password on a login page and been verified using an existing authentication method. Authentication methods include the local FortiNAC database, an LDAP directory, a RADIUS Server or a combination in which a user is authenticated by a RADIUS server and registered using data in LDAP. An authenticated user has a specific icon in the User View that is separate from the icon representing their computer on the Host View.

A single computer can have more than one icon if it has more than one network interface. For example, if a user has a laptop computer with both wired and wireless access to the network, you may see several records and icons for that user and host combination. You will see one record in the User View for the User, one record in the Host View for the computer itself and two records in the Adapter View for the wired and wireless adapters. The two network interfaces are called siblings because they reside on the same computer. If the host is disabled by FortiNAC both adapters are automatically disabled also. Adapters can be disabled individually if they are disabled manually.

Registration process

FortiNAC uses the Host Registration process to create registered hosts in its database. A registered host is a known entity that has an ID. Hosts can be computers, gaming devices, IP phones or any device that requires network services.

Existing host

A host attempts to connect to the network.

FortiNAC compares the host information with the host records in its database.

If the host record exists and has not been disabled, FortiNAC allows access to the network.

New host - captive portal

If the host record does not exist, a Registration web page is displayed, forcing the user to register the equipment.

The user selects the type of registration, such as guest, network user or gaming device.

On the next page, the user enters a user name and password. This provides identity for the computer or gaming device being registered.

If a computer is being registered, the security policy for this user may require that the user download an agent to scan the computer. See Determining host operating system on page 418.

When the computer has met all of the criteria of the scan, it is registered and allowed access to the network.

New host - Passive Agent registration

When a user logs onto or off of the network a Passive Agent is served to the user's computer.

The computer is scanned and registered. See Passive Agent on page 495.

Registration logs

FortiNAC generates a log entry for each host that registers. A new log file is created for each day. The log is a delimited text file. The file is stored in the /home/cm/registration directory. The file name is RegistrationLog.mm.dd.yyyy, such as RegistrationLog.03.15.2009. The record for each host contains the following information:

Settings

Data	Description
First Name	User’s first name as entered on the Registration page.
Last Name	User’s last name as entered on the Registration page.
Login	User’s login for the network.
Hardware Type	User’s hardware type; for example, wired, wireless.
Location	Hardware's location on your network.
IP address	The IP address assigned to the hardware’s location.
Physical Address	The physical (MAC) address of the hardware.
E-Mail	The e-mail address to be used to contact the user.
Position/Grade	The position of the user; for example, Professor, or Administration. Or, the grade of the student; for example, year of graduation.
Address	User Contact information.
City	
State	
Zip/Postal Code	
Phone	
PC Name	The name of the PC.
PC Type	The type of the PC; for example, a server, laptop or desktop.
PC Serial Number	The serial number of the PC.
Registration Date/Time	The date and time the user and equipment were registered. The format is MM.DD.YYY HH:MM:SS AM(PM); for example: 09.05.2008 09:45:33 AM

Adapter view

The Adapter View is part of a window that includes menu options for Users, Adapters, Hosts, and Applications. Use the Adapter View to locate and manage adapters connected to your network.

The relationship between Users, Hosts and Adapters is hierarchical. Users own or are associated with one or more hosts. Hosts contain one or more Adapters or network interfaces that connect to the network. By displaying Host and Adapter data in a group, the relationships are maintained. For example, if you search for a host with IP address 192.168.5.105, you are in fact searching for the IP address of the adapter on that host. When the search displays the host, you can click on the Adapters option, the search is automatically re-run and you see the adapter itself. If there is an associated user, you can click on the Users option to re-run the search and see the associated user.

Hover over the icon in the Status column to display a tooltip with detailed information about this adapter. For Settings see View and search settings on page 820. For information on Status icons see the Icons on page 30.

The Displayed and Total fields in the title bar represent the number of records displayed versus the total number of records in the database.

Navigation, menus, options, and buttons

For information on selecting columns displayed in the Adapter View Some menu options are not available for all adapters. Options may vary depending on adapter state.

Double-click on an adapter to display Adapter Properties.

Field	Definition
Navigation	Across the top of the Adapters tab are navigation tools that allow you to quickly move through large numbers of records. These tools include the following: • **<<first**—Takes you to the first page of records. • **<prev**—Takes you back one page. • **Page Number**—Current page number is displayed. • **next>**—Takes you forward one page. • **last>>**—Takes you to the last page. • **Drop-down Box**—Allows you to select the number of records to be displayed on each page.
Quick Search	Enter a single piece of data to quickly display a list of adapters. Search options include: IP address, MAC address, Host Name, User Name and User ID. Drop-down arrow on the right is used to create and use Custom Filters. If you are doing a wild card search for a MAC address you must include colons as separators, such as, 00:B6:5*. Without the separators the search option cannot distinguish that it is a MAC address. When Quick Search is enabled, the word Search appears before the search field. When a custom filter is enabled, Edit appears before the search field.
Right click options	
Adapter Properties	Opens the Properties window for the selected adapter. See Properties on page 821.
Disable Adapters	Disables the selected adapter(s) preventing them from accessing the network. See Enable or disable an adapter on page 822.
Enable Adapters	Enables the selected adapter(s) if they were previously disabled. Restores network access.
Modify Adapter	Opens the Modify Adapter window for the selected adapter. See Modify an adapter on page 823.
Port Properties	Opens the Port Properties window for the port where the selected adapter is connected. See Port properties on page 784.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847.

Field	Definition
	You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.
Enable Hosts	Enables the host(s) associated with the selected adapter(s) if they were previously disabled. Restores network access.
Disable Hosts	Disables the host(s) associated with the selected adapter(s) and all of its other adapters preventing them from accessing the network. See Enable or disable an adapter on page 822.
Host Health	Opens a dialog with the contents of the Host Health tab from the Host Properties view. See Host health and scanning on page 803.
Host Applications	Opens the Applications window for the selected host and lists installed applications. See Application inventory on page 805.
Go To Host(s)	Opens the Hosts tab and displays the hosts associated with the selected adapters.
Modify Host	Opens the Modify Host window for the host associated with the selected adapter. Applies only to registered hosts.
Register As Device	Changes the host associated with the selected adapter to a device in the FortiNAC database. See Register a host as a device on page 812.
Register As Host	Changes the Rogue host associated with the selected adapter to a registered host. Displays the Modify Host window. See Add or modify a host on page 807.
Scan Hosts	Scans the associated host with the Security Policy that applies to the host at that moment. The host must be online and must have a Persistent Agent. If the host is online but does not have a Persistent Agent, it is marked "at risk" for the Security Policy that most closely matches the host at the moment.
Run NMAP Scan	Determines open ports and operating systems on the device being scanned
Send Message	Sends a text box message to the associated host(s). User can send messages to hosts with the Persistent Agent or Mobile Agentinstalled. See Send a message to a host on page 814.
Set Host Expiration	Launches a tool to set the date and time for the associated host(s) to age out of the database. See Set host expiration date on page 813.
Set Host Role	Assigns a role to the associated host.
Create Device Profiling Rule	Displays the Add Device Profiling Rule dialog with some information pre populated from the selected Adapter.
Test Device Profiling Rule	Ability to test an adapter against a DPC Rule to see if it matches or not
Go To User(s)	Opens the Users tab and displays the users associated with the selected adapters.
Set User Expiration	Launches a tool to set the date and time for the user associated with the selected adapter to age out of the database. See Set user expiration date on page 655.

Field	Definition
Reprofile Rogue(s)	Ability to run DPC rules against one or more Rogues seleted.
Set User Role	Assigns a role to the user associated with the selected adapter. See Role management on page 553.
Buttons	
Import/Export	Use Import and Export options to import hosts into the database from a CSV file or export a list of selected hosts to CSV, Excel, PDF or RTF formats. See Import hosts, users or devices on page 696 or Export data on page 710.
Options	The Options button displays the same series of menu picks displayed when the right-mouse button is clicked on a selected host.

View and search settings

The fields listed in the table below are displayed in columns on the Adapter View based on the selections you make in the Settings window. These fields are also used in Custom Filters to search for adapters. See Search and filter options on page 18. Additional fields that can be displayed on the Adapter View are fields for the user or the host associated with the selected adapter.

Settings

Field	Definition
Access Value	Name or number of the Network Access identifier given to this adapter based on the state of the host and the device to which the adapter is connected, such as VLAN ID, VLAN Name or Aruba Role.
Description	Free form notes entered by the Administrator about this adapter.
IP address	The primary IP address assigned to this adapter that is used to communicate with FortiNAC. If the adapter is offline, this is the last known IP address for the adapter. Supports both IPv4 and IPv6 addresses.
All IPs	All IP addresses assigned to the adapter. Supports both IPv4 and IPv6 addresses. • For IPv6, all addresses used for IPv6 communication will be displayed. • For IPv4, IP addresses used for registration, remediation, isolation, etc., will be displayed along with the production IP until a L3 poll determines the single IP being used. • Depending on the ARP cache aging of the L3 device itself and the poll interval that FortiNAC polls it, multiple production IP addresses may be displayed simultaneously for an adapter.
Location	Name of the switch and port where this adapter is connected to the network. If the adapter is offline, this is the last known location where the adapter connected to the network.
Media Type	Indicates whether this is a wired or wireless adapter.

Field	Definition
Physical Address	MAC address of the adapter.
Status	Current or last known status is indicated by an icon, see Icons on page 30. Hover over the icon to display additional details about this adapter in a tool tip. • **Connected** — Indicates whether host is online or offline. • **Access** — Indicates whether host is enabled or disabled. • **Valid Physical Address** — Indicates whether or not the system knows the MAC address for the adapter that has connected to the network.
Vendor Name	Name of the Vendor that matches the Vendor OUI for this device.

Properties

The Adapter Properties view provides access to detailed information about a single adapter. From this view you can access the associated user's properties by clicking on the User tab or the associated host by clicking on the Host tab. Adapter properties also provides access to the Device Identity tab. See Device identity on page 821.

1. Select **Hosts > Adapter View**.
2. Search for the appropriate adapter.
3. Select the adapter and either right-click or click the **Options** button.
4. From the menu, select **Adapter Properties**.

Settings

Field	Description
IP address	IP address assigned to the adapter.
Physical Address	MAC address of the adapter.
Location	Switch and port where the adapter is connected to the network.
Media Type	Indicates whether this is a wired or wireless adapter.
Adapter Status	Radio buttons indicating whether the adapter is Enabled or Disabled. To enable or disable the adapter, click the appropriate button and then click Apply.
Description	Free form notes section for the Administrator.
Apply	Saves changes to the Adapter Properties.
Reset	Resets the values in the Adapter Properties window to their previous settings. This option is only available if you have not clicked Apply.

Device identity

The Device Identity tab displays the Physical Address, Vendor Name, and DHCP fingerprint for selected Adapter. A separate record is added every time a new fingerprint is heard for a MAC. For example, if the adapter on a host is moved from a registration VLAN to a production VLAN and as a result requests a new IP address this creates a new record. If two records are displayed for the same MAC and port, but with different OSs, the host is most likely a dual-boot host. This generates the Device Fingerprint Changed event. This view is informational only.

Settings

Field	Definition
Physical Address	MAC address of the host interface or adapter.
Vendor Name	Manufacturer of the host. This is based on the Vendor OUI.
Learned Time	The first time a DHCP packet was heard by FortiNAC for this Physical address. This is not the time that the host connected to the network nor is it the time the host was created in the database.
Last Heard	The last time a DHCP packet was heard by FortiNAC for this host. Updated every time a DHCP packet with a matching identity is heard.
Host Name	The name for this host extracted from the DHCP packet.
Option List	Displays a list of option numbers from the DHCP packet used to provide information about the host.
Parameter List	Combination of parameters contained in the DHCP packet that allows FortiNAC to infer the Operating System for this host.
Vendor Class	Vendor Class Identifier extracted from the DHCP packet. Allows the DHCP server to return specific information based on the host's hardware type.
Device Type	Indicates the type of hardware detected.
Message Type	DHCP message type, including • **Discover** — Host broadcast initial DHCP request for an IP address. • **Request** — DHCP server has responded. Host requests an IP address from a specific DHCP server. • **Passive** — Generated when something about the DHCP fingerprint has changed since the last message, such as a different Operating System.
Operating System	Operating system of the host. If more that one record is displayed with different operating systems, this host may be dual boot.

Enable or disable an adapter

Use this option to disable or enable adapters. A message window appears indicating the successful disabling or enabling of the selected adapters. If a host has more than one adapter, only the selected adapter is disabled.

1. Select **Hosts > Adapter View**.
2. Use the **Quick Search** or **Custom Filter** to locate the appropriate adapter(s).
3. Select the adapters to be enabled/disabled.
4. Click either **Enable** or **Disable** at the bottom of the **Adapter View**.

Modify an adapter

1. Select **Hosts > Adapter View**.
2. Search for the appropriate adapter.
3. Select the adapter and either right-click or click the **Options** button.
4. From the menu, select **Modify Adapter**.
5. The **Physical Address** field cannot be modified.
6. Click in the **Media Type** field and select either **Wired**, **Wireless** or **Unknown**.
7. In the **Tags** field, enter mapping values to be applied to the firewall via the SSO Agent. Tags will take precedence over the user ID
8. In the **Description** field, enter any notes on this adapter.
9. Click **OK** to save your changes.

Aging out host or user records

Host and User records remain in the database indefinitely unless you set expiration dates for those records. There are several methods for setting expiration dates.

As new hosts, users or Administrative Users are added to the database, the **Expiration Date** and/or **Inactivity Date** are automatically populated based on settings elsewhere in FortiNAC. Aging settings are configured using the methods listed below. If no global settings have been established and hosts or users are added without Expiration or Inactivity dates, those dates can be added later by configuring the settings below.

If you set age times for existing users or hosts, you may inadvertently cause them to be deleted from the database. If the expiration date calculated for those hosts or users is before today's date, those records will be removed from the database.

Aging a large number of hosts or users at the same time can cause processing delays with FortiNAC if users attempt to re-register within a short period of time of each other. It is recommended that you stagger the aging times to reduce the number of possible re-registrations at any given time.

Host age times are evaluated every ten minutes. If you specify a date and time, the host may not be removed from the database for up to ten minutes after the time selected.

The user inactivity timer is started when all hosts registered to a user are seen as offline. When a host is seen as connected, the timer is cleared. The timer is also cleared when the user logs into FortiNAC.

Directory	If the **Time To Live** option is enabled in the Directory Attribute Mappings window, the value stored in the Directory is used to calculate the dates for Expiration Date and Inactivity Date. This is based on the user's record in the directory. For the user, only the Expiration Date is calculated. For the host, both the Expiration Date and the Inactivity Date are calculated. This may also apply to Administrative Users. The host must be associated with a user to inherit these settings.
System Settings	Age times under **System > Settings > User/Host Management > Aging** are used to populate Expiration Date and Inactivity Date for hosts as they are added to the database and Expiration Date for Users. If these settings are configured after Administrative Users, network users or hosts have been added to the database, those without age times or that are not set to Never Expire, will be automatically updated. Records with age times are not modified. See Aging on page 242.
Group Aging	You can create a host group and use Group Aging to populate the Expiration Date and/or the Inactivity Date fields for hosts in that group. All hosts in the group are modified even if they already have an age time set, except those set to Never Expire. See Aging hosts in a group on page 843.
Host Aging	You can enter or override aging values for individual hosts by clicking the Set button on the Host Properties window or using the Set Host Expiration Date option on the Host View. See Set host expiration date on page 813.
User Aging	You can enter or override those values for individual users, including Administrative Users, by clicking the Set button on the User Properties window or using the Set User Expiration Date option on the User View. See Set user expiration date on page 655.
Administrator User Aging	Administrator users never age out of the database under any circumstances. These users must be removed from the database manually from the Admin Users View.
Administrative User Aging	Administrative Users (Operator, Help Desk) are treated like regular network users when aging settings are applied, depending on how they are added to the database. Below are ways to set the expiration date for an Administrative User: • When adding an Administrative User from the Admin User view, the new user will receive an expiration date based on the information in the global aging settings, the Time To Live setting in the directory or based on a group setting if they are placed in a group. See Aging on page 242. • Manually give any Administrative User an expiration date by selecting the user on the Admin Users View and using the Set Expiration option. See Set user expiration date on page 655. • When an Administrative User is added by converting an existing network user to an Administrative User, the new Administrative User can have aging set through any of the possible aging options. • If you assign Admin User Profiles based on directory groups, there are circumstances in which an Administrative User would be assigned an expiration date. See Set admin privileges based on directory groups on page 692. • If a non-administrative user registered a host through the captive portal and a directory synchronization is run, the user would then be converted to an Administrative User. However, it would have an expiration date based on the global aging settings. This also occurs when a host is registered to a user

	manually by an administrative user.
Guest Aging	A Guest user's expiration date is set based on the Account Duration entered in the Guest Template used to create the Guest. The host registered to the Guest inherits its expiration date from the Global Aging settings. When the Guest user's account expires, both the Guest user's account and the guest's registered host are automatically removed from the database. If the host's expiration date is earlier than the Guest user's expiration date, the host is removed from the database, but the Guest user account remains.

Application view

The Application View is part of a window that includes menu options for Users, Adapters, Hosts, and Applications.

Applications for scanned hosts connected to your network appear in the Application view. As hosts are scanned, the list of applications is updated.

You may not have access to all of the fields listed in this table. Access depends on the type of license key installed and which features are enabled in that license.

The fields listed in the table below are displayed in columns on the Application view based on the selections you make in the Settings window. See Configure table columns and tooltips on page 641. Most of these fields are also used in Custom Filters. See Search and filter options on page 642.

Settings

Field	Definition
Add Filter drop-down list	Allows you to select a field from the current view to filter information. Select the field from the drop-down list, and then enter the information you wish to filter. Options include: • Name • OS • OS Version • Package Name • Source • Threat Override. Select Trusted or Untrusted. For Automated Threat Response (ATR) only. • Threat Score (ATR only) - Enter a single number or a range of numbers (e.g., 8-10) • Vendor • Version See Filters on page 15.
Update button	Displays the filtered data in the table.
Security events	
Name	The name of the application.

Field	Definition
Threat Score	The threat score assigned to the application. This field appears only when the ATR license is enabled. You must have ATR enabled in your licensing package in order to use ATR features.
Version	The version of the application being scanned. (This information may not be available.)
Vendor	The name of the vendor providing the application. (This information may not be available.)
Operating System	The operating system of the device containing the application.
Operating System Version	The operating system version for the device. (This information may not be available.)
Source	The agent that is used to scan the application.
Threat Override	Indicates whether an application as Trusted or Untrusted according to the threat score. This field appears only when the ATR license is enabled. You must have ATR enabled in your licensing package in order to use ATR features.
Package Name	The namespace in which the application is run. (This information may not be available.)
Submit Date	The date when the application was last submitted to a Threat Analysis Engine. This field appears only when the ATR license is enabled.
Host Count	The number of hosts that have the application.
Buttons	
Export	The Export option allows you to export a list of selected applications to CSV, Excel, PDF or RTF formats.
Options	The Options button displays the same series of menu picks displayed when the right-mouse button is clicked on a selected user.
Show Hosts	Opens the Host View displaying the host(s) containing the application. Users can also right-click in the Applications table to access this option.
Delete	Deletes the selected application. Users can also right-click in the Applications table to access this option.
Rescan	Rescans the selected application for threat analysis. Users can also right-click in the Applications table to access this option.

Field	Definition
	This field appears only when the ATR license is enabled.
Set Threat Override	Marks an application as Trusted or Untrusted, overriding the existing threat score. The original threat score is not changed, and the override may be set back to "none". Users can also right-click in the Applications table to access this option. This option appears only when the ATR license is enabled. You must have ATR enabled in your licensing package in order to use ATR features.

Show the host(s) containing an application

1. Select **Hosts > Application View** to access the **Application View**.
2. Select an application in the table and click the **Show Hosts** button, or right-click an application and select **Show Hosts** from the menu.

The Host View is displayed showing the host(s) that contain the application.

Set the threat override for an application

Set threat override lets users mark an application as trusted or untrusted, overriding the existing threat score. The original threat score is not changed, and the override may be set back to "none".

You must have ATR enabled in your licensing package in order to use ATR features.

1. Select **Hosts > Application View** to access the **Application View**.
2. Select an application in the table and click the **Set Threat Override** button, or right-click an application and select **Set Threat Override** from the menu.
3. Select **Trusted** or **Untrusted** from the drop-down menu.
4. Click **OK**.

Device identity

FortiNAC continuously collects identity records as hosts connect to the network. These records are used to rapidly identify and categorize new devices as they connect to the network. A list of Device Identities can be viewed using the Device Identity View. Reports can be exported to CSV, Excel, XML, PDF or RTF file formats.

View individual host Device Identity data from the Host properties view for that host. If two Device Identities are learned for the same MAC and port, but have a different OS, the host is most likely dual-booting. If this occurs, the Device Fingerprint Changed event and its associated alarm are generated. See Device identity on page 821 for additional information.

To access the Device Identity View select **Hosts > Device Identity**.

Settings

Field	Definition
Learned Time	Date/time that the first DHCP packet was heard for a host.
Last Heard Time	Date/time that the most recent DHCP packet was heard for a host.
Physical Address	MAC Address of a host.
Host Name	Host Name contained in the DHCP packet heard for a host.
Vendor Class	This is Option 60 from the DHCP Packet, which is used to identify the vendor type and configuration of a DHCP host such as, MSFT 50 for Windows PCs..
Device Type	Indicates the type of hardware detected.
Message Type	This is the type of DHCP Packet heard. Types include: DHCP DISCOVER, DHCP REQUEST, NMAP, Directory Authentication, Passive Fingerprinting, IP address Profiling, Vendor OUI.
Operating System	Operating system of the host. If more that one record is displayed with different operating systems, this host may be dual boot.
Option List	Displays a list of option numbers from the DHCP packet used to provide information about the host.
Parameter List	Combination of parameters contained in the DHCP packet that allows FortiNAC to infer the Operating System for this host. This is Option 55 from the DHCP Packet. To filter, enter a comma separated list of Option 55 Parameter numbers. It is possible that multiple Operating Systems will resolve to the same fingerprint.
Views	Click the Adapter icon to open the Adapter Properties View.
Buttons	

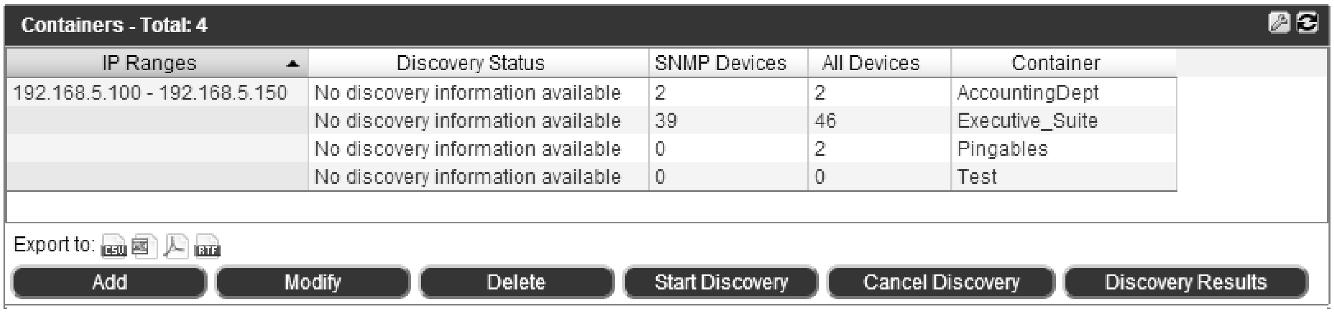
Field	Definition
Delete	Allows you to delete selected records from the table.
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.

Containers view

The Containers view contains a modifiable list of containers for network devices. These containers provide a mechanism for you to logically group your devices. For example, you might make a container for switches and another for routers. You could make a separate container for each building that connects to your network or containers could represent departments in your business. If new devices have been connected to your network but have not been added to the device list, use the **Start Discovery** button to add them. From the Containers view you can add, modify or delete containers.

Deleting a Container deletes the devices it contains. Move the devices to another container before deleting the selected container.

Access Containers from **System > Quick Start > Network Device Settings**.



Containers - Total: 4

IP Ranges	Discovery Status	SNMP Devices	All Devices	Container
192.168.5.100 - 192.168.5.150	No discovery information available	2	2	AccountingDept
	No discovery information available	39	46	Executive_Suite
	No discovery information available	0	2	Pingables
	No discovery information available	0	0	Test

Settings

Field	Definition
IP Ranges	Range of IP addresses within which the discovery process searches for devices.
Discovery Status	Status of the device discovery process for the selected container. To update this field click the Refresh button at the top of the window.
SNMP Devices	Number of devices that are managed via SNMP within the selected container.
All Devices	Total number of devices within the selected container. Included both SNMP and non-SNMP devices.
Container	Name of the container. Containers are user-defined folders or groups for devices. Used to group devices by building or type.
Right-click menu options	
Delete	Deletes the selected container.
Modify	Opens the Modify Container dialog for the selected container.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847

Field	Definition
	You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.
Start Discovery	Searches the network based on user specified IP ranges and determines what SNMP enabled devices exist on the network. Once a device is discovered, FortiNAC creates a model for the device in the database and places the device in the Network Devices list. See Discover devices on page 735.
Cancel Discovery	Cancels the device discovery process for the selected container.
Discovery Results	Displays the results of the network scan used to discover devices in a separate Results View for the selected container. See Discovery results on page 738.

Configure container for devices

Containers are similar to folders and are used to group devices within your FortiNAC database. The Containers view also has a status column. As devices for a container are being discovered by FortiNAC the status of that process is displayed in the Status column. You must click the Refresh button at the top of the window to update the status.

When you delete a container, all associated devices are also deleted. To avoid this issue move your devices to a new container first, then delete the unwanted container.

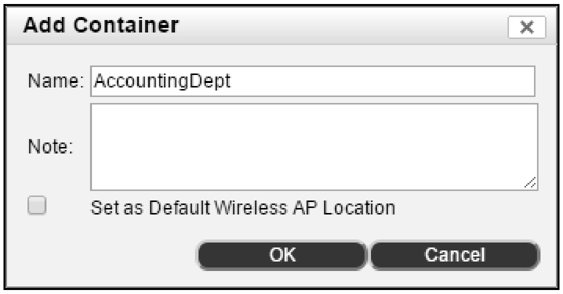
Access Containers from one of the following locations:

- **System > Quick Start > Network Device Settings**
- **Network Devices > Topology > Customer Icon**

Add a container

1. Select **Containers**.
2. On the Containers panel click **Add**.
3. Enter the Container Name and click **OK**.
4. Select the **Set as Default Wireless AP Location** check box to specify that the container is the default container where Wireless APs will be added. This will occur if there is no alternative AP location specified on the wireless

device's model configuration view.



Add Container

Name: AccountingDept

Note:

□ Set as Default Wireless AP Location

Modify a container

1. Select **Containers**.
2. On the Containers panel, select the container to be modified.
3. Click **Modify**.
4. Edit the name and click **OK**.
5. Select the **Set as Default Wireless AP Location** check box to specify that the container is the default container where Wireless APs will be added. This will occur if there is no alternative AP location specified on the wireless device's model configuration view.

Delete a container

1. Select **Containers**.
2. In the Containers panel select the Container to be removed.
3. Click **Delete**.

Network devices

The Network Devices window is one in a series of initial setup windows designed to help you get your FortiNAC program up and running as quickly as possible. Similar functions exist in other parts of the software, but this window provides access to the most essential device configuration information.

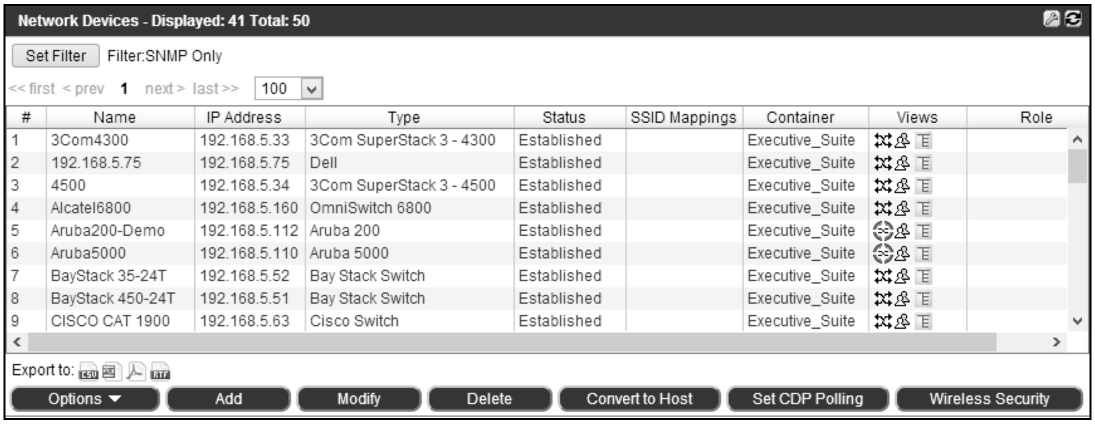
The Network Devices window displays devices connected to your network. The window is divided into two panels, Containers and Network Devices.

The list of existing network devices includes both those managed via SNMP and non-SNMP or pingable devices, such as a security camera or an alarm system. Configuration can be done individually or by brand/type of device. Devices can be added, deleted or configured. Use the Discover button on the Containers panel to search for connected devices within an IP address range.

Network devices should have static IP addresses or dynamic IP addresses that are reserved. Once a device that provides network services had been identified in FortiNAC there is no mechanism to automatically update the IP address for that device if there is a change. If the IP address on the device itself is changed, the device appears in FortiNAC to be offline or to have a communication error.

Network Devices can be accessed from **Network Devices > Topology** or from **System > Quick Start > Network Device Settings**; however, configuration steps point you to **Network Devices > Topology**.

See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.

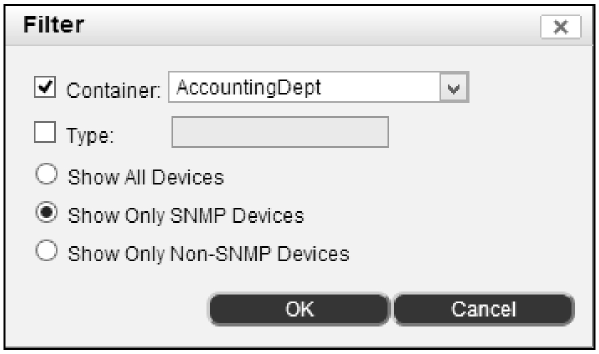


Network Devices - Displayed: 41 Total: 50

Filter:SNMP Only

#	Name	IP Address	Type	Status	SSID Mappings	Container	Views	Role
1	3Com4300	192.168.5.33	3Com SuperStack 3 - 4300	Established		Executive_Suite		
2	192.168.5.75	192.168.5.75	Dell	Established		Executive_Suite		
3	4500	192.168.5.34	3Com SuperStack 3 - 4500	Established		Executive_Suite		
4	Alcatel6800	192.168.5.160	OmniSwitch 6800	Established		Executive_Suite		
5	Aruba200-Demo	192.168.5.112	Aruba 200	Established		Executive_Suite		
6	Aruba5000	192.168.5.110	Aruba 5000	Established		Executive_Suite		
7	BayStack 35-24T	192.168.5.52	Bay Stack Switch	Established		Executive_Suite		
8	BayStack 450-24T	192.168.5.51	Bay Stack Switch	Established		Executive_Suite		
9	CISCO CAT 1900	192.168.5.63	Cisco Switch	Established		Executive_Suite		

Set filter


Filter

☑ Container: AccountingDept

□ Type:

○ Show All Devices

● Show Only SNMP Devices

○ Show Only Non-SNMP Devices

1. Click the **Set Filter** button on the Network Devices window.
2. To filter by Container, mark the **Container** check box with a check mark to enable it. Select the container from the drop-down list. This is the Container from the Topology View.
3. To filter by Type, mark the **Type** check box with a check mark to enable it. Enter the name of the type to use as the filter. This data corresponds to the Type column in the Network Devices window. Wildcard entries can be used. This field is case sensitive.
4. Enable one of the **Show** options:
   - **Show All Devices** — Shows both SNMP Devices and Non-SNMP devices.
   - **Show Only SNMP Devices** — Shows only those devices that are managed via SNMP, such as switches or routers.
   - **Show Only Non-SNMP Devices** — Shows only pingable devices. Pingable devices are devices that are not managed via SNMP but are connected to your network, such as HVAC systems, security cameras, alarms or cash registers. For more information on pingable devices see Add or modify a pingable device on page 725.
5. Click **OK**. Filter settings are displayed to the right of the Set Filter button.

Filter settings are stored for each user.

Settings

Field	Definition
#	Indicates the order of display.
Name	Name of the selected device.
IP address	IP address of the selected device. IP addresses or Address Ranges are used to add or discover devices.
Type	Indicate the type of devices, such as, switch, printer, router, etc.
Status	Indicates whether or not communication has been established with the device. Displays either Established or Lost.
SSID Mappings	Number of SSID configurations for the selected wireless device. An SSID mapping contains SSID configuration information such as the RADIUS server, access and isolation VLANs, and Supplicant Configuration information.

Field	Definition
	A red zero, 0, indicates that no SSID Mappings have been configured for a device that supports SSID Mappings.
Container	Container where the device resides. Containers are used to group devices.
Views	Series of icons that can be clicked to provide additional details about the selected device. Icons provide access to Device Properties, Group Membership, Ports and Hosts List, and SSIDs List. Click an icon to access the view.
Last Polled	Date and time the server last attempted to poll the device.
Last Polled Success	Date and time that the device was last polled successfully.
Role	Displays the role assigned to this device. To modify the role go to Device Properties for this device. This field does not list the roles associated with this device through Network Device Roles. To view Role Membership right-click on the device in the Topology View.
CDP Polling	Indicates whether CDP polling is enabled or disabled for the device and displays the polling interval. Disabled (unsupported) displayed in this column, indicates that the first CDP poll was unsuccessful because CDP queries are not supported by the device or may not be configured on the device. If the device has ever been successfully polled for CDP, later unsuccessful polls are not interpreted as a problem with CDP on the device.
CDP Last Polled	Date and time the server last attempted a CDP poll of the device.
CDP Last Poll Success	Date and time of the last successful CDP poll.
Right click options	
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.
Delete	Deletes the selected devices.
Resync Interfaces	Reads the interface information from a modeled device and updates FortiNAC's representation of that device. This information includes the interface's index, description, name, and status. See Resync interfaces on page 767.
Model Config	Opens the Model Configuration window for the selected device to configure data such as passwords for communication with the device, VLANs, and RADIUS server information. See Model configuration on page 767.
Global Model Config	Opens the Global Model Configuration window to configure data for multiple devices of the same brand, such as passwords for communication with the device, VLANs, and RADIUS server information. See Global model configuration on page 772.
Running Configuration	View the configuration running on the selected device (device dependant). This option is only available for some devices.
Static Port Configuration	Allows you to designate a specific port as a Dead-End VLAN and use that port to disable hosts. The MAC address of the disabled host is placed in a list on the device which indicates it only has permission to use the port designated as secure or static. See Secure port/static port overview on page 776.

Field	Definition
Modify	Modify the selected device. Moves multiple devices selected in the Network Devices window to the container you specify. Accessed using the Modify button when more than one device is selected. See Move a device to a different container on page 745.
Convert To Host	Converts one or more selected non-SNMP or pingable devices to hosts. After conversion these devices are removed from Network Devices but do display both in the Topology View and the Host View. See Convert all pingables to hosts on page 734. Wireless Access Points added as pingables cannot be converted to hosts.
Set CDP Polling	Performs two functions. Allows you to enable or disable the Global CDP (Cisco Discovery Protocol) feature. When the Global option is disabled, settings on individual switches are ignored and the CDP feature is not used. Allows you to enable CDP polling for one or more selected devices and set the polling interval. When enabled, CDP polling allows FortiNAC to query devices about other connected devices on the network. If a device has this discovery protocol enabled it gathers and stores information about devices it manages and devices it can contact on the network. Only devices with CDP enabled will respond to a CDP query. The device must be CDP capable and have CDP configured. See Set CDP polling on page 773.
Wireless Security	Allows you to configure SSID Mappings for the selected wireless device.

Network device groups

During the Setup process devices are added to FortiNAC. As devices are added, either through Discovery or manually, they are evaluated. Any device that is capable of L2 polling (polling hosts) is immediately placed in both the L2 Network Devices group and either the L2 Wired Devices or L2 Wireless Devices sub-group. These are default groups that are created in the database and populated for you. Devices that are not in one of these groups do not display on the L2 Network Devices window.

Additional L2 device sub-groups can be created and populated from the L2 Polling window.

A default L3 (IP -->MAC) group is created in the database also, but is not populated for you. You must add devices to this group manually from the L3 Polling (IP -->MAC) window. See L3 polling (IP address to MAC address) on page 750 for additional information.

If your device has multiple interfaces, each with a different IP address that is configured with its own SNMP settings, multiple representations of the same device will be added to FortiNAC. FortiNAC does not consolidate the duplicates in this case.

Add devices

Devices can be added to groups from either the L2 Polling window or the L3 Polling window.

1. Click **Network Devices > L2 Polling (Resync Hosts)** or **Network Devices > L3 Polling (IP-->MAC)**.
2. The Devices window displays.
3. Select one or more devices from the list. To select all devices click the **Select All** button.
4. Click **Add To Group**.
5. Click in the **Select Group** field and select a group for this device. If the group you need does not exist, click the **New** button and create the group first.

   Groups added from this window become a sub-group of the L2 Network Devices group or the L3 (IP --> MAC) group depending on where you are when the group is added. Groups that are not sub-groups of the L2 Network Devices group or the L3 (IP --> MAC) group cannot be seen in the Select Group drop-down. Click the Group Membership icon in the Views column of the Devices window to modify other types of groups for the selected device.
6. Click OK.

Remove devices

Devices can be removed from groups from either the L2 Polling window or the L3 Polling window.

1. Click **Network Devices > L2 Polling (Resync Hosts)** or **Network Devices > L3 Polling (IP-->Mac)**.
2. The Devices window displays.
3. Select one or more devices from the list. To select all devices click the **Select All** button.
4. Click **Remove From Group**.
5. Click in the **Select Group** field and select the group from which this device should be removed.
6. Click **OK**.

Groups view

Groups allow you to put like items together. By creating groups you eliminate the need to configure and control items within the group individually. For example, if you put a set of ports in a group, you can modify the group settings and affect all of the ports simultaneously. Groups can contain other groups.

Use the Groups view to add, modify, and delete groups within FortiNAC. FortiNAC comes with some standard groups over which it maintains ownership. These are marked as system groups. Create user-owned groups to group devices, ports, hosts or users. Associate these groups with scheduled tasks to perform a variety of functions.

Groups can be used to assign policies or roles to hosts or users.

If there are more than 2000 groups in the database, the groups are not automatically displayed. Instead, a confirmation dialog is shown asking if you would like to continue. Note that large numbers of records may load very slowly if not filtered. Choose **Yes** to display all groups or **No** to reduce the number displayed by using the filters.

See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.

Settings

Field	Definition
Name	Name used to identify the group.
Type	Indicates whether this is a group of ports, devices, IP phones, hosts, users or administrators.
Owner	Creator of the group. **System** indicates that the group was created by FortiNAC. **User** indicates that an administrative user created the group.
Members	The number of items contained within the group. For example, if this is a host group, this number indicates the total number of hosts in the group. If this group contains sub-groups, the number includes those items in each sub-group.
Days Valid	This column only applies to Host groups. The Expiration Date for hosts in this group is calculated using the number of days valid. For example, if a host is added to the group on 01/01/2011 and days valid is set to 30, the host's Expiration Date is set to 01/31/2011. The Expiration Date is set when a host is added to the group or when the Days Valid is edited. See Aging hosts in a group on page 843 for more information.
Days Inactive	This column only applies to Host groups. The number of days of network inactivity after which hosts in this group are removed from the database. For example, if this is set to three and a host in this group has not connected to the network for three days, the host record is removed from the database. See Aging hosts in a group on page 843 for more information.
Description	User specified description for the selected group.
Last Modified By	User name of the last user to modify the group.
Last Modified Date	Date and time of the last modification to this group.
Right click options	

Field	Definition
Copy Group	Creates a copy of the selected group.
Delete	Deletes the selected group.
Group Member Of	Displays groups in which this group is a member. A group can be a sub-group of another group of the same type. See Group membership on page 842.
In Use	Provides a list of other features that reference this group, such as a Policy Mapping or a Scheduled Task. See Group in use on page 842. System-owned groups will not be displayed as "In Use", even though they are in use by the system.
Manages	Applies only to Administrator groups. Administrator groups can be designated to manage groups of devices or hosts. See Limit user access with groups on page 841.
Modify	Opens the Modify Group window. See Modify a group on page 841.
Modify Device Properties	Applies only to Device groups. Allows you to modify multiple devices at the same time.
Set Aging	Allows you to set Days Valid and Days Inactive for the selected Host group. Days Valid and Days Inactive are used to calculate the date when the host is aged out of the database. Date is set when a host is added to the group or when Days Valid or Days Inactive fields are modified. See Aging hosts in a group on page 843.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.
Buttons	
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF.
Show Members	Opens the Group Members window and displays a list of all of the items within the group. Indicates whether the item is a member of the main group or a sub-group. See Show group members on page 842.

Add groups

Create additional groups to logically group elements that require network resources.

1. Select **System > Groups**.
2. From the Group view, click **Add**.

3. Enter a **Group Name**
4. Select a **Member Type**, which indicates the types of items that will be included in the group.

Type	Description
Administrator	Admin Users that access FortiNAC.
Hosts	Hosts that access the network.
Devices	Devices such as switches, computers, or printers.
Ports	Ports on switches on the network.
IP Phones	Internet phones that are connected to the network.
Users	Users that log onto the network.

5. For Host groups you have options for **Days Valid** and **Days Inactive**. These fields are used to calculate the expiration date used to age hosts out of the database. They are optional and should not be set if you have another mechanism that sets the expiration date. See Aging out host or user records on page 823 before you set these fields.
6. Enter a **Group Description**.
7. In the **All Members** pane select one or more items to be included in the group, then click the right arrow to move them to the Selected Members pane. For lists that do not include check boxes, select multiple items by holding down the Ctrl key while clicking.
8. To remove an object from the group, click on it and then click the left arrow.
9. To add subgroups to a group, select the **Groups** tab and select one or more groups to add as subgroups.
10. Click **OK** to save the new group.

Copy a group

1. Select **System > Groups**.
2. Locate the group to be copied.
3. Right-click on the group and select **Copy Group**.
4. Enter a name for the new group and click **OK**.
5. The new group appears in the **Groups View**. This group is owned by the user and not FortiNAC.

Delete a group

1. Select **System > Groups**.
2. Locate the appropriate group.
3. Right-click the group to select it and choose **Delete** to remove the group from the list.
4. Click **Yes** to confirm that you wish to delete the group.

Limit user access with groups

To control which hosts and ports Admin users can access you can place those Admin users in special groups. Then designate those special Admin groups to manage groups of hosts or ports.

Example:

Assume you have two Administrative Users that are responsible for monitoring medical devices and nurses in a hospital. They should not see any other data. To accomplish this you must configure the following:

- Place the nurses' workstations into a host group.
- Place the medical devices to be monitored into a host group.
- Place the ports where the medical devices connect into a port group.
- Place these two Administrative Users in a special Administrator Group.
- Assign these two Administrative User to a profile with permissions for Manage Hosts & Ports. Make sure the Manage Hosts & Ports setting on the General Tab of the profile is set to Restrict by Groups.
- Set the Administrator group to manage the nurses group, the medical device group and the port group.
- Remove these two Administrative Users from the All Management Group or they will have access to all hosts and ports.

When those Administrative Users log into the Admin user interface, they can only see data associated with the nurses, medical devices or the ports in the groups they manage.

Make sure to remove affected Administrative Users from the All Management group or they will continue to have access to all hosts and ports.

Administrative Users can still view all hosts and users from the Locate View if their Admin Profile gives them permission for that view, but they can only modify those that are in the group they are managing.

1. Create the group of hosts or ports. See Add groups on page 839 for instructions.
2. Create an Admin Profile for with permissions for Manage Hosts & Ports. Make sure the **Manage Hosts & Ports** setting on the **General Tab** of the profile is set to **Restrict by Groups**. See Add an admin profile on page 671
3. Create an Administrator group that contains the Administrative Users responsible for the devices or ports.
4. Remove the Administrative Users from the All Management group. See Modify a group on page 841 for instructions.
5. Right-click on the Administrator group of Administrative Users and select **Manages**.
6. On the **Manages** window, select the group(s) to be managed by marking them with a check mark.
7. Click **OK**.

Modify a group

Modify a group by adding additional items to the group or removing members from the group. Group description, Days Valid and Days Inactive can also be modified.

1. Select **System > Groups**.
2. Select the group.
3. Click the **Modify** button at the bottom of the window.
4. If this is a host group, **Days Valid** and **Days Inactive** can be modified. See Aging out host or user records on page 823 before modifying these numbers.
5. To remove items from the group, Ctrl-click items in the **Selected Members** panel, then click the left arrow button.
6. To modify subgroups, click the **Groups** tab and check or uncheck groups in the displayed list.
7. To add members to the group, Ctrl-click items in the **All Objects** panel, then click the right arrow button.
8. When you have selected all the members that are to be part of the group, click **OK**.

Group membership

Displays the groups that contain the selected group and allows you to modify group membership. For example, if you had a group called Staff, you might want to further sub-divide that by department, therefore you could have sub-groups such as Accounting or Human Resources within Staff. Selecting Human Resources from the Groups View and opening the Group Membership window would show that hierarchy. In addition the selected group can be added to or removed from other groups.

1. Select **System > Groups**.
2. Locate the appropriate group.
3. Right-click the group to select it and choose **Group Member Of** to display the groups that contain the selected group.
4. Modify the groups as needed and click **OK** to save your changes.

Show group members

This option displays a list of all of the items within the selected group. Indicates whether the item is a member of the main group or a sub-group.

1. Select **System > Groups**.
2. Select the group and click **Show Members** to display the list of items within the group.
3. Use the **Find** field to search for a particular item by typing in any part of its name and clicking **Next** or **Previous**. This field is case sensitive.

Group in use

To find the list of FortiNAC features that reference a group, select the group from the Groups View and click the In Use button. A message is displayed indicating whether or not the group is associated with any other features. If the group is referenced elsewhere, a list of each feature that references the group is displayed.

System-owned groups will not be displayed as "In Use", even though they are in use by the system.

Aging hosts in a group

Use the Set Aging window to set aging for the hosts in a selected Host group. Using the Aging feature populates the Expiration Date and the Inactivity Date fields on the Host Properties window. Hosts with existing age times are modified. This option is only valid for Host groups. If a host is a member of more than one group, the aging time is applied based on the last group to which the host was added or the last group whose aging times were modified.

Adding age times to existing hosts can cause some hosts to be removed from the database immediately depending on the creation date of the host record. If, for example, the creation date is 01/01/2010, today's date is 02/02/2010 and Days Valid is set to 5, then the Expiration Date calculated is 01/06/2010. The record is deleted immediately.

If hosts have been manually set to Never Expire, the Expiration Date and Inactivity Date fields for those hosts will not be modified by adding those hosts to a group with aging settings. See Properties on page 801, Set host expiration date on page 813 and Aging out host or user records on page 823 for additional information.

1. Select **System > Groups**.
2. Right-click on the host group and select **Set Aging**.
3. Enter a number for **Days Valid** or **Days Inactive**. The number in days valid is used to calculate the expiration date for each host in the group. The number in days inactive is used to calculate the inactivity date for each host.
4. Click **OK**.

System groups

The groups listed below are default system groups that exist within the FortiNAC database. They cannot be deleted. Some groups need to be fine tuned to your network. Details are included in the table below.

Group	Definition
Administrator	
All Management	FortiNAC administrative users with all management access rights. Initially contains only *Admin, root*. New Administrator and Administrative Users are added to this group automatically. This is the default group for e-mail notifications triggered by alarms. Add users to your own specific Administrator groups to give them privileges to manage (disable and enable) specific hosts and ports. If you place a user into your own Administrator group, be sure to remove that user from the All Management group. See Limit user access with groups on page 841.
Port	

Group	Definition
Access Point Management	Ports with authorized access points connected and FortiNAC serving DHCP. Examples are dumb hubs or wireless units. FortiNAC provides management of hosts connecting through these access points.
Authorized Access Points	Ports that have authorized access points connected. Access points that connect to these ports do not generate Multi Access Point Detected events or alarms and the port is not switched to another VLAN during, for example, Forced Registration or Role Management VLAN Switching. Access points that connect to ports that are not in this group do generate an event or alarm. Add switch ports that connect to hubs and wireless access points to this group.
Forced Authentication	Ports that participate in forced authentication when unauthenticated users connect. If you have a port in this group, when a host connects to this port and is unauthenticated, the port is put into isolation VLAN and the host is forced to authenticate.
Forced Registration	Ports that participate in forced registration when unregistered hosts connect. Add switch ports that participate in forced registration when an Unregistered Host connects to the Forced Registration port group. Only ports that participate have their VLAN ID set to the Registration VLAN when an Unregistered Host connects.
Forced Remediation	Ports that participate in forced remediation VLAN switching when hosts connect.
Reset Forced Default	Ports that return to the default VLAN when hosts disconnect.
Reset Forced Registration	Ports that return to Registration when hosts disconnect.
Role-Based Access	Ports that participate in role-based access and switch VLANs, based on the role of network devices, such as printers, when they connect. Add switch ports that participate in VLAN switching. Ports that participate have their VLAN ID set to the role specified for the connected network device. **Example:** A printer is set up with the role “Accounting”. When the printer connects to a port in this group, the printer is switched to the VLAN associated with the “Accounting” role.
System DHCP Port	The port used to discover unauthorized DHCP servers and validate authorized DHCP servers.
Device	
Authorized DHCP Servers	Servers that are authorized to serve DHCP on the network.
Bridging Devices	Devices that support the SNMP bridging MIB. This group has been replaced by the L2 Network Devices Group.

Group	Definition
Device Interface Status	Devices created through Discovery or created manually are automatically added to this group. Use this group in conjunction with the task scheduler to periodically update the interface status for each device in the group.
L2 Network Devices	Devices that support the Standard 802.1d Bridge Table. This group is also used for filtering the list of devices displayed on the L2 Network Devices window. As new L2 devices are discovered they are added automatically to this group and to either L2 Wired Devices or L2 Wireless Devices.
L2 Wired Devices	A sub-group of L2 Network Devices that is used for filtering on the L2 Network Devices window. L2 Wired Devices are added to this group automatically as they are discovered.
L2 Wireless Devices	A sub-group of L2 Network Devices that is used for filtering on the L2 Network Devices window. L2 Wireless Devices are added to this group automatically as they are discovered.
L3 (IP-->MAC)	This group must be populated manually with your L3 devices. The L3 group can be used for filtering on the L3 Polling window.
Physical Address Filtering	Devices that participate in the enabling and disabling of hosts. Add switches that participate in host disabling to this group. If a host is connected to a switch that is not in the Physical Address Filtering group, and that host is disabled through FortiNAC, the host remains connected to the network and is displayed as in violation. Add the switch regardless of whether a host is disabled through a Dead End VLAN, or through MAC address security.
Host	
Forced Scan Exceptions	Hosts that do not participate in forced scans.
Forced User Authentication Exceptions	Hosts that do not participate in forced user authentication.
Forced Remediation Exceptions	Hosts are scanned and can be marked "at risk", but are never put into remediation. Scan results are stored allowing the administrator to review the results and take corrective action without disrupting users on the network.
Global Agent Update Exceptions	Hosts in this group are excluded from automatic Persistent Agent Updates. Updates are controlled by MAC Address. If a host has more than one MAC Address, as long as any one of its MAC Addresses is listed in this group the host is not updated.
Registered Hosts	Group of all registered hosts.
Rogue Hosts	This group has a special property that controls whether or not rogue hosts can access the network. Under Group Properties for this group, the Access field can be set to either Deny or Allow. • **Deny**—If the Access field is set to Deny, rogue hosts in this group are denied network access until they register and any new unregistered hosts are automatically put into the group as they connect to the network. • **Allow**— If the Access field is set to Allow, rogue hosts in this group are permitted to access the network and any new unregistered hosts are not added to the group.

Group	Definition
	Devices that are not in the Topology View but are connected to managed switches are created as rogue hosts. If rogue hosts are denied access to the network, they are disabled. To prevent this from causing problems with new devices such as printers, lab hosts or servers, you must register them as devices or as hosts. See Register a host as a device on page 812 or Add or modify a host on page 807 for detailed instructions.

Customer defined groups

User-owned groups are typically created to associate devices, ports, IP phones or hosts. You can associate these groups with scheduled actions to perform a variety functions. Typical groups include the following:

Groups	Notes
Ports	Port groups can be used for a variety of purposes. Use the Fixed Day Task option in the Scheduler with the Disable Ports and Enable Ports actions to disable or enable ports on a date or time schedule. You can nest port groups to make it easier to add ports to the FortiNAC owned groups, such as Forced Registration groups.
Departments, Staff, Divisions	You can use Host groups for a variety of purposes. Use Disable Hosts and Enable Hosts on a date or time schedule with the Fixed Day Task option in the FortiNAC Scheduler. Nest host groups to make it easier to control access over large groups of students. Create host groups for each grade level to control each group through its own scheduled task. You can also create a host group that contains each grade level and schedule it to disable or enable the entire student population with a single task.
Administrator	This group contains Administrative Users who can manage (disable and enable) ports or hosts contained in the associated port or host groups. For example, place Administrative User "John Smith" in the Northeast Admins group. Set the Northeast Admins group to manage the "Department 1 Ports" and the "Department 1 hosts". When John Smith logs in to FortiNAC, he can find and disable any host or port in those groups. See Limit user access with groups on page 841.

Admin auditing

The Admin auditing log tracks all changes made to an item in the system. Users with admin auditing permissions will see a change in the admin auditing log whenever data is added, modified, or deleted. Users can see what was changed, when the change was made, and who made the change.

Changes made through the CLI are tracked in the admin auditing log; however, the user ID for the user who made the change will appear as "CLI Tool".

Changes can be filtered by the name of the item that was changed, the action taken, the date when the change occurred, the user ID for the user who made the change, and the type of item that was changed.

Changes made to the following items are not currently audited:

- Trap MIB Files
- NTP and Time Zone settings
- Adapters
- RADIUS Domain Mappings
- RADIUS Server Defaults (Primary RADIUS Server Default, Secondary RADIUS Server Default)
- Security Applications
- Alarms
- Certificates
- Portal SSL Settings
- Portal Configuration Styles
- Mobile Providers
- Database Backup settings (excluding the Backup Timeout)
- Changes to the License Key

Changing the name of a device or moving a device to a new container will result in a separate audit entry for each port on the device.

Similar to Events and Alarms, Admin Auditing archives and purges audits made to Hosts, Users, or Elements.

Configuration

Users must have the Admin Auditing permissions in order to view the Admin Auditing log.

1. Click **Users > Admin Profiles**.
2. Select an admin profile from the list.
3. Click **Add** or select an admin profile and click **Modify**.
4. Select the **Access** check box next to **Admin Auditing**.
5. Click **OK**.

Accessing the auditing log

1. Click **Logs > Admin Auditing**.
2. Click a row to view the entire list of changes in **Audit Details**.
3. Click the name of the item that was changed to open a dialog displaying all changes that have been made to the item.

Settings

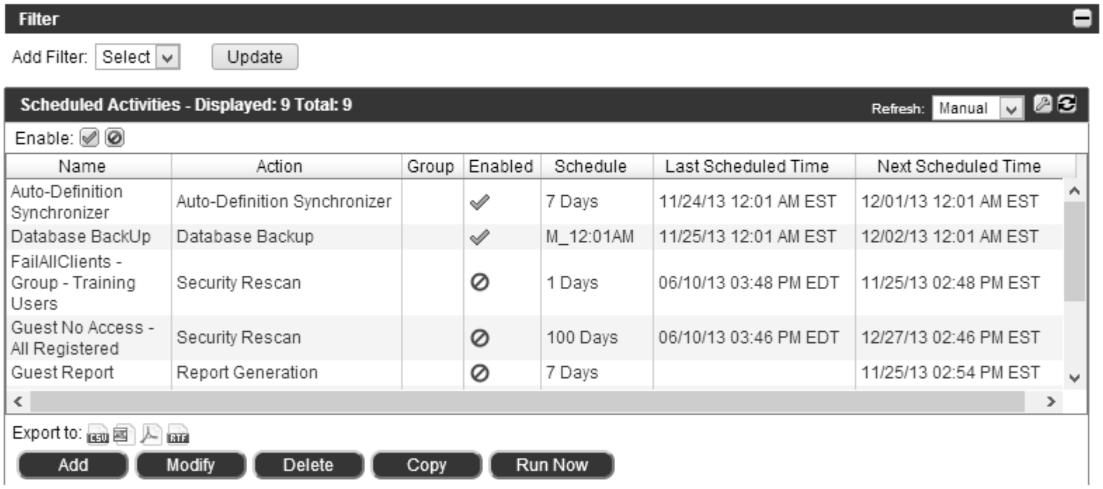
Field	Definition
Add Filter drop-down list	Allows you to select a field from the current view to filter information. Select the field from the drop-down list, and then enter the information you wish to filter. See Filters on page 15.
Update button	Displays the filtered data in the table.
Admin auditing	
Date	The date and time when the change was made.
User ID	The user ID of the user who made the change. The user ID appears as "CLI Tool" when changes are made using CLI tools.
Action	Shows whether the change involved adding, modifying, or deleting information.
Type	The type of item that was changed.
Name	The name of the item that was changed. Click the name to view a dialog containing all changes that have been made to the area.
Summary	The first four lines of what was changed on the specified date.
Audit Details	Displays all details of the change made to the item on the specified date. This information appears when you click a row representing a change in the Admin Auditing table.
Buttons	
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.

Scheduler view

Use the scheduler view to add, modify and delete scheduled tasks within FortiNAC. A task is an action that is scheduled to occur at a specified time and is usually associated with a specific group.

There are two types of scheduling: fixed day and repetitive. A fixed day task is one in which you schedule a task to run on a combination of days of the week and times of the day, such as Mondays at 1:00 pm and Fridays at 10:00 am. A repetitive task is one that you schedule to start on a given day, at a certain time, for the number of times you specify, such as every 10 days starting today. You can set the repetition rate to any number of minutes, hours, or days.

See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.



Scheduled Activities - Displayed: 9 Total: 9

Name	Action	Group	Enabled	Schedule	Last Scheduled Time	Next Scheduled Time
Auto-Definition Synchronizer	Auto-Definition Synchronizer		✓	7 Days	11/24/13 12:01 AM EST	12/01/13 12:01 AM EST
Database BackUp	Database Backup		✓	M_12:01AM	11/25/13 12:01 AM EST	12/02/13 12:01 AM EST
FailAllClients - Group - Training Users	Security Rescan		⊘	1 Days	06/10/13 03:48 PM EDT	11/25/13 02:48 PM EST
Guest No Access - All Registered	Security Rescan		⊘	100 Days	06/10/13 03:46 PM EDT	12/27/13 02:46 PM EST
Guest Report	Report Generation		⊘	7 Days		11/25/13 02:54 PM EST

Settings

Fields used in filters are also defined in this table.

Field	Definition
Enable Disable Buttons	Enables or disables the selected task.
Name	User created name for the task.
Action	Action being performed by the scheduler.
Group	Action is limited to the group listed.
Enabled	Indicates whether the task is enabled or disabled. Disabled tasks do not execute.
Schedule	Days and times that this task is scheduled to run.
Last Scheduled Time	Last time the task was executed by the scheduler.
Next Scheduled Time	Next time the task will execute.
Description	User specified description of the scheduled task.

Field	Definition
Last Modified By	User name of the last user to modify the scheduled task.
Last Modified Date	Date and time of the last modification to this scheduled task.
Right click options	
Copy	Copy the selected task to create a new record.
Delete	Deletes the selected task.
Disable	Disables the selected task.
Enable	Enables the selected task.
Modify	Opens the Modify Scheduled Activity window for the selected rule.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.
Run Now	Executes the selected task immediately.
Buttons	
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.

Add a task

1. Select **System > Scheduler**.
2. From the **Scheduler** view, click **Add**.
3. The **Enabled** check box is selected by default. Uncheck it if you want this task to be disabled.
4. Enter a **Name** for the task and an optional description.
5. In the **Action Type** field, select either **System** or **CLI**. System actions are predefined tasks that you can choose to execute. CLI actions are sets of command line instructions that are created in the CLI Configuration View and saved to be executed elsewhere in the program.
6. Select the **Action** from the list of system or CLI actions. Refer to the table below the instructions for more information.

   See CLI configuration on page 928 for information on creating CLI actions.

7. From the **Group** dropdown list, select the group that the action will be performed on. The list contains only the group types specific to that Action.

8. From the **Schedule Type** drop down list, select either **Fixed Day** or **Repetitive** and set the day and time that the task is to be performed.
9. A **Fixed Day Task** is one in which you schedule a task to run on a combination of days of the week and times of the day, such as Mondays at 1:00 pm and Fridays at 10:00 am. Select the day(s) and time to run the task.
   a. Click the box next to the day(s) to select the day.
   b. Click the down arrows and select the hour, minutes, and AM or PM from the drop-down list for each day.
   c. To enter days/times more quickly, use the **Set Multiple Days** button to set multiple days with the same time.
   d. To remove all settings click the **Clear All** button.
10. A **Repetitive Task** is one that you schedule to start on a given day, at a certain time, for the number of times you specify, such as every 10 days starting today. The repetition rate can be set to any number of minutes, hours, or days.
    a. Enter the **Repetition Rate** using whole numbers.

A repetition rate of zero causes the task to run only once.

    b. Click the down arrow and select **Minutes**, **Hours**, or **Days** from the drop-down list.
    c. Enter the date and time for the task to run in the **Next Scheduled Time** field using the format MM/DD/YY hh:mm AM/PM Time Zone.
    d. Click **Update** to update the **Next Scheduled Time** field or change the **Repetition Rate**.

The new Repetition Rate does not take effect immediately. It starts the next time the scheduled task runs. For the new Repetition Rate take effect immediately, click the **Update** button.

11. Click **OK**.

Actions

Actions	Group Type	Description
Certificate Expiration Monitor	None	Generates a warning, critical warning, and expiration events for the certificates listed in Certificate Management. See Certificate management on page 161
Custom Script	None	Executes the selected command line script located in /home/cm/scripts.
Database Archive and Purge	None	Archives and purges Event, Connection, and Alarm records that are older than 7 days. The number of days is configurable in the Event And Alarm Age Time field on the FortiNAC Properties window. See Database archive on page 210.
Database Backup	None	Back up the FortiNAC database. The database backup files are stored on the local appliance at `/bsc/campusMgr/master_loader /mysql/backup`.

Actions	Group Type	Description
		See Backup to a remote server on page 220 for more information on configuring backups to a remote server.
Disable Adapters	Hosts	Prohibits network access to all adapters in the associated host group. Disables the adapters but not the host itself.
Disable HP/NT Port Security	Devices	Disables port security configuration on all HP/NT devices in the associated group. Use Port Security to disable hosts if DeadEnd VLANs are not used on the network.
Disable Ports	Port	Administratively disables all ports in the associated group.
Enable Adapters	Hosts	Allows network access to all hosts in the associated group.
Enable HP/NT Port Security	Devices	Enables port security configuration on all HP/NT devices in the associated group. Use Port Security to disable hosts if DeadEnd VLANs are not used on the network.
Enable Ports	Port	Administratively enables all ports in the associated group.
Modify Device VLAN Values	Ports	Writes the indicated VLAN value to the switch and changes only the Current VLAN value in the FortiNAC device model. You must specify the VLAN value.
Purge Remediation Output Files (Reports)	None	Purges the output files from all the Nessus scans performed since the last purge. Nessus Servers and scans are no longer supported.
Resynchronize Device	Devices	Allows you to sync a device with FortiNAC after making a change to the device (e.g., adding a VLAN, role or SSID for a wireless device).
Role Assignment	Hosts	Modifies the Role for the associated group of hosts or users. You must specify the new role.
SSID Assignment	Devices	Maps VLAN IDs to SSIDs. You must specify the both the VLAN ID and the SSID.
System Backup	None	Back up the FortiNAC system files. The system backup files are stored on the local appliance at `/bsc/backups/<server name>` See System backups on page 223.

Actions	Group Type	Description
Update Default VLAN Values	Ports	Sets the Default VLAN value for the port in FortiNAC device model to the value entered in the scheduled task. You must specify the VLAN value.
Update Interface Status	Devices	Reads and updates the interface status for each port on the devices in the associated groups.
Update Remediation Center	None	Connects to Nessus.org and updates the Nessus server with the scan IDs for the version running on the application server. Also connects to Fortinet and updates the server with the latest scan profiles. If you create scan profiles with Nessus Wx, you must run this task to ensure that those scan profiles will work properly. Nessus Servers and scans are no longer supported.

Add other scheduled tasks

Tasks can be added to the Scheduler in two ways. You can go directly to the scheduler and create a new task for a group. Certain tasks can only be created from other configuration windows. For example, to schedule a weekly update of your Auto-Def file you must go to the Auto-Def Update window. This task is created and displays on the Scheduler window, but it cannot be created within the Scheduler window. The table below describes scheduled tasks that are created outside the Scheduler window, but, once created, display within that window.

Task	Definition
Scan	Scans that are part of Endpoint Compliance Policies for hosts can be set to run at regular intervals. See Schedule a scan on page 441.
Proactive Scanning	Security Policy schedules are affected by Proactive Scanning.
Report Generation	Schedule reports to be automatically generated. See Schedule reports on page 908.
Auto Definition Synchronizer	Weekly updates to your Auto-Def file can be scheduled.
Synchronize Users From Directory	Schedule your LDAP or Active Directory to synchronize with your user database. See Schedule synchronization on page 93.
Security Rescan	Schedule your scanned host list to be cleared so that Admin scans can begin again. See Clear scanned hosts list on page 484.
Verify DHCP Servers	Schedule a poll for rogue DHCP servers. See Rogue DHCP server detection on page 122.

Copy a task

1. Select **System > Scheduler**.
2. Use the filters to display a list of tasks.
3. Click the task to select it.
4. Click **Copy**.
5. Enter a name for the new task.
6. Modify other fields as needed.
7. Click **OK**.
8. The new task appears in the **Scheduler**.

Delete a task

1. Select **System > Scheduler**.
2. Use the filters to display a list of tasks.
3. Click the task to select it.
4. Click **Delete**.
5. Click **Yes** to delete the task.

Modify a task

You can change a task from a Repetitive task to a Fixed Day task by changing the task's date, time, and repetition rate. You can also change the group associated with the task and the name of the task. For Settings see Add a task on page 850.

1. Select **System > Scheduler**.
2. Use the filters to display a list of tasks.
3. Click the task to select it.
4. Click **Modify**.
5. Modify the data as needed.
6. Click **OK**.

Run task now

To run a scheduled action at any time:

1. Select **System > Scheduler**.
2. Use the filters to display a list of tasks.

3. Click the task to select it.
4. Click **Run Now**.

Event management

Event management allows you to specify which events to generate and whether to log the event records on another server in addition to the local appliance. You can limit the number of events generated by selecting a group for each event. Event messages are only created when the event occurs within the specified group.

Specify threshold values for the self-monitoring events by clicking the **Event Thresholds** button at the top of the view. These thresholds affect the **Performance Summary Panel** on the dashboard. They can be edited here or from the **Performance Summary Panel**. See Performance on page 43 for additional information.

Some events are generated frequently and may not be necessary for day to day operations. Review the list of events and determine which ones to enable to provide you with the most useful feedback. You may choose to enable an event for a short period of time, such as to find a particular host when it connects to the network. See the example below for a scenario in which enabling a particular event might be useful.

Example: Finding a stolen device

This is a scenario for locating a stolen or missing host:

1. Create a group that contains only the information for that host (including all wired and wireless sibling records).
2. Enable the Host Connected event for the new group. When the stolen host connects to the network through the wired or wireless connection, a Host Connected event is generated.
3. Map the Host Connected event to an alarm to receive a notification that the host has connected. You may also take an action against that host if you specified one in the mapping.
4. When you are notified that the stolen host has connected to the network, use the Host View to determine the device and port to which this host is connected.

Events are generated for all components, such as devices, hosts or ports, unless you reduce the output by selecting a specific group . See Events and alarms list on page 868 for event definitions.

Events can be sent to an external log host. See Log events to an external log host on page 860.

See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.

Settings

Fields used in filters are also defined in this table.

Field	Definition
Event Thresholds	Opens the Event Thresholds dialog to set thresholds to monitor license usage, memory usage, process thread counts, and disk space. Exceeding these thresholds generates specific events. See Event thresholds on page 858.
Events	
Log	Indicates the state of the selected event and where it will be logged if it is generated. • **Disabled**—Event is disabled and will not be generated or logged anywhere. • **Internal**—Logs only to an internal events database. • **External**—Logs only to an external host.

Field	Definition
	• **Internal & External**—Logs both to an internal events database and an external host.
Event Name	Name of the event.
Group	Group name of a group of elements, such as, port group, device group or user group used to limit generation of the selected event to the items in the group. If set to All Groups, then the event is generated for all items, such as ports, devices, hosts or users. If no group is displayed, an event is generated for the system, and not a specific item.
Group Type	Indicates whether this event applies to a group of ports, devices, hosts, users or administrators.
Last Modified By	User name of the last user to modify the event.
Last Modified Date	Date and time of the last modification to this event.
Right click options	
Modify Group	Opens the Modify Group window.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847. You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671.
Disable Logging	Disables the event is disabled. The event will not be generated or logged anywhere.
Log Internal	Logs the event only to an internal events database.
Log External	Logs the event only to an external host.
Log Internal & External	Logs the event to both an internal events database and an external host.
Buttons	
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.
Options	Allows you to change the log or group setting for one or more selected events.
Modify Group	Change the group setting for one or more selected events.

Enable and disable events

Use the Event Management window to select which events will be logged.

Events for the system

1. Click **Logs > Event Management**. The Event Management view appears.
2. Use the Filters to locate the appropriate event. Refer to Event management on page 856 for Filter Settings.
3. To enable an event, select one or more events and click the **Options** button. Select one of the following:
   - **Internal**—Logs only to an internal events database.
   - **External**—Logs only to an external host.
   - **Internal & External**—Logs both to an internal events database and an external host.

   Any event that is logged is enabled.
4. To disable an event, select one or more events and click the **Options** button. Select **Disable Logging**.

To log events on an external log host, you must first add the log host to FortiNAC. See Log events to an external log host on page 860 for instructions.

Events for a specific group

Logging events for a specific group limits the number of times the event is generated. The event will only be generated for members of the selected group.

1. Click **Logs > Event Management**. The Event Management view appears.
2. Use the filters to locate the appropriate event. Refer to Event management on page 856 for filter settings.
3. Select one or more events and click the **Options** button. Choose one of the logging options to enable the event.
4. Click the **Modify Group** button.
5. Click in the **Group** drop-down box and select the group for which this event will be enabled.
6. Click **OK**.

Event thresholds

This option allows you to monitor license usage, memory usage, process thread counts, and disk space, and establish thresholds for the processes and hard drives. Each process type has its own thread count and maximum memory allocations. The percentages in the thresholds are not relative to the total memory available on the appliance; they are relative to the maximum amounts of memory that each loader process is allowed to consume.

View the memory allocated to each process in the Performance panel on the Dashboard. The number of threads used by the process is also contained in the panel. See Performance on page 43.

When a threshold is exceeded, an event is generated. Each event has an associated alarm which is mapped by default. Each specific event or alarm mapping is configured so that multiple events for a specific process or threshold results in a single alarm. Modify the default mappings in Event to Alarm Mappings. You can also configure a specific action, such as email notification. See Map events to alarms on page 888 for details.

Settings

Threshold	Description
License thresholds	
Concurrent Licenses Warning/Critical	Generated when the license usage threshold is reached. This threshold is a percentage of the total number of licenses configured. Default Warning = 75%. Default Critical = 95%.
Hardware thresholds	
Hard Disk Usage Warning / Critical	Generated when the disk usage threshold is reached. This threshold is a percentage of the space allocated for the bsc and var partitions. The percentage is calculated for each partition separately. When any one partition reaches the threshold the event is generated. Thresholds calculated for individual partitions are never combined. Therefore if the combined total crosses the threshold, no event is generated. Default Warning = 85%. Default Critical = 95%.
Memory Usage Warning / Critical	Generated when the memory usage threshold is reached for the appliance. This threshold is a percentage of the total allocated memory. Default Warning = 85%. Default Critical = 95%.
Network Topology Size Warning / Critical	Generated when the system sizing tool detects that the appliance has reached the threshold for possible connections. This threshold is a percentage of the total connections that the appliance can manage. Default Warning = 85%. Default Critical = 95%.
Software thresholds	
Process Thread Count Warning / Critical	Generated when the process thread count threshold is reached. This threshold is a specific number of threads the process is using. MasterLoader: Default Warning = 500. Default Critical = 575. Nessus: Default Warning = 100. Default Critical = 125.
Process Memory Usage Warning / Critical	Generated when the memory usage threshold is reached for the process. This threshold is a percentage of the total allocated memory. Default Warning = 85%. Default Critical = 95%.

Set thresholds for self-monitoring events

1. Click **Logs > Event Management**.
2. Click the **Event Thresholds** button at the top of the window.
3. Click the **License Tab**. Enter the value for the warning and critical levels of the license usage.
4. Click the **Hardware Tab**. Enter the value for the warning and critical levels of the hardware thresholds for hard disk and memory usage.
5. Click the **Software Tab**. Enter the value for the warning and critical levels of the software thresholds for each

system process.

6. Click **OK**.

Log events to an external log host

To log events on an external log host, you must first add the log host to the Log Receivers View. Once you have added the log host server, configure the events to be logged externally on the Event Management View. The events will be sent as Syslog messages or SNMP Traps.

Add a server

1. Click **System > Settings**.
2. In the tree on the left select **System Communication > Log Receivers**.
3. Click **Add** to add a log host.
4. Select the type of server.
5. Enter the IP address of the server.
6. Enter the configuration parameters for the type of log host. The standard port information for each host type is automatically entered. See the table below for detailed information on each type of server.
7. Click **OK**.

Settings

Field	Definition
Type	Type of server that will receive Event and Alarm messages. Options include: Syslog CSV, SNMP Trap, and Syslog Command Event Format (CEF).
IP address	IP address of the server that will receive Event and Alarm messages.
Port	Connection port on the server. For Syslog CSV and Syslog CEF servers, the default = 514. For SNMP Trap servers the default =162

Field	Definition
Facility	Displays only when Syslog is selected as the Type. Allows you to configure the message type. The default is 4. Options include: • 0 kernel messages • 1 user-level messages • 2 mail system • 3 system daemons • 4 security/authorization messages • 5 messages generated internally by syslogd • 6 line printer subsystem • 7 network news subsystem • 8 UUCP subsystem • 9 clock daemon • 10 security/authorization messages • 11 FTP daemon • 12 NTP subsystem • 13 log audit • 14 log alert • 15 clock daemon • 16 local use 0 (local0) • 17 local use 1 (local1) • 18 local use 2 (local2) • 19 local use 3 (local3) • 20 local use 4 (local4) • 21 local use 5 (local5) • 22 local use 6 (local6) • 23 local use 7 (local7)
Security String	Displays only when SNMP is selected as the Type. The security string sent with the Event and Alarm message.

Configure events to log externally

1. Click **Logs > Event Management**.
2. Use the filters to locate the appropriate event. Refer to Event management on page 856 for filter settings.
3. For each event that should be logged externally, select one or more events and click the Options button. Select one of the following:
   - **External**—Logs only to an external host.
   - **Internal & External**—Logs both to an internal events database and an external host.

Syslog format

The following is an example of a syslog message:

```
<37>Apr 10 11:42:16 : 2009/04/10 11:42:16 EDT,3,2587,Probe - MAP IP To MAC
Success,0,1127,,BuildingB-3750,192.168.10.1,,Successfully read IP address mappings
from device BuildingB-3750
```

Format

Column	Data From Example	Definition
1	<37>	Syslog category: This is the defined facility and the severity Default Facility = 4 Security message Severity = 5 Notice
2	Apr 10 11:42:16 :	Time of the syslog generation.
3	2009/04/10 11:42:16 EDT	Log time.
4	3	Log type: • 1 Event • 2 Alarm • 3 Security Alarm
5	2587	Database ID AlarmID or ElementID
6	Probe - MAP IP To MAC Success	Name of the event that generated the syslog message.
7	0	Severity: • 0 Normal • 1 Minor • 2 Major • 3 Critical
8	1127	Entity ID
9		Unique Identifier (User ID)
10	BuildingB-3750	Entity Name
11	192.168.10.1	Entity IP address
12		Entity Physical Address
13	Successfully read IP address mappings from device BuildingB-3750	Log Message

SNMP trap format

The following is an example of an SNMP message:

```
1.3.6.1.4.1.16856.1.1.5="2009/04/10 11:37:02 EDT", 1.3.6.1.4.1.16856.1.1.6=1,
1.3.6.1.4.1.16856.1.1.7=2585, 1.3.6.1.4.1.16856.1.1.8="Probe - MAP IP To MAC
Success", 1.3.6.1.4.1.16856.1.1.9=0, 1.3.6.1.4.1.16856.1.1.10=1127,
1.3.6.1.4.1.16856.1.1.15=, 1.3.6.1.4.1.16856.1.1.11=BuildingB-3750,
1.3.6.1.4.1.16856.1.1.12=192.168.10.1, 1.3.6.1.4.1.16856.1.1.13=,
1.3.6.1.4.1.16856.1.1.14="Successfully read IP address mappings from device
BuildingB-3750."
```

Format

MIB Object	Data From Example	Definition
1.3.6.1.4.1.16856.1.1.5	"2009/04/10 11:37:02 EDT"	The log time stamp in the format YYYY/MM/DD hh:mm:ss z
1.3.6.1.4.1.16856.1.1.6	1	The type of log message 1 - Event message 2 - Alarm Message
1.3.6.1.4.1.16856.1.1.7	2585	The database identifier of the log message
1.3.6.1.4.1.16856.1.1.8	"Probe - MAP IP To MAC Success"	Name of the event that generated the syslog message.
1.3.6.1.4.1.16856.1.1.9	0	The log severity 0 - Normal 1 - Minor 2 - Major 3 - Critical
1.3.6.1.4.1.16856.1.1.10	1127	The database identifier of the log entity
1.3.6.1.4.1.16856.1.1.15		The unique identifier of the log entity "User ID"
1.3.6.1.4.1.16856.1.1.11	BuildingB-3750	The textual name of the log entity
1.3.6.1.4.1.16856.1.1.12	192.168.10.1	The IP address of the log entity. The format is 0.0.0.0"
1.3.6.1.4.1.16856.1.1.13		The Physical address of the log entity. The format is 00:00:00:00:00:00"
1.3.6.1.4.1.16856.1.1.14	"Successfully read IP address mappings from device BuildingB-3750."	The textual log message

Common event format (CEF)

Fields contained within a CEF syslog message include:

```
CEF:Version|Device Vendor|Device Product|Device Version|Signature
ID|Name|Severity|Extension
```

Example:

```
<37>Jul 22 11:24:20 : CEF:0|Fortinet|NAC Control Server|4.1.1.219.P9|6111|Login
Failure|1|rt=Jul 22 11:24:20 602 EDT cat=Network shost=NAC Director msg=User qa
failed to log in.
```

Format

Column Title	Data From Example	Definition
Facility	<37>	Syslog category: This is the defined facility and the severity Default Facility = 4 Security message Severity = 5 Notice This is not part of the CEF format, but is contained within the syslog message.
Date/Time	Jul 22 11:24:20	Date and time the syslog message was generated. This is not part of the CEF format but is contained within the syslog message.
CEF: Version	CEF:0	Version number defines the fields that are expected to follow this field.
Device Vendor	Fortinet	These fields uniquely identify the type of device sending the syslog message. In this case, the sending entity is FortiNAC.
Device Product	NAC Control Server	
Device Version	4.1.1.219.P9	
Signature ID	6111	Unique identifier per event type. This can be a string or an integer.
Name	Login Failure	Name of the event that generated the syslog message.
Severity	1	Severity: 0 Normal 1 Minor 2 Major 3 Critical
Extension	rt=Jul 22 11:24:20 602 EDT cat=Network shost=NAC Director msg=User qa failed to log in.	Extension is a place holder for additional data. The extensions contained in this message include: **rt** - receiptTime - Time stamp that indicates when the event was generated. **cat**-category-Type of device sending the syslog message. **msg** - message- Message giving more details about the event.

Examples of syslog messages

Here are some examples of syslog messages that are returned from FortiNAC. In these examples, the Syslog server is configured as follows:

- Type: Syslog
- IP address: a.b.c.d
- Port: 514
- Facility: Authorization

Event	Description	Syslog Message
Login Success	This is the event that is logged with a user logs into the Admin UI.	02-28-2014 08:16:04 Auth.Notice 192.168.34.31 Feb 27 22:16:14 : 2014/02/27 22:16:14 EST,1,545570,Login Success,0,12,,,,,User root logged in.
Map IP To MAC Failure	This is a legacy event logged when a scheduled task runs (these are no longer used for IP-MAC) and the ARP is not read.	--
Probe - Map IP To MAC Failure	This is the event when we fail to poll and L3 device for IP->MAC (reading Arp Cache) L3 Polling	02-28-2014 09:00:14 Auth.Notice 192.168.34.31 Feb 27 23:00:24 : 2014/02/27 23:00:24 EST,1,545702,Probe - MAP IP To MAC Failure,0,28,,Switch,192.168.34.1,,Failed to read IP address mappings from device Switch.
User Logged Out	This is the event that is logs when a user logs out of the Admin UI.	02-28-2014 08:48:55 Auth.Notice 192.168.34.31 Feb 27 22:49:04 : 2014/02/27 22:49:04 EST,1,545670,User Logged Out,0,12,,,,,User root Logged Out.
User Logged off Host	This event is logged when a user logs off a host	02-28-2014 08:44:25 Auth.Notice 192.168.34.31 Feb 27 22:44:34 : 2014/02/27 22:44:34 EST,1,545655,User Logged off Host,0,4155,,,,,"User Man, Bat logged off session 1 on host BRADSUPP7-LT
User Logged onto Host	This event is logged when a user logs onto a host	02-28-2014 08:37:58 Auth.Notice 192.168.34.31 Feb 27 22:38:07 : 2014/02/27 22:38:07 EST,1,545633,User Logged onto Host,0,4155,,,,,"User Man, Bat logged onto session 1 on host BRADSUPP7-LT"
User Remotely Connected to Host	An event that is logged when a user remotely connected to a terminal session on a host using the PA	--
User Locked Session	This event is logged when a user locks his workstation	02-28-2014 08:49:53 Auth.Notice 192.168.34.31 Feb 27 22:50:03 : 2014/02/27 22:50:03 EST,1,545681,User Locked Session,0,4155,,,,,"User Man, Bat locked session 2 on host BRADSUPP7-LT"

Event	Description	Syslog Message
User Unlocked Session	This event is logged when a user unlocks his workstation	02-28-2014 08:52:07 Auth.Notice 192.168.34.31 Feb 27 22:52:16 : 2014/02/27 22:52:16 EST,1,545691,User Unlocked Session,0,4155,,,,,"User Man, Bat unlocked session 2 on host BRADSUPP7-LT"

View events currently mapped to alarms

1. Select **Logs > Event to Alarm Mappings**. The Event to Alarm Mappings view appears.
2. To add a new mapping see Add or modify alarm mapping on page 892 for instructions.

Events view

The events view displays the contents of the events log. The events log is an audit trail of significant network and FortiNAC incidents. Events are logged when they are enabled in the events management view. See Enable and disable events on page 857.

To access the events view, select **Logs > Events**.

Settings

Field	Definition
First Name	First Name of the user associated with the event, such as the registered owner of a host or an admin user.
Last Name	Last Name of the user associated with the event.
Login Name	User name from the credentials of the user who was logged in and associated with the event.
Element Name	Name of the device, Admin User, server or process associated with the event.
Element Type	Type can be Device, Port, Container, Process, or All.
Group	Group name of a group of elements, such as, port group, device group or user group.
Pause	If enabled, prevents the Events List from refreshing and adding new records to the screen. In an environment with a large number of events, you may need to pause the refresh in order to research an issue.
Date	Date and time that the event occurred.
Event	Event name. See Events and alarms list on page 868.
Element	Element associated with the event, such as a user, Admin User, device, port, or process.
Message	A textual description of the selected entry.
Note	An area for user notes.
Buttons	
Import	Import historical events from an Archive file. See Import archived data on page 696.
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.
Set Note	Opens a notes window and allows you to add notes to the selected event. See Event notes on page 868.

Event notes

You can add notes to an event entry to clarify why the event happened, track the resolution of a problem, or add general information.

1. Select **Logs > Events**.
2. Use the filters to locate the appropriate event. Refer to Events view on page 867 for Filter Settings.
3. Select the event.
4. Click **Set Note**.
5. Enter the note text or modify the existing note.
6. Click **OK**.
7. The note text appears on the **Notes** column on the **Events View**.

Events and alarms list

When events are enabled, they can be enabled for All Groups or for a single group. Depending on the event you may not want to enable it for all groups because the volume of events would be overwhelming. For example, if you enabled the Host Connected event for all groups, you would receive an event message every time someone connects to the network.

When you look at an event in the Event Viewer, additional information is provided about that occurrence of the event. It might include information such as, user name, IP address, MAC Address or location.

Each event has a corresponding alarm that can be configured. See Map events to alarms on page 888.

Event names highlighted in gray are no longer used. However, they are still available in the Event Log to accommodate importing older data that may contain those events.

Events and alarms

Event	Definition
Access Configuration Modified	Generated whenever an Access Configuration is modified.
Access Policy Modified	Generated whenever an Access Policy is modified.
Adapter Created	Generated whenever an adapter is added to a host.
Adapter Destroyed	Generated whenever an adapter is removed from a host.
Add/Modify/Remove Blocking via REST API	Generated whenever a REST API request is received that creates or removes a Control Task.
Add/Modify/Remove Host	Generated whenever a trap is received that adds, modifies or removes a host record in the database.
Add/Modify/Remove Host via REST API	Generated whenever a REST API request is received that adds, modifies or removes a host record in the database.

Event	Definition
Add/Modify/Remove User	Generated whenever a trap is received that adds, modifies or removes a user record in the database.
Add/Modify/Remove User via REST API	Generated whenever a REST API request is received that adds, modifies or removes a user record in the database.
Admin User Created	Admin user created. User types are not included in the event message.
Admin User Destroyed	Admin user deleted from the database.
Admin User Logged Out	Admin user logged out of the user interface.
Admin User Login Failure	Admin user failed to log into the user interface.
Admin User Login Success	Admin user logged into the user interface.
Admin User Timed Out	Admin user was logged out of the User Interface based on the settings in **Users > Admin Users > Timeout Settings** in the Administrative Interface Inactivity Time (Minutes) field.
Administrative Status Success	User has gone into Port Properties for an individual port and successfully turned the Admin Status on or off.
Agent - Unrecognized Vendor OUI	No longer used. Generated when an agent scans a host and returns MAC addresses that have a Vendor OUI that is not included in the Vendor OUI Management list in FortiNAC.
Agent Update Failure Agent Update Success	Indicates whether or not an agent updated successfully.
Agent Message Sent	Message sent from FortiNAC user to one or more hosts. Only hosts running the Persistent Agent can receive messages. This event is not generated if the message fails to send.
Alarm Created	Indicates that an event has caused an alarm.
Appliance Weak Password(s)	Indicates that password for the appliance and/or the Admin UI are either a default factory password or are not complex enough. It is recommended that you modify the password. Otherwise, your network may be at risk for a security breach.
Application Server Contact Lost	Generated when contact is lost to the Nessus plugin in a 1200/8200 pair. Requires contact to be established before contact can be lost.
Application Violation	FortiNAC can receive traps from external applications hosted on servers modeled in the Topology tree as Pingable or Server devices. This event is generated when a trap is received. Traps might be used to indicate intrusion or that a threshold has been exceeded. A Host Application Violation event can be generated at the same time.

Event	Definition
Application Violation Reset	Generated based on a trap sent from an external application. Indicates that the condition that caused the Application Violation event is no longer happening and operations can return to normal. For example, if hosts have been marked at risk, they can now be marked safe and can access the network. A Host Application Violation Reset can be generated at the same time with host specific information.
Authenticated User	Successfully verified users credentials with the directory.
Authentication Configuration Modified	Generated whenever an authentication configuration is modified.
Authentication Failure	Unable to verify users credentials with the directory.
Authentication Policy Modified	Generated whenever an authentication policy is modified.
Authentication Time-out Failure	User did not authenticate within the alloted time.
Authentication Trap Receive	Received an authentication trap from the directory.
Certificate Expiration Warning	Generated when a certificate is due to expire within 30 days.
Certificate Expiration Warning (CRITICAL)	Generated when a certificate is due to expire within 7 days.
Certificate Expired	Generated when a certificate has expired.
cipSecTunnelStop	Generated when VPN connection IPsec Phase-2 Tunnel becomes inactive.
CLI Configuration Failure CLI Configuration Success	Generated when a user tries to configure a Scheduled task that involves applying a CLI Configuration to a group. Indicates whether or not the configuration of the scheduled task was successful.
CLI Data Substitution Failure	Indicates failure to substitute the "Port, VLAN, IP, or MAC" data into the CLI.
Communication Lost with BigFix Server	Event indicates that the BigFix patch management server cannot be reached.
Communication Lost with Palo Alto User Agent	Palo Alto User Agent is a component of the Palo Alto Firewall. If configured FortiNAC sends User ID and IP address to the Palo Alto User Agent each time a host connects to the network. Event indicates that the Palo Alto User Agent modeled in the Topology View cannot be reached.
Communication Lost with PatchLink Server	Event indicates that the PatchLink patch management server cannot be reached.
Communication Lost with RADIUS/SSO Agent	Fortinet SSO Agent is a component of the FortiGate Firewall. If configured FortiNAC sends User ID and IP address to the Fortinet SSO Agent each time a host connects to the network. Event indicates that the Fortinet SSO Agent modeled in the Topology View cannot be reached.

Event	Definition
Communication Lost with Script	Generated if a Custom Script SSO Agent is configured in Topology. FortiNAC sends User ID and IP address as parameters to the script each time a host connects to the network. Event indicates that the script configured in the Topology View failed to run.
Communication Lost with iboss	If configured FortiNAC sends User ID and IP address to iboss each time a host connects to the network. Event indicates that the iboss SSO Agent modeled in the Topology View cannot be reached.
Conference Created	Using Guest/Contractor Accounts you can create a batch of conference user accounts. This event is generated when those accounts are created and indicates the number of accounts created.
Contact Established	Contact with a device has been established.
Contact Lost	Contact with a device has been lost.
Container Created	New container has been created in the database. Containers are a grouping mechanism for devices that display in the Topology View.
Container Destroyed	Container has been deleted from the database. Deleting a container deletes all of the devices it contains.
DHCP Host Name Changed	Generated when a known host connects to the network and its host name is different. Indicates that the host name in the database associated with the MAC address and existing DHCP finger print for that host is different.
Database Archive/Purge Failure Database Archive/Purge Success	Indicates whether or not the scheduled database archive/purge was successful.
Database Backup Failure Database Backup Success	Indicates whether or not the scheduled database backup was successful.
Database Replication Error	Occurs in a High Availability situation when the MasterLoader database is not replicating. Can also be triggered when the database on the secondary server is not running.
Database Replication Succeeded	Occurs in a High Availability situation when the MasterLoader database is successfully replicated to the secondary server.
De-authenticated	User logged off from host.
De-authentication Failure	Unable to log off user from host. User not found.
Deleted Host Successfully	Host or FortiNAC user has been successfully deleted from the database. If multiple records are deleted at once, a separate event is generated for each record.
Device Cold Start	Device was restarted using the power switch.
Device Created	New managed device has been created in the database.
Device Destroyed	Managed device has been deleted from the database.

Event	Definition
Device Fingerprint Changed	Host is using a different operating system than the one with which the host was registered. This could occur on a host with a dual-boot. For example, the host registers with a Windows operating system. The user later boots the host using Linux and tries to access the network. That change would trigger this event. An upgrade within a family of operating systems would not normally trigger this event, such as from Windows XP to Windows Vista. Operating system is determined by the DHCP fingerprint.
Device Identity	No longer used.
Device Link	A device has linked to port X on the network.
Device Link Down	A device link goes down on a specific port because a device was disconnected from the port.
Device Link Up	Generated when a device link goes up on a specific port.
Device Profile Rule Match	A rogue host has matched a Device Profiling rule allowing it to be assigned a device type and registered.
Device Profiling Automatic Registration	A rogue host has been registered by device profiling based on a device profiling rule.
Device Profiling Rule Missing Data	Indicates that Device Profiler cannot compare a rogue against a rule because FortiNAC does not have enough information about the rogue, such as a DHCP fingerprint. If Device Profiler cannot compare a rogue against a rule it does not continue processing that rogue, and moves on to the next rogue.
Device Rule Confirmation Failure Device Rule Confirmation Success	Devices identified by a Device Profiling rule maintain their association with that rule. If enabled, the associated rule and the device are checked periodically to see if the rule is still valid for the device. These event messages indicate whether or not the device matched the associated rule.
Device Warm Start	Device was restarted from the command line interface.
Directory Connection Failure	The connection to a directory, such as Active Directory or LDAP, failed. The directory could have refused the connection because the user name and password were incorrect. This event can be triggered when testing the connection to the directory with the Test button on the Directory Configuration window.
Directory Group Disabled Directory Group Enabled	Users can be disabled/enabled in a Directory such as LDAP based on Group membership. When the FortiNAC database synchronizes with the Directory, users that are members of the group are enabled. Users that are not members of the group are disabled.
Directory Synchronization Failure Directory Synchronization Success	Indicates whether or not a directory, such as Active Directory or LDAP, synchronized with the user database. Could be caused if FortiNAC fails to connect to the directory. This synchronization is a one time task done when the Directory is configured. See Schedule synchronization on page 93.

Event	Definition
Directory User Disabled Directory User Enabled	Users can be disabled/enabled in a Directory such as LDAP. When the FortiNAC database synchronizes with the Directory, users can be disabled/enabled based on their Directory setting.
Disable Host Failure Disable Host Success	Generated when a user manually disables a host on the Host View. Indicates whether or not the host was successfully disabled.
Disable Hosts Failure Disable Hosts Success	Indicates whether or not hosts in a group were successfully disabled using a scheduled task.
Disable Port Failure Disable Port Success	Indicates whether or not a particular port was disabled by an alarm action.
Disable Ports Failure Disable Ports Success	Indicates whether or not ports in a particular group were disabled by a scheduled task.
Disable User Success	Indicates that a user selected from the User View was successfully disabled.
Disabled Authenticated	No longer used.
Discovery Completed	The device discovery process that adds new devices to FortiNAC has completed. IP address range is included in the completion message.
Duplicate Host For Device	No longer used.
Duplicate Physical Address	No longer used.
Duplicate Users Found in Directory	Two users with the same last name and/or ID were found in the Directory. FortiNAC is case in-sensitive. For example, two users with last names listed as SMITH and smith are treated as if they were the same person. The newer of the two users is ignored.
Email Failure	Alarms can be configured to send E-mail Notifications to FortiNAC Admin users. If the Admin user has no e-mail address or the e-mail fails in any other way, this event is generated.
Enable Host Failure Enable Host Success	Indicates whether or not a host selected from the Host View was successfully enabled.
Enable Hosts Failure Enable Hosts Success	Indicates whether or not hosts in a group were successfully enabled using a scheduled task.
Enable Port Failure Enable Port Success	Indicates whether or not a particular port has been enabled by an alarm action in response to a previous event.
Enable Ports Failure Enable Ports Success	Indicates whether or not ports in a particular group were enabled by a scheduled task.
Enable User Success	Indicates that a user selected from the User View was successfully enabled.
Endpoint Compliance Configuration Modified	Generated whenever an Endpoint Compliance Configuration is modified.
Endpoint Compliance Configuration Platform Setting Modified	Generated whenever an Endpoint Compliance Configuration Platform Setting is modified.

Event	Definition
Endpoint Compliance Modified	Generated whenever an Endpoint Compliance is modified.
Enterasys Dragon Violation	Enterasys Dragon is an Intrusion Protection/Detection System. An event is generated when an intruder is detected.
Failed to Disable Adapters	Attempted to disable hosts using an Alarm Action. Hosts failed to be disabled.
Failed to Disable HP Port Security	Scheduled task that enables port security configuration on all HP/NT devices in an associated group has failed.
Failed to Enable Adapters	Attempted to enable hosts using an Alarm Action. Hosts failed to be enabled.
Failed to Enable HP Port Security	Scheduled task that enables port security configuration on all HP/NT devices in an associated group has failed.
FireEye IPS High Violation	Generated whenever a high violation event is received from FireEye.
FireEye IPS Low Violation	Generated whenever a low violation event is received from FireEye.
FireEye IPS Medium Violation	Generated whenever a medium violation event is received from FireEye.
FortiOS 4.0 High Violation	Generated whenever a high violation event is received from FortiOS 4.0.
FortiOS 4.0 Low Violation	Generated whenever a low violation event is received from FortiOS 4.0.
FortiOS 4.0 Medium Violation	Generated whenever a medium violation event is received from FortiOS 4.0.
FortiOS 5.0 High Violation	Generated whenever a high violation event is received from FortiOS 5.0.
FortiOS 5.0 Low Violation	Generated whenever a low violation event is received from FortiOS 5.0.
FortiOS 5.0 Medium Violation	Generated whenever a medium violation event is received from FortiOS 5.0.
Found Ignored MAC Address	A host or device has connected with a MAC address that is in the MAC Address Exclusions list. This connection is not being managed by FortiNAC and the host or device has access to the production network. See MAC address exclusion on page 245.
Found Microsoft LLTD or Multicast Address	A host or device has connected with a MAC address in the Microsoft LLTD or Multicast Address range. Those ranges are managed in the MAC Address Exclusion list. FortiNAC ignores these MAC addressed for 48 hours after the first one is seen and then treats them as rogues unless the configuration is updated on the MAC Address Exclusion list. See MAC address exclusion on page 245.
Gaming Device Registration	A gaming device was registered by a user.
Group Does Not Exist for Scan	FortiNAC attempted to perform a scan or scheduled task for a particular group and the group no longer exists in the database. Either recreate the group or remove the scan or scheduled task.
Guest/Contractor Pre-allocation Critical	No longer used. If you are setting up Guest/Contractor users in advance, an event can be generated if you set up more Guest/Contractor users than you have licenses.

Event	Definition
Guest/Contractor Pre-allocation Warning	No longer used. If you are setting up Guest/Contractor users in advance, an event can be generated if you set up enough Guest/Contractor users to use 75% of the available licenses.
Guest Account Created	New guest account is created.
Guest Account Deleted	Guest account is deleted.
Hard Disk Usage Critical	Generated when the disk usage critical threshold is reached. This threshold is a percentage of the space allocated for the bsc and var partitions. The percentage is calculated for each partition separately. When any one partition reaches the threshold the event is generated. Thresholds calculated for individual partitions are never combined. Therefore if the combined total crosses the threshold, no event is generated. Default = 95%
Hard Disk Usage Warning	Generated when the disk usage warning threshold is headteacher threshold is a percentage of the space allocated for the bsc and var partitions. The percentage is calculated for each partition separately. When any one partition reaches the threshold the event is generated. Thresholds calculated for individual partitions are never combined. Therefore if the combined total crosses the threshold, no event is generated. Default = 85%
Host Aged Out	Host has been removed from the database based on the time or expiration date on the associated Host Properties window. See Properties on page 801.
Host Application Violation	Generated against a FortiNAChost based on the IP, MAC, or ID information contained within an Application Violation trap. If IP, MAC, or User ID match any records in the FortiNAC database, this event is generated. See Events and alarms list on page 868 in this list.
Host Application Violation Reset	Generated against a FortiNAC host based on the IP, MAC, or User ID information contained within an Application Violation Reset trap. If IP, MAC, or User ID match any records in the FortiNAC database, an event is generated. The reset event occurs when the host is no longer in violation. See Events and alarms list on page 868 in this list.
Host At Risk	An Admin user marked a selected host At Risk or the host failed a scan.
Host At Risk Failure Host At Risk Success	Indicates whether an alarm action triggered by an At Risk host succeeded or failed.
Host At Risk Status Not Enforced	Generated whenever a host fails a scan, but it is not enforced.
Host CLI Task Success Host CLI Task Failure	Indicates whether or not the CLI commands associated with host/adapter based ACLs have been successful.
Host Connected	Generated whenever a registered host connects to the network.

Event	Definition
Host Copied From NCS	In an environment where multiple FortiNAC appliances are managed by a FortiNAC Control Manager, hosts and their corresponding information can be copied from one appliance to another based on settings in the FortiNAC Control Manager under **System > Settings > Network Control Manager > Server Synchronization**. When hosts are copied from one appliance to another this event is generated.
Host Created	Generated whenever a host is created.
Host Destroyed	Generated whenever a host is destroyed.
Host Disassociated	Generated whenever a host is destroyed.
Host Disconnected	Generated whenever a registered host disconnects from the network.
Host Identity Changed	Indicates that a registered host's name or operating system has changed since the last time it was read by the Persistent or Dissolvable Agent, and that it is possibly a dual boot device. This could also indicate MAC spoofing. An operating system change , such as an upgrade could also trigger this event.
Host Pending At Risk	A host failed a scan for an Endpoint Compliance Policy. The policy was configured for delayed remediation indicating that hosts that fail the scan are not sent to remediation for x number of days. The event is generated when the host is marked Pending At Risk. Scan status "Failure Pending" triggers this event.
Host Registration Failure Host Registration Success	Host has gone to the Registration page and the user attempted to register the host. Indicates whether the registration succeeded or failed.
Host Rejected - No MAC	Host rejected because it is missing a MAC address.
Host Rejected - No VLAN	Host rejected because there is no VLAN defined for current state.
Host Safe	Generated when a user goes to **System > Settings > Control > Quarantine**. On the Quarantine view there is a button that allows the user to mark all hosts as Safe. If this button is clicked the event is generated for each host that was affected.
Host Safe Failure Host Safe Success	Indicates whether or not an alarm action associated with marking a host as safe has failed. See Host Safe on page 876 in this list.
Host Session Logged On Host Session Logged Off	Agent has detected that the user has logged on or off the host. Applies only to Windows hosts.
Incomplete User Found in Directory	FortiNAC requires the Last name and ID fields for each user. If either of those fields is missing, the user record is incomplete.
Interface Status Failure Interface Status Success	Indicates whether or not the Update interface status scheduled task was successful. The task reads and updates the interface status for each port on the devices in the associated groups.

Event	Definition
Internal Scheduled Task Failure Internal Scheduled Task Success	Indicates whether or not a scheduled task has failed. The name of the task is provided.
Invalid Physical Address	The MAC Address of the specified host or device is not recognized by FortiNAC because the corresponding Vendor OUI is not in the FortiNAC database. Update the Vendor OUI database either manually or by using Auto-Def Updates. See and .
L2 Poll Failed L2 Poll Succeeded	Indicates whether or not FortiNAC successfully contacted the device to read the list of connected hosts.
L3 Poll Failed L3 Poll Succeeded	Indicates whether FortiNAC successfully read IP address mappings from a device.
Load In Limit Exceeded	No longer used. Max % In setting on the Bandwidth window has been met or exceeded.
Load In Limit Rearmed	No longer used. After the first “Load In Limit Exceeded” event occurs the server does not generate a “Load In Limit Rearmed” event until the percentage of bandwidth bytes in falls below Rearm % In value.
Load Out Limit Exceeded	No longer used. Max % Out setting on the Bandwidth window has been met or exceeded.
Load Out Limit Rearmed	No longer used. After a “Load Out Limit Exceeded” event occurs the server creates a “Load Out Limit Rearmed” event once the percentage of bytes out falls below this the Rearm % Out value.
Lost Contact with Persistent Agent	This event can only be generated accurately when FortiNAC has up-to-date network connectivity data (in order to determine a host's online status). This requires the following: - Wired network devices are being polled at a regular interval (typically 1 hour). - Wired network devices are sending either Link Up/Link Down or Mac Notification traps. - Wireless devices are being polled at a regular interval (typically 15 minutes).
MAC Learned	Switch has learned the MAC address of a host that has connected and has added that address to its forwarding table.
MAC Removed	Switch has removed the MAC address of a host who has disconnected from its forwarding table.
MAC change event on uplink	This event is generated when a MAC notification trap is received for a port in FortiNAC is any of the uplink types.
Management Established	Generated when management of a device is established.
Management Lost	Generated when management of a device is lost.

Event	Definition
Map IP to MAC Failure Map IP to MAC Success	No longer used. Mapping IP addresses to physical addresses for a selected group using a scheduled task failed or succeeded.
Maximum Blacklist Clear Attempts Reached	Maximum number of attempts to remove a host from a controller's blacklist have been reached and the host remains on the blacklist.
Maximum Concurrent Physical Address Warning	No longer used. Generated when host connections exceed 6000 or 12000 depending on the size of the appliance.
Maximum Concurrent Connections Critical	Concurrent Connection licenses in use has reached or exceeded 95% of total licenses. Threshold is configurable. See Event thresholds on page 858.
Maximum Concurrent Connections Exceeded	Concurrent Connection licenses in use has reached 100% of total licenses.
Maximum Concurrent Connections Warning	Concurrent Connection licenses in use has reached or exceeded 75% of total licenses. Threshold is configurable. See Event thresholds on page 858.
Maximum Guest/Contractor Critical	No longer used. Guest Manager licenses in use has reached or exceeded 95% of total licenses. Threshold is configurable.
Maximum Guest/Contractor Exceeded	No longer used. Guest Manager licenses in use has reached 100% of total licenses.
Maximum Guest/Contractor Warning	No longer used. Guest Manager licenses in use has reached or exceeded 75% of total licenses. Threshold is configurable.
Maximum Hosts Critical	No longer used. Access Manager licenses in use has reached or exceeded 95% of total licenses. Threshold is configurable.
Maximum Host Warning	No longer used. Access Manager licenses in use has reached or exceeded 75% of total anesthesiologist is configurable.
Maximum Hosts Exceeded	No longer used. Access Manager licenses in use has reached 100% of total licenses. No new accounts can be created.
Maximum Known Device Critical	No longer used. Device Tracker licenses in use has reached or exceeded 95% of total licenses. Threshold is configurable.
Maximum Known Device Warning	No longer used. Device Tracker licenses in use has reached or exceeded 75% of total licenses. Threshold is configurable.

Event	Definition
Maximum Known Devices Exceeded	No longer used. Device Tracker licenses in use has reached 100% of total licenses.
Maximum User Critical	No longer used. Shared Access Tracker licenses in use has reached or exceeded 95% of total licenses. Threshold is configurable.
Maximum User Warning	No longer used. Shared Access Tracker licenses in use has reached or exceeded 75% of total licenses. Threshold is configurable.
Maximum Users Exceeded	No longer used. Shared Access Tracker licenses in use has reached 100% of total licenses.
Maximum Blacklist Clear Attempts Reached	Generated when the maximum number of attempts to remove a MAC address from a device's black list has been exceeded. Currently the maximum is set to 3 attempts.
Memory Usage Critical	Generated when the memory usage critical threshold is reached for the appliance. This threshold is a percentage of the total allocated memory. Default = 95% Threshold is configurable. See Event thresholds on page 858.
Memory Usage Warning	Generated when the memory usage warning threshold is reached for the appliance. This threshold is a percentage of the total allocated memory. Default = 85% Threshold is configurable. See Event thresholds on page 858.
Message	Cabletron/Enterasys Event Log Message OID = 1.3.6.1.4.1.52.1280
Multi-Access Point Detected	Generated when multiple MAC addresses are detected on a port. However, if the port is in the Authorized Access Points group an event is not generated. See Network device on page 130 .
NAT Device Registered	Generated when a NAT Device (router) is registered.
Nitro Security Violation Nitro Threat Level 1 - 6	Generated based on traps received from the NitroGuard Intrusion Protection/Detection system on your network. The IPS/IDS must be modeled in your Topology View.
No CDP Announcement	Generated when a device that has sent at least one CDP announcement has stopped sending those announcements. This is based on the polling time set for the device. For example if the poll time is one hour, a new event message is sent each time the hour elapses with no message from the device.
Operating System Is Up to Date	Indicates that there are no new updates available after the Operating System Update Status scheduled task is run (1pm every Sunday, by default).
Operating System Status Check Failure	Indicates that the Operating System update check failed due to multiple running checks. This may be caused by a configuration or network issue.
Operating System Update Initiated	Indicates that an Operating System Update was started from the Admin UI. See Updating CentOS on page 235.

Event	Definition
Operating System Updates Available	Indicates that there are updates available after the Operating System Update Status scheduled task is run (1pm every Sunday, by default).
Packeteer Configuration Failure Packeteer Configuration Success	No longer used. Indicates whether or not communication has been established with the Packeteer PacketShaper software after Packeteer has been modeled in the Topology View.
Packeteer Monitor	If Packet Shaper has been configured to generate threshold violation events and if a threshold violation occurs, the event triggers an SNMP trap from PacketShaper to FortiNAC. This trap causes FortiNAC to generate a Packeteer Monitor event.
Packeteer Monitor 2	No longer used. If a Packeteer product has been configured to generate events for OID 13.6.1.3.6.1.4.1.2334.1.1 and the event triggers an SNMP trap from the Packeteer to FortiNAC. This trap causes FortiNAC to generate a Packeteer Monitor 2 event.
Persistent Agent Communication Resumed	Persistent Agent Contact Status has been restored to normal. **Note:** This event is only generated on hosts running Persistent Agent 4.0 or better.
Persistent Agent Not Communicating	This event can only be generated accurately agents when FortiNAC has up-to-date network connectivity data (in order to determine a host's online status). This requires the following: - Wired network devices are being polled at a regular interval (typically 1 hour). - Wired network devices are sending either Link Up/Link Down or Mac Notification traps. - Wireless devices are being polled at a regular interval (typically 15 minutes). This event is only generated on hosts running Persistent Agent 4.0 or better.
Persistent Agent Scan Not Performed	This event can only be generated accurately when FortiNAC has up-to-date network connectivity data (in order to determine a host's online status). This requires the following: - Wired network devices are being polled at a regular interval (typically 1 hour). - Wired network devices are sending either Link Up/Link Down or Mac Notification traps. - Wireless devices are being polled at a regular interval (typically 15 minutes).
Policy Warning	Host was scanned by an Endpoint Compliance Policy. The host does not meet all of the scan requirements, but the scan rules state that a warning be issued instead of making compliance a requirement. Scan status "Warning" triggers this event.

Event	Definition
Poll For Hosts Failure Poll For Hosts Success	No longer used. Indicates whether a scheduled task to poll switches for hosts has succeeded or failed. Switches are contained in a device group and that group is polled.
Port CLI Task Failure Port CLI Task Success	Indicates whether a CLI configuration applied to a port ran and failed or succeeded.
Port in Authorized Access Points Group	Failed to enable/disable port because it is in the Authorized Access Points group.
Port Link Down Port Link Up	Trap received from the switch each time there is a link up or a link down on a port. Link up and link down happen each time a host is switched from one VLAN to another.
Port Security Incomplete	Maximum number of users on a port has been reached.
Port Segmented	Trap received from an Enterasys or Cabletron switch indicating that a link is down. This port may have been logically disconnected due to an excessive collision level or it may be physically disconnected.
Port Uplink Configuration Modified	An administrator modified the uplink setting of a port. The switch name, port and administrator are included in the event.
Port in Authorized Access Points Group	Scheduled task for a port in the Authorized Access Points group failed.
Possible MAC Address Spoof	Indicates that the same MAC address has been detected for more than five minutes on two different devices simultaneously. One is possibly spoofing the other's MAC address.
Possible NAT Device, MAC Spoofed	This event has been replaced with NAT Device Registered. It remains visible to allow you to restore an old backup and view occurrences of this event. See NAT Device Registered on page 879 in this list.
Possible NAT User	Generated on each host. One per MAC address on the NATd host. For example, if a host has both a wired and wireless connection, an event is generated for each.
Process Memory Usage Critical	Generated when the memory usage critical threshold is reached for the process. This threshold is a percentage of the total allocated memory. Default = 95%
Process Memory Usage Warning	Generated when the memory usage warning threshold is reached for the process. This threshold is a percentage of the total allocated memory. Default = 85%
Process Thread Count Critical	Generated when the process thread count warning threshold is reached. This threshold is a specific number of threads the process is using. Default = 575 This event is disabled by default. The threshold will dynamically increase by 25 for every 8 CPU cores that are added.

Event	Definition
Process Thread Count Warning	Generated when the process thread count warning threshold is reached. This threshold is a specific number of threads the process is using. Default = 500 This event is disabled by default. The threshold will dynamically increase by 25 for every 8 CPU cores that are added.
Profile Modified	Generated when a user modifies a User/Host Profile. Event message contains user information for the user who made the change, whether the change was an add, remove or replace, and the complete profile after the changes.
RADIUS Rate Exceeded	Generated when the 60 requests-per-second threshold is exceeded. This event is disabled by default.
RADIUS Time Threshold	Indicates that the time threshold for a response from the RADIUS server has been exceeded. This threshold is not configurable.
Regained Contact with Persistent Agent	Host has regained contact with the persistent Agent .
Remote Access Excessive Session Process Time	Generated when the time to process the remote client exceeds a threshold (set through the "MaxClearTime" attribute on the ASA device).
Reports Purged	Lists the file names of all reports that were deleted when reports were purged from the /home/cm/reports directory.
SNMP Failure	Generated when FortiNAC receives an SNMP failure during communication with a SNMP enabled Network Device. This includes any error message received from the SNMP packet.
SNMP Read Error	Did not receive all data when reading a switch using SNMP. Device name and error code are included in the event message.
Scan Does Not Exist For Scheduler Task	FortiNAC has attempted to run a scan using a scheduled task. The scan referred to in the task no longer exists in the database. You must either recreate the scan or remove the scheduled task from the scheduler.
Secondary Contact Lost	Event triggered when the primary loses contact with the secondary.
Service Down - Tomcat Admin Service Down - Tomcat Portal Service Down -dhcpd Service Down -httpd Service Down -mysqld Service Down -named Service Down -sshd	Event triggered when a specific service is no longer running. These services are required. FortiNAC tries to restart the service every 30 seconds. In a High Availability environment, failover occurs after the fourth failed restart attempt. For the httpd service: After the system confirms that the httpd service is running, the system also attempts to connect to ports 80 and 443. If the system fails to connect to either port, the httpd service is restarted. If the primary is unable to communicate with the secondary to confirm it is running, service down will not trigger a failover.

Event	Definition
Service Started - Tomcat Admin Service Started - Tomcat Portal Service Started -dhcpd Service Started -httpd Service Started -mysqld Service Started -named Service Started -sshd	Event triggered when one of the listed services is started. These services are required and must be running in order to use FortiNAC.
Service Down - Analytics Agent	Event triggered when the service is down and it is required for FortiNAC to send data to Analytics.
Service Down - Radius Service Down - Samba Service Down - Winbind	Event triggered when one of the listed the services is no longer running and it is required for the RADIUS Manager.
Service Started - Analytics Agent	Event triggered when the service is started. This service is required and must be running in order to use Analytics.
Service Started -Radius Service Started - Samba Service Started - Winbind	Event triggered when one of the listed services is started. These services are required in order to use RADIUS Manager.
Set Default VLAN Failure Set Default VLAN Success	When a host disconnects from a port, the port can be set to return to its default VLAN. Indicates whether or not the port successfully returns to the default VLAN.
Sophos AntiVirus: Virus Found	Sophos AntiVirus can be configured to send traps to FortiNAC when a virus is found on a host. Host information is included in the trap. If a Sophos Trap is received, this event is generated.
Sourcefire Error Sourcefire IPS Action Sourcefire IPS High Violation Sourcefire IPS Low Violation Sourcefire IPS Medium Violation	Generated based on syslog events received from an Intrusion Protection/Detection system on your network. The IPS/IDS must be modeled in your Topology View. **Sourcefire IPS Action**—Indicates that an action has been triggered by a syslog message from Sourcefire.
StealthWatch	SNMP trap has been sent from a StealthWatch device OID = 1.3.6.1.4.1.8712
StealthWatch Email Rejects	Host is receiving a significant number of rejected mail attempts.
StealthWatch Email Relay	Host is operating as an email relay.
StealthWatch High Concern	A host has exceeded the Concern Index threshold set for it. This usually means that an inside host is no longer operating as it was during the tuning period and should be examined for possible compromise, misuse, or policy violations. An external host with a High Concern index is often attempting to violate your network integrity.
StealthWatch High File Sharing	Host is transferring files.
StealthWatch High Volume Email	Host is infected with an email worm.

Event	Definition
StealthWatch Max Flows Initiated	Host has had an excessive number of total flows active.
StealthWatch New Flows	Indicates that a host exceeds a total number of new flows in a 5-minute period.
StealthWatch Port Flood	The host has attempted to connect on an excessive number of ports on the Target IP. This may indicate a DoS attack or an aggressive scan by the source IP.
StealthWatch SYN Flood	The host has sent an excessive number of TCP connection requests (SYN packets) in a 5-minute period. This may indicate a DoS attack or non-stealthy scanning activity
StealthWatch Suspect Long Flow	Host has a long duration flow.
StealthWatch Worm Activity	A host has scanned and connected on a particular port across more than one subnet. The details section of this alarm specifies the port on which the activity was observed.
StealthWatch Worm Propagation	Host has scanned and connected on port 5 across more than 1 subnet.
StealthWatch Zone Violations	Host has connected to a server in a zone that it is not allowed to access.
StoneGate IPS High Violation StoneGate IPS Low Violation StoneGate IPS Medium Violation	Generated based on syslog events received from an Intrusion Protection/Detection system on your network. The IPS/IDS must be modeled in your Topology View. See Syslog management on page 190 .
StoneGate Violation	Generated based on syslog events received from an Intrusion Protection/Detection system on your network. The IPS/IDS must be modeled in your Topology View. See Syslog management on page 190 .
Success Disabling Port Security Success Enabling Port Security	Generated when the Enable or Disable HP/NT Port Security scheduled task runs successfully. This task enables or disables port security configuration on all HP/NT devices in the selected group. Port Security is used to disable hosts if DeadEnd VLANs are not used on the network.
Synchronize Users with Directory Failure Synchronize Users with Directory Success	Indicates whether or not the FortiNAC user database has successfully synchronized with the selected directory such as LDAP or Active Directory. These events are triggered by the failure or success of the scheduled synchronization set up on the Directory Configuration window. See Configuration on page 82.
Syslog Error	Generated when the FortiNAC server receives an inbound syslog message for a host that is not currently managed by FortiNAC.
System Backup Failure System Backup Success	Indicates whether a system backup has succeeded. The system backup is run by a scheduled task. The system backup may succeed, but will still fail if remote backup is enabled and fails. It is recommended that you create an alarm action to send an email if system backup fails.

Event	Definition
System Created Uplink	If Uplink Mode on a Port's properties is set to Dynamic, FortiNAC converts the port to an uplink port when the number of MAC addresses on the port exceeds the System Defined Uplink count and generates this event.
System Fail Over	In a High Availability environment, this event indicates that the primary server has failed and the secondary has taken over.
System Power Off	Indicates that the user specified in the event message powered off the FortiNAC server. See Power management on page 219
System Reboot	Indicates that the user specified in the event message rebooted the FortiNAC server. See Power management on page 219.
System Automatically Restarted	Server was restarted because a primary system process was down. Processes include: MasterLoader, IP to MAC, Communication and Nessus. This event was System Restart in prior versions.
TippingPoint SMS High Violation TippingPoint SMS Low Violation TippingPoint SMS Medium Violation	Generated based on syslog events received from an Intrusion Protection/Detection system on your network. The IPS/IDS must be modeled in your Topology View. See Syslog management on page 190 .
Top Layer IPS High Violation Top Layer IPS Low Violation Top Layer IPS Medium Violation	Generated based on syslog events received from an Intrusion Protection/Detection system on your network. The IPS/IDS must be modeled in your Topology View. See Syslog management on page 190 .
Unauthorized SSID/VLAN	No longer used.
Unknown User in Group	No longer used.
Unsupported Trap	Generated when FortiNAC receives a trap that it cannot interpret from a device. The device's OID is included in the event.
Update SSID Failure Update SSID Success	SSID assignment scheduled task maps VLAN IDs to SSIDs. Event indicates whether or not the task succeeded.
Update VLAN ID Failure Update VLAN ID Success	Indicates that the user specified in the event message powered off the FortiNAC server. See Power management on page 219. Update Default VLAN Values scheduled task sets the Default VLAN value for the port in FortiNAC device model to the value entered in the scheduled task. Event indicates whether or not the task succeeded.
User Aged Out	Indicates that the user specified in the event message rebooted the FortiNAC server. See Power management on page 219. User has been aged out of the database based on the data stored in the Age Time section of the User Properties view.
User Created User Destroyed	Network user created in or deleted from the database. This is a non-administrative user.

Event	Definition
User not NATd	This event is generated on each host that had been previously NATd but are not any longer. One per MAC address on the NATd host. For example, if a host has both a wired and wireless connection, an event is generated for each.
Users Removed From Directory	User has been removed directly from a Directory such as LDAP. When the FortiNAC user database is synchronized with the Directory this discrepancy triggers the event. If Remove User is selected on your Directory configuration, the missing user is removed from the FortiNAC database.
Valid DHCP Server	Generated when has verified that the DHCP server is running a valid DHCP server application.
Vendor OUI Added	Generated when a new Vendor OUI has been added to the database.
Vendor OUI Removed	Generated when a Vendor OUI was removed from the database.
VLAN Switch Failure	VLAN failed to change for port X.
VLAN Switch Success	VLAN was changed successfully for X port.
Vulnerability Scan Failed	Generated when the host failed the Vulnerability Scan.
Vulnerability Scan Finished	Generated when the Vulnerability rescan has finished.
Vulnerability Scan Ignored	Generated when scan results from the vendor include hosts that were added to the Vulnerability Exceptions Group, indicating which hosts were ignored. Hosts in this group are allowed onto the network, regardless of scan results.
Vulnerability Scan Incomplete	FortiNAC polls the vendor for scan results for a configured scan, but scan results are unavailable because the scan was not run by the vendor.
Vulnerability Scan Passed	Generated when the host passed the Vulnerability Scan.
Vulnerability Scan Removed	A Vulnerability Scan that was added to FortiNAC was removed from the Vulnerability Scanner.
Vulnerability Scan Request Refused (Qualys Integration only)	The IP address targeted by a rescan is not included in the list of Qualysasset IPs.
Vulnerability Scan Skipped	The Vulnerability Scanner has not run the scan since FortiNAC previously polled it, so FortiNAC skipped the scan during processing.
Vulnerability Scan Started	Generated when the Vulnerability rescan has started.
Vulnerability Scanner Concurrent API Limit Exceeded (Qualys Integration only)	Exceeded the limit that is set for the number of requests that can be processed concurrently.
Vulnerability Scanner Connection Failure	The connection to the Vulnerability Scanner has failed.
Vulnerability Scanner Deleted	A Vulnerability Scanner was deleted from FortiNAC.
Vulnerability Scanner Periodic API Limit Exceeded (Qualys Integration only)	Qualys rejected an API request because the periodic API limit has been exceeded. The event message includes the number of seconds until the scanner will accept an API request.

Alarms view

Use the alarms view to view and manage the contents of the alarm log. The alarm log is a list of all current alarms. The Severity column indicates how serious the alarm is. Severity levels include: critical, minor, warning, informational.

The state of an alarm is either acknowledged or not acknowledged. The event-to-alarm mapping determines the behavior and characteristics of the alarm. The event-to-alarm mapping feature gives you the option of sending alarms to an external log host. See Map events to alarms on page 888 for details.

You can remove alarms from the log in two ways:

- Manually, when you select and clear the alarm
- Automatically, when the *clear event* defined in alarm mapping occurs

To access the alarms view, select **Logs > Alarms**.

Settings

Field	Definition
First Name	First Name of the user associated with the alarm, such as the registered owner of a host or an admin user.
Last Name	Last Name of the user associated with the alarm.
User ID	User name from the credentials of the user who was logged in and associated with the alarm.
Element Name	Name of the device, Admin User, server or process associated with the alarm.
Element Type	Type can be Device, Port, Container, Process, or All.
Group	Group name of a group of elements, such as, port group, device group or user group.
Pause	If enabled, prevents the Alarms List from refreshing and adding new records to the screen. In an environment with a large number of alarms, you may need to pause the refresh in order to research an issue.
Severity	Category indicating how serious the alarm is. Options include: Critical, Minor, Warning and Informational
Date	Date and time the alarm was triggered.
Alarm	Alarm name. See Events and alarms list on page 868.
Element	Element associated with the alarm entry, such as a user name, a host name, a switch name or an application name.
Trigger Rule	Rule that determine the conditions under which an alarm is triggered based on an event. Options include: • **One Event to One Alarm**—Every occurrence of the event generates a unique alarm. • **All Events to One Alarm**—The first occurrence of the event generates a unique alarm. Each subsequent occurrence of the event does not generate an alarm, as long as the alarm persists when subsequent events occur. When the alarm clears, the next occurrence of the

Field	Definition
	event generates another unique alarm. • **Event Frequency**—Number of the occurrences of the event generated by the same element within a user specified amount of time determines the generation of a unique alarm. • **Event Lifetime**—Duration of an alarm event without a clearing event within a specified time, determines the generation of a unique alarm.
Acknowledged Date	Indicates the date the alarm was acknowledged. If this field is blank, it indicates that the alarm was never acknowledged.
Buttons	
Import	Import historical records from an Archive file. See Import archived data on page 696.
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.
Acknowledge	Acknowledges the selected alarm but does not clear it. The Alarm remains in the displayed until you clear it. A date is displayed in the Acknowledged column when the alarm is acknowledged.
Clear	Clears the selected alarm and removes it from the list.
Show Details	Displays the Details Panel for the selected alarm. See Show or hide alarm details on page 888.

Show or hide alarm details

The Alarm Details panel launched from the Alarms View displays a detailed narrative about the cause of the selected alarm and the event that triggered it. For example, if there is an alarm indicating that an L2 Poll failed, the possible causes are displayed indicating that the security string may be incorrect or the telnet credentials are incorrect. This gives the administrator two things to verify when trying to correct the problem.

1. Select **Logs > Alarms**.
2. Use the filters to locate the appropriate alarm. Refer to Alarms view on page 887 for Filter Settings.
3. Select the alarm.
4. Click **Show Details**.
5. Review the details displayed.
6. Click **Hide Details** to close the panel.

Map events to alarms

An event indicates that something significant has happened within FortiNAC. All events that are generated are logged in the event log. If an event is mapped to an alarm, you are immediately informed by the alarm notification system. Some events are mapped to alarms by default.

To view events that are mapped to alarms select **Logs > Event to Alarm Mappings**. For a list of possible alarms see Events and alarms list on page 868.

If an event is disabled, the associated Alarm Mapping is grayed out and has a line through it. To enable the event, right click on the Alarm Mapping and select one of the Enable options.

See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.

Enable/disable alarm mappings

When mapping events to alarms, you have the option to disable an alarm mapping to prevent the generation of alarms when the selected event occurs. This may be useful during periods you know will generate many events. An example of this is during the repair of a modeled network device. You may want to block the Device Contact Lost and Established events from getting to the system since they will be expected. Another example is to block the Rogue User Detected event during an Open House when many rogues will be detected. Use the Enable and Disable buttons at the top of the view to enable and disable selected Alarm Mapping records.

Settings

Refer to Add or modify alarm mapping on page 892 for additional information on each field.

Field	Definition
Enable Buttons	Enables or disables the selected Alarm Mappings. Disabled mappings do not trigger an alarm when the associated event is generated.
Enabled	A green check mark indicates that the mapping is enabled. A red circle indicates that the mapping is disabled.
Event	Name of the Event that triggers this alarm.
Alarm	Name of the Alarm that is mapped to the event.
Clear Event	Name of the event that must be generated to clear the alarm mapped in this Alarm and Event combination.
Severity	Critical, Minor, Warning, or Informational. Only the text of the severity is displayed. Severity icons do not display in the Alarm Mappings table.
Notify Users	Indicates who will be notified if this alarm is triggered, such as, All Management Group.
Trigger Rule	Rules that determine when the alarm is triggered. Options include: • **One Event to One Alarm**—Every occurrence of the event generates a unique alarm. • **All Events to One Alarm**—The first occurrence of the event generates a unique alarm. Each subsequent occurrence of the event does not generate an alarm, as long as the alarm persists when subsequent events occur. When the alarm clears, the next occurrence of the event generates another unique alarm. • **Event Frequency**—Number of the occurrences of the event generated by the same element within a user specified amount of time determines the generation of a unique alarm. • **Event Lifetime**—Duration of an alarm event without a clearing event within a

Field	Definition
	specified time, determines the generation of a unique alarm.
Apply To	Elements to which this alarm mapping applies. Options include: • **All**—Applies this mapping to all elements. • **Group**—Applies this mapping to a single group of elements. • **Specific**—Applies this mapping to an element that you select from a list.
Action	If an Action is enabled in the mapping, displays the action that will be taken when this alarm is triggered. Options include: • **Host Access Action**—Host is disabled and then re-enabled after the specified time has passed. • **Host Role**—The host's role is changed and then set back to the original role after the specified time has passed. • **Host Security Action**—Host is set At Risk and then set to Safe after the specified time has passed. • **Command Line Script**—You can specify a particular command line script to be executed as an alarm action. • **Email User Action**—An email is sent to the user associated with the host. • **SMS User Action**—An SMS Message is sent to the user associated with the host. • **Port State Action**—Port is disabled and then re-enabled after the specified time has passed. • **Send Message to Desktop**—Send a text message to the desktop of a host(s) with the Persistent Agent or Mobile Agent installed.
Send To External Log Hosts	Indicates whether this alarm is sent to an external log host when the trigger event occurs, select this check box. Default = No. To configure remote hosts that will receive externally logged alarms, see Log receivers on page 169.
Send To Custom Script	Name of the command line script to be executed when this alarm is triggered. These command line scripts are for advanced use, such as administrator-created Perl scripts. Scripts are stored on the server in the following directory: `/home/cm/scripts` The script will receive one packed argument that the script can parse for the desired data. **Example** 'type="Network" name="FortiNAC" msg="Alarm Admin User Login Failure asserted on FortiNAC Mon Feb 27 14:34:35 EST 2017. The following Events caused the Alarm. Admin user efewfwf failed to log in. Admin user efewfwf failed to log in. Admin user efewfwf failed to log in. "'
Event Logging	Indicates where the event is being logged or if logging has been disabled. Options include:

Field	Definition
	• **Disabled**—Event is disabled and will not be generated or logged anywhere. • **Internal**—Logs only to an internal events database. • **External**—Logs only to an external host. • **Internal & External**—Logs both to an internal events database and an external host.
Event Logging Group	Group name of a group of elements, such as, port group, device group or user group used to limit generation of the selected event to the items in the group. If set to All Groups, then the event is generated for all items, such as ports, devices, hosts or users.
Last Modified By	User name of the last user to modify the mapping.
Last Modified Date	Date and time of the last modification to this mapping.
Right click options & buttons	
Delete	Deletes selected mappings from the database.
Modify	Opens the Modify dialog and allows you to modify the selected mapping. When multiple mappings are selected, opens a limited Modify dialog and allows you to modify Severity and Notification settings. See Bulk modify alarm mappings on page 896.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Admin auditing on page 847 You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671
Enable	Enables the selected mappings.
Disable	Disables the selected mappings.
Event Logging - Disable	Disables the events associated with the selected mappings.
Event Logging - Internal	Enables the events associated with the selected mappings and logs to an internal events database.
Event Logging - External	Enables the events associated with the selected mappings and logs to an external host.
Event Logging - Internal & External	Enables the events associated with the selected mappings and logs to both an internal events database and an external host.
Export	Exports data to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.

Add or modify alarm mapping

1. Select **Logs > Event to Alarm Mappings**.
2. Click **Add** or double-click on an existing mapping to modify it.
3. Refer to the table below for detailed information about each field.
4. The new mapping is enabled by default. If you wish to disable it, remove the check mark from the **Enabled** check box.
5. In the **Apply To** section, select the element affected by this mapping. You can apply mappings to all elements, a single group of elements, or specific elements.

Available selections vary depending upon the selected trigger event.

6. Click the box and select an element from the drop-down list.
7. If you choose to **Apply To a Group**, you can select a group from the list or use the icons next to the group field to add a new group or modify the group shown in the drop-down list. Note that if you modify a group, it is modified for all features that make use of that group. See Add groups on page 839 for additional information.
8. Select the **Notify Users** settings.
9. If you choose to notify users, you can select an admin group from the list or use the icons next to the **Group** field to add a new group or modify the group shown in the drop-down list. Note that if you modify a group, it is modified for all features that make use of that group. See Add groups on page 839 for additional information.
10. Select the **Trigger Rule** for the event from the drop-down list. Rules determine when an Event triggers the creation of an Alarm.
11. If you enable the **Action** option, select the action to take when the event occurs and the alarm is asserted. These are basic actions that FortiNAC executes on a given alarm.
12. Action parameters display. Select the **Primary Task** from the drop-down list.
13. For some actions there is a secondary task. If desired, click the **Enable** box in the **Run Secondary Task** section, select **Min**, **Hr**, or **Day** and enter the corresponding value.
14. Click **OK**. The new mapping is saved and appears in the **Event/Alarm Map View**.

Settings

Field	Definition
Alarm definition	
Enabled	If checked, the alarm mapping is enabled. Default = Enabled.
Trigger Event	Event that causes the alarm. Whenever this event occurs, its associated alarm is generated. The alarm is automatically listed when you select the event.
Alarm to Assert	The alarm generated when the event occurs.
Severity	Sets the severity of the alarm. Select one of the values from the drop-down list: Critical, Informational, Minor, and Warning. This value may be changed for existing Alarm and Event mappings.

Field	Definition
Clear on Event	To automatically clear the alarm when a specific event occurs, select this check box. Select the event that, when generated, causes this alarm to be removed. If you leave the check box unchecked, you must manually clear the alarm. Default = Unchecked (Disabled)
Send Alarm to External Log Hosts	The alarm is sent to an external log host when the trigger event occurs, select this check box. See Log receivers on page 169 for details on configuring an external log host. Default = Unchecked (Disabled)
Send Alarm to Custom Script	You can specify a particular command line script to be executed when this alarm is triggered. These command line scripts are for advanced use, such as administrator-created Perl scripts. First, write the script that is to be used as the alarm action. Store the script in this directory: `/home/cm/scripts` If there are no scripts in the directory, this field is not available. Click the check box to enable the option and select the correct script from the drop-down list. The arguments that are automatically passed to the script are as follows: • **type** — EndStation. User or Network Device • **name** — name of element • **ip** — IP address • **mac** — MAC address • **user** — userID • **msg** — email message from alarm
Apply To	• **All**—Applies this mapping to all elements. • **Group**—Applies this mapping to a single group of elements. • **Specific**—Applies this mapping to the element that you select from a list.
Notify users	
Notify	If checked, the administrators in the selected group are notified when an alarm occurs.
Send Email	If checked, the administrators in the selected group are sent an email when the alarm occurs. Administrators must have an email address configured in the Modify User dialog to receive this email.
Send SMS	If checked, the administrators in the selected group are sent an SMS message when an alarm occurs. Administrators must have a Mobile Number and Mobile Provider configured to receive this SMS message.
Trigger rules	
One Event to One Alarm	Every occurrence of the event generates a unique alarm.
All Events to One Alarm	The first occurrence of the event generates a unique alarm. Each subsequent occurrence of the event does not generate an alarm, as long as the alarm persists when subsequent events occur. When the alarm clears, the next occurrence of the event generates another unique alarm.

Field	Definition
Event Frequency	The number of the occurrences of the event generated by the same element within a user specified amount of time determines the generation of a unique alarm. Settings are updated when the Action is configured. Example: Assume the “Host Connected” event is mapped to an alarm and the frequency is set to 3 times in 10 minutes. Host A connects 3 times in 10 minutes and the alarm is triggered. Host A connects 2 times and host B connects 2 times, there are 4 connections in 10 minutes. No alarm is generated because the hosts are different. Host A connects at minutes 1, 8 and 12. No alarm is triggered because the host did not connect 3 times in 10 minutes. Host A connects at minutes 1, 8, 12, and 14. An alarm is triggered because connections at minutes 8, 12 and 14 fall within the 10 minute sliding window.
Event Lifetime	The duration of an alarm event without a clearing event within a specified time, determines the generation of a unique alarm. Example: Event A occurs. If Event B (clear event) does not occur within the specified time, an alarm is generated.
Actions	
Action	If checked, the selected action is taken when the alarm mapping is active and the alarm is asserted.
Host Access Action	Host is disabled and then re-enabled after the specified time has passed.
Host Role	The host's role is changed and then set back to the original role after the specified time has passed. Roles are attributes of the host and are used as filters in User/Host Profiles. Those profiles determine which Network Access Policy, Endpoint Compliance Policy or Supplicant EasyConnect Policy to apply. Note: If roles are based on a user's attribute from your LDAP or Active Directory, this role change is reversed the next time the directory and the FortiNAC database resynchronize.
Host Security Action	Host is set At Risk and then set to Safe after the specified time has passed.
Command Line Script	You can specify a particular command line script to be executed as an alarm action. These command line scripts are for advanced use, such as administrator-created Perl scripts. First, write the script that is to be used as the alarm action. Store the script in this directory: `/home/cm/scripts` The IP and MAC address arguments that are automatically passed to the script are in the format shown in this example: `/home/cm/scripts/testScript 192.168.10.1 00:00:00:00:00:00`
Email User Action	An email is sent to the user associated with the host. The text of the email is entered in the Email Host Action dialog box. HTML tags may be added to text within the content of the email in order to format the text, convert the text to a link, etc.

Field	Definition
	For example, you can add the <b> and </b> tags to text in the Email message window to bold the selected text in the recipient's email message.
SMS User Action	An SMS Message is sent to the user associated with the host. The text of the message is entered in the SMS User Action dialog box. The recipient must have a Mobile Number and Mobile Provider configured.
%host%	Allows you to include information specific to the non-compliant host in the email or SMS alert message. For example, this message: The system referenced below has been found at risk. Please contact your Help Desk for assistance in remediating this issue. %host% is displayed as: The system referenced below has been found at risk. Please contact your Help Desk for assistance in remediating this issue: Host: Host Name: TestUser-MacBook-Pro-2 OS: macOS 10.7.5 Network Adapters: Connected 3C:07:54:2A:88:6F,192.168.10.143,Concord-3750 Fa3/0/46 Disconnected 60:C5:47:8F:B1:66,192.168.4.70,Concord_Cisco_1131.example.com VLAN 4
%event%	Allows you to include information specific to the event in the email or SMS alert message. For example, this message: The system referenced below has been found at risk. Please contact your Help Desk for assistance in remediating this issue: %event% is displayed as: The system referenced below has been found at risk. Please contact your Help Desk for assistance in remediating this issue: Host failed Test-Host Tests: Failed :: Anti-Virus :: ClamXav MAC Address: 3C:07:54:2A:88:6F Last Known Adapter IP: 192.168.10.143

Field	Definition
	Host Location: Concord-3750 Fa3/0/46 . Remediation Delayed.
Port State Action	The port is disabled and then re-enabled after the specified time has passed.
Send Message to Desktop	Send a text message to the desktop of a host(s) with the Persistent Agent or Mobile Agent installed.

Bulk modify alarm mappings

This option displays on the right-click menu only when multiple mappings are selected in the Event to Alarm Mappings View. It provides a limited Modify dialog with options to modify Severity and Notification settings.

1. Select **Logs > Event to Alarm Mappings**.
2. Use Ctrl or Shift to select multiple alarm mappings.
3. Right-click on the selected records and choose **Modify** from the pop-up menu.
4. Use the table below to modify the selected mappings.

Field	Definition
Severity	Enables the Severity drop-down. The severity level of the alarm. Options include: Critical, Informational, Minor and Warning.
Notify Users	Enables the Notify Users settings.
Notify Group	Drop-down list of Admin groups. Use this to determine who will be notified when this alarm is triggered. The default is the All Management Group which contains all Admin users.
Send Email	If enabled, Admin Users in the selected group receive an email when this alarm is triggered.
Send SMS	If enabled, Admin Users in the selected group receive a text message when this alarm is triggered. Admin Users must have a mobile phone number and a mobile provider listed on their user records to receive SMS messages.

5. Click **OK** to save your changes.

Delete alarm mapping

1. Select **Logs > Event to Alarm Mappings**.
2. Select the appropriate mapping record from the list displayed.
3. Click **Delete**.
4. At the prompt, click **OK**.

Reports view

Use the reports view to see standard reports and to create custom reports based on the information in the database. The report data may be output to HTML, CSV, EXCEL, XML, RTF, and PDF formats.

The template reports include: guest registration, registration, and scan results. You can set the schedule for the standard reports and preview the results prior to scheduling, including sections of the report related to failures.

Custom reports include: registrations, registration failures, scan results, and connection logs. For custom reports, configure the report by selecting parameters, filters, scheduling, and type of output. You can import the output files into other report generation tools.

Archives include reports that have been run based on a scheduled task and are archived for you to view at your convenience. You can schedule both standard and custom reports to run at a particular time and be sent via email to an administrator group.

Compliance reports are used to verify that data security standards are being met for different industries such as HIPPA for the health industry or PCI for customers who process credit cards. At this time the only compliance reports available are PCI reports. PCI report templates were developed using Crystal Reports. The Crystal Reports engine and viewer are included to provide access to these reports.

To use report templates created in Crystal Reports you must be running Tomcat version 5.5 or higher on your FortiNAC server.

The Crystal tab allows you to upload report templates that you have created or edited with Crystal Reports. If the templates have been created correctly, they can be run against the FortiNAC database and reports display in the Crystal Reports Viewer.

Access the reports by selecting **Logs > Reports**.

Standard report templates

Use the Templates tab to access standard Guest Registration, Registration and Scan Results reports. The Guest Registration report includes information on Guests/Contractors that have logged into the system. The Registration reports include statistics on successful and failed attempts to register and login errors. The Scan Results reports include Endpoint Compliance Policy Scan results information.

You can schedule these reports to be sent to an Administrator group. The email contains graphical data as well as tabular data in report form. See Schedule reports on page 908 for details.

To access this window select **Logs > Reports**, select **Templates** on the left.

Preview standard report templates

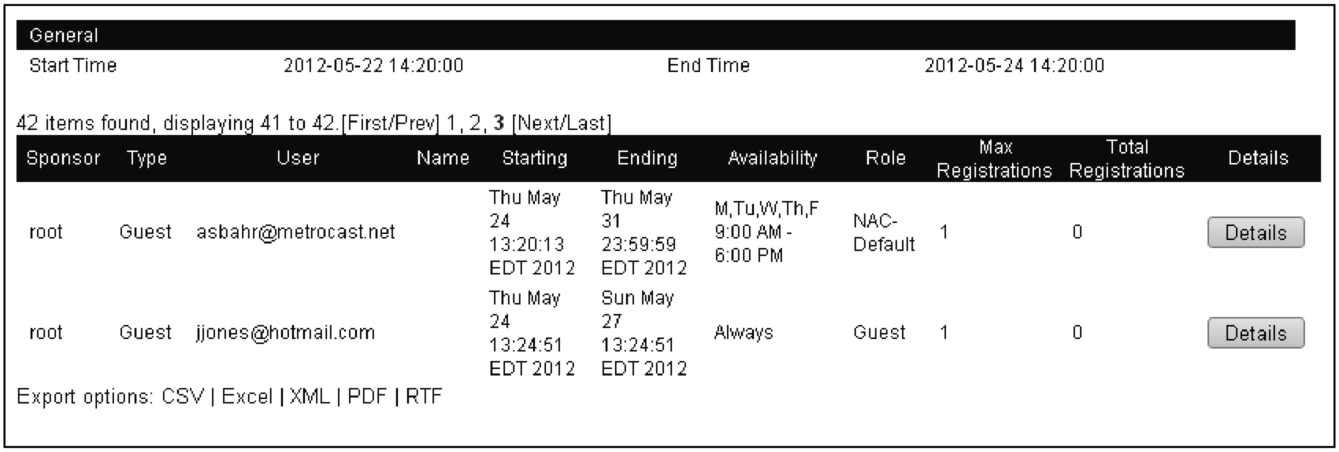
Use the Preview Settings section to see the report that will be generated from the report parameters you have selected. If the results are acceptable, enter the parameters into the report schedule view.

1. Select **Logs > Reports**.
2. Select **Templates** from the menu on the left.
3. Select the **Report Type**.
4. Enter the number of hours, days, or weeks in the **Data** range field and select the range from the drop down list.
5. Enter the range end time in the format MM/DD/YY hh:mm AM/PM.
6. Click **Preview**.
7. Click **Details** to view additional information.

Guest registrations report

This report provides you with a list of guest accounts created between the specified dates. See Preview standard report templates on page 898 for instructions on generating this report.

When the report has multiple pages, use the [First/Prev] or [Next/Last] options to view the pages of the report, or click a page number to view a specific page.



General

Start Time	2012-05-22 14:20:00	End Time	2012-05-24 14:20:00

42 items found, displaying 41 to 42.[First/Prev] 1, 2, **3** [Next/Last]

Sponsor	Type	User	Name	Starting	Ending	Availability	Role	Max Registrations	Total Registrations	Details
root	Guest	asbahr@metrocast.net		Thu May 24 13:20:13 EDT 2012	Thu May 31 23:59:59 EDT 2012	M,Tu,W,Th,F 9:00 AM - 6:00 PM	NAC-Default	1	0	Details
root	Guest	jjones@hotmail.com		Thu May 24 13:24:51 EDT 2012	Sun May 27 13:24:51 EDT 2012	Always	Guest	1	0	Details

Export options: CSV | Excel | XML | PDF | RTF

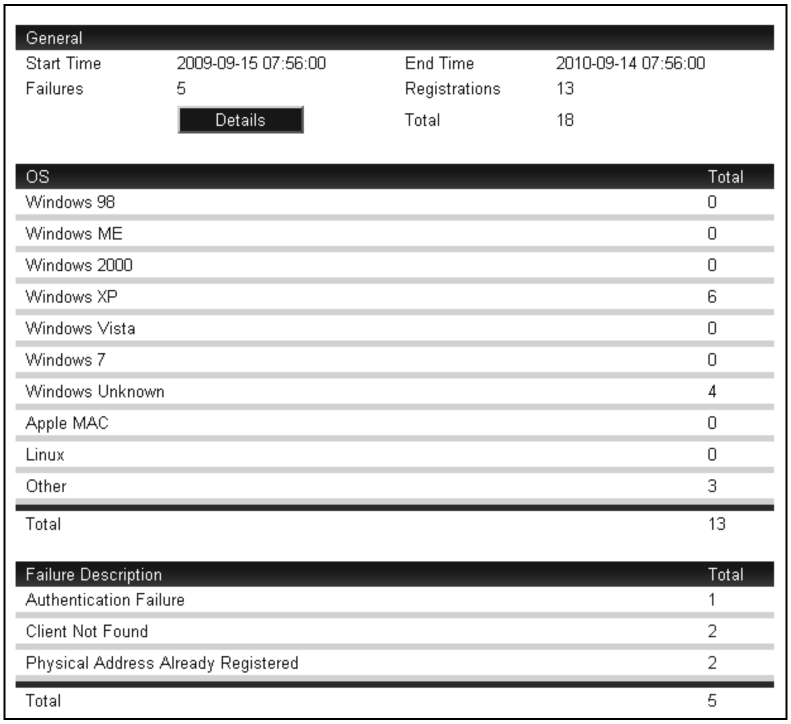
Settings

Field	Definition
Start Time	Start time and date of the report. This time is automatically set to one month prior so that you can see guest or contractor accounts and registrations for a month.
End Time	End time and date are set automatically to the time and date that you view the report.
Sponsor	Sponsor that created the guest or contractor account.
Type	Type of user, such as guest or contractor.
User	User’s email address.

Field	Definition
Name	Name of the user.
Starting	Account start date and time.
Ending	Account end date and time.
Availability	Times and days that the user can log into their account.
Role	Role of the user. For more on roles see Role management on page 553 .
Max Registrations	Maximum number of registrations that can be made on this account. For example, a conference with the same username and password for all attendees requires that all register under the same account.
Total Registrations	Total number of hosts that have been registered for each account.
Details	Click the Details button adjacent to each record to see additional information about the guest, including additional data fields that were added to the Guest, Contractor, or Conference template. The details appear only if the guest is registered.
Export Options	To export this report click an output format and follow the instructions to save the file at the desired location. The available options are: CSV, Excel, XML, PDF, RTF.
Details	
User	Guest user name. Typically this is the guest's email address.
Registration Time	Date and time that the guest registered his computer on the network. This would be the first time that the guest accessed the guest account.
Email First Name Last Name Phone Address City State Zip/Postal Code	Guest's demographic information.
Location	Switch and port where the guest last connected to the network.
Host Name	Name of the host the guest registered on the network.
Operating System	Operating system of the host the guest registered on the network.

Registrations report

This report provides you with the number of host registrations by operating systems between the specified dates. See Preview standard report templates on page 898 for instructions on generating this report.



General			
Start Time	2009-09-15 07:56:00	End Time	2010-09-14 07:56:00
Failures	5	Registrations	13
	Details	Total	18

OS	Total
Windows 98	0
Windows ME	0
Windows 2000	0
Windows XP	6
Windows Vista	0
Windows 7	0
Windows Unknown	4
Apple MAC	0
Linux	0
Other	3
Total	13

Failure Description	Total
Authentication Failure	1
Client Not Found	2
Physical Address Already Registered	2
Total	5

Settings

Field	Description
Start Time	Start time and date of the report selected when the report was requested.
End Time	End time and date are set automatically to the time and date that you view the report.
Failures	Number of failed registrations. If the same user has failed to register his host more than once, each failure increments the total count.
Registrations	Number of successful registrations.
OS	Total successful registrations by Operating System.
Failure Description	Reasons for failed registrations and the number of occurrences of each reason.
Details	
OS	Total successful registrations by Operating System. Only displays those Operating Systems for which there were registrations.
User	User name of the network user who attempted to register and failed.
Failure Description	Reason that the user failed to register his host.
Total	Total number of failed registration attempts for each user/failure reason combination.

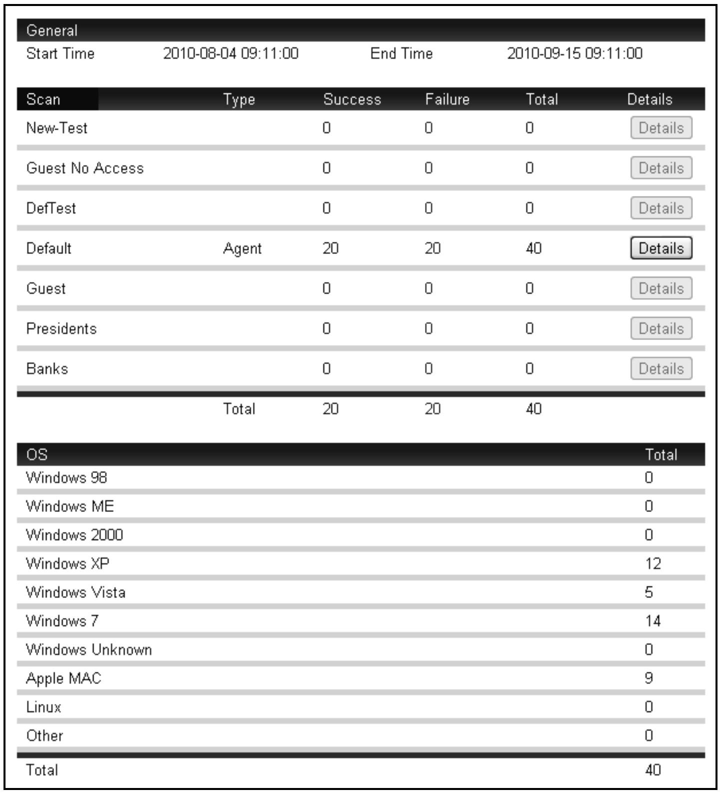
Scan results report

The Scan Results Report provides Success and Failure rates for each Scan in your database. Data is broken out by operating system. See Preview standard report templates on page 898 for instructions on generating this report.

Note that a host may be scanned more than once, particularly if it does not pass the scan the first time. Each time a host is scanned the totals are incremented. For example, if a host was scanned and failed nine times and then scanned and passed once, the Success total is incremented by one, the Failure total is incremented by nine, the total for the Scan name is incremented by ten and the total for all scans is incremented by ten.

Typically, a host will not be evaluated against more than one Scan unless something about that host changes. For example, assume you have a user who is typically at a desk and is assigned an Endpoint Compliance Policy for employees. The user is invited to a meeting and goes to a different corporate building. When he connects to a switch there, he is assigned a different policy based on his new connection location. In a case like this a host might be counted in more than one scan because it was indeed evaluated by two different Scans contained within two different Endpoint Compliance Policies.

As you drill down into the details windows the report becomes more and more granular causing the totals to increase. In the samples shown below the Default scan starts out with 40 scans. However, as the individual requirements for each scan are counted the numbers increase to 2580. For any given scan you can require Anti-Virus. Within those categories you can indicate what the preferred software is. For example, your company may prefer that users have AVG on their hosts but allow several other brands of Anti-Virus software. If a user has no Anti-Virus software on his host, the host fails the scan for the preferred Anti-Virus. The number of failures for the preferred Anti-Virus does not indicate the number of hosts with no Anti-Virus. It simply indicates the number of times a scan ran and failed. The same host could have been scanned and failed multiple times.



General			
Start Time	2010-08-04 09:11:00	End Time	2010-09-15 09:11:00

Scan	Type	Success	Failure	Total	Details
New-Test		0	0	0	Details
Guest No Access		0	0	0	Details
DefTest		0	0	0	Details
Default	Agent	20	20	40	Details
Guest		0	0	0	Details
Presidents		0	0	0	Details
Banks		0	0	0	Details
	Total	20	20	40	

OS	Total
Windows 98	0
Windows ME	0
Windows 2000	0
Windows XP	12
Windows Vista	5
Windows 7	14
Windows Unknown	0
Apple MAC	9
Linux	0
Other	0
Total	40

Scan results settings

Field	Definition
General	
Start Time	Start time and date of the report selected when the report was requested.
End Time	End time and date are set automatically to the time and date that you view the report.
Scan list	
Policy	Name of the scan used to evaluate the host.
Type	Type of scan engine. Types include: System, Nessus, Admin and Agent. Agent scans are run using the Persistent Agent (SMA), Mobile Agent, Dissolvable Agent or the Passive Agent. For information on System, Nessus and Admin Scans see Add a scan on page 481.
Success	Number of times hosts passed the scan. This scan may have been run on the same host more than once. Each time a scan is run it increments the totals.
Failure	Number of times hosts failed the scan. This scan may have been run on the same host more than once. Each time a scan is run it increments the totals.
Totals	Totals for Successful scans, Failed scans and all scans performed within the time range you selected.
Details Button	Click to display additional details about a specific Scan.
OS	Total scans broken down by host operating system.

Scan details settings

Field	Definition
General	
Start Time	Start time and date of the report selected when the report was requested.
End Time	End time and date are set automatically to the time and date that you view the report.
OS list	
Type	Type of scan engine. Types include: System, Nessus, Admin and Agent. Agent scans are run using the Persistent Agent (SMA), Dissolvable Agent or the Passive Agent. For information on System, Nessus and Admin Scans see Add a scan on page 481. To configure the Vulnerability Scanner Integration, see Vulnerability scanner on page 204.

Field	Definition
Totals	Total number of scans broken down by host operating systems using the policy selected in the previous page. This does not indicate the number of hosts scanned because a single host could be scanned more than once.
Scan categories	
Type	Indicates the type of scan engine used to scan the host.
Category	Lists categories included in the selected policy for which the engine is scanning, such as Operating System or Anti-Virus. This indicates that there are requirements in the policy for these types of items. For example, if you have indicated in your policy that users must have either AVG or McAffee as an Anti-Virus, then each host that is assigned this policy is scanned for items in the Anti-Virus category.
Success	Number of successful scans for items within the category.
Failure	Number of failed scans for items within the category.
Totals	Total scans that succeeded, failed and the sum of all scans that were run.

Additional details settings

Field	Definition
General	
Start Time	The start time and date of the report selected when the report was requested.
End Time	The end time and date is set automatically to the time and date that you view the report.
OS list	
OS Details	Total occurrences of the selected scan broken down by operating systems of the hosts that were scanned. This view breaks the list of operating systems down by providing more information about specific service packs or versions.
Category list	
Type	Type of scan engine. Types include: System, Nessus, Admin and Agent. Agent scans are run using the Persistent Agent (SMA), Dissolvable Agent or the Passive Agent. For information on System, Nessus and Admin Scans see Add a scan on page 481. To configure the Vulnerability Scanner Integration, see Vulnerability scanner on page 204.
Category	Lists categories included in the selected policy for which the engine is scanning, such as Operating System or Anti-Virus. This indicates that there are requirements in the policy for these types of items. For example, if you have indicated in your policy that users must have either AVG or McAffee as an Anti-Virus, then each host that is assigned this policy is scanned for items in the Anti-Virus category.

Field	Definition
Name	Name of the specific required item for which the engine is scanning, such as AdAware 2007 or Windows Vista Edition.
Success	Number of successful scans for a specific item within the category.
Failure	Number of times hosts failed the scan for a specific item.
Totals	Total scans for specific items that succeeded, failed and the sum of all scans that were run.

Custom reports

Custom reports allow you to add reports in addition to the standard Templates reports provided.

Reports that you add appear in the drop-down list. You can preview, schedule, modify, and remove the reports. To access Custom Reports select **Logs > Reports**. Select **Custom** from the menu on the left.

Custom reports are stored and displayed for the logged in user. These reports are not globally accessible. Users cannot access other user's custom reports.

Add a custom report

You can add and customize Registrations, Registration Failures, Scan Results, and Connection Logs reports.

1. Select **Logs > Reports > Custom**.
2. Click **Add**.
3. Select the type of report.

Report Type	Description
Registrations	Successful attempts at registration are displayed based on the selected criteria.
Registration Failures	Failed attempts at registration and login errors are displayed based on the selected criteria.
Scan Results	Endpoint Compliance Policy Scan results are displayed based on the selected criteria. In the Scan Results view or the Health Tab of Host Properties the results display a Passed result for Security/Critical Updates as well as the AutoUpdate. This occurs for all Windows Scans regardless of whether the scan was configured to require the updates. Rogue hosts are not checked unless the scan is configured to require this test. Rogue hosts will otherwise automatically pass the scan.
Connection Logs	Host connections usage information is displayed based on the selected criteria.

4. Enter the name for the report. This name will appear in the drop-down list on the **Custom** tab.

If exporting the report results to .pdf format, do NOT use a colon (**:**) in the filename.

5. Select the format for the file. For each of the options, the output will be one of the following:
   - HTML
   - CSV
   - EXCEL
   - XML
   - RTF
   - PDF
6. Click **Next** to select the criteria for the report.

Report type	Columns	
Registrations	Address City Description E-mail First Name Host ID IP address Last Name	Location Operating System Phone Physical Address Sponsor State Time Title User Zip/Postal Code
Registration Failures	Failure Code Failure Description ID IP address	Operating System Physical Address Time
Scan Results	Host ID IP address Location Operating System Physical Address	Scan Status Tests Time Type
Connection Logs	Bytes In Bytes Out Connect Time Disconnect Time	ID IP address Location Physical Address

7. Click the item(s) in the list that you want in your report. To move items, use Shift-click to select a range of items or CTRL-click to select individual items.

The items that you select are the column headings on report results.

8. Selected items are highlighted. In the Available Columns panel, click the Right Arrow button to move them to the Selected Columns panel.
9. Click an item in the Selected Columns panel to select it. Use the Up and Down Arrow buttons in the center to rearrange the items in the order that the columns are to appear on the report.

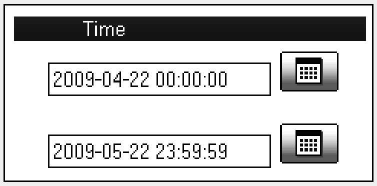
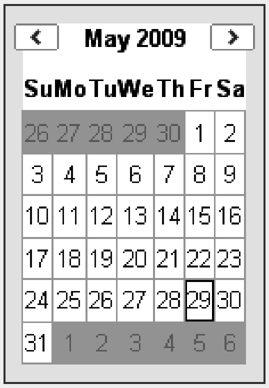
Top to bottom in the list appear left to right in the results.

10. Click Next.
11. Enter parameters for the report. These are filters that limit the amount of data returned in the report. Filters are not case sensitive. If you enter smith, the filter returns results for Smith and SMITH.

    You can use wildcards when you filter, such as, S* in the last name field would return anyone whose last name begins with S. *s* in the last name field would return anyone whose last name contained an s.
12. Click **Finish**. The report is added to the drop-down list on the **Custom** tab.

Parameters

Report type	Parameters	
Registrations	Additional Hardware Information • IP address • Physical Address • Operating System • Location • Description • Host Time (See Calendar Icon on page 907) • Starting • Ending	User Information • ID • Title • Last Name • First Name • Address • City • State • Zip/Postal Code • Phone • E-mail
Registration Failures	User Information • ID Time (See Calendar Icon on page 907) • Starting • Ending	Hardware Information • IP address • Physical Address • Operating System
Scan Results	Host Information • ID • IP address	Scan Details • Status • Type

Report type	Parameters	
	• Physical Address • Location • Host • Operating System Time (See Calendar Icon on page 907) • Starting • Ending	• Scan Name
Connection Logs	Host Information • ID • IP address • Physical Address	Device Information • Location Connection Time (See Calendar Icon on page 907) • Starting • Ending
Calendar Icon	 Time 2009-04-22 00:00:00 2009-05-22 23:59:59  May 2009 Su Mo Tu We Th Fr Sa 26 27 28 29 30 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 1 2 3 4 5 6	Enter the times for Start and End. Format for date and time is YYYY-MM-DD hh:mm:ss Or use the calendar icon to select the Starting and Ending times for the report. Time for the selected Start date defaults to 00:00:00. Time for the selected End date defaults to 23:59:59. Edit the time parameters to specify a more limited range of data for the generated report. If you select a start time but no end time, the report is generated with data up to the current time. If you select an end time, but no start time, the report is generated with all data up to the specified end time.

Preview a custom report

When you have completed adding the Custom report, you can preview the results and export the report to a file for later use. The export formats are HTML, CSV, EXCEL, XML, RTF, and PDF.

1. Select **Logs > Reports**.
2. Select **Custom** from the menu on the left.

3. From the **Custom** tab, select the report name from the drop-down list.
4. Click **Preview**. The report displays in a new browser window.
5. Scroll to the bottom of the report and click an output format.
6. When prompted, click to select **Open** or **Save to Disk**.
7. When selecting Save to Disk, navigate to the appropriate folder, enter a filename, and click **Save**.

Modify a custom report

When you have completed adding and previewing the custom report, you can modify the report to refine the results.

1. Select **Logs > Reports**.
2. Select **Custom** from the menu on the left.
3. From the **Custom** tab, select the report name from the drop-down list.
4. Click the **Modify** button.
5. The existing type and format information are displayed. Click **Next**.
6. Change the parameters used in the report. See Add a custom report on page 904 for parameters.
7. Click **Next**.
8. Change the information for the report.
9. Click **Finish**. Use the **Preview** function to review the changes.

Remove a custom report

To remove custom reports that are no longer needed:

1. Select **Logs > Reports**.
2. Select **Custom** from the menu on the left.
3. Select the report name from the drop-down list.

The report is removed immediately so be certain that the report name shown in the Reports field is the one you want removed.

4. Click the **Remove** button.
5. If the report was previously scheduled, select **System > Scheduler** and delete the scheduled report from the list of **Scheduled Tasks**.

Schedule reports

Both the standard report templates and custom reports can be scheduled to run on a regular basis. Custom reports are output to the file format selected by the user when adding the report. The standard reports are output to .pdf files with the filename format `ReportType.MM.DD.YYYY-hh-mm-AM/PM.pdf` with the following filenames:

- PolicyCharts
- PolicyOSReport

- PolicyTestSummary
- RegistrationFailure
- RegistrationOSReport

View scheduled reports by selecting **Logs > Reports > Archives**. The output may be sent to administrators or other users via email. A list of Administrator groups is displayed in the Email group drop-down list in the report schedule view.

Reports via e-mail prerequisites

- The Administrator users who will receive the email must be members of an Administrator group. This can be the All Management Group or another Administrator group that has been created. See Groups view on page 838 for details on creating groups.
- The members of the Administrator group must have an email address in their user record(s) to receive email. See Add an admin user on page 685 for more information.
- The mail server information must also be entered under System > Settings. See Email settings on page 169 for more information.

1. Select **Logs > Reports**.
2. To schedule a standard report: Go to the **Templates** tab, select a **Report Type** and click **Schedule**.
3. To schedule a custom report: Go to the **Custom** tab, select a report and click **Schedule**.
4. Enter a **Name** for the Scheduled task.
5. Select an **Email Group** if you want to share the report.
6. Enter the **Data Range** and select **Days**, **Hours**, or **Weeks** from the drop-down list.
7. Enter the **Schedule Interval** and select **Days**, **Hours**, or **Weeks** from the drop-down list.
8. Enter the **Next Scheduled Time**.
9. Click **Apply**.

Settings

Field	Definition
Name	Name for the scheduled task.
Email Group	Group containing the Administrator users who will receive the email report results when the scheduled task runs.
Data Range	Number of hours, days, or weeks of data in the report.
Schedule Interval	Length of time the scheduled task waits before running again.
Next Scheduled Time	Initial date/time the task is scheduled to run. Format is MM/DD/YY hh:mm AM/PM.

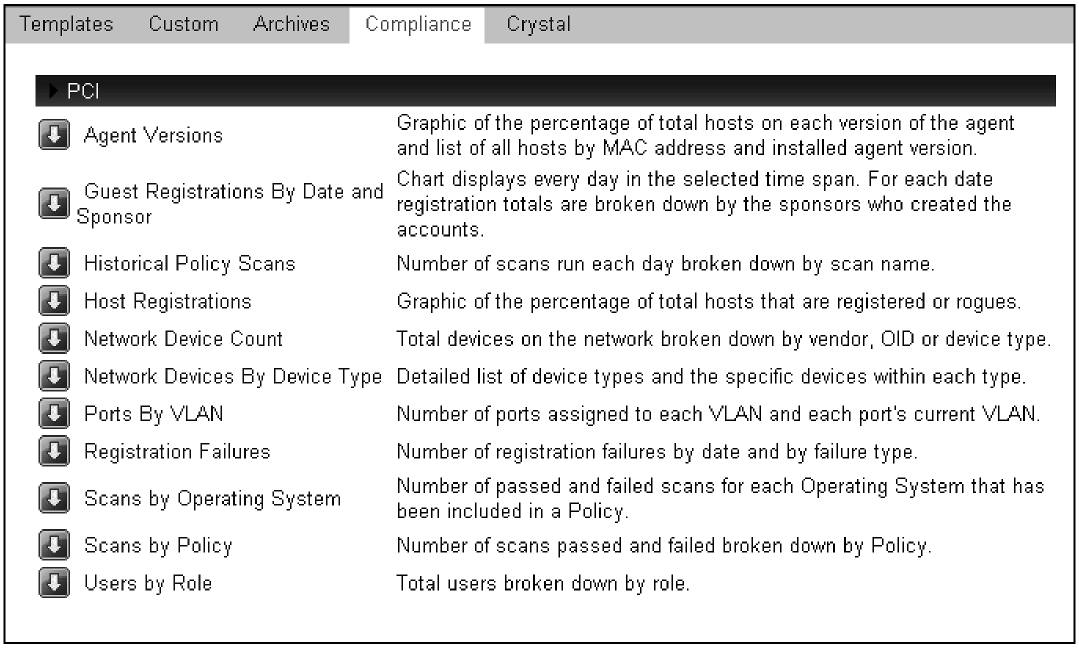
Archived reports

Archived reports are generated when the scheduled task runs for Templates and Custom reports. View these reports from the Archive tab on the Reports View.

1. Select **Logs > Reports > Archives**.
2. Click a report in the list to view the contents.
3. Click a heading to sort the reports by **Name** or **Time Generated**.

Compliance reports

The Compliance tab on the Reports View provides access to report templates that are associated with compliance reporting for different industries, such as PCI reports for organizations that process credit card transactions. Many of the same reports can be helpful in meeting other compliance requirements, such as HIPAA or SOX.



Agent Versions	Graphic of the percentage of total hosts on each version of the agent and list of all hosts by MAC address and installed agent version.
Guest Registrations By Date and Sponsor	Chart displays every day in the selected time span. For each date registration totals are broken down by the sponsors who created the accounts.
Historical Policy Scans	Number of scans run each day broken down by scan name.
Host Registrations	Graphic of the percentage of total hosts that are registered or rogues.
Network Device Count	Total devices on the network broken down by vendor, OID or device type.
Network Devices By Device Type	Detailed list of device types and the specific devices within each type.
Ports By VLAN	Number of ports assigned to each VLAN and each port's current VLAN.
Registration Failures	Number of registration failures by date and by failure type.
Scans by Operating System	Number of passed and failed scans for each Operating System that has been included in a Policy.
Scans by Policy	Number of scans passed and failed broken down by Policy.
Users by Role	Total users broken down by role.

The table below provides a list of PCI requirements and the Compliance reports that can be used as supporting documentation for those particular requirements.

PCI Requirements	Report Title
1.0	Network device count on page 913 Network devices by type on page 913
1.3, 8.1	Daily network access by role on page 915
1.4, 11.2	Scans by policy on page 919
5.1, 11.2	Scans by operating system on page 918
5.2	Historical scans on page 916 Agent versions on page 911
6.3.2	Ports by VLAN on page 914
7.1.1, 7.1.2	Users by role on page 919

PCI Requirements	Report Title
8.1	Host registrations on page 917
10.2	Registration failures on page 917
12.0	Guest registrations on page 912

PCI reports

Compliance reports are used to ensure that data security standards are being met for different industries. PCI is a set of security standards for payment account data protection that applies to businesses who process credit card transactions. PCI reports provided with FortiNAC allow you to verify that your network is meeting these security standards. To access PCI Reports:

1. Select **Logs > Reports**.
2. Click **Compliance** on the left.
3. If the list of PCI reports is not displayed, click the arrow to the left of the PCI Reports title bar. This drops down the list of available reports.

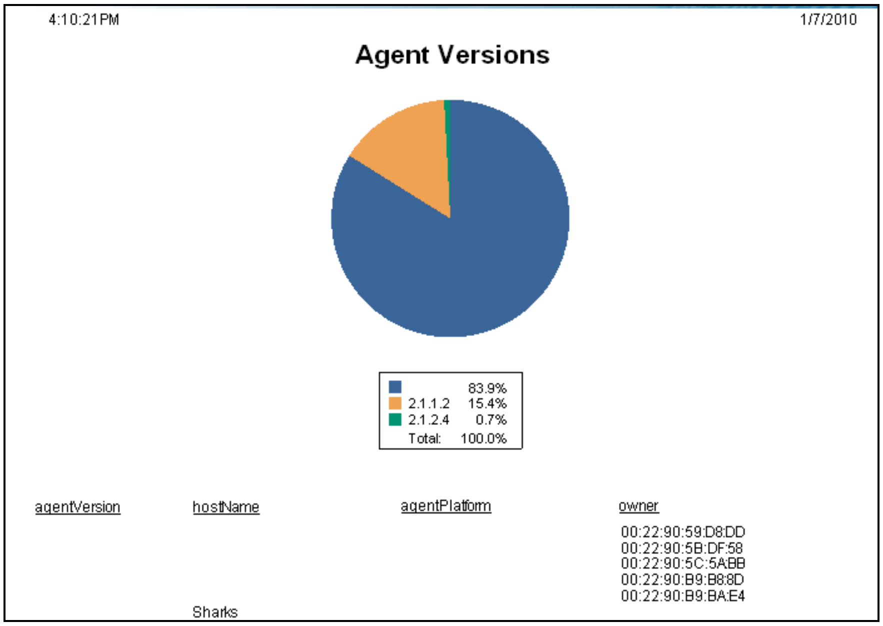
PCI reports include:

- Agent versions on page 911
- Guest registrations on page 912
- Network device count on page 913
- Network devices by type on page 913
- Ports by VLAN on page 914
- Daily network access by role on page 915
- Historical scans on page 916
- Registration failures on page 917
- Host registrations on page 917
- Scans by operating system on page 918
- Scans by policy on page 919
- Users by role on page 919

Agent versions

This PCI Compliance report provides a pie chart of the percentage of total hosts on each version of the agent. Following the chart is a list of all hosts with information on the installed agent version, host name, platform and owner.

Use this report to verify that all hosts can be scanned because they have an agent installed and that each user has a unique identifier.



4:10:21PM 1/7/2010

Agent Versions

agentVersion hostName agentPlatform owner

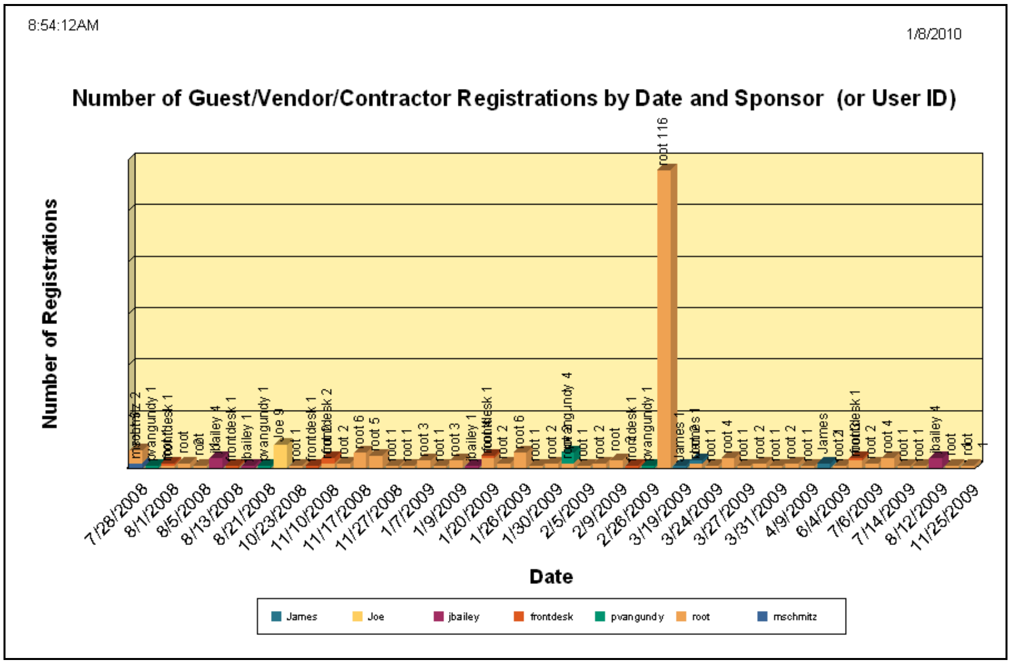
00:22:90:59:D8:DD
00:22:90:5B:DF:58
00:22:90:5C:5A:BB
00:22:90:B9:B8:8D
00:22:90:B9:BA:E4

Sharks

Guest registrations

This PCI Compliance report provides a chart of the number of guests registrations that were processed broken down by the sponsor who created the guest account and the date.

Use this report to verify that all guests have gone through the registration process and therefore were presented with an “Acceptable Use” page containing information about network usage.



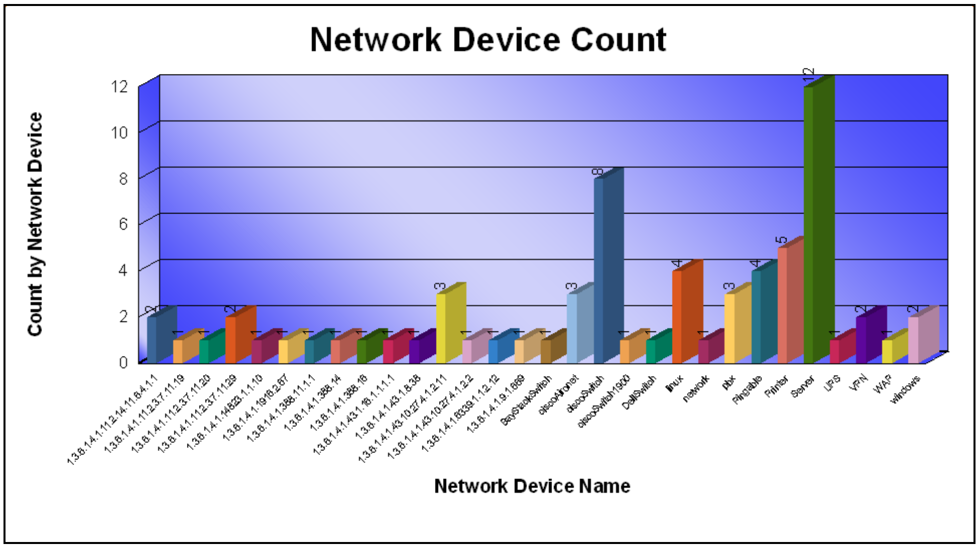
8:54:12AM 1/8/2010

Number of Guest/Vendor/Contractor Registrations by Date and Sponsor (or User ID)

Network device count

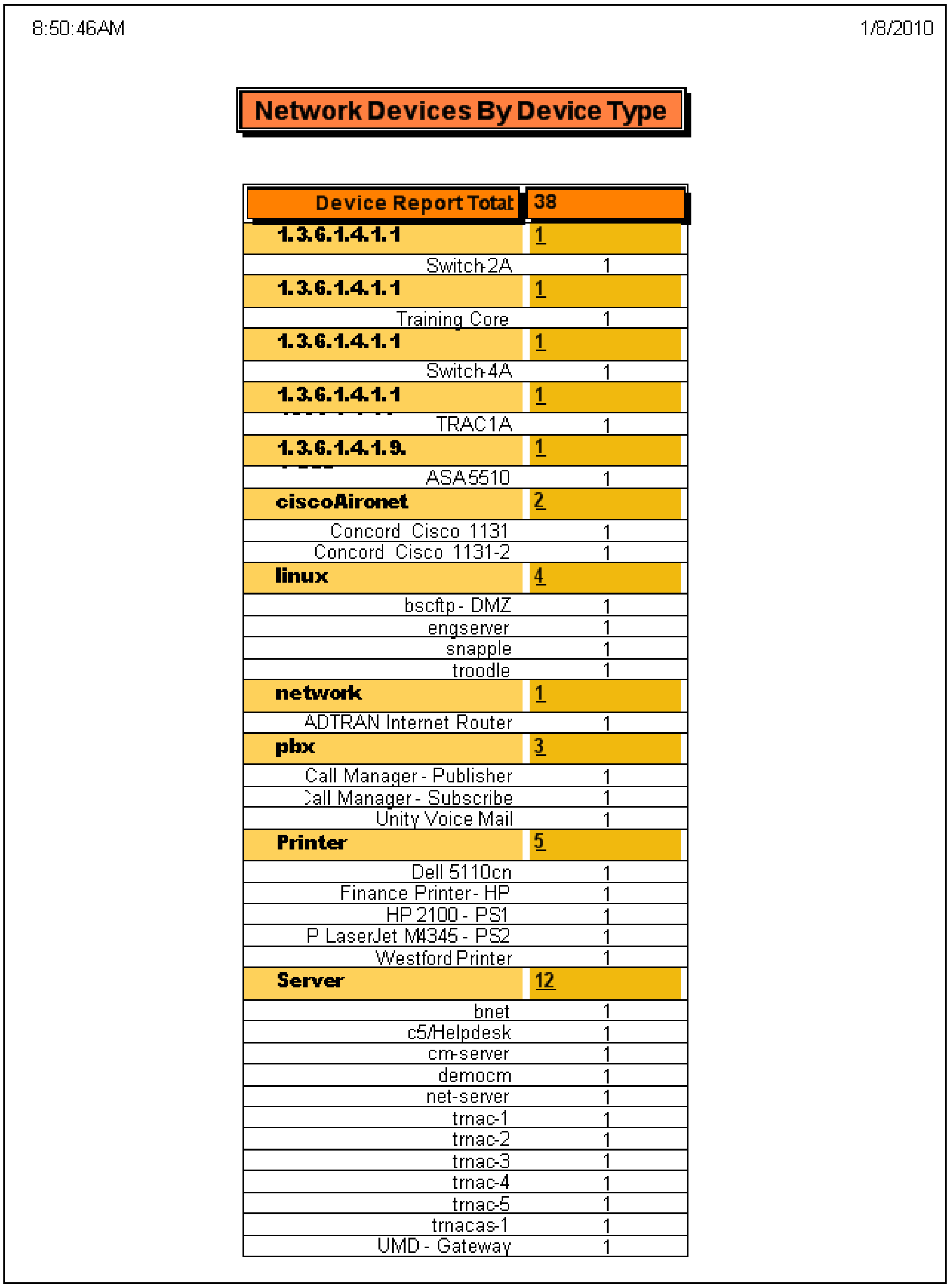
This PCI Compliance report provides a chart of all of the devices on your network broken down by device type, vendor or OID. Below the chart is a detailed list of each device that includes device name, vendor, the ID number of the topology container in which the device resides, IP address and MAC address.

Use this report to verify the list of components that build and maintain a secure network environment.



Network devices by type

This PCI Compliance report provides a table of devices broken down by type. Below the table is a list of each device and includes device name, type, IP address and MAC address. Use this report to verify the list of components that build and maintain a secure network environment.



8:50:46AM 1/8/2010

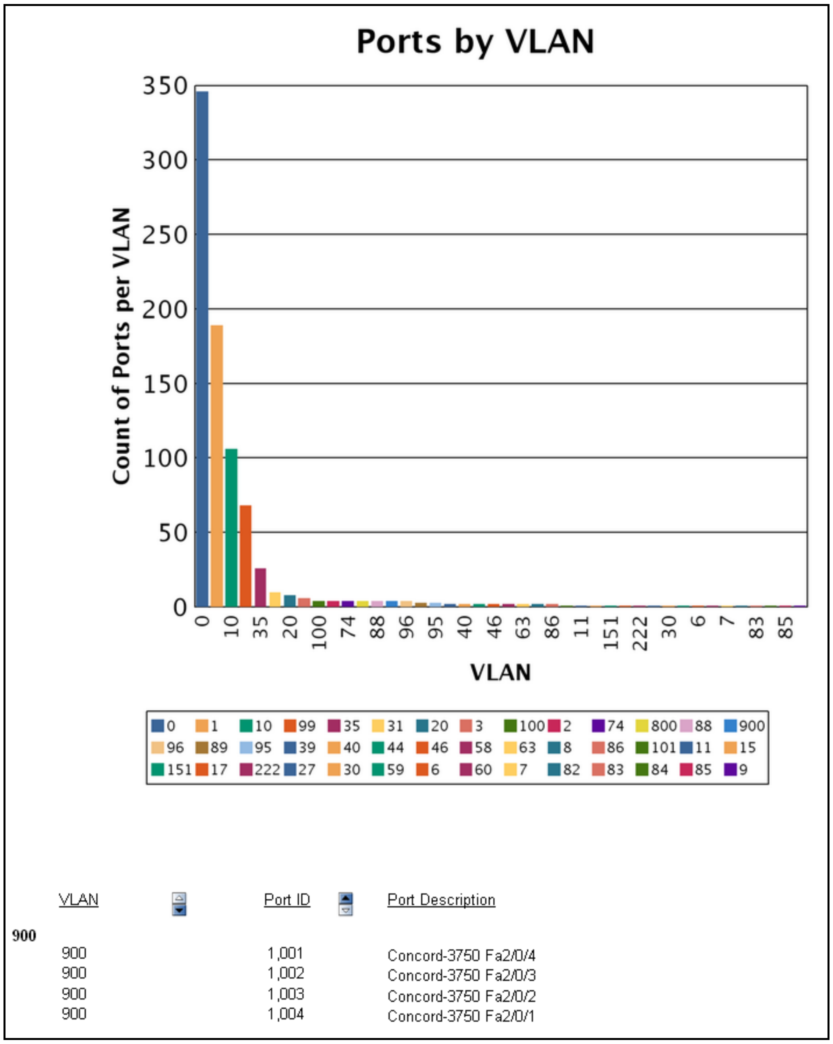
Network Devices By Device Type

Device Report Total	38	
1.3.6.1.4.1.1	1	
Switch-2A		1
1.3.6.1.4.1.1	1	
Training Core		1
1.3.6.1.4.1.1	1	
Switch-4A		1
1.3.6.1.4.1.1	1	
TRAC1A		1
1.3.6.1.4.1.9.	1	
ASA5510		1
ciscoAironet	2	
Concord Cisco 1131		1
Concord Cisco 1131-2		1
linux	4	
bscftp - DMZ		1
engserver		1
snapple		1
troodle		1
network	1	
ADTRAN Internet Router		1
pbx	3	
Call Manager - Publisher		1
Call Manager - Subscribe		1
Unity Voice Mail		1
Printer	5	
Dell 5110cn		1
Finance Printer - HP		1
HP 2100 - PS1		1
P LaserJet M4345 - PS2		1
Westford Printer		1
Server	12	
bnet		1
c5/Helpdesk		1
cm-server		1
democm		1
net-server		1
trnac-1		1
trnac-2		1
trnac-3		1
trnac-4		1
trnac-5		1
trnacas-1		1
UMD - Gateway		1

Ports by VLAN

This PCI Compliance report provides a chart of the number of ports in each VLAN at the time the report is generated. Below the chart is a list of each port and its current VLAN.

Use this report to verify that ports used for development and ports used for testing are kept separate. Roles assigned to ports force ports to be placed in particular VLANs.

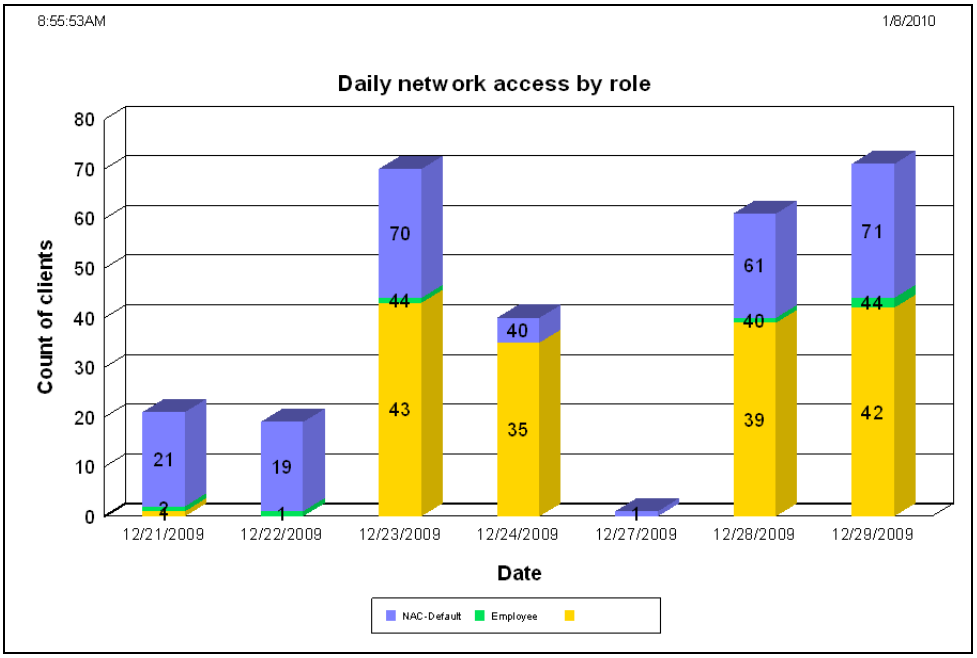


VLAN	Port ID	Port Description
900		
900	1,001	Concord-3750 Fa2/0/4
900	1,002	Concord-3750 Fa2/0/3
900	1,003	Concord-3750 Fa2/0/2
900	1,004	Concord-3750 Fa2/0/1

Daily network access by role

This PCI Compliance report provides a chart of the number of users in each role that accessed the network by date. Below the chart is a list of each connection with information on the user, the IP address and MAC address of the host used to access the network, the users role, when they connected and disconnected and the switch and port where the host was connected.

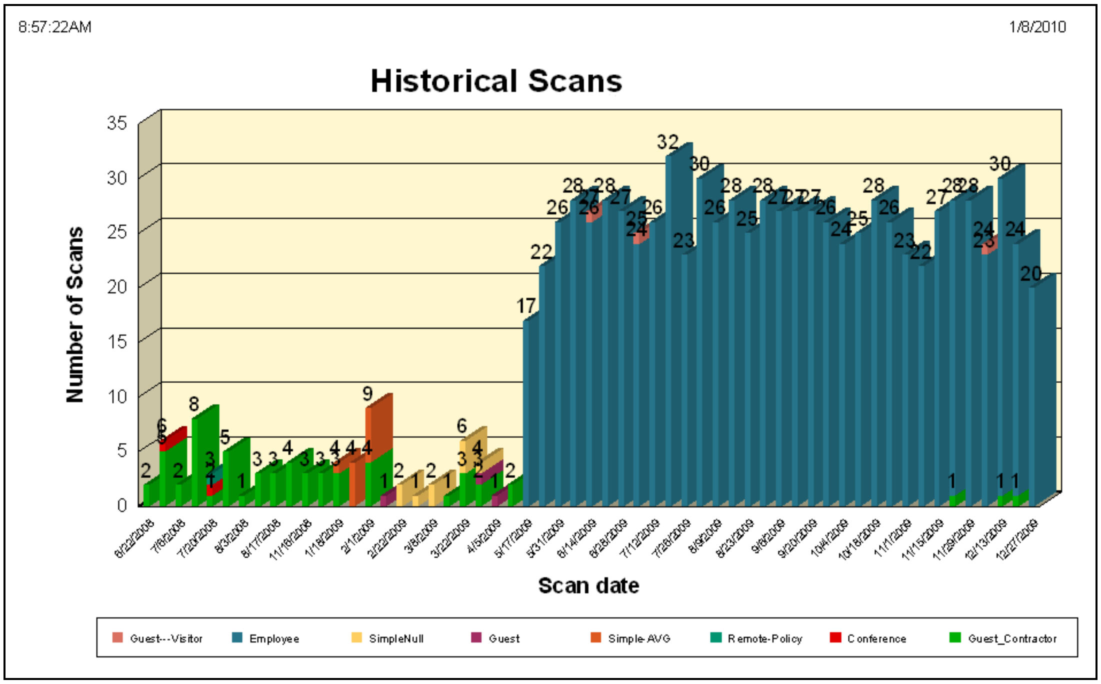
Use this report to verify that network users' access was limited to specific segments of the network by the role to which they were assigned. This report also provides the required list of unique user IDs.



Historical scans

This PCI Compliance report provides a chart of the number of times a particular scan was run each day. For example, the number of times the OS Check scan was used to evaluate hosts on 10/22/2010. Below the chart is a list of each scan that was done with the date, time, name of the scan used, scan status, user name and MAC address of the host.

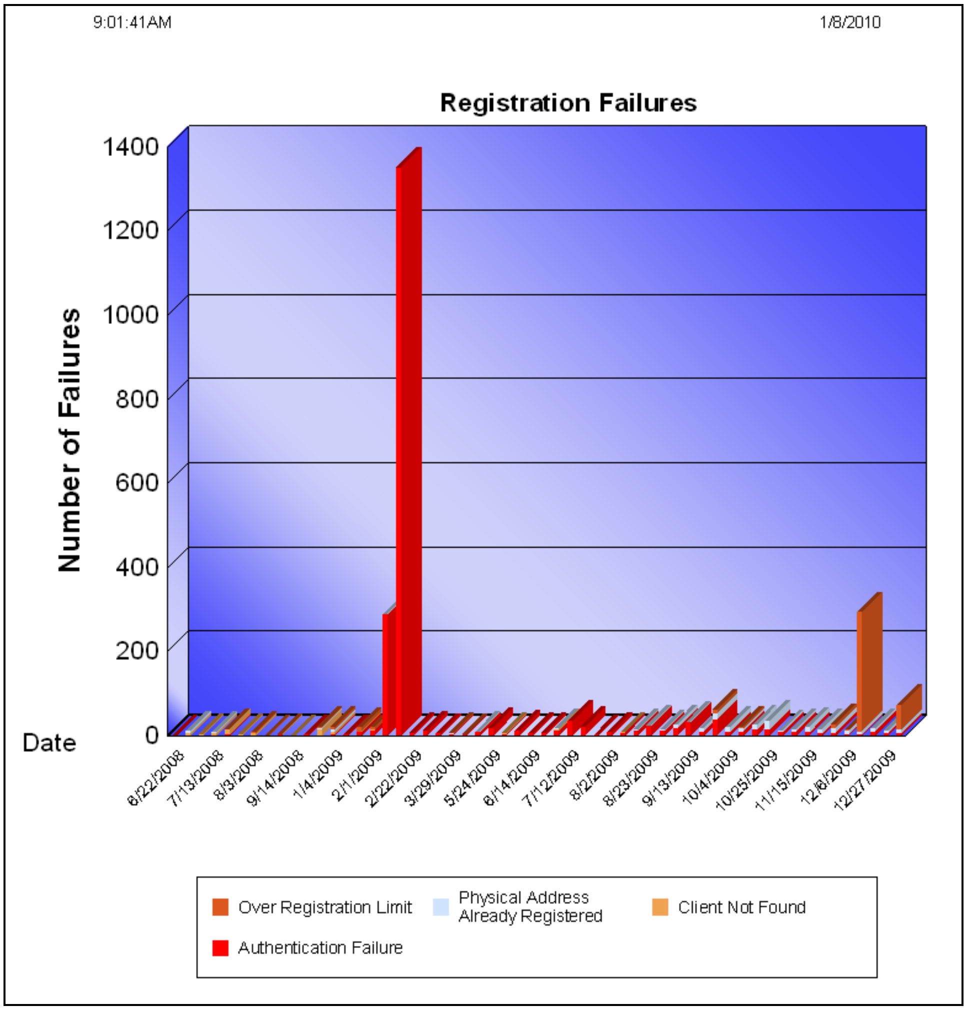
Use this report to verify that hosts have been scanned and forced to maintain the most recent version of Anti-Virus and Anti-Spyware software.



Registration failures

This PCI Compliance report provides a chart of the number of registration failures by date and by type. Below the chart is a list of registration failures with the date, time, user ID, the failure code, a description of the failure and a tally for each day.

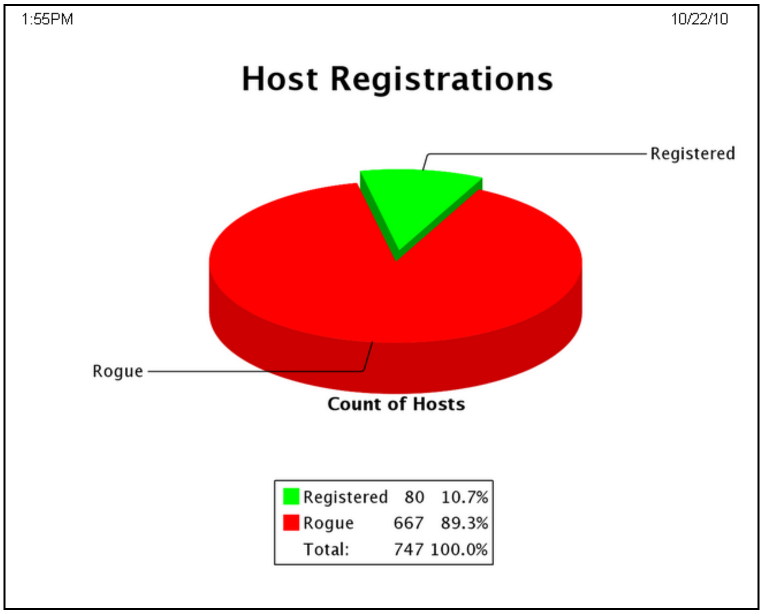
Use this report to verify invalid network access attempts. Hosts that fail to register are not given network access.



Host registrations

This PCI Compliance report provides a chart of the percentage of total hosts in the database that are registered or rogues. Below the chart is a list of each registered and rogue host with host name and registered user where applicable.

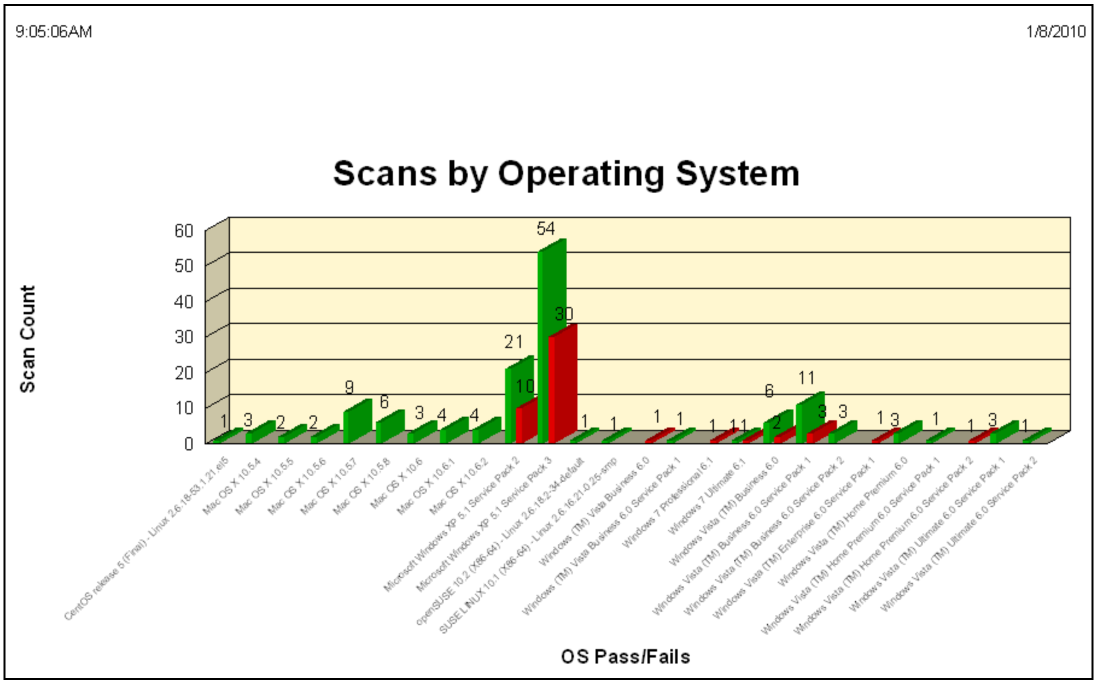
Use this report to verify that each host and user has a unique identifier.



Scans by operating system

This PCI Compliance report provides a chart of the number of passed and failed scans for each Operating System that has been included in a Policy. Below the chart is a list of each scan with the date, time, policy name, scan status, user ID and the MAC address of the host.

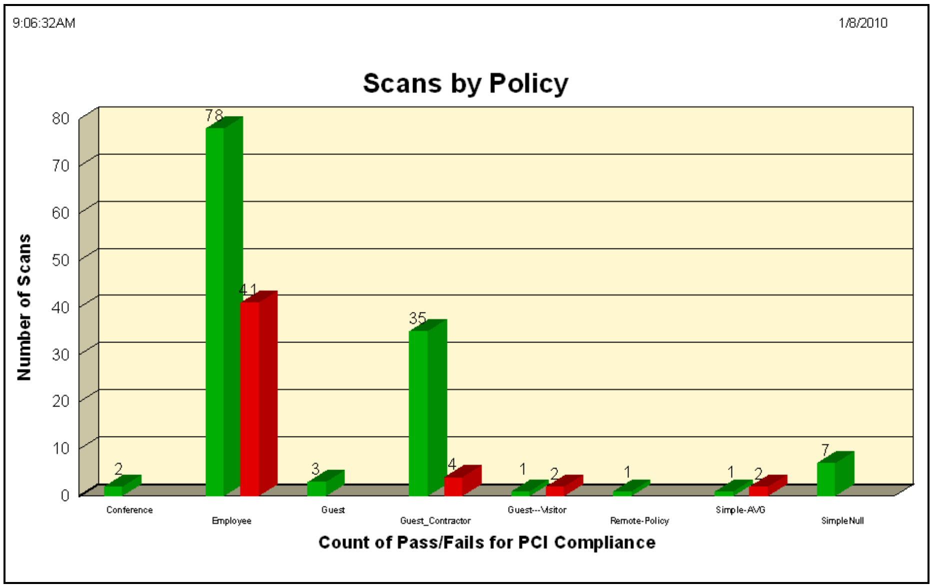
Use this report to verify the policies for which hosts have been scanned. Policies can be configured to scan for the latest Operating System updates, the existence of Anti-Virus and Anti-Spyware software and corresponding updates



Scans by policy

This PCI Compliance report provides a chart of the number of scans passed and failed broken down by policy. Below the chart is a list of each scan with the date, time, policy name, scan status, user ID and the MAC address of the host.

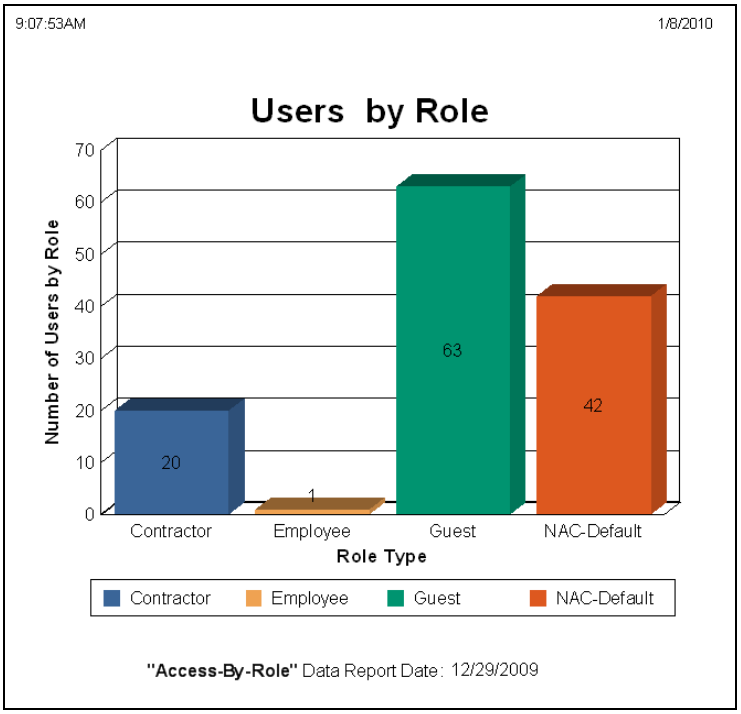
Use this report to verify that users' computers have been scanned for a firewall based on the policy applied. Hosts that fail such a policy are not allowed on the network. In addition, this report verifies that network hosts have undergone periodic security scans.



Users by role

This PCI Compliance report provides a chart of the total number of users broken down by role. Below the chart is a list of each role and the users within it.

Use this report to verify access restrictions based on the role assigned to the user.



Download or run compliance report templates

Compliance report templates were created using Crystal Reports. These templates can be run to generate reports or downloaded to your host to be modified. To modify a report template you must have a copy of Crystal Reports.

Run reports

1. Select **Logs > Reports > Compliance**.
2. Click on the name of the report you wish to run.
3. The report displays in a separate tab in your browser.
4. Use the arrows at the top of the window to scroll from page to page.
5. Click the **Print** button to send to report to your default printer.

Download reports

1. Select **Logs > Reports > Compliance**.
2. Click on the green **Download** button to the left of the report title.
3. The report template is downloaded to your default download directory.

Crystal reports

The Crystal tab on the Reports view allows you to upload your own Crystal Report templates created outside FortiNAC. You can also download and edit templates from the Compliance tab, then upload the modified templates on the Crystal tab.

To create your own reports using data from the FortiNAC database you must complete the following tasks:

- Create a User Name and Password for the FortiNAC MySQL database. See Configure a database password on page 922.
- Download and install the MySQL ODBC Connector. See Install and configure MySQL ODBC connector on page 922.
- Configure the ODBC connection. See Install and configure MySQL ODBC connector on page 922.
- Install Crystal Reports on your local host. Only required for users that will create or edit templates. Users running templates that have already been created elsewhere do not need to install Crystal Reports. You must use Crystal Reports 2008.
- Configure the connection between the database and your Crystal Reports installation. Only required for users running Crystal Reports. See Configure the database connection on page 923.

Instructions in this document pertaining to Crystal Reports are based on Crystal Reports 2008.

You must have a copy of the full Crystal Reports software to create new templates or edit existing templates.The Crystal Reports engine is installed on the FortiNAC server.

Upload custom templates

There are no special requirements for uploading templates. Templates uploaded through the Crystal tab are stored in: `/bsc/campusMgr/ui/ROOT/user`

1. Select **Logs > Reports**.
2. Click on the **Crystal** tab.
3. Click the **Upload Report** button.
4. In the pop-up window, click **Choose File**.
5. Browse to the template, select it and click **Open**.
6. Click **OK** in the pop-up window.
7. The report template displays in the **Custom Crystal Reports** drop-down list.

Run custom templates

There are no special requirements for running templates.

1. Select **Logs > Reports**.
2. Click on the **Crystal** tab.
3. Select a report template from the **Custom Crystal Reports** drop-down list.

4. Click **Run**.
5. The report displays in a separate tab in your browser.

Configure a database password

To create your own report templates using FortiNAC data, Crystal Reports must be able to access your MySQL database. Due to security concerns, a default reports password is not provided. You must create a database password before configuring your ODBC connection. If you have multiple FortiNAC appliances, create a password for each database that will be used for reports.

1. Navigate to the command line on your FortiNAC Server or FortiNAC Control Server.
2. Log in as a root user.
3. Navigate to the `/bsc/campusMgr/bin` directory. This directory contains the `CreateDBAccount` script. By default the privileges are set to SELECT which provides Read-Only access.
4. Run the `CreateDBAccount` script and supply the required parameters. To run the script type the following:

   ```
   CreateDBAccount <username> <password> <serverip or %>
   ```

   Where:

   `username` is the username for the remote account

   `password` is the password for the remote account

   `serverip` is the IP address of the host used to connect to the database. Using this parameter ensures that the user can connect with this username and password only from that host. If you wish to allow the user to connect from any host use % instead of the IP address.

   `%` is a wild card for the IP address of the host used to connect to the database. This allows the user to connect with the created username and password from any host.

   Example:

   ```
   CreateDBAccount reports abc123 %
   ```
5. The new database user name and password are now available for reports.

To remove a MySQL account use the DeleteDBAccount script.

Install and configure MySQL ODBC connector

The MySQL ODBC connector is required only if you plan to create or edit Crystal Report templates and upload them to the FortiNAC server.

Installation

1. Use a browser to go to the MySQL web site at www.mysql.com.
2. Go to the **Downloads** section.
3. Select or search for **Connectors**.
4. Download the appropriate Connector-ODBC for your operating system.

5. Download or display the Connector-ODBC installation instructions.
6. Follow the installation instructions and install the connector.

Configuration

Before configuring the ODBC Data Source, you must determine who should have access to this Data Source for reports.

- To provide access for only the current logged in user, create the data source using the User DSN tab.
- To provide access to all users connecting through this computer, create the data source using the System DSN tab.
- To provide access to any user on any computer that has the MySQL Connector-ODBC installed, use the File DNS tab and save the Data Source to a network or shared drive.

The instructions below describe configuring the Data Source for the current logged in user. Options for System DSN and File DSN are similar, use the Help for additional instructions.

1. From your Windows Desktop select Start > Run.
2. In the Run window type odbcad32 and click OK. This logs you into the Microsoft ODBC Administrator.
3. Make sure you are on the User DSN tab and click Add to create a new ODBC data source. The Create New Data Source window displays.
4. Click Finish. The ODBC Data Source Configuration window displays. Use this window to configure the connection to your FortiNAC appliance and its database. The database is on the FortiNAC Server or Control Server.

> If you have more than one FortiNAC Server or Control Server, you must configure a separate connection for each one.

5. In the **Data Source Name** field type the name of your FortiNAC Server or Control Server. This is a user defined name and is not used to connect to the database.
6. In the **Description** field enter a description of the FortiNAC Server or Control Server.
7. In the **Server** field enter either the IP address or the DNS name of the FortiNAC Server or Control Server.
8. In the **User** field enter the user name you created to access the MySQL database on your FortiNAC Server.
9. In the **Password** field enter the password you created to access your MySQL database.
10. Click the **Test** button to test the connection and populate the Database field with available databases on the selected server.
11. In the **Database** field, select **bsc** as the database and click **OK**.
12. You are returned to the ODBC Data Source Administrator window and your new data source is displayed. Click **OK** to save.

Configure the database connection

1. Start Crystal Reports.
2. Click **File > Log On or Off Server**. The **Data Explorer** window displays.
3. Open the **Create New Connection** folder.
4. Double-click the **ODBC (RDO)** folder or open it and select **Make New Connection**.
5. The ODBC (RDO) window is displayed. Make sure the **Select Data Source** option is selected.
6. Click on the appropriate data source in the list displayed and click **Next**.
7. On the next window, enter the MySQL **User ID** and **Password** you created for reports.

8. Make sure the **Database** field is set to **bsc** and click **Finish**. The new connection displays in the **Data Explorer Window**.
9. Repeat this process for each FortiNAC server or control server being used for reports.

Scan results view

The scan results view displays the results that are maintained in the FortiNAC database of Dissolvable and Persistent Agents, and system scans. Access the scan results view from the **Hosts** menu.

See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.

Settings

Fields used in filters are also defined in this table.

Field	Definition
Scan results	
Time	Time the scan was run.
Scan	Name of the scan used.
User ID	User name of the owner of the host registered in FortiNAC or the MAC Address for Rogue hosts.
IP address	IP address of the host at the time it was scanned.
Host	Host name from the Rogue host records or the Host Name from Registered host records.
Operating System	OS on the host.
Location	Name of the switch/port where the host was connected for the scan.
Type	Type of scan performed.
Status	Includes Passed, Failed, Script Failed or Warning.
Right click options & buttons	
Export	Exports data to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.
Show Details	Displays additional details about the selected scan including: MAC address for all interfaces on the host and the results of any Custom scans associated with the scan used.
Archive & Clear All Scans	Creates an archive of all scans in the database and then removes all scans from the database.
Archive & Clear Selected Scans	Creates an archive of the scans selected in the Scan Results table and then removes those scans from the database.

Show details

The Details window provides information about the scan selected in the Scan Results table. Additional information includes the MAC address for each interface on the host and the results of any Custom Scans associated with the scan used to evaluate the host. Scans can have one or more associated custom scans. See Custom scans on page 448.

1. Click **Hosts > Scan Results**.
2. Use the filters to display a list of scans.
3. Select the appropriate scan from the list and click **Show Details**.

Archive and clear all scans

Use this option to archive and clear all the Scan Results records. The archived records can be imported later. See Import archived data on page 696 for details.

1. Click **Hosts > Scan Results**.
2. Click **Archive & Clear All Scans**.
3. Click **Yes** on the confirmation window.
4. All the records are archived in a file using the following name format: `RESULTS_Archive_YY_MM_DD:hh:mm:ss.bua.gz`

Archive and clear selected scans

Use this option to archive and clear the selected Scan Results records. You can import archived records at another time. See Import archived data on page 696 for details.

1. Click **Hosts > Scan Results**.
2. Use the filters to display a list of scans.
3. Click a record to select it. Use either Shift-click or Ctrl-click to select additional records.
4. When you have selected the records, click **Archive & Clear Selected Scans**.
5. Click **Yes** on the confirmation window.
6. The selected records are archived in a file with the following name format: `RESULTS_Archive_YY_MM_DD:hh:mm:ss.bua.gz`

Connections view

The connections view displays the contents of the connection log—a list of historical host/user network connections.

To access the connections view, select **Logs > Connections**.

Settings

Field	Definition
Connect Time	Time the connection was established.
Disconnect Time	Time the connection was terminated.
User ID	ID used to log onto the network.
Name	Name of the associated user or vendor name, if neither is available MAC address is displayed. A host registered as a device may not have a user or vendor name.
Host Name	Name of the host for the selected connection record.
Location	Current or last known location of the device that made the connection.
IP address	IP address of the device that made the connection.
Physical Address	MAC address of the host or device that made the connection.
Host Type	Indicates whether the host is Registered or a Rogue.
Buttons	
Import	Import historical connections from an Archive file. See Import archived data on page 696.
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.

Top users

The **Top Users** panel displays the top *n* hosts that were online for the longest time when you click the Top Online Users button.

1. Click the Top Users button at the bottom of the Connections View.
2. Enter the number of users to display and click Refresh.

CLI configuration

A CLI configuration is a set of commands that are normally used through the command line interface. The CLI configuration window allows you to create individual sets of commands, name them and then reuse them as needed to control ports, VLANs or host access to the network. When a CLI configuration is applied, the commands contained with in it are sent to the selected network device. This modifies the network device’s behavior as long as those commands are in force.

This software currently supports CLI commands for Cisco, D-Link, HP ProCurve, Nortel, Enterasys, Brocade, and Extreme wired and wireless devices. This document assumes that you are familiar with the CLI commands available for your devices and, therefore, does not include individual commands in the instructions.

It is recommended that you test all CLI commands or sets of commands using the console for the switch, router or other device before implementing CLI commands through FortiNAC. FortiNAC does not detect errors in the structure of the command set being applied on the device. CLI commands are applied to the device exactly as they are created.

You can create a set of CLI commands to perform an operation, and a separate set to undo the operation. Undo is triggered when FortiNAC recognizes that the host or device has disconnected from the port. The do and undo command combination is sometimes referred to as Flex-CLI. Note that by using both Set and Undo, the CLI configurations do not become cumulative on the device.

To access the CLI Configuration View, go to **Network Devices > CLI Configuration**.

See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.

Settings

Field	Definition
Name	Name used to identify the CLI Configuration.
Description	User specified description for the CLI Configuration.
Last Modified By	User name of the last user to modify the configuration.
Last Modified Date	Date and time of the last modification to this configuration.
Right click options	
Copy	Creates a copy of the selected CLI Configuration.
Delete	Deletes the selected CLI Configuration.
In Use	Provides a list of other features that reference this CLI Configuration, such as a Role Mapping or a Scheduled Task. See Configuration in use on page 930.
Modify	Opens the Modify CLI Configuration window. See Add or modify a configuration on page 931.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item.

Field	Definition
	For information about the Admin Auditing Log, see Admin auditing on page 847 You must have permission to view the Admin Auditing Log. See Add an admin profile on page 671
Buttons	
Show CLI	Opens the CLI window and displays a all of the commands in the Set and Undo sections of the configuration. See Show configuration on page 930.

There are several CLI Configuration events that can be enabled and mapped to alarms for notification:

Event	Definition
CLI Configuration Failure CLI Configuration Success	Generated when a user tries to configure a Scheduled task that involves applying a CLI Configuration to a group. Indicates whether or not the configuration of the scheduled task was successful.
Host CLI Task Failure Host CLI Task Success	Indicates whether or not the CLI commands associated with host/adapter based ACLs have been successful.
Port CLI Task Failure Port CLI Task Success	Indicates whether or not the CLI commands associated with port based ACLs have been successful.
Port CLI Data Substitution Failure Port CLI Data Substitution Success	Indicates success or failure to substitute the "Port, VLAN, IP, or MAC" data into the CLI.

Using CLI configurations you can do the following:

- Apply or remove specific CLI configurations to networking devices based on control states, such as Registration, Authentication or Quarantine. See Apply a port based configuration via the model configuration on page 935.
- Apply or remove ACL based CLI configurations to hosts connected to the network on a Layer 2 or Layer 3 device. The ACL modified by the CLI configuration controls host access to the network. These configurations can be applied or removed based on control states, such as Registration, Authentication or Quarantine. See Apply a host based configuration via the model configuration on page 936 and Requirements for ACL based configurations on page 943.
- Apply specific CLI configurations for roles. Note that roles are associated with device or port groups. Be sure to group devices with common CLI capabilities. See Role management on page 553 and Apply a CLI configuration using a role on page 937.
- Apply specific CLI configurations for Network Access Policies. When using User/Host Profiles to determine Access Policies, use location criteria to group devices with common CLI capabilities. See Network access policies on page 407 and Apply a CLI configuration using a network access policy on page 941.
- Create a scheduled task for a CLI configuration to be applied to a device group. See Apply a CLI configuration using a scheduled task on page 941.
- Use port logging capabilities to see which port control changes and CLI configurations were applied and when. See Port changes view on page 942.

Variable options

Substitution Data	Port Based DO	Port Based UNDO	Host Based DO	Host Based UNDO
%port%	Yes	Yes	Yes	No
%vlan%	Yes (if specified in Network Access Configuration)	Yes (from present "current" vlan of the port)	Yes (from present "current" vlan of the port)	No
%ip%	No	No	Yes	Yes
%mac%	No	No	Yes	Yes

Configuration in use

To find the list of FortiNAC features that reference a CLI Configuration, select the configuration from the CLI Configurations View and click the In Use button. A message is displayed indicating whether or not the configuration is associated with any other features. If the configuration is referenced elsewhere, a list of each feature that references the configuration is displayed.

Show configuration

This option displays a all of the commands within the CLI Configuration.

1. Select **Network Devices > CLI Configurations**.
2. Select the configuration and click **Show CLI** to display the commands within the configuration.

FortiNAC provides the proper login command sequence and final logout or exit commands. Your CLI should include exit commands to exit modes entered within the CLI. The final session logout or exit is done by FortiNAC.

Port based and host based configurations

Port based CLI configurations are used to switch VLANs for a host, modify port behavior for a host or to reconfigure settings on a group of switches. Host based CLI configurations are used in environments where you have many hosts connecting through a single port and those hosts need to be controlled individually instead of based on the least secure host.

Host based CLI configurations leverage the use of ACLs stored on a Layer 3 device by adding or removing IP addresses from the ACL.

Below is a list of devices and the types of CLI configurations supported.

Devices	Port Based	Host Based
Cisco	Yes	Yes
D-Link	Yes	Yes
Enterasys	Yes	Yes
Extreme	Yes	Yes
Brocade	Yes	Yes
HP ProCurve	Yes	Yes
Nortel	Yes	No

Add or modify a configuration

FortiNAC provides the proper login command sequence and final logout or exit commands. Do no include the login commands and logout or exit commands in the CLI.

1. Select **Network Devices > CLI Configuration**.
2. To create a new CLI configuration, click **Add**.
3. To modify a CLI configuration, select it from the CLI Configuration view and click **Modify**.
4. Right-click in any of the three main text areas for a pop-up menu with editing options: Undo, Cut, Copy, Paste, Delete, and Select All. You can also use Ctrl+x, Ctrl+c, and Ctrl+v to cut, copy, and paste.
5. Enter a name for the CLI configuration. This name displays in other parts of the software allowing you to choose and implement this configuration.
6. If you plan to use MAC address in your CLI configuration, select the **MAC Address Format** that is recognized by the device to which you are applying this configuration.
7. Click in the **Commands To Set** field and enter the CLI commands to be stored as a configuration.
8. If you would like to reverse those commands when the port state or host state changes, go to the **Commands To Undo** field and enter the appropriate commands. Use the **Copy** button to copy commands from Commands To Set to Commands To Undo.

   In the event of a device failure or power cycle, changes made by CLI command sets to the device configuration could be lost. FortiNAC will not resend CLI command sets that were sent successfully. It is recommended that you include a command such as, write mem, in the creation of your CLI command sets to ensure that the most recent configuration is saved on the device.

9. Enter a **Description** of the CLI configuration. This field is not required.
10. Click **OK** to save.

Settings

Field	Definition
Name	Required. Assign a descriptive name to the CLI command set.
MAC Address Format	If you choose to modify an ACL by adding or removing MAC addresses, you must select the MAC address format that is recognized by your device. If this format is incorrect, the device will not be able to interpret the MAC address information in the ACL.

Commands To Set	Required. Enter the commands that comprise the configuration. Following is an example:
	`config t`
	`interface %port%`
	`speed 10`
	`duplex half`
	`exit`
	`exit`
	You can use shorthand if it is supported on your networking device.
	The commands you enter in the CLI Configuration window dynamically populate port/interface, VLAN IDs, IP addresses and MAC addresses based on your choice of CLI control mechanism.
	Each variable in the CLI configuration is treated as a separate entity. You can use the variables any number of times or not at all, based on your choice of CLI commands.

%port% button %vlan% button	The **%port%** and **%vlan%** buttons for the Commands to Set and Commands to Undo text areas simplify adding this substitution parameter.
%ip% button	The **%ip%** button allows you to quickly add this parameter into the CLI configuration and can be used to add or remove IP addresses from an ACL. Can be used only on Layer 3 devices such as routers.
%mac% button	The **%mac%** button allows you to quickly add this parameter into the CLI configuration and can be used to add or remove MAC addresses from an ACL. When you click this button it also inserts the MAC Address format selected at the top of the window. Can be used only on Layer 2 devices.
Copy to Undo	Click this button to copy the commands from the Commands to Set pane to the Commands to Undo pane. Edit the commands in this pane to add a negate command.

Commands To Undo	Optional. This field allows you to reverse commands in the Commands To Set field. For example, if you change speed or duplex on a port for a host, you may need to return that configuration to its default setting when a different host connects. See the example below:
	`config t`
	`interface %port%`
	`speed auto`
	`duplex auto`
	`exit`
	`exit`

Field	Definition
CLI Description	Detailed description of the command set for reference and clarification.

Sample configurations

The Port and Host based CLI configurations shown below are samples of different types of configurations that may help you develop your own.

Example 1: Port based configuration - port speed

The configuration shown below modifies the speed and duplex configuration of the port and then returns it to its normal state.

Set/Undo	CLI Configuration

Commands To Set	`config t`
	`interface %port%`
	`speed 10`
	`duplex half`
	`exit`
	`exit`

Commands To Undo	`config t`
	`interface %port%`
	`speed auto`
	`duplex auto`
	`exit`
	`exit`

Example 2: Port based CLI configuration - device configuration

This configuration is used in conjunction with the Scheduler to configure devices to send traps to the FortiNAC Server. The sample IP address shown is the address of the FortiNAC Server that should receive the traps. In this case no Undo commands are used.

Set/Undo	CLI Configuration
Commands To Set	config t snmp-server host 192.168.102.110 public end write mem
Commands To Undo	

Example 3: Host based CLI configuration - IP address

The configuration shown below modifies an IP address ACL on the device to switch access for the host's IP address from the FortiNAC software DNS server to the production DNS server. When the host is restricted to the FortiNAC software DNS server, it is essentially in isolation and can be forced to register. When the host has access to the production DNS server, it can connect to the network and access the Internet.

Set/Undo	CLI Configuration
Commands To Set	config t ip access-list extended Nac 1 deny udp host %ip% host 192.168.34.2 eq domain 2 permit ip host %ip% host 192.168.105.2 exit ip access-list resequence Nac 10 1 end write mem
Commands To Undo	config t ip access-list extended Nac no deny udp host %ip% host 192.168.34.2 eq domain no permit ip host %ip% host 192.168.105.2 end write mem

In the example above 192.168.34.2 is the production DNS server and 192.168.105.2 is the FortiNAC software DNS server. In the second line, Nac is the name of the ACL. ACL name is case sensitive. If the name is not correct, the ACL is not modified.

The ip access-list resequence Nac 10 1 command is important because it controls the sequence in which the host IP addresses are entered into the ACL. Starting with line 10, each IP address is added to the beginning of the list. Addresses already in the list are incremented by one.

If FortiNAC cannot determine the IP or any data substitution value of the host, the CLI will not be run. A CLI Substitution Failure Event is generated describing the data which could not be substituted.

Example 4: Host based CLI configuration - MAC address

The configuration shown below modifies a MAC filtering ACL on the device to deny access to a particular MAC address sent by FortiNAC.

Set/Undo	CLI Configuration

Commands To Set	`config t`
	`mac access-list extended Nac`
	`1 deny %macXXXX.XXXX.XXXX% any`
	`exit`
	`mac access-list resequence Nac 10 1`
	`end`
	`write mem`

Commands To Undo	`config t`
	`mac access-list extended Nac`
	`no deny %macXXXX.XXXX.XXXX% any`
	`end`
	`write mem`

In the example above, Nac is the name of the ACL. ACL name is case sensitive. If the name is not correct, the ACL is not modified.

The mac access-list resequence Nac 10 1 command is important because it controls the sequence in which the host MAC addresses are entered into the ACL. Starting with line 10, each MAC address is added to the beginning of the list. Addresses already in the list are incremented by one.

Implement configurations

CLI configurations can be implemented on the device itself to control network access based on host state using the Model Configuration window. They can also be associated with a role or a Network Access Policy. Devices that connect to devices or ports with that role trigger the application of the CLI configuration. Hosts that connect to devices or ports associated with the Network Access Policy trigger the application of the CLI configuration. CLI configurations can be applied to device or port groups based on a scheduled task.

When a CLI Configuration has been applied based on one of the criteria listed above, it remains in effect until something else happens. For example, if a CLI configuration is applied based on a Network Access Policy, when the host connects to a port and both the host and the port are included in the policy, the associated CLI configuration is applied. The CLI configuration remains applied to the port until a different CLI configuration is applied or the UNDO commands are triggered. A host disconnect or a VLAN change will trigger the UNDO.

Apply a port based configuration via the model configuration

When hosts connect to the network, the FortiNAC software determines the host’s state. Based on that state the host may be sent to Registration, Quarantine, Authentication, Dead End or the production network. The configuration of the device to which the host has connected controls the host’s network access.

Use the Model Configuration window of your FortiNAC software to set just a VLAN for each host state, a VLAN and a CLI configuration for any of those states or nothing. If you set a CLI configuration for a state, you must also set a VLAN for that state even if it is just the production VLAN. When both a VLAN and a CLI configuration are set for a particular host state, they can work in conjunction with each other. For example, if Authentication is set to VLAN 10 and a CLI configuration is also applied, that configuration might reduce bandwidth while the user is in the Authentication VLAN.

CLI configurations will not be applied if there is no VLAN selected in the Network Access section of the Model Configuration.

This option is used when you would like to apply a CLI configuration to hosts who do not match a Network Access Policy. Typically these hosts would not have a policy because they have not registered or been authenticated and the FortiNAC software does not know who they are.

1. Select **Network Devices > Topology**.
2. Right-click on the device and then click **Model Configuration**.
3. In the **General** section, enter the **User Name** and **Password** for CLI access to the device.
4. In the **Protocol** section, select the communication protocol for this device.
5. In the **Network Access** section, if there is a Read VLANs button, click it to populate drop-downs for each host state. Select the VLANs used for each host state. Note that you should not fill in the Default field if ports on this device have different default VLAN settings. Default VLANs should be set on the **Network Access/VLANS** window. If all ports on the device use the same Default VLAN you can set it here.
6. In the **CLI Configurations** section, select the type as **Port based**. Port based configurations affect the port directly.
7. Select a **CLI Configuration** for the host states you wish to affect. If you select a CLI configuration you must set a corresponding VLAN.
8. If you are using a RADIUS server for authentication, the default servers are displayed and do not need to be modified. If this device should use a different RADIUS server for authentication, select it from the drop-down list and enter the matching RADIUS Secret.
9. Click **Apply** to save your changes.

Apply a host based configuration via the model configuration

Host-based CLI configurations modify ACLs stored on the switch or router. CLI configurations that modify IP address ACLs can only be used on Layer 3 devices.

or removes IP addresses from a corresponding ACL based on the host state. When the host connects, the FortiNAC software determines whether or not they need to be sent to registration, authentication, remediation or remain in a dead end. When the host has satisfied the requirements of its state and is ready to be put on the production network, the state change triggers the undo portion of the CLI configuration updates the ACL again. This allows the host onto the production network. See Basic Setup Requirements For ACL Based CLI Configurations.

1. Select **Network Devices > Topology**.
2. Right-click on the device and then click **Model Configuration**.
3. In the **General** section enter the User Name and Password for CLI access to the device.
4. In the **Protocol** section select the communication protocol for this device.
5. In the **Network Access** section if there is a Read VLANs button, click it to populate the VLAN drop-downs. Set the VLANs used for each host state. Note that you should not fill in the Default field if ports on this device have different default VLAN settings. Default VLANs should be set on the Network Access / VLANS window. If all ports on the device use the same Default VLAN you can set it here.
6. In the **CLI Configurations** section, select the type - **Host Based**. Host based configurations control host access through the use of an ACL stored on the device and referenced in the CLI configuration.
7. Select a CLI configuration for the host states you wish to affect. If you select a CLI configuration you must set a

corresponding VLAN.

Right-click the device and select the Applied ACLs menu option to view or clear applied ACL settings. The Applied ACL menu option is available after a Host Based Configuration is applied. You may need to refresh the Topology View.

8. If you are using a RADIUS server for authentication, the default servers are displayed and do not need to be modified. If this device should use a different RADIUS server for authentication, select it from the drop-down list and enter the matching RADIUS Secret.
9. Click **Apply** to save your changes.

View/clear applied ACL settings

If you have applied host based CLI configurations, you may want to see and/or remove changes to the ACL on the device. This option is accessed via the Applied ACL window.

1. Select **Network Devices > Topology**.
2. Expand the **Container** holding the device.
3. Right-click on the device. Select the device name and then click **Applied ACLs**.

The Applied ACL menu option is available after a Host Based Configuration is applied. You may need to refresh the Topology View.

The Applied ACLs window opens, displaying the name, MAC address, IP address, CLI, and Host for each Applied ACL.

4. Select the ACL(s) you wish to delete, and then click **Delete**. If there is an Undo configuration, it will be run.
5. Click **Close** to exit.

Apply a CLI configuration using a role

CLI configurations applied based on a role are typically port based not host based. It is not recommended that you use host based CLI configurations with roles.

Network Device Roles allow you to control network access based on combinations of devices and connection locations. Each role that is created can be applied to individual devices.

Devices that require network services can only have one role. Switches or ports to which devices connect for network access can be mapped to more than one role. The role mapping provides the switches and ports with rules when something with a matching role connects.

To provide more flexible control using roles you can apply a CLI configuration instead of just switching VLANs.

Refer to Assigning roles on page 554 to set roles for hosts, network devices and ports. Then refer to for step-by-step instructions.

Role assignments

Roles can be assigned to users, hosts, network devices and ports. Each one of these entities has a role field on its corresponding Properties window. Assignment of roles is accomplished by setting the role field for the user, host, device or port either manually or using one of the options listed in the table.

When a user and a host have different roles, the user role is applied if the user logs into the host. In the case of a gaming device that the user does not log into, it has its own role that may or may not be the same as the user's.

In the event that multiple methods are used to set a role, the order of precedence is determined by the order of the roles on the Roles View. Starting from the top of the list, the first role match found is used. For example, assume you have assigned roles to hosts based on groups. Later you add the host to a new group, if that group is associated with a role that is ranked above the host's original role, the host's role will be changed.

In the event that multiple methods are used to assign a role to a host, a hierarchy determines which role to assign. Roles assigned through Portal pages (typically for gaming), have the lowest precedence and will be overwritten by a role determined by any other method. Roles assigned by Directory Attributes have the highest precedence and will overwrite a role that is assigned by any other method. Roles assigned by Group Membership have the middle level of precedence, overwriting roles assigned through Portal Pages, but being overwritten by roles assigned via Directory Attributes. Roles assigned via Group Membership will change when the host's group membership changes. When this occurs, the roles are ranked, with low-numbered ranks having the highest precedence.

Roles	Definition
User roles	
User Roles Based On Groups	Users can be assigned roles by placing them in a group and then associating that group with a role on the Role View. See Add a role on page 559 for additional information on adding roles. Once the group of users has been created and you have assigned them a role, you must associate that role with a device group or a port group and a corresponding VLAN or CLI configuration. User groups can also be created based on groups in the Directory. These groups are treated the same as groups created manually within FortiNAC. If a user is a member of more than one group the group that is found first when matching users to roles determines the role assigned to the user. When assigning Roles to users, the use of Directory attributes over Directory groups is recommended. Attribute data is retrieved directly from the directory as the user registers, while group information is retrieved from data cached on the FortiNAC server and could be out-dated.
User Roles Based On A Directory Field	Network users can be assigned a role based on a field in LDAP or Active Directory. For example, you might choose to have roles based on a field in the directory called Department. The data within the Department field would be the name of the role, such as, Accounting or Customer Service. In a university environment a user might have a role based on whether he is a Student or Faculty.

Roles	Definition
	To assign roles based on a field in a directory you must indicate which field in the directory is to be used as a role. See to map the role field. Users in the directory with matching data in this field constitute a group, even though the group is not shown anywhere. For example, users with Accounting in their department field are treated as an Accounting group for the purpose of assigning roles. Next, you must create a Role with the exact same name as the data contained in the directory field. For example, if the user's role in the directory is Accounting, you must create a Role on the Role View that is named Accounting. When a user registers, the role field in User Properties is set to match the data in that user's role field in the directory.
User Roles Based On Fields In Captive Portal	When registering a host through the Captive Portal, if the user fields on the portal page have a role set, that role is assigned to the user, such as during registration or authentication.
Individual User Roles	In some situations you may want to assign a role to a single user. First create the role on the Roles View. Then, navigate to the User Properties window and modify the Role field.
Host roles	
Host Roles Inherited From Users	When registering a rogue to a user on the Host View, you have the option to use the user's role or to select a different role for the device. See Add or modify a host on page 807. When registering a host through the Captive Portal, if the portal does not have a role set, the host inherits the role of the user. If the users role changes, regardless of how it is changed, any host registered to that user that has the same role will be changed also. **Example:** John Doe is a student and has two registered hosts. John Doe's Role: **Student** John Doe's Host 1 Role: **Student** John Doe's Host 2 Role: **Gaming** John Doe graduates and becomes faculty, so the University makes the change in AD and runs a Directory Sync. John's role is changed to Faculty. John Doe's Role: **Faculty** John Doe's Host 1 Role: **Faculty** John Doe's Host 2 Role: **Gaming** Host 2 did not match John's original role of Student, so it is not changed.
Host Roles Assigned Through Captive Portal	When registering a host through the Captive Portal, if the portal page has a role set, that role is assigned to the host during registration. If the role field is blank, the host inherits the role of the user.

Roles	Definition
Host Roles Based On Groups	Hosts can be assigned roles by placing them in a group and then associating that group with a role on the Roles View. See Add a role on page 559 for additional information on adding roles.
Host Roles Assigned Manually	This would typically be used to assign a role to hosts, such as a medical device that connects to the network. To register rogues and set their role: Select one or more rogues on the Host View. Right-click on the selected records and choose Register as Device from the menu. On the registration pop-up you can select device type and role. See Register a host as a device on page 812. To set roles for registered devices: Select one or more devices on the Host View. Right-click on the selected records and choose Set Host Role. Select the new role from the drop-down list in the pop-up window.
Host Roles Assigned By Device Profiler	This would typically be used to assign a role to hosts, such as a medical device that connects to the network. Devices that are hosts, such as, medical devices, gaming devices, or printers can be assigned a role and a device type based on Device Profiling Rules. If you are using the Device Profiler feature, you can create or use default rules that allow FortiNAC to determine the device type and assign the device to a role. When a new host device connects to the network it becomes a rogue because it is unknown. FortiNAC compares information received from the device with the Device Profiling Rules in its database until it comes up with a match. Based on the parameters defined in the rule, the device is assigned a type and a role. See Device profiler on page 348 and Rules on page 350. The role assigned by Device Profiler takes precedence over any role associated with the Vendor OUI.

Configure a role with CLI

1. Select **Policy > Roles**.
2. Click **Add** at the bottom of the **Roles View**.
3. In the **Name** field, enter a name for the new role.
4. Click the **Select** button next to the Groups field. Choose one or more groups by clicking on the names in the **All Groups** column and clicking the right arrow to move them to the **Selected Groups** column. Click **OK** to continue.
5. Click in the **Note** field to add any user defined information needed for this role.
6. Click **OK** to save the role.
7. Click on **Network Device Roles** in the menu on the left to create a mapping for this role.
8. Click the **Add** button at the bottom of the screen.
9. Click the **Role** check box to enable the role drop-down. If this is not enabled, this mapping can apply to any device that matches the other criteria in the mapping, such as Location. The word Any displays in the Role column on the Network Device Roles View if this box is unchecked.
10. Select the role you created earlier from the drop-down list.

11. To apply a CLI configuration, click the **CLI** check box to enable it and select the CLI configuration from the drop-down list.
12. If applicable, in the **Access Value** field type the Network Access identifier for this mapping, such as a VLAN ID, VLAN Name, Aruba Role or for a VPN concentrator enter a group policy name.
13. Click the **Select** button next to the Location field. Choose one or more device or port groups by clicking on the names in the **All Groups** column and clicking the right arrow to move them to the **Selected Groups** column. Click **OK** to continue.
14. Click in the **Note** field to add any user defined information needed for this mapping.
15. Click **OK** to save the mapping.

Apply a CLI configuration using a network access policy

CLI configurations applied based on a Network Access Policy are by default port-based not host based.

Network Access Policies use User/Host Profiles to match a host with a Network Access Configuration. Network Access Configurations contain VLAN and/or CLI configuration information. Each User/Host Profile used to apply a CLI configuration should contain the group of devices or ports to which the host must be connected and the rules or filters that determine whether or not the Network Access Configuration should apply to the connecting host. The groups of devices or ports should contain devices that can accept CLI configurations.

To provide more flexible control using Network Access Policies you can apply a CLI configuration instead of just switching VLANs.

Refer to Network access policies on page 407 to set policies for hosts, network devices and ports.

1. Select **Policy > Policy Configuration**.
2. In the menu on the left select **Network Access**.
3. Click the **Add** button or select an existing Policy and click **Modify**.
4. Click in the **Name** field and enter a name for this policy.
5. Click the **Add** icon next to **User/Host Profile**. Only certain devices can accept CLI configurations. At minimum you must configure the Where (Location) field for the User/Host Profile to ensure that CLI configurations are applied only to devices that can accept them. The remainder of the User/Host Profile can be configured any way you wish. Click **OK** to save the profile. Connecting users/hosts must match this User/Host Profile to be assigned the Network Access Configuration specified in the next step.
6. Click the **Add** icon next to **Network Access Configuration**.
7. Enter a name for the configuration.
8. Mark the **CLI configuration** check box to enable it and select a CLI configuration from the drop-down list. Click **OK** to save the Network Access Configuration. See Add or modify a configuration on page 414 for additional information.
9. The **Note** field is optional.
10. Click **OK** to save your Policy.

Apply a CLI configuration using a scheduled task

This option is typically used when configuring a group of devices that can interpret the same set of CLI commands. For example, if you are configuring devices to send traps back to your FortiNAC software, you can apply a CLI configuration using a scheduled task to configure them all at once instead of logging into each device individually.

1. Select **System > Scheduler**.
2. From the **Scheduler** view, click **Add**.
3. Enter a **Name** for the task and an optional description.
4. In the **Action Type** field select CLI. CLI actions are sets of command line instructions that are created in the CLI Configuration View and saved to be executed elsewhere in the program.
5. Select the **Action** from the list of CLI actions.
6. From the **Select a Group** drop-down list, select the group of devices to which the CLI configuration will be applied.
7. From the **Schedule Type** drop-down select either **Fixed Day** or **Repetitive** and set the day and time that the task is to be performed.
8. A **Fixed Day Task** is one that you can schedule to run any day at any time. Selects the day(s) and time to run the task.
    a. Click the box next to the day(s) to select the day.
    b. Click the down arrows and select the hour, minutes, and AM or PM from the drop-down list for each day.
    c. To enter days/times more quickly, use the **Set Multiple Days** button to set multiple days with the same time.
    d. To remove all settings click the **Clear All** button.
9. A **Repetitive Task** is one you configure to run on a given day, at a specific time for a specified number of repetitions. The repetition rate can be set to any number of minutes, hours, or days.
    a. Enter the **Repetition Rate** using whole numbers.

    A repetition rate of zero causes the task to run only once.

    b. Click the down arrow and select Minutes, Hours, or Days from the drop-down list.
    c. Enter the date and time for the task to run in the **Next Scheduled Time** field using the format MM/DD/YY hh:mm AM/PM Time Zone.
    d. Click **Update** to update the **Next Scheduled Time** field or change the **Repetition Rate**.

    The new Repetition Rate does not take effect immediately. It starts the next time the scheduled task runs. For the new Repetition Rate to take effect immediately, click the **Update** button.

10. Click **OK**.

Port changes view

When the port’s VLAN changes or when a port-based CLI configuration is applied, entries are written to the Port Changes view.

See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.

Settings

Fields used in filters are also defined in this table.

Field	Definition
Port changes	
Date	Date that the change occurred.
CLI Config Name	CLI Configuration used to modify the port state.
Port Change Reason	Reasons for changes in port state. Reasons include: • **Registration**—Port was moved into the Registration VLAN. • **Remediation**—Port was moved into the Remediation VLAN. • **Dead-End**—Port was moved into the Dead-End VLAN. • **Default**—Port was moved to the Default VLAN • **Role**—Port was moved into the VLAN specified by the role associated with the end-station and the port. • **Authentication**—Port was moved into the Authentication VLAN. • **Undo**—Port was changed based on Undo commands in a CLI configuration.
Role/Access Policy	Name of the Network Device Role or the Network Access Policy that triggered the port change. Not all port changes are associated with a role or a policy.
Port	Port that was changed. Includes device name and port number.
VLAN	ID or Name of the VLAN where the port was moved.
Device	Filters results by the device where the affected ports reside. Use the Sort By button to resort devices in the drop-down list by name or by IP address.
Buttons	
Export	Exports data to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See Export data on page 710.
Show CLI Button	Displays the commands within the CLI Configuration selected in the CLI Config Name column.

Access port changes view

1. Select **Logs > Port Changes**.
2. In the **Port Changes** window, use the filter options to select the appropriate group of records.
3. To see the actual CLI configuration that was applied, click the **Show CLI** button at the bottom of the window. As you hover over CLI configurations in the **Port Changes** view, the contents are displayed in the **Show CLI** view.

Requirements for ACL based configurations

CLI configurations can be created in your FortiNAC software to modify ACLs based on host state. These CLI configurations are applied via the Model Configuration window for the device that contains the ACLs. See Apply a host based configuration via the model configuration on page 936. This section provides an overview of the basic setup required within FortiNAC along with some sample ACLs and CLI configurations.

Requirements For IP ACL based configurations

- Devices to which these IP address based CLI configurations are applied must be Layer 3 devices, such as a router or a Layer 3 switch.
- VLAN Switching and MAC Filtering must be disabled for the device. To disable these options locate the device in the Topology View. Right-click and select Properties.
- Switches connected to Layer 3 devices should not be modeled in FortiNAC.
- In order to control access to the production network, the ACL permits or denies access to either the FortiNAC DNS server or your regular DNS servers. By doing this the host retains the same IP address throughout the transition to the production network. Therefore, the DHCP server for your hosts should be your regular DHCP server and not FortiNAC.
- Since hosts are switched to the FortiNAC DNS server during isolation, you must add the FortiNAC IP address to the Production DHCP's list of DNS servers.
- Make sure that the lease pool and lease times are large enough that hosts always receive the same IP address. If a host's IP address changes before the registration process is complete, then the ACL is not updated correctly.
- The host's browser caches the registration page. After a host has successfully registered, the success page tells the host to close the browser. If you are using the Dissolvable Agent, the Renew IP option must be enabled. This forces the IP address to be released and clears the cache.

Create the Cisco extended ACL

An extended ACL is an ordered list of statements that can deny or permit packets based on source and destination IP address, port numbers and upper-layer protocols.

This ACL is a sample of the type of ACL you might create to work in conjunction with your FortiNAC software and its CLI configurations. Be sure that you know the IP address of the FortiNAC appliance and the IP range of the DHCP scope for your hosts. Log into the device and create an extended access list.

All information in an ACL is case sensitive.

Example

```
Configure term
ip access-list extended Nac
500 permit udp 192.168.34.0 0.0.0.255 host 192.168.105.2 eq 4567
501 deny ip 192.168.34.0 0.0.0.255 host 192.168.105.2
502 permit ip any any
end
write memory
```

Settings

Command	Definition	Data From Example
ip access list extended	Indicates the type of ACL and the user specified name of the ACL. In this example, the name is Nac.	ip access list extended Nac
permit or deny	Allow or block traffic. This is a required field.	
protocol	IP, TCP, UDP, ICMP, GRE and IGRP. TCP, UDP and ICMP use IP at the network layer.	udp ip
source	This is the Source IP address. This is a required field. In the example, this is the IP range for your hosts. When <any> is used it indicates that any IP address can connect.	192.168.34.0 any
source mask	Wildcard mask; 0 indicate positions that must match, 1s indicate don't care positions (inverted mask). Required.	0.0.0.255
destination	Destination IP address. This is the IP address of the FortiNAC appliance that is used for isolating hosts who are not registered or who have failed a security policy scan. When <any> is used it indicates that the host can connect to any IP address.	host 192.168.105.2 any
operator destination port	It, gt, eq, neq (less than, greater than, equal, not equal) and a port number. In this example 4567 is the port number through which the Persistent Agent communicates with the FortiNAC appliance. This must remain available if you are using the Persistent Agent to scan your hosts.	eq 4567

In the example 192.168.34.0/24 is the hosts IP range. The host IP 192.168.105.2 is the Isolation interface on the FortiNAC appliance. This is the default state of the all registered hosts. It allows the hosts to go to anywhere on the network except the Isolation interface.

Apply the ACL to the physical interface

Once you have created one or more ACLs you must apply them to the port or ports on the device where the edge switches connect. These ports will be controlled by the ACL based on the host state. Below is an example of the command needed to apply the ACL. This may vary depending on the device.

```
Configure term
interface FastEthernet1/0/11
ip access-group Nac in


end
write mem
```

Poll the switch/router

In order for FortiNAC to monitor the hosts connected to the device, it must poll the device periodically. Polling is set up automatically as devices are added to FortiNAC.

As devices are added they are evaluated. Any device that is capable of L2 polling (polling hosts) is immediately placed in either the L2 Wired Devices or L2 Wireless Devices sub-group. These are default groups that are created in the database and populated for you. The default polling interval is 10 minutes for wireless devices and one hour for wired devices.

To modify polling intervals select **Network Devices > L2 Polling**. See L2 polling (resync hosts) on page 748 for additional information.

High availability

The FortiNAC high availability solution consists of a common management process, supporting scripts, and configuration and monitoring options in the admin user interface. High availability can be used to ensure redundancy for FortiNAC Servers, FortiNAC Control Server and Application Server pairs, and FortiNAC Control Manager appliances.

The high availability management process provides messaging between the primary and secondary appliances. The process mirrors critical information, controls services, and performs system maintenance functions on all appliances. The management process also manages and determines which server is in control. It starts the secondary appliances in the event of a failover.

Supporting scripts determine whether the database replication is working. These scripts are also used to restore the database and/or files from the secondary to the primary and restart the primary server.

Database synchronization is handled by MySql replication to provide complete data integrity. For additional information on the MySql replication see http://dev.mysql.com/doc/refman/4.1/en/replication.html.

The high availability diagrams shown below define two possible High Availability configurations using FortiNAC Control Server and Application Server pairs. The first diagram illustrates the use of a shared IP address or host name that is moved between appliances during a failover and recovery. This provides the administrator with a single point of management access regardless of which appliance is in control. To use a shared IP address all of the appliances must be in the same subnet on the network. See Using a shared IP address (Layer 2) on page 950.

The second diagram displays a high availability setup in which the appliance are on different subnets. To leverage high availability with appliances on separate subnets do not include a shared IP as part of the High Availability configuration. If you are using a Control Server and Application Server pair and you are not using a shared IP address, during failover both appliances will failover to their corresponding secondary appliances regardless of which one actually failed. If you are using a shared IP address only the appliance that failed will failover to the secondary. See Servers on different subnets (Layer 3) on page 951.

In a high availability configuration eth1 on the server is disabled until that server is in control. For example, eth1 on the secondary server is disabled until the primary server fails over and the secondary takes control.

It is recommended that you use a Shared IP address in your high availability configuration whenever possible. This prevents the administrator from having to use separate IP addresses to manage the servers that are in control and alleviates communication issues with the Persistent Agent.

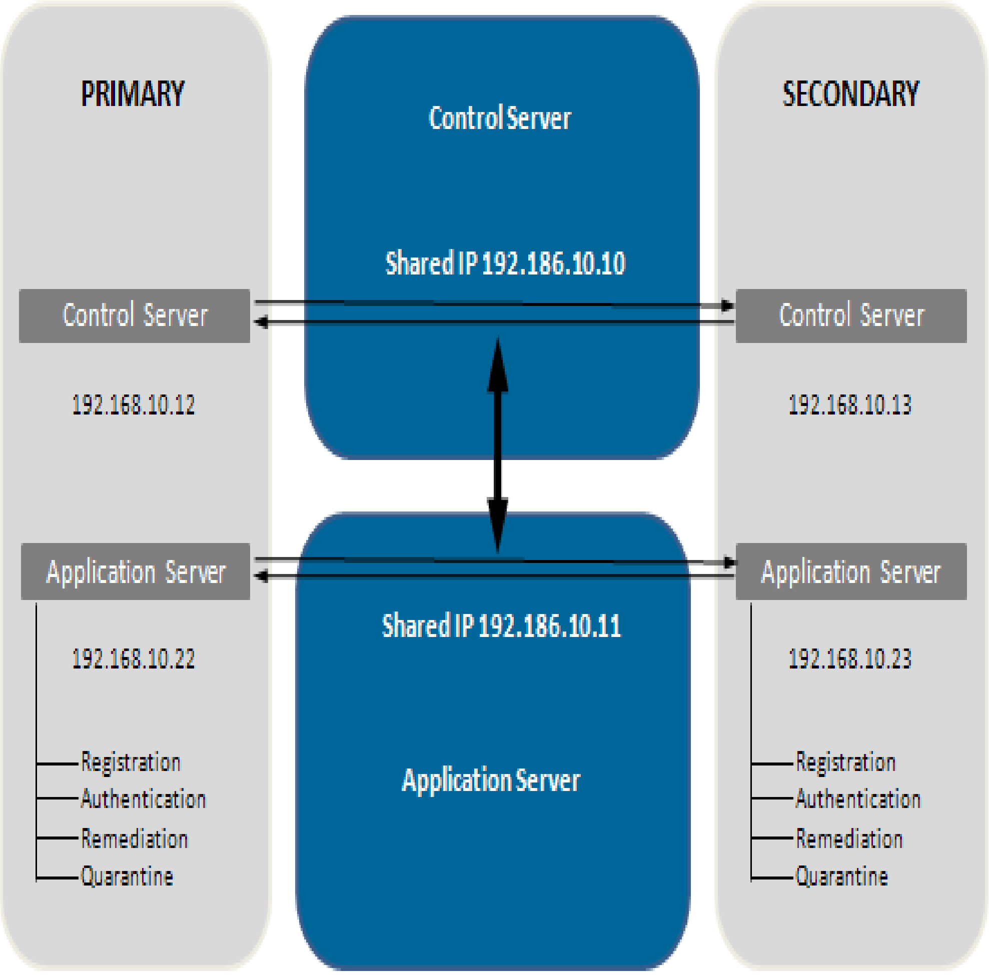
If your primary and secondary servers are on different subnets, make sure that communication between the subnets is configured in advance.

Terminology

Term	Definition
Primary	The active server or servers of the high availability pair that is in control by default. Sometimes referred to as the Master.
Secondary	The "backup" server or servers that takes control when the primary fails. Sometimes referred to as the Slave.
Management Process	The process which manages and determines which server is in control.
Idle	High Availability state in which the management process is functional, but the secondary server will not take control even if connectivity is lost with the primary server.

Server communication

Shared IP - same subnet

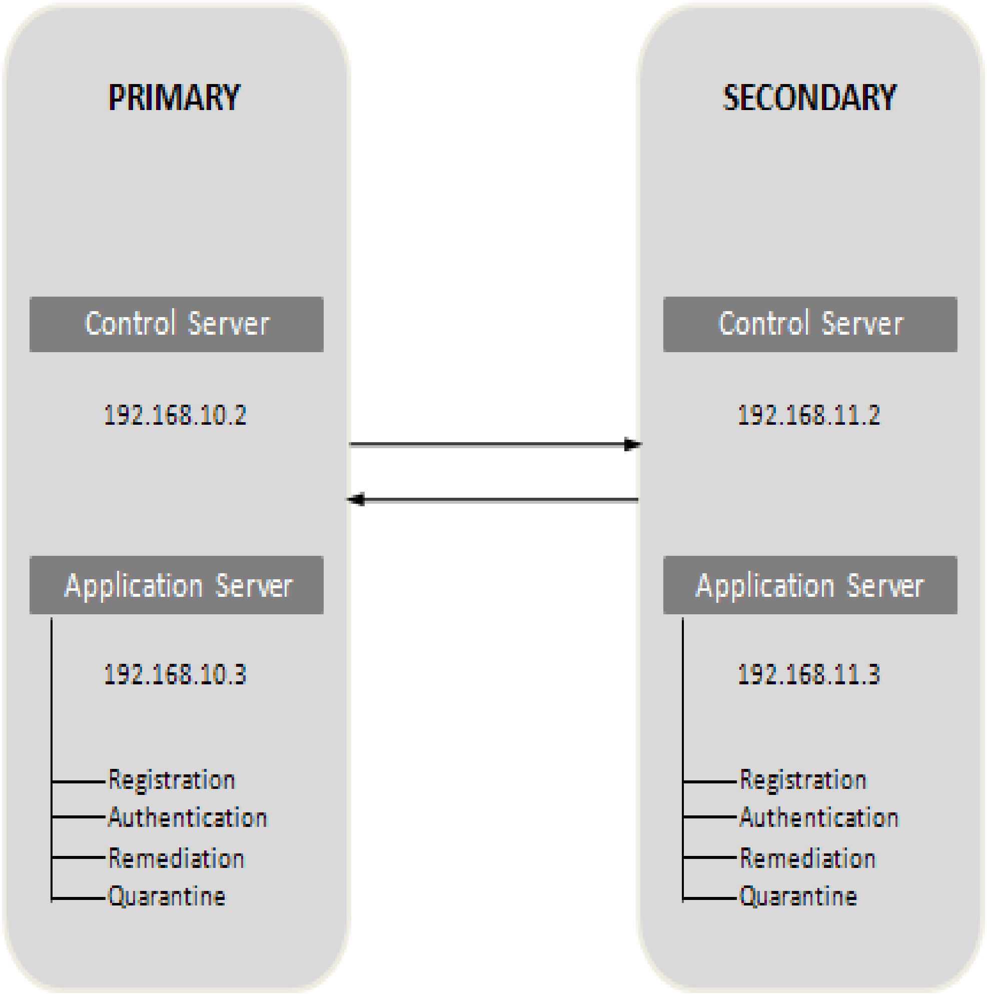


In a FortiNAC Control Server and FortiNAC Application Server configuration that uses a shared IP, the FortiNAC Application Server appliances are separate standbys from the FortiNAC Control Server appliances.

Examples:

- If the primary FortiNAC Control Server fails, the secondary FortiNAC Control Server communicates with whichever FortiNAC Application Server is in control (either the primary or the secondary).
- If the primary FortiNAC Application Server fails, the primary FortiNAC Control Server communicates whichever FortiNAC Application Server is in control.

No shared IP - different subnets



In a FortiNAC Control Server and FortiNAC Application Server configuration that does not use a shared IP, the FortiNAC Application Server and FortiNAC Control Server appliances failover in pairs.

Examples:

- If the primary FortiNAC Control Server fails the primary FortiNAC Application server is also brought down and the Secondary pair of appliances take control.

- If the primary FortiNAC Application Server fails, the primary FortiNAC Control Server is also brought down and the Secondary pair of appliances take control.

Using a shared IP address (Layer 2)

Network infrastructure

- Configure all network devices to send traps to both the primary and secondary FortiNAC server IP addresses.
- Configure RADIUS servers to use both the primary and secondary addresses.
- If you are setting up FortiNAC as the RADIUS server for a device in a Fortinet High Availability environment, you must use the actual IP address of the primary control server, not the Shared IP address. Set up the secondary control server as a secondary RADIUS server using its actual IP address. Regardless of the environment, you may also want to set up your actual RADIUS server to be used in the event that none of your FortiNAC appliances can be reached. This would allow users to access the network, but they would not be controlled by FortiNAC.
- If the primary and secondary servers are running on the same subnet and use a shared IP address, make sure that the Persistent Agent and all other features use the shared IP or host name. Refer to the Help on Persistent Agent Properties.
- In a High Availability configuration changes to the database on the primary server are replicated immediately to the secondary server. If the latency is too long and/or the bandwidth between redundant servers is not sufficient, the secondary may not have all of the database changes made on the primary when a failover occurs. It is impossible to predetermine the network requirement due to the fact that it will vary based on product usage and load. The follow formula can be used to calculate your specific network bandwidth requirements.

The starting latency and bandwidth recommendations are as follows:

- latency between remote data nodes must not exceed 20 milliseconds
- bandwidth of the network link must be a minimum of 4.8 Mbps

Your usage of the product will impact the network requirements. Fortinet recommends using the "Database Replication Error" event and the corresponding alarm action to notify administrators when an error occurs. There are two possible caused, first there was a momentary network outage that caused the failure. If the event happens continuously then network speed of the must be increased.

Appliance configuration

- Make sure all appliances have a license key that includes High Availability and that all appliances have matching licenses.
- Use the Configuration Wizard to configure each of the appliances. Refer to the Appliance Installation Guide that comes with the appliances for information on using the Configuration Wizard.
- Establish the address to use as the Shared IP address (optional) and the IP addresses for the primary and secondary appliances. This enables communication with the other appliances in the High Availability configuration.
- Go to the Administration - High Availability Tab and configure IP addresses and communication between appliances. See Primary and secondary configuration on page 953.
- Apply the configuration to restart your appliances. This replicates the database on the Secondary and copies any

necessary files. Portal pages are copied every 10 minutes.

If you are using DHCP Management in a High Availability environment, the ports to which the DHCP Interfaces connect must be added to the System DHCP Port group. Refer to Help on Modifying a Group. In the event of a failover, it is important that these fields be setup correctly or DHCP monitoring will not run.

- Ensure that the DHCP plugins on both the Primary and Secondary are configured.

Servers on different subnets (Layer 3)

In a High Availability environment with an L3 configuration where redundant FortiNAC servers are on different subnets and do not use a shared IP address, you must select the Layer 3 network option in the Configuration Wizard. L3 High Availability configurations are not supported with Layer 2 Isolation settings.

Network infrastructure

- If your Primary and Secondary servers are on different subnets, a Shared IP address cannot be used. Make sure that communication between the subnets is configured in advance.
- Configure two DHCP Helpers (eth1 on the Primary and eth1 on the Secondary) for isolation VLANs. FortiNAC returns two DNS servers (eth1 on the Primary and eth1 on the Secondary) for isolation VLANs.

  Upon failover the isolated hosts will have two DNS entries for use. Should the host stay in isolation longer than the DHCP time to live, then the host will fail to renew its IP from the primary. It will redo DHCP discovery and get an IP address from the secondary application server. The secondary application server will have responded with two DNS servers (secondary eth1 and primary eth1).
- If you are using high availability for a FortiNAC Control Server and Application Server pair, when failover occurs both servers failover. See Recovery on page 959.
- Configure all network devices to send traps to both the primary and secondary FortiNAC server IP addresses.
- Configure RADIUS servers to use both the primary and secondary addresses.
- If you are setting up FortiNAC as the RADIUS server for a device in a Fortinet High Availability environment, you must use the actual IP address of the primary control server, not the Shared IP address. Set up the secondary control server as a secondary RADIUS server using its actual IP address. Regardless of the environment, you may also want to set up your actual RADIUS server to be used in the event that none of your FortiNAC appliances can be reached. This would allow users to access the network, but they would not be controlled by FortiNAC.
- If your primary and secondary servers are running on different subnets and do not use a shared IP address, make sure that the Persistent Agent and all other features use the individual IP addresses or host names of the primary and secondary servers. Refer to the Help on Persistent Agent Properties.
- If you are using the Guest Self-Registration feature, you must configure settings to generate the correct links in the emails sent to Sponsors when a guest requests access. See Configure the email link on page 611.
- In a High Availability configuration changes to the database on the primary server are replicated immediately to the secondary server. If the latency is too long and/or the bandwidth between redundant servers is not sufficient, the secondary may not have all of the database changes made on the primary when a failover occurs. It is impossible

to predetermine the network requirement due to the fact that it will vary based on product usage and load. The follow formula can be used to calculate your specific network bandwidth requirements.

The starting latency and bandwidth recommendations are as follows:

- latency between remote data nodes must not exceed 20 milliseconds
- bandwidth of the network link must be a minimum of 4.8 Mbps

Your usage of the product will impact the network requirements. Fortinet recommends using the "Database Replication Error" event and the corresponding alarm action to notify administrators when an error occurs. There are two possible caused, first there was a momentary network outage that caused the failure. If the event happens continuously then network speed of the must be increased.

Appliance configuration

- Make sure all appliances have a license key that includes High Availability and that all appliances have matching licenses.
- Use the Configuration Wizard to configure each of the appliances. Refer to the Appliance Installation Guide that comes with the appliances for information on using the Configuration Wizard.

  You must run the Configuration Wizard on both the Primary and Secondary servers and make sure that the necessary Route scopes are filled in for both servers. If you do not enter scopes on both servers, the High Availability configuration will be incomplete and will not work correctly.

- Go to the Administration - High Availability Tab and configure IP addresses and communication between appliances. See Primary and secondary configuration on page 953.
- Apply the configuration to restart your appliances. This replicates the database on the Secondary and copies any necessary files. Portal pages are copied every 10 minutes.

  If you are using DHCP Management in a High Availability environment, the ports to which the DHCP Interfaces connect must be added to the System DHCP Port group. See Modifying a Group in the FortiNAC Administration and Operation documentation for additional information. In the event of a failover, it is important that these fields be setup correctly or DHCP monitoring will not run.

- Ensure that the DHCP plugins on both the Primary and Secondary are configured.

Connectivity configuration

To access the Admin user interface that is available through a web browser, the appliances use the "nac" alias to identify which IP address/hostname will be allowed in the URL.

In High Availability configurations entries for the "nac" alias are entered automatically in the /etc/hosts file for your FortiNAC Server appliances. Each of the appliances in the High Availability configuration must be resolvable in the DNS or you must enter them in the hosts file of your administration PC. Make sure the entries contain the IP address, the fully qualified domain name (FQDN), and the short name.

Example:

```
192.168.10.1 ApplianceName.Subdomain ApplianceName
```

Consider the following:

- If the appliance is a FortiNAC Control Manager there should be no nac alias entry in the /etc/hosts file. Use either the shared or individual IP address to access this server.
- If the High Availability appliances are being managed by the FortiNAC Control Manager, verify that none of the appliances have an entry for nac alias in the /etc/hosts file. Using nac alias in this configuration would stop the FortiNAC Control Manager from accessing the appliances it manages. To access the managed appliances use either the direct or shared IP address.
- If the High Availability appliances are not being managed by the FortiNAC Control Manager use these guidelines:
  - If the appliance is a FortiNAC Server, verify that the nac alias is mapped nac alias to the shared IP address. Use the shared IP address (or shared host name) in the URL.
  - If the appliance is the FortiNAC Control Server or FortiNAC Control Manager, verify that the nac alias has been removed from the /etc/hosts file and use the shared or the individual IP addresses (or host names) in the URL.

The 'nac' alias must not be included in DNS. For example, do not use an alias like "nac.abc.def.com" anywhere in DNS.

Primary and secondary configuration

Configure the High Availability appliances through the High Availability tab on the Administration view.

It is recommended that you use a Shared IP address in your High Availability configuration whenever possible. This prevents the Administrator from having to use separate IP addresses to manage the servers that are in control and alleviates communication issues with the Persistent Agent.

If your Primary and Secondary servers are on different subnets, a Shared IP address cannot be used. Make sure that communication between the subnets is configured in advance.

To access the High Availability configuration view on FortiNAC Server or Control Server appliances, click **System > Settings > System Management > High Availability**.

To access the High Availability tab on FortiNAC Control Manager appliances:

1. Log into FortiNAC Control Manager.
2. Select the **Management View** tab.
3. Click the **Administration** button.

4. Click the **High Availability** tab.
5. Additional information is available in the FortiNAC Control Manager documentation.

When you click Apply on the Administration High Availability Tab, the primary server tries to communicate with the secondary to ensure that the database will be replicated. If the primary server cannot communicate with the secondary, it continues to try until communication is established.

High availability

The information you enter into the view is written to files on all of the appliances involved, configures the ssh keys for all the specified appliances and configures mysql for replication. All appliances in the configuration are restarted and placed into High Availability mode when you click Apply and acknowledge the success message.

Use the High Availability tab for all changes to the configuration. If you manually edit the files on the appliance, values in the files will not be reflected on the High Availability tab.

Settings

Field	Description
Shared IP configuration	
Use Shared IP address	Enables the use of a shared IP address in the High Availability configuration. If enabled, the administrator can manage whichever appliance that is in control with the shared IP address instead of the actual host IP address. If your primary and secondary servers are not in the same subnet, do not use a shared IP address.
Shared IP address	The shared IP address for the High Availability configuration. Added to the /etc/hosts file when the configuration is saved.
Shared Subnet Mask (bits)	The shared subnet mask in bits. For example, 255.255.255.0 = 24 bits. If you are using a Shared IP address, this field is required.
Shared Host Name	Part of the an entry in the /etc/hosts file for the shared IP address. Admin users can access the UI using either the Shared IP address or the shared host name.
Server configuration	
Primary Appliance	• **IP address**—IP address assigned to eth0 for the primary. • **Gateway IP address**—IP address pinged by the appliances to determine if network connectivity is still available. • **CLI/SSH root Password [User:root]**—root password on the appliance itself. Allows settings to be written to the appliance. • **Retype root CLI/SSH Password [User:root]**—retype the password entered in the CLI/SSH root Password field for confirmation.
Secondary Appliance	• **IP address**—IP address assigned to eth0 for the secondary.

Field	Description
	• **Host Name** — Name assigned to the secondary. • **Gateway IP address**—IP address that pinged by the appliances to determine if network connectivity is still available. • **CLI/SSH root Password [User:root]**—root password on the appliance itself. Allows settings to be written to the appliance. • **Retype root CLI/SSH Password [User:root]**—retype the password entered in the CLI/SSH root Password field for confirmation.

Update software

To update your servers in a High Availability environment note the following:

- The Primary server must be running and in control in order to update the system.
- The Secondary server(s) must be running.
- The Primary server must be able to communicate with the Secondary server(s).
- The Primary server automatically updates the Secondary server(s).
- If the Secondary server(s) is in control, FortiNAC prevents you from updating and displays a message with detailed instructions indicating that the Primary must be running and in control.

Update the Primary server following the instructions for a regular system update in the FortiNAC Admin UI. See **Settings > Updates > System Update** in the Help for update instructions.

If you have a FortiNAC Control Manager that manages your FortiNAC servers, you can run the update from the FortiNAC Control Manager and select all managed servers to propagate the update throughout your environment.

High availability concepts

The concepts of High Availability configurations include the startup and control sequences as well as the communication for both the primary and secondary servers.

Startup

Primary server startup

1. The management process starts up.
2. The condition of the secondary server is checked.
3. If the secondary is in control, the secondary retains control until a manual recovery is performed to return control to the primary server. See Recovery on page 959.
4. If the secondary is not in control, the startup of the primary continues and the primary is in control.

If any of the following processes does not start, the appliance is not in control: httpd, dhcpd, named, mysqld, sshd, TomcatAdmin and TomcatPortal. If any of these processes fail, then failover from primary to secondary is started.

Secondary server startup

1. The management process starts up.
2. The condition of the primary server is checked.
3. If the primary is in control, database replication is started on the FortiNAC Server, FortiNAC Control Server, or FortiNAC Control Manager. Other processes are not started on the secondary.
4. If the primary is not in control and the secondary is not idle then the startup of the secondary continues.
5. The secondary remains in control until you manually perform the recovery that returns control to the primary server.

Management process

The Management process starts when the appliance is booted up or by running the following command:

```
startupCampusMgr
```

If the appliance is in control the appropriate processes are started.

If any of the following processes does not start, the appliance is not in control: httpd, dhcpd, named, mysqld, sshd, TomcatAdmin and TomcatPortal. If any of these processes fail, then failover from primary to secondary is started.

Monitor

Monitoring current status

These events are not generated for the FortiNAC Control Manager.

The status of your High Availability appliances can be viewed on the Dashboard in a Summary panel.

The High Availability appliances also write to a date stamped log file named `output.processManager.<datestamp>` located in this directory: `/bsc/logs/processManager`.

The file shows current status as well as debug output.

Process down events

These events are not generated for the FortiNAC Control Manager.

FortiNAC generates events and alarms whenever any of the required processes fails or does not start as expected. FortiNAC tries to restart the process every 30 seconds. In a High Availability environment failover occurs after the fourth failed restart attempt. These events are enabled by default and each event has a corresponding alarm.

Events for failed processes include:

- Service Down - Tomcat Admin
- Service Down - Tomcat Portal
- Service Down -dhcpd
- Service Down -httpd
- Service Down -mysqld
- Service Down -named
- Service Down -sshd

When the system confirms that the httpd service is running, the system then attempts to connect to ports 80 and 443. If the system fails to connect to either port, the service is restarted.

Process started events

These events are not generated for the FortiNAC Control Manager.

FortiNAC generates events whenever any of the required processes is started. These events are enabled by default and each event has a corresponding alarm. Alarms for process started events are not typically enabled. They can be enabled manually using Alarm Mappings.

In the Event View, event messages for started processes include the name of the process and the IP address of the host where the process started. For example, if the named process started you would see the following message associated with the event:

```
A critical service (/bsc/services/named/sbin/named) on 192.168.5.228 was
not running and has been started.
```

Events for started processes include:

- Service Started - Tomcat Admin
- Service Started - Tomcat Portal
- Service Started -dhcpd
- Service Started -httpd
- Service Started -mysqld
- Service Started -named
- Service Started -sshd

Other events

These events are not generated for the FortiNAC Control Manager.

An Event appears in the Events view and can have an alarm configured to send email to you when it occurs.

- **Database Replication Error** — This event is generated if the database on the secondary appliance is not replicating.
- **System Failover** — This event is generated when a failover occurs.

Control sequence

Required processes

In a High Availability environment the primary fails over to the secondary when certain processes don't start or fail while running. If any process listed in the table below fails on the primary, then the secondary attempts to take control. Depending on the appliance and platform being used, different processes are required. See the table below for additional information.

Required Process	FortiNAC Control Manager	FortiNAC Control Server	FortiNAC Application Server	FortiNAC Server
mysql	X	X		X
sshd	X	X	X	X
dhcpd			X	X
httpd			X	X
named			X	X
tomcat-admin	X	X		X
tomcat-portal			X	X

Determining whether the secondary needs to take control

The secondary server pings the primary server every 30 to 60 seconds depending on the time spent "validating" the connection to determine whether the primary is still in control.

If the secondary receives no response from the primary after five attempts, the secondary pings the gateway configured in the High Availability Tab and the default gateway for the appliance. See Primary and secondary configuration on page 953.

- If the gateway is reachable, after 30 seconds the secondary takes control, since the primary is assumed to be isolated from the network.
- If the gateway is not reachable, the secondary will not take control since the secondary is assumed to be isolated from the network and the primary could be functioning properly.

If the secondary is Idle, it does not take control. For example, the secondary can be set to Idle when Reboot and Shutdown commands are run on the primary.

CLI control scripts

The following scripts are used by FortiNAC to control the server and are located in `/bsc/campusMgr/bin`

Script	Description
hsIsSlaveActive	Determines if the secondary SQL server is performing replication.
hsRestartCMMaster	Executed on the Primary FortiNAC Server, FortiNAC Control Server, or FortiNAC Control Manager appliance to recover after a failover. It copies the database and other files from the secondary appliance. Also resets the process states back to the master and restarts both servers.
hsRestartCMRCMaster	Executed on the primary FortiNAC Application Server to recover after a failover. It copies all the required files from the secondary FortiNAC Application Server. Also resets the process states back to the master and restarts both servers.

Recovery

If high availability has been implemented and a failover has occurred, you must correct the reason for the failover before restarting your Primary Server.

Restart the primary server

Use the Resume Control button on the Dashboard Summary panel to start the primary again. When the Resume Control button is clicked, critical files are copied from the secondary back to the primary and control is returned to the primary. On the FortiNAC Server, FortiNAC Control Server and FortiNAC Control Manager appliances, the database is also copied.

If you are using high availability for a FortiNAC Control Server and Application Server pair and this configuration does not use a shared IP address, when failover occurs both servers failover. To return control to the primary pair, click the Resume Control button on the Dashboard Summary panel for either of the two servers in the pair. This causes both the FortiNAC Control Server and Application Server in the primary pair to start again and control is returned to both servers in the primary pair.

If for any reason the database was not replicated correctly on the secondary before failover, the recovery process gives you the option of retaining the older database located on the primary.

1. Click **Bookmarks > Dashboard**.
2. Scroll to the **Summary** panel.
3. Click the **Resume Control** button for the server that should resume control.

4. The primary server restarts. Database and configuration files are copied from the secondary to the primary. Processes are started on the primary. Then the secondary server relinquishes control.

This process may take a few moments while the data is synchronized between the two servers.

Manually restart, stop or force a failover

The scripts in the table below allow you to control High Availability from the CLI. Scripts to restart the primary servers vary depending on the configuration implemented. For configuration options see Primary and secondary configuration on page 953.

CLI scripts

Server Type	Primary Recovery	Shutdown Without Failover	Shutdown With Failover
Shared IP address			
FortiNAC Server FortiNAC Control Server FortiNAC Control Manager	hsRestartCMMaster	shutdownCampusMgr	shutdownCampusMgr -kill
FortiNAC Application Server	hsRestartCMRCMaster	shutdownNessus	shutdownNessus -kill
No shared IP address			
FortiNAC Control Server	hsRestartPair (restarts both servers in the pair)	shutdownCampusMgr	shutdownCampusMgr -kill
FortiNAC Application Server	hsRestartPair (restarts both servers in the pair)	shutdownNessus	shutdownNessus -kill

Stop the primary server

To stop the processes on the primary Server **without** causing a failover (for example, for routine maintenance and quick restart), use this command: `shutdownCampusMgr`. When you use the `shutdownCampusMgr` command on the primary, the management process tells the secondary not to take control by setting the secondary state to Idle. This prevents a failover from occurring.

When the command listed below is run on the primary server, it stops the campusMgr processes and causes a failover to the secondary Server.

```
shutdownCampusMgr -kill
```

Troubleshooting tips

Prior to configuring High Availability, ensure that all appliances are able to communicate (i.e. firewall is not blocking communication).

Use these troubleshooting tips to:

- If you have implemented High Availability using a Shared IP address, determine which appliance has the shared IP.
- Determine the status of your appliances including:
  - which is primary/secondary
  - which has control
  - is secondary idle
- Confirm that replication of the database is occurring.
- Verify whether the license key is configured for High Availability.

Determine which appliance has the shared IP

Enter `ip addr sh dev eth0` at the command prompt and look at the output to determine which eth0 interface has the Shared IP address (eth0 of the primary or eth0 of the secondary):

```
root@host name:/bsc/campusMgr/bin
> ip addr sh dev eth0
2: eth0: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast qlen 100
link/ether 00:30:48:79:62:24 brd ff:ff:ff:ff:ff:ff
inet 192.168.5.231/24 brd 192.168.5.255 scope global eth0
inet 192.168.5.230/24 scope global secondary eth0
```

In this example the shared IP address is 192.168.5.230. The eth0 on the secondary has the shared IPaddress.

Using a shared IP address in your high availability configuration is optional.

Determine appliance status

The **Summary** panel on the **Dashboard** indicates the status of all appliances, which appliance has control and if an appliance is idle. To access this panel select **Bookmarks > Dashboard** and scroll to the **Summary** panel.

Confirm database replication

When the primary server is started it attempts to communicate with the secondary. It continues to attempt communication until it connects to the secondary and can begin replicating the database.

When you make a change in the database of the primary, the database replication process makes the same change in the database of the secondary.

Navigate to the /bsc/campusMgr/bin/ directory on the Secondary. Run the following script: `hsIsSlaveActive`

You should receive a response that is similar to the following:

```
root@Host Name:/bsc/campusMgr/bin
> hsIsSlaveActive
Host Host Name
SQL version 5.0.18,
slave is inactive
```

If the response contains the line slave is inactive, database replication is not active. If the response contains the line slave is active, database replication is active.

If for any reason the database is not replicated correctly on the secondary before failover, the recovery process gives you the option of retaining the older database located on the primary.

Verify license key

The license key on both the Primary and Secondary appliances must be configured to be High Availability capable. The steps below provide verification that the key is configured correctly.

1. Navigate to the `/bsc/campusMgr/bin` directory.
2. Enter the following at the command prompt: `RunClient DumpKey.class`
3. Look for Plugins: `Hot-Standby-Capable`
4. If this line is not displayed, the license key does not support High Availability. A new key is required.

Receive data from external devices

FortiNAC can be configured to receive data or messages from other devices on the network, such as an IPS/IDS device. FortiNAC can accept data from a trap or Syslog message to add records to the database or trigger events and alarms. If events and alarms are triggered, alarms can be configured to take action on hosts or users and notify administrators via e-mail or SMS messages.

There are several options that can be used to leverage data from other devices. Each of these options is independent of all of the others. They can be used simultaneously but they do not work together.

Syslog management

The Syslog Management feature in FortiNAC allows you to create specific configurations used to parse inbound syslog messages. Supported message formats include CSV, TAG/VALUE and CEF. New events and alarms are automatically created for each syslog configuration you create. When an inbound message is received, FortiNAC can react based on the event and alarm generated. See Syslog management on page 190.

Trap MIB

The Trap MIB feature allows you to configure FortiNAC to receive SNMPv1 and SNMPv2 traps from external devices that contain information about the connecting host. New events and alarms are created for these configurations and they display based on the OID of the sending device. When a trap is received FortiNAC can react based on the event and alarm generated. See Trap MIB files on page 202.

SNMPv3

SNMPv3 traps can be leveraged to populate the FortiNAC database with hosts and users as they connect to the network. When a trap is received from an external device, host and user records are added, modified or removed in the database. Events and alarms associated with these traps can be used to notify administrators or take actions on connecting hosts and users.

MDM services

MDM Services allows you to configure communication with one or more Mobile Device Management servers. Based on the information received from the MDM server you can take action on hosts, such as disabling them. See MDM services on page 172.

Send SMS messages

FortiNAC has the ability to send SMS messages to administrators, guests or users. These messages are used to provide guests with user names and passwords, to notify administrators when an alarm has been triggered or to notify a user when an alarm has been triggered based on his host. FortiNAC sends SMS messages by sending email to a mobile phone number through a special email address provided by the mobile provider. For example, if you have a guest who is a Verizon Wireless customer and you need to send that guest an SMS message, the message is sent to xxxxxxxxxx@vtext.com (where xxxxxxxxxxx is the guest's cell phone number).

Both the Mobile Number and Mobile Provider must be entered into the guest, administrator or user record. SMS messages are sent via email. Without provider information FortiNAC cannot send SMS messages.

Long SMS messages might be divided up into multiple messages or truncated depending on how the Mobile Provider and the mobile telephone process long messages.

Implementation

To enable the SMS Messaging feature you must configure the following:

General

- Configure a connection to an out bound email server to send your SMS messages. See Email settings on page 169 for instructions.
- Review the list of Mobile Providers. Enable the providers that should be available to assign to guests, users, and administrators. The list is long so you may not want to enable them all. Add any providers that are not included in the list. Providers can be modified as needed. See Mobile providers on page 175.

SMS for guests

- Modify your current guest templates or create new ones to include Send SMS message as an option. Two data fields have been added to the Data Fields tab on the Add/Modify Template dialog to accommodate Mobile Number and Mobile Provider. Make sure you do not remove these fields or guests will not have a place to provide their mobile information when they register. See Create templates on page 569.
- If you have existing guests that you would like to send messages to you must delete their guest records and recreate them using a template that has the Send SMS option enabled. Make sure to add Mobile Number and Mobile Provider for these guests.
- When guest accounts are created, you have the option to select one or more accounts from the list and send those guests an email and/or an SMS message containing their user name and password. See Provide login information

on page 601.

This is also true if you have set up a Kiosk for guests to create their own accounts. Guests can send themselves an SMS message with their credentials. To set up a Kiosk see Using a kiosk on page 606.

If you have implemented Guest Self Registration and included Send SMS message in the template for those guests, guests can receive login credentials via SMS. See Guest self-registration on page 609.

- Mapping events to alarms and setting an SMS user notification action allows FortiNAC to send an SMS message to a guest. For example, if you want to send guests a message when their host is marked at risk and their network access is disabled, you can map the Host At Risk event to an alarm and send a message. The guest account must be associated with a template that has Send SMS enabled and the guest must have a Mobile Number and Provider entered on the Add/Modify User dialog. See Add or modify alarm mapping on page 892.

SMS for administrators

- Add a Mobile phone number and Mobile provider to each admin user that should receive SMS messages. See Add an admin user on page 685. This information can also be added by exporting Admin Users and re-importing them with their Mobile information. See Import admin users on page 704.
- Admin users that should receive SMS messages based on alarm mappings must be in one or more Administrator groups. Add Admin users to the appropriate Administrator groups either from the Groups View or from the Admin Users View. See Group membership on page 694.
- Mapping events to alarms, enabling options for notification and sending SMS messages to an Administrator group allows FortiNAC to send an SMS message to every Admin user in the group. For example, if you want to send Admin users a message if the database backup fails, map the Database Backup Failure event to an alarm and send an SMS message notifying Admin users about the problem. See Add or modify alarm mapping on page 892.

SMS for users

- Add a Mobile phone number and Mobile provider to each user that should receive SMS messages. See Add or modify a user on page 651. This information can also be added by exporting Users and re-importing them with their Mobile information. See Import hosts, users or devices on page 696.
- Mapping events to alarms allows FortiNAC to send an SMS message to a user. For example, if you want to send a user a message if their host has been disabled, map the Host Disabled Success event to an alarm and send an SMS message notifying the user about the problem. See Add or modify alarm mapping on page 892.

IP phone integration

FortiNAC does not provide any special integration logic for different IP phone vendors. Typically, the network administrator deploys the organization's IP phone infrastructure independently of configuring the FortiNAC. Because FortiNAC's focus is on hosts daisy-chained to the phone, the type of phone that is used is unimportant.

Switch ports are usually configured for IP phones by defining some sort of tagged VLAN or special voice VLAN for the phone, which operates independently of the untagged VLAN that governs other traffic (data) on that port. FortiNAC does not involve itself with these VLANs. In fact, it is purposefully ignorant of them.

Do not trunk Cisco ports that have IP Phones connected. Configure the access (untagged) VLAN and voice VLAN for the port. FortiNAC does not manage trunked ports.

Overview

The following table lists FortiNAC features applicable to IP phone support.

Feature	Description
Ignore IP phone MAC addresses when determining the appropriate VLAN for a port	As long as the device is identified as an IP phone, FortiNAC does not consider its presence when calculating the VLAN for the port. The administrator must associate the device type IP Phone with the device in FortiNAC.
Learn comings/goings of hosts daisy-chained to the phone	Traps or other notifications are needed to inform FortiNAC when hosts come and go from the phone ports, since FortiNAC cannot rely on the linkUp/linkDown traps per usual. For example: Cisco supports a Mac Notification trap (learned and removed) that can provide this information HP has just added a similar Mac Notification trap capability to a few of their switches RADIUS authentication can also provide half the picture for some switches, though it is difficult to know when hosts disconnect
Automatic phone provisioning on a port	This provides ability to plug an IP phone into any port and have that port automatically configured for the phone. FortiNAC has limited support for this by leveraging the FlexCLI feature to specify the switch-specific commands to manage this process. When a phone plugs in, the configured CLI commands are applied to the port. To aid in this process, an IP phone group was added (functions as part of the Role-based CLI mapping function).

IP phone integration process

1. Configure a Voice VLAN on switches to which IP phones will be connected. Typically this is a tagged VLAN. FortiNAC ignores devices on tagged VLANS and manages devices on untagged VLANs such as PCs.
2. If supported, configure MAC Notification traps on the same set of switches. FortiNAC supports MAC Notification traps on Cisco and some HP switches.
3. For Cisco switches, go to the Model Configuration View in FortiNAC and enter a comma separated list of Voice VLANs. This indicates to FortiNAC that devices on that VLAN should not be moved to any other VLAN ever. See Model configuration on page 767.
4. Provision the phones with their proprietary configuration.
5. Add IP Phones to the FortiNAC database using one of the methods listed.
   - Import IP Phones using a .csv file. See Import hosts, users or devices on page 696.
   - Connect your phones to the network and then convert the rogue hosts to IP phones using the Register As Device tool. See Register a host as a device on page 812.
   - Connect your phones to the network and use the Device Profiler feature to automatically register them as IP Phones. See Device profiler on page 348.
   - Add a new host in the host view and choose Register As A Device in the Add window, then select IP Phone as the device type. See Add or modify a host on page 807.

   IP phones should be added to an IP Phone group to aid in management later. Make sure that the device type is set to IP Phone. By identifying these devices as IP Phones you indicate to FortiNAC that they should be ignored when determining the VLAN for the port.
6. Connect the PC to the phone and attempt to access the network.
7. Once an IP Phone is connected to a port, FortiNAC does not bring down the interface to change VLANs. If there is an agent installed on the connected host, the agent does a release/renew of the IP address which forces the VLAN change. If there is no agent installed, the user must wait for the IP address lease to expire. If you are not using agents on hosts, you may want to configure shorter lease times for IP addresses.

Host connection process through phone port

1. PC connects to the port on the back of the phone.
2. If MAC Notification Traps are enabled, a trap is sent to FortiNAC.
3. If MAC Notification Traps are not enabled, the presence of the host connection is not detected until the next L2 Poll. The host will connect immediately to the network or VLAN to which the port is currently set. If the polling interval is very long, a host may have to wait before being able to register or moving to the correct VLAN.
4. FortiNAC determines the MAC Address of the PC and looks for it in the database to determine whether or not it is registered.
5. If it is not registered, the PC is placed in the Registration VLAN but the phone remains in the Voice VLAN.
6. If it is registered, the PC is placed in the Production VLAN and the phone remains in the Voice VLAN.

Additional reading

Log into your SalesForce account to find the following information:

- Solution 1498: Voice VLAN Assigned as Default by Mistake
- Solution 1378: VLANs Out of Sync Between Switch and FortiNAC Model Configuration
- Solution 1502: HP ProCurve: Configuring MAC-Notification Traps
- How To: Cisco Using MAC Notification Traps For Better Performance

Wireless integration

Refer to the vendor documentation for your Wireless Device for detailed set up and configuration information. Refer to the Fortinet Customer Portal for information on specific devices.

FortiNAC integrates with both intelligent access points (IAPs) and centralized controller-based wireless solutions.

- Intelligent access points manage both the access point and its connecting hosts.
- Controller-based solutions manage multiple access points and their connecting hosts.

To manage wireless hosts with FortiNAC you must configure FortiNAC as the RADIUS server to authenticate users for IAPs and controllers . FortiNAC responds to the RADIUS authentication requests with an accept or reject message. When accepting users, FortiNAC can include information that identifies the network the connecting host can access. Network access is based upon the host's current FortiNAC state and the Network Access Policy that applies to the host/user at the time network access is required. Configuration of host network access varies depending on the device and can include: VLAN IDs and names or proprietary network identifiers.

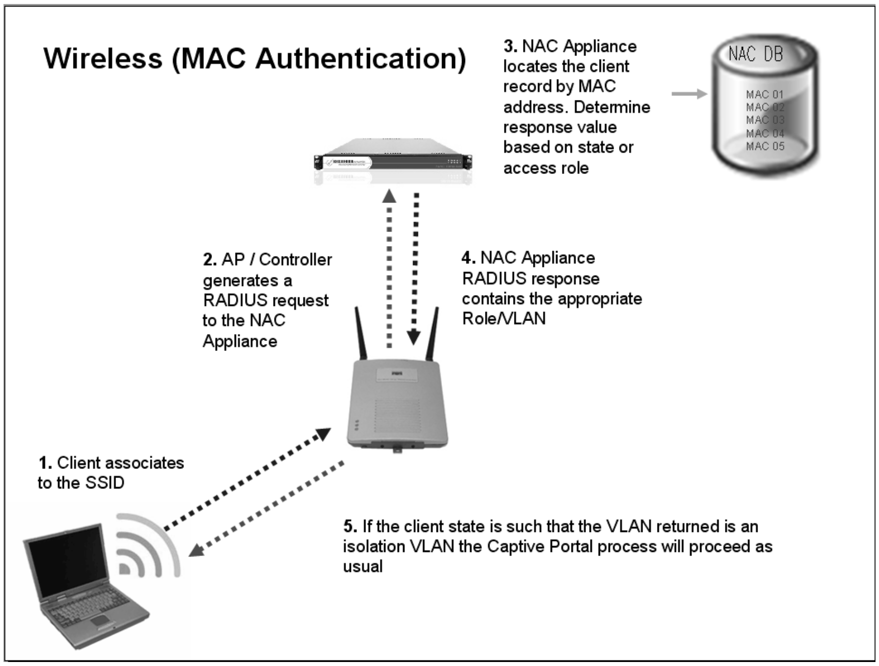
Authentication

Intelligent Access Points (IAPs) and controllers support two methods of RADIUS based authentication: RADIUS MAC authentication and 802.1x authentication.

RADIUS MAC

With RADIUS MAC authentication, users on connecting hosts are validated based on their physical addresses, and FortiNAC functions as the terminating RADIUS server. In these types of requests, FortiNAC supports only Password Authentication Protocol (PAP) for RADIUS authentication.

When FortiNAC receives an authentication request, FortiNAC attempts to locate the host's MAC Address in its database. If the MAC address is found, FortiNAC uses the host's state in addition to other user-defined policy criteria to determine the appropriate response. If the host state is unrecognized by FortiNAC, or is known but is disabled or at risk, the response will either reject the request or respond with information necessary to isolate the host on the network. The exact behavior is dependent upon the type of network device and how the administrator has configured the FortiNAC system. If the host is known and in good standing with the system, the response may depend upon varied criteria specified in FortiNAC policies.


Wireless (MAC Authentication)
3. NAC Appliance locates the client record by MAC address. Determine response value based on state or access role
NAC DB
MAC 01
MAC 02
MAC 03
MAC 04
MAC 05
2. AP / Controller generates a RADIUS request to the NAC Appliance
4. NAC Appliance RADIUS response contains the appropriate Role/VLAN
1. Client associates to the SSID
5. If the client state is such that the VLAN returned is an isolation VLAN the Captive Portal process will proceed as usual

Domain name mappings

The table below provides a summary of the various formats which FortiNAC uses to interpret the Fully Qualified User Name and to identify the user portion (which can sometimes be a host), the domain portion and the separator.

Fully Qualified Username	User	Domain
user	user	no domain specified
user@domain.com	user	domain.com
user@domain	user	domain
domain\user	user	domain
domain.com\user	user	domain.com
host/machinename.domain.com	host/machinename	domain.com

The user portion can be further delimited by dots (e.g., first.last@hostname.domain.com).

802.1x

802.1x defines the authentication of users on connecting hosts based on their user credentials or certificates. Unlike RADIUS MAC, for 802.1x requests, FortiNAC acts as a proxy RADIUS server and forwards requests to an independent production RADIUS server. As the proxy server, FortiNAC passes EAP messages between the network device and the production authentication server, which is the EAP termination point.

When the authentication process completes, the production RADIUS server responds to FortiNAC with the accept or reject message which FortiNAC passes onto the network device. If configured to do so, FortiNAC inserts network access information into the authentication response.

If FortiNAC Authentication is enabled in an 802.1x environment, and the EAP type configured in the host supplicant identifies the user (such as with PEAP), users who log in can automatically be authenticated and therefore bypass the authentication captive portal. If the user ID is encrypted or not provided (such as with EAP TTLS or EAP TLS), FortiNAC cannot identify it in the RADIUS request, and therefore cannot bypass its own authentication process.

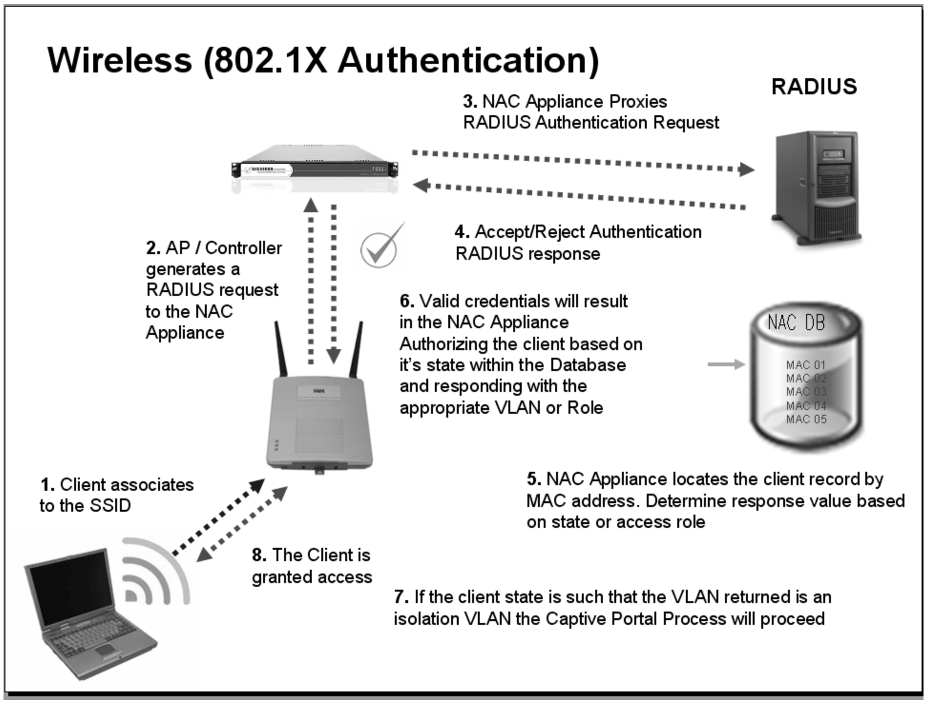
EAP

The EAP type must be configured on the supplicant and the Authentication server. Supported EAP types include:

- EAP-PEAP
- EAP-TTLS
- EAP-TLS

The following EAP types have not yet been tested with FortiNAC:

- EAP-MD-5
- EAP-Fast
- Cisco LEAP


Wireless (802.1X Authentication)
RADIUS
3. NAC Appliance Proxies RADIUS Authentication Request
4. Accept/Reject Authentication RADIUS response
2. AP / Controller generates a RADIUS request to the NAC Appliance
6. Valid credentials will result in the NAC Appliance Authorizing the client based on it's state within the Database and responding with the appropriate VLAN or Role
NAC DB
MAC 01
MAC 02
MAC 03
MAC 04
MAC 05
5. NAC Appliance locates the client record by MAC address. Determine response value based on state or access role
1. Client associates to the SSID
8. The Client is granted access
7. If the client state is such that the VLAN returned is an isolation VLAN the Captive Portal Process will proceed

Requirements

1. Configure your device to use FortiNAC as the RADIUS Server. If you are setting up FortiNAC as the RADIUS server for a device in a Fortinet High Availability environment, you must use the actual IP address of the primary control

server, not the Shared IP address. Set up the secondary control server as a secondary RADIUS server using its actual IP address. Regardless of the environment, you may also want to set up your actual RADIUS server to be used in the event that none of your FortiNAC appliances can be reached. This would allow users to access the network, but they would not be controlled by FortiNAC.

FortiNAC's capacity for processing RADIUS requests is approximately 60 requests per second. Capacity is affected by the use of other features in the program such as the Persistent Agent or MAC Notification Traps. Any requests that are not immediately processed are placed in queue. After 5 seconds any unprocessed requests are discarded. If you are in an environment where you expect to receive more than 60 RADIUS requests per second you may need additional FortiNAC appliances to handle the load.

2. Do not use asymmetric routing between your device and the FortiNAC server. RADIUS requests and responses between the FortiNAC server and the wireless device must travel through the same interface on the FortiNAC server.
3. When using 802.1x, PAP encryption must be set up on the RADIUS server for encryption/decryption of user names and passwords that are sent to and from FortiNAC, such as the user name and password for the Validation Account used for communication between FortiNAC and the RADIUS server.
4. Configure network access control features on your device. Go to the Customer Portal on the Fortinet web site for device specific configuration information.
5. High performance network devices have the ability to generate large numbers of connection requests each of which must be processed by FortiNAC. As a best practice to improve overall performance it is recommended that you throttle the rate of connection requests accepted from any individual host using the rate-limiting features available on your wireless device.
6. Add your device in FortiNAC. See Network devices on page 833.
7. Network devices should have static IP addresses or dynamic IP addresses that are reserved. Once a device that provides network services had been identified in FortiNAC there is no mechanism to automatically update the IP address for that device if there is a change. If the IP address on the device itself is changed, the device appears in FortiNAC to be offline or to have a communication error.
8. Model your wireless device in FortiNAC. See Model configuration on page 767.
9. For network devices configured to authenticate hosts using RADIUS, FortiNAC must be configured as the RADIUS server.

When FortiNAC acts as a RADIUS Server in a busy environment, it could become a bottleneck for authentications, resulting in RADIUS processing delays.

Devices that use RADIUS authentication need to be configured with RADIUS timeouts that are large enough to allow some transaction delays. Many devices use default timeout values under 10 seconds. It is recommended that you use larger values for busy environments, though you may have to experiment to find the optimal value.

10. The RADIUS Secret must be the same in the following locations:
    - RADIUS Server settings in FortiNAC. See 802.1x environments on page 103 and Configure profiles on page 104.
    - Model configuration for the wireless device when it is modeled in FortiNAC. See Model configuration on page 767.
    - If individual SSIDs are configured, the RADIUS secret must be the same in the SSID configuration. See SSID configuration on page 788.
    - Configuration of the device itself.

11. For some wireless devices, FortiNAC supports management of individual SSIDs in which different treatment is provided to hosts depending on the SSID to which they are connected. To use this feature, you must create an SSID configuration for each SSID that you wish to manage differently from the parent device that controls the SSID. If no SSID configuration exists, the Model Configuration for the device is used. For example if you have a corporate SSID and a guest SSID, you may want to allow the guest SSID to provide Internet access only and the corporate SSID to provide access to the corporate network. They can be configured separately. See SSID configuration on page 788.
12. If you configure SSIDs individually, you can allow the configuration to inherit the RADIUS server information from the device's Model Configuration or you can configure it for the SSID itself. You would not typically need to select a RADIUS server that is different than that used for the device.
13. Do not set FortiNAC as the trap receiver on any wireless devices. FortiNAC does not process traps from wireless devices.
14. APs appear as rogue hosts in FortiNAC until they are identified by the controller as managed devices. As APs are identified, either as a result of device profiling or of AP discovery from a wireless device, the rogues will automatically be removedModify a group on page 841.
15. If you are working in a High Availability environment using RADIUS authentication you must configure your managed wireless devices to point to the FortiNAC Server or FortiNAC Control Server eth0 address - NOT the virtual address.

    Configure a secondary RADIUS server for the device to be the failover eth0 address. This ensures that if the primary FortiNAC Server or FortiNAC Control Server appliance goes down, the backup will take over and will be able to respond and take over RADIUS responsibility. An IAP/controller will switch over to the backup FortiNAC Server or FortiNAC Control Server appliance if it fails to get responses from the primary.
16. Network Access Policies can be created to provide flexible network assignments based on different host and user criteria. SSIDs can be used in network access policies by assigning SSID models to port groups and including the port groups within User/Host Profiles. See Modify A Group and Network Access Policies.

    For example, a guest user with role Guest connecting to the corporate SSID can be restricted to a Dead-end VLAN while a corporate user with role Staff connecting to the same SSID can be place into the Production VLAN. Likewise, a guest user with role Guest connecting to the Guest SSID can be placed in a guest VLAN that provides Internet-only access while a corporate user with role Staff connecting to the same Guest SSID can be placed in the Dead-End VLAN.
17. When a network device supports hot standby with virtual IP assignment, special considerations can apply since FortiNAC must be able to identify the device sending the request. If the RADIUS request originates from an address different than the one discovered and modeled by FortiNAC, the request must identify the device by information in the RADIUS request packet. FortiNAC looks for this device identity information in the NAS-IP and NAS-ID attributes.

WLAN management

Most Intelligent Access Points (IAPs) and controllers allow you to create multiple, independent Wireless LANs (WLANs) that can be accessed through separate SSIDs. The configuration of each WLAN on these devices usually includes support for separate authentication parameters for each WLAN. For example, a wireless network could contain two separate WLANs, one for employees or residents and one for guests. The employee/resident WLAN might authenticate connecting users to a central directory prior to granting access to network resources. A guest WLAN might avoid authentication and provide connecting users with limited access only to the external Internet.

In such an environment, you can have FortiNAC secure only a subset of the available WLANs. To do this, you only need to configure the secured WLANs on the wireless devices to use FortiNAC as their authentication server (RADIUS). WLANs that use no authentication or that use a different authentication server bypass FortiNAC’s control. FortiNAC continues to provide visibility for all hosts connecting to the wireless network devices, but does not control their access to the network. The means of configuring this behavior differs based on the particular characteristics of the wireless device model. Refer to the vendor's documentation for configuration details.

If your network has SSIDs that are broadcast on multiple APs, you must ensure that the production and isolation VLANs configured for those SSIDs are the same on all APs. For example, if SSID OfficeWorkers is broadcast from AP1 and AP2 and the production VLAN for that SSID is 10 for both APs, then FortiNAC can manage hosts on that SSID. If the production VLAN is 10 on AP1 and 20 on AP2, then FortiNAC cannot manage hosts on that SSID because within FortiNAC there is no concept of the AP/SSID combination. The SSID is treated as a single entity with only one setting for the production VLAN. Therefore, when FortiNAC sends a VLAN change to the SSID for a host, depending on the AP involved, the VLAN could be invalid.

On wireless controller devices that provide identification of the AP in the authentication request, it is possible to create network access policies with user host profiles that contain AP rather than SSID information. This allows for network selection based on AP location rather than SSID, providing a partial exception to limitation described in the previous paragraph.

If your device supports independent authentication for individual SSIDs, FortiNAC can secure a subset of available WLANs. If your device does not support this option, FortiNAC secures all WLANs on the device.

When configuring a wireless device with multiple SSIDs that will be managed by FortiNAC, FortiNAC typically only allows a single VLAN mapping for each isolation state per device. For example, if the Remediation VLAN is VLAN 10 on one SSID it has to be VLAN 10 on all SSIDs, and if Dead End is VLAN 25 it has to be VLAN 25 for all SSIDs. However, for some wireless devices, FortiNAC allows for separate VLAN mappings based on individual SSIDs. If SSID Configuration is not done, the configuration is inherited from the Model Configuration of the parent device and behavior remains as it was in previous product releases.

In an environment where there are multiple SSIDs that have the same name, FortiNAC cannot manage those SSIDs individually. Make sure that SSIDs do not have the same name.

Individual SSID configuration

FortiNAC allows configuration of individual SSIDs for wireless devices that provide the necessary management capability. See WLAN management on page 973 for the list of devices.

Configuring SSIDs separately allows you to provide different treatment to hosts depending on the SSID to which they are connected. The VLAN or Role into which a host is placed is determined by one or more of the following:

- Host state
- VLANs/Roles configured on the device for the selected SSID.
- Device model configured in FortiNAC.
- SSID configuration in FortiNAC.

Configuration of the options listed above will vary depending on the treatment desired for hosts. The use cases below outline possible scenarios and suggestions for configuring them. Many additional configuration scenarios and variations exist. These are simply to provide some examples.

Assign different VLANs

The administrator wants a public SSID that will allow users to access the Internet but prohibit access to the internal network. Unknown users would not be required to register when accessing this public network. The administrator also wants a second secure SSID that will allow users with proper credentials to access the internal network. Corporate users connected to the public SSID would not be required to authenticate but would be prevented from accessing the internal network. They would be treated the same as unknown users. To configure this scenario you would do the following:

- Configure the device with two SSIDs, one public and one secure.
- On the device configure a VLAN or Role for each isolation state you wish to enforce (Dead-End, Registration, Quarantine and Authentication) and each production network you wish to provide.
- In FortiNAC run Discovery or add the wireless device to Topology. See Add or modify a device on page 723 or Discover devices on page 735.
- Configure the device model in the database using Model Configuration. See Model configuration on page 767.
- On the Model Configuration view click Read VLANS or Roles to read the available VLANs or Roles configured on the device. This also reads SSIDs from the device.
- In Topology, locate the public access SSID, go to the SSID Configuration view and complete the configuration. See SSID configuration on page 788.
  - Set the Default Host State to the Access Value or VLAN for Internet only access.
  - Set the Access Enforcement field for the remaining Host Isolation States to Bypass to allow all hosts access to the Default Access Value.
- In Topology, locate the internal SSID, go to the SSID Configuration view and complete the configuration. Set the Access Value for the Default Host State to the production VLAN.
  - Set the Access Enforcement fields for the Isolation states configured on the device to Enforce. For example if you configured a VLAN on the AP or controller for a Quarantine condition, set the Access Enforcement field for Quarantine to Enforce and select that VLAN from the drop-down in the Access Value field.
  - Set the Access Enforcement field for any state not configured on the device to Deny or Bypass.

Assign an endpoint compliance policy

The administrator wants to scan hosts on SSID 1 with Policy A and hosts on SSID 2 with Policy B. Endpoint Compliance Policies are applied to a host based on the User/Host Profile associated with the policy. In this scenario FortiNAC groups are used to control the Endpoint Compliance Policy assigned based on the SSID to which the host connects.

- Configure the device with two SSIDs, one public and one secure.
- On the device configure a VLAN or Role for each isolation state you wish to enforce (Dead-End, Registration, Quarantine and Authentication) and each production network you wish to provide.
- In FortiNAC run Discovery or add the wireless device to Topology. See Add or modify a device on page 723 or Discover devices on page 735.
- Configure the device model in the database using Model Configuration. See Model configuration on page 767.
- On the Model Configuration view click Read VLANS or Roles to read the available VLANs or Roles configured on the device.
- In this case, SSID configuration within FortiNAC is not required. Settings are inherited from the parent device.
- Create a port group for each SSID and place one SSID in each group. For example, create Port Group 1 and place SSID 1 in that group. See Add groups on page 839.
- Create two User/Host Profiles that will be used to identify users and hosts that connect on each of the two different SSIDs. Associate each User/Host Profile with a different Port Group. See User/host profiles on page 389.
- Create an Endpoint Compliance Configuration for each of the SSIDs. The configuration contains the scans that should be run on the connecting hosts. See Endpoint compliance configurations on page 420.

- Create the two Endpoint Compliance Policies that will be used for the two different SSIDs. Associate each policy with a different User/Host Profile and Endpoint Compliance Configuration. For example, associate a policy to User/Host Profile 1 and Endpoint Compliance Configuration 1. Users and hosts that match the Profile will receive the Configuration. Associate a different policy to User/Host Profile 2 and Endpoint Compliance Configuration 2. Users and hosts that match Profile 2 will receive Configuration 2. See Endpoint compliance policies on page 415.

Prevent user types from sharing SSIDs using roles

The administrator has two types of users Employees and Students. He wants to prevent Employees from accessing their secure network when they are on SSID 1, but allow access when Employees are on SSID 2. When Students are on either SSID they can only access the open network. FortiNAC roles can be used to control the VLAN or Device Role assigned based on the SSID to which the host connects.

- Configure the device with two SSIDs, one public and one secure.
- On the device configure a VLAN or Role for each isolation state you wish to enforce (Dead-End, Registration, Quarantine and Authentication) and each production network you wish to provide.
- In FortiNAC run Discovery or add the wireless device to Topology. See Add or modify a device on page 723 or Discover devices on page 735.
- Configure the device model in the database using Model Configuration. See Model configuration on page 767.
- On the Model Configuration view click Read VLANS or Roles to read the available VLANs or Roles configured on the device.
- In this case, SSID configuration within FortiNAC is not required. Settings are inherited from the parent device.
- Create a port group for each SSID and place one SSID in each group. For example, create Port Group 1 and place SSID 1 in that group, then create Port Group 2 and place SSID 2 in that group. See Add groups on page 839.
- Make sure that users are assigned to either an Employee Role or a Student Role. See Role management on page 553.
- Create User/Host Profiles that filters for each of the following combinations:

  Profile 1

  - Where (Location) = Port Group 1 (contains SSID 1)
  - Who/What by Attribute = User Role Employee

  Profile 2

  - Where (Location) = Port Group 2 (contains SSID 2)
  - Who/What by Attribute = User Role Employee

  Profile 3

  - Where (Location) = Port Group 1 or Port Group 2
  - Who/What by Attribute = User Role Student
- Create a Network Access Configuration for each Profile as follows:

  For Profile 1 and 3:

  - Create Network Access Configuration A that provides access to the Open Production VLAN

For Profile 2:

  - Create Network Access Configuration B that provides access to the Secure Production VLAN

- Create three Network Access Policies that map each User/Host Profile to a Network Access Configuration as follows:

Network access policy for employees on SSID 1

  - Use Profile 1 and Network Access Configuration A. When a User with Role Employee connects to SSID 1, that connection/user matches Profile 1. Profile 1 is mapped to Network Access Configuration A. This puts the user's host on the Open VLAN.

Network access policy for employees on SSID 2

  - Use Profile 2 and Network Access Configuration B. When a User with Role Employee connects to SSID 2, that connection/user matches Profile 2. Profile 2 is mapped to Network Access Configuration B. This puts the user's host on the Secure VLAN.

Network access policy for students on SSID 1 or 2

  - Use Profile 3 and Network Access Configuration A. When a User with Role Student connects to either SSID 1 or SSID 2, that connection/user matches Profile 3. Profile 3 is mapped to Network Access Configuration A. This puts the user's host on the Open VLAN.

Configure wireless access points

When lightweight access points (LAP) and their associated wireless controllers are connected to a network being managed by FortiNAC, the access points initially appear as rogue adapters/hosts on the network. These access points could be sent into isolation depending on whether or not the ports to which they connect are in any of the "Forced" groups, such as Forced Registration.

When adding a new controller and LAPs or just new LAPs to extend an existing wireless network, the same guidelines apply. You must disable isolation enforcement on the ports to which the LAPs connect to avoid having them placed into an isolation network where the LAPs will be unable to communicate with their controller.

The following steps provide an overview for adding LAPs:

- Remove isolation enforcement on the ports to which LAPs are connected by removing the ports from all of the following groups: Forced Registration, Forced Remediation, and Forced Authentication. See Groups view on page 838.
- If you plan to control those ports for hosts later, create a port group in FortiNAC to contain the ports to which LAPs are connected. After the LAPs have been configured you can quickly add the ports back to the Forced groups by adding this new group to each of the "Forced" groups.
- Connect each LAP to one of the uncontrolled ports.
- Allow the LAPs and controller to communicate.
- Discover the new LAP by opening the Model Configuration view for the controller and clicking either **Read Roles** or **Read VLANs** depending on the controller. If this option is not available on the Model Configuration for the controller, navigate to the Topology View, right-click on the controller and select **Network Access/VLANs**. Click Read Roles or Read VLANs. FortiNAC discovers the LAPs, creates pingable LWAP models in the Topology View

and removes the corresponding rogues. See Model configuration on page 767 or Network access/VLANs on page 745.

- When all of the LAPs have been discovered, add the new port group you created to the appropriate "Forced" groups to enforce isolation on those ports.

Wired and wireless connections

When you use a wired connection in a wireless hot spot, wireless interfaces that are enabled often attempt to connect to a local AP. It is recommended that you instruct users to disable their wireless interfaces on their laptops when they use wired ports for the following reasons:

1. The wireless connection attempt may or may not succeed. RADIUS traffic is created to authenticate the host even though it is already connected to the network through its wired connection. If the host is authenticated on the wireless device (either through RADIUS or the local AP), the host is connected and no additional traffic is generated. However, if the host is rejected for any reason, the host will often retry continuously. For some APs, this generates a steady stream of RADIUS requests and creates an unnecessary load on the FortiNAC appliance and the supporting network.
2. If a wireless interface connects simultaneously with a wired interface, each interface could be placed on a different VLAN or network. In cases where the network administrator is enforcing authentication or where separate networks have been defined for their wired and wireless users, this will always occur. When this happens, depending on the network access given to the different network connections, the host may experience abnormal network behavior as the host chooses different interfaces for network access.

There are steps users can take to configure a host running Windows OS to favor their wired over their wireless, but the best course of action is to simply disable the wireless when not in use.

Aruba IAP configuration

An Aruba IAP (Instant Access Point) WLAN consists of at least one IAP access point. Any access point within the WLAN may function as the virtual controller for the entire WLAN. If the access point serving as virtual controller is taken offline, another access point will take over the virtual controller function.

After you set up and deploy the first access point, the virtual controller automatically configures all of the subsequent access points you add to the network.

To configure the Aruba IAP, follow these steps:

1. Connect the Aruba IAP to your wireless network. At the **Login** screen, enter your network user name and password.
2. Connect a computer to the network.
3. Open a web browser and navigate to `https://IP_Address:4343/#home`. This brings up the Aruba Networks main screen.
4. Choose the name of the IAP you want to configure from the Networks list. The **WLAN Settings** screen is displayed.
5. Click **Next**. The **VLAN** screen is displayed.
6. For **Client IP assignment**, choose **Network Assigned For Client VLAN assignment**, click **Default**.
7. Under **VLAN Assignment Rules**, set the **Tunnel-Private-Group-ID**.
8. Click **Next**. The **Security** screen is displayed.

9. Use the slider on the left to adjust the security level to **Enterprise**.
10. Select the type of network key using the drop-down menu.
11. In the **Authentication server 1** field, type in the name of the first authentication server and click **Edit**. The **Authentication Servers** tab is displayed.
12. Enter the information (IP address, shared key, retry count, etc. for the authentication server.
13. Click **OK**.
14. Click **OK** again to return to the **Security** screen.
15. Enter information about the second authentication server, and so on. When you have finished, click **Next**. The **Access** screen is displayed.
16. Use the slider to select **Role-based access**.
17. To create a new access role, click **New** under **Roles**.
18. Give the role a name, and then configure access to the network. Assign an access rule as a role assignment.
19. When you are done creating and configuring roles, click **Finish**.

Meraki configuration

Cisco Meraki configuration

It is recommended that Meraki APs are configured with a static IP address.

Configure one or more SSIDs that you want FortiNAC to control.

From the access control page

1. Set the association requirements to either **MAC-based access control** or **WPA2-Enterprise**.
2. Configure FortiNAC as the RADIUS server.
3. Set Client IP assignment to **Bridge mode: Make clients part of the LAN** to allow for different DHCP servers for the different VLANs used for production and isolation.
4. Select **Use VLAN tagging** from the VLAN tagging drop-down menu.
5. In the VLAN ID section, create VLANs to support the level of management desired. If FortiNAC is enforcing isolation, the VLANs used for isolation must be created on the AP.
6. Set the RADIUS override option to **RADIUS response can override VLAN tag**.

From the network-wide settings page

1. In the Logging section, configure FortiNAC as a Syslog server, with the Roles set to include:
   - Wireless event log.
   - The Flows role may also be necessary if FortiNAC does not obtain the IP address of wireless sessions efficiently from other L3 devices.
2. In the SNMP section, SNMP access must be enabled for v1/v2 or V3 access to allow for FortiNAC device discovery.

RADIUS accounting is not utilized for Meraki APs.

Other options can be set as desired, though any settings that may interfere with the features stated above might have an impact on the integration.

FortiNAC configuration

1. Discover or create the Meraki APs in FortiNAC. Use the SNMP values previously configured on the Meraki APs.
2. Once discovered, find the devices in the FortiNAC
   Topology view and access the AP's Model Configuration View.
3. From that view, configure the following:
   - RADIUS server definitions if FortiNAC is managing any 802.1x SSIDs.
   - Session timeout values for isolation and production. Because the Meraki APs offer no post-connection method of control, VLAN assignment can only be accomplished at authentication time. Decreasing the Session-Timeout values allows for more frequent VLAN assignment when host state changes occur in FortiNAC.

     Therefore, for isolation networks (VLANs), where hosts are not expected to reside for extended periods, smaller timeframes are desired to allow for VLAN transitions into production after registration or remediation events. However, for production networks (VLANs), longer periods are reasonable since it is expected that hosts will reside in those networks for longer periods.

     These values directly impact how many authentication requests will be generated for host connections on managed SSIDs, so values set too low could adversely impact NS performance characteristics.

   - The Additional Access Values section allows for the addition of VLANs that FortiNAC can assign to connecting hosts. Since VLANs cannot be read directly from the Meraki APs, this list should include all the VLANs that were configured on the Meraki AP for all SSIDs controlled by FortiNAC.

Wireless security

In an environment that is predominantly wireless, where employees and guests are increasingly bringing personal devices and attempting to connect to the wireless network, wireless security is a powerful configuration tool. It allows you to quickly connect to wireless controllers and access points and configure the integration between those devices and FortiNAC.

Wireless devices are added to the Network Devices view based on their IP addresses. FortiNAC reads the configuration on the device. For any given wireless device you can configure multiple Secure SSIDs (802.1x) or Open SSIDs (unsecured) as needed. FortiNAC saves the SSID configuration to its own database.

Wireless security is currently only supported for Xirrus Arrays, HP MSM controllers, and Ruckus controllers. Other wireless devices can be added using the Network Devices View. See Network devices on page 833.

For HP Wireless devices in teaming mode, only the controller that is the Team Manager needs to be configured. Only the virtual IP address of the team should be used for configuration.

Wireless security leverages the Quick Start wizard, but does not use all of the steps in the wizard. Network Devices allows you to add wireless controllers and access points and configure the appropriate SSIDs. Underlying data required to support the SSID configurations is created by FortiNAC as needed.

If you have purchased only the Wireless Only license and not the entire FortiNAC product, you can add only five wired devices. You cannot use the Discovery tool to scan the network for devices.

Implementation

General

1. Configure your wireless devices via the Admin Interface for each device. Make sure that hosts can connect to the network before integrating the devices with FortiNAC.
2. Review the integration document for your wireless device that is available on the Fortinet web site.
3. Use the Discovery option to enter IP address ranges and device credentials and search your network for devices. This option is not available if you have the Wireless Only License. See Discover devices on page 735.
4. Review the results of the Discovery process to make sure all devices have been found. If there are missing devices, check the IP address ranges entered, add any missing ranges and run the Discovery process again. See Discovery results on page 738.
5. If you plan to authenticate network users through a Directory, configure the integration with one or more directories. See Directories on page 79.
6. Configure the Captive Portal. See Portal configuration on page 248.

Guest Management

1. Configure Guest Templates. Guest templates control parameters of guest accounts, such as account duration, password length, or times when the network can be accessed, as well as the SSIDs to which guests can connect. Create a guest template for each unique type of guest. For example, if you have guests who should only have access from 9 in the morning until 5 in the evening, create a template for them. If you have guests who should only be allowed to access a special VLAN or Access Group, create a template for them.
2. If you would like to delegate guest account creation and management to other employees, create Sponsor Administrative Accounts for those users. A sponsor account allows the user to log into the FortiNAC Admin UI and create accounts for guests, send account credentials to guests and respond to guest self-registration requests. See Add a guest manager profile on page 578.
3. Create guest accounts as needed for incoming guests. See Guest or contractor accounts on page 592.
4. Guest Management SSIDs configured using Wireless Security require at least one Guest Management SSID configuration for each Guest Template that is in use. Guests may connect to your network in other ways. If there are Guest Templates for guests that will never connect via one of the SSIDs you are configuring, those Templates do not require an SSID configuration.

   Guest Templates are part of the filter that determines the Access Group or VLAN to which the guest is assigned. If a guest has a Guest Template but the template has not been associated with an SSID the guest will not be able to access the network using one of the SSIDs configured through Wireless Security. The Guest may need to access the network using another wireless connection or a wired connection. SSID options include a Secure (802.1x) SSID or an Open SSID. See Network devices on page 833 and SSID mappings on page 989.

   - For the Secure SSID configuration you must have a primary RADIUS Server. If you do not have one configured you can add it when configuring the SSID.
   - For the Open SSID configuration you must provide the RADIUS secret configured on the array.

Device Onboarding

1. Add Secure (802.1x) or open SSIDs configurations for Device Onboarding to quickly register new devices and users on your network. See Network devices on page 833 and SSID mappings on page 989.
   - For the Secure SSID configuration you must have a primary RADIUS Server. If you do not have one configured you can add it when configuring the SSID.
   - For the Open SSID configuration you must provide the RADIUS secret configured on the device.
2. If your configuration requires that a Supplicant be installed on a device for it to connect to a Secure SSID, do the following:
   - Configure an Open SSID for Device Onboarding that contains a Supplicant Configuration with the security configuration for a Secure SSID. See and Supplicant configurations on page 476.
   - Configure the Secure SSID to which hosts or devices should connect after the Supplicant is installed. See Secure SSID for device onboarding on page 994.

Auto-configured data

To simplify the configuration process for the Wireless Security feature some required pieces of data are generated automatically. For example, if you configure an SSID for Guest Access, the underlying User/Host Profile and Network Access Policy are created for you.

If you modify auto-configured data after you have run the Quick Start wizard, running this tool again may undo the modifications you have made.

Data Type	Data	Notes
Containers	Container Names: Wireless Controllers Wireless APs	Containers are used within FortiNAC to group devices together. As wireless devices are added using either Discovery or by entering them manually on the Network Devices View they are also added to Topology.
Port Groups	Group Names: Name of the Open or Secure SSID	Groups are used to gather like items that require similar treatment. The groups created here are port groups and are used to map Network Access Policies for the Secure and Open SSIDs. When you configure an SSID a port group is created based on the name of the SSID. Each SSID is placed in a separate port group. For example if you add a SSID with the name MegaTech Secure, then a port group with the same name is automatically created and contains the MegaTech Secure SSID.
Host Groups	Group Names: Name of the group from the Directory	Directory Groups are used to group users and their corresponding hosts. Group membership is used in User/Host profiles to determine which Network Access, Endpoint Compliance or Supplicant Policies to apply.
Model Configuration	Model Configuration: Name of the device	When a device that provides network services is added to FortiNAC a model of that device's configuration is stored in the database. This model includes information such as CLI User Names, Passwords, communication protocol, RADIUS Server information and Isolation and Production VLANs. For devices configured through Wireless Security, the following settings are entered: • RADIUS = Use Defaults • Network Access = Deny for Dead End, Registration and Quarantine. Authentication is set to Bypass.
SSID Configuration	SSID Configuration: Name of the SSID	Individual SSIDs can be configured separately instead of inheriting settings from the device's Model Configuration, such as settings for default Isolation and Production VLANS. Use Network Devices View to select a device and access the SSID Configuration. For devices configured through Wireless Security, the following settings are entered for all SSIDs regardless of whether they are open or secure: • RADIUS: Primary and Secondary RADIUS servers are selected if they were selected in the SSID Mappings. • Network Access = Enforce and the Isolation VLAN are set for Dead End, Registration and Quarantine. Authentication is set to Bypass and None for Network Access.

Data Type	Data	Notes
Polling	L2 and L3 Polling settings	Wireless devices are automatically added to the L2 and L3 Polling groups and polling is enabled for the device. The polling interval for L2 is every 10 minutes and L3 is set to every 30 minutes. Use Network Devices View, L2 Polling View or L3 Polling View to modify polling information.
Roles	Role Names: Name of Guest Template associated with guest.	Roles are added as attributes to users or hosts. Role mapping is accomplished by creating a User/Host Profile configured with the SSID port group as the connection location and the Who/What by Attribute field set to one of these role names. A Network Access Policy maps this User/Host Profile to a Network Access Configuration containing the User Group/VLAN where the host will be placed. • A role is created for each Guest Template. • User/Host Profile contains an SSID port group (Where) and a Role name matching a guest template (Who/What by Attribute). • There is a separate User/Host Profile for each guest template and SSID port group combination.
User/Host Profile		User/Host Profiles are created when a new SSID Mapping is added on the Network Devices view. **Guest Management SSID Mappings** — A User/Host profile is created for each SSID and Guest Template combination. Names of these User/Host profiles are based on the SSID name and the combination of data contained within the profile. **Example:** Mobile Security Wizard Profile: GuestAccess Production XR4830 Open • **Mobile Security Wizard** indicates that the User/Host Profile was generated by Quick Start/Wireless Security for Guest Management. • **Profile** indicates that this is a User/Host profile. • **GuestAccess** is the name of the guest template the user has and the Role assigned to guests and hosts when the guest registers in the captive portal. • **Production** is the name of the User Group/VLAN where the connecting host will be placed. • **X-R4830 Open** is the name of the SSID and the name of the port group where the SSID has been placed. The User/Host Profile is configured as follows: • Name of the SSID port group as its connection location in Where. • Role Name derived from guest template name as an attribute of the user in Who/What by Attribute. **Device Onboarding SSID Mappings** — A User/Host profile is created for each SSID, Directory Group and Operating System list combination. Names of these User/Host profiles are based on the SSID name and the combination of data contained within the profile.

Data Type	Data	Notes
		Example: XAM BYOD Profile: Domain Admins [Windows,macOS,iOS,Android,RIM,Windows Phone] Production XR4830 Secure • **XAM BYOD** indicates that the User/Host Profile was generated by Quick Start for Device Onboarding (BYOD). • **Profile** indicates that this is a User/Host profile. • **Domain Admins** is the name of the Directory Group where the user must be a member. A corresponding Host group is created and hosts are placed in that group as they are registered by the user. • **[Windows,macOS,iOS,Android,RIM,Windows Phone]** is the list of operating systems selected in the SSID Mapping as a match for a connecting host. • **Production** is the name of the Xirrus User Group/VLAN where the connecting host will be placed. • **XR4830 Secure** is the name of the SSID and the name of the port group where the SSID has been placed. The User/Host Profile is configured as follows: • Name of the SSID port group as its connection location in Where. • Selected Directory Group in Who/What by Group. • Selected operating systems as attributes of the host in Who/What by Attribute.
Network Access Configuration Network Access Policy		Network Access Configurations and Network Access Policies are created when a new SSID Mapping is added using Wireless Security. **Guest Management SSID Mappings** — A Network Access Configuration and Network Access Policy are created for each SSID and Guest Template combination. Names are based on the SSID name and the combination of data the items contain. **Example:** Network Access Configuration = Mobile Security Wizard Configuration: GuestAccess Production XR4830 Open Network Access Policy = Mobile Security Wizard Access Policy: GuestAccess Production XR4830 Open • **Mobile Security Wizard** indicates that the data was generated by Quick Start / Wireless Security for Guest Management. • **Configuration** indicates that the record is a Network Access Configuration. • **Policy** indicates that the record is a Network Access Policy. • **GuestAccess** is the name of the guest template the user has and the Role assigned to guests and hosts when the guest registers in the captive portal. • **Production** is the name of the User Group/VLAN where the connecting host will be placed.

Data Type	Data	Notes
		- **X-R4830 Open** is the name of the SSID and the name of the port group where the SSID has been placed. **Device Onboarding SSID Mappings** — A Network Access Configuration and Network Access Policy are created for each unique SSID, Directory Group and Host Operating System combination. **Example:** Network Access Configuration = XAM BYOD Configuration: Domain Admins [Windows,macOS,iOS,Android,RIM,Windows Phone] Production XR4830 Secure Network Access Policy = XAM BYOD Policy: Domain Admins [Windows,macOS,iOS,Android,RIM,Windows Phone] Production XR4830 Secure - **XAM BYOD** indicates that the User/Host Profile was generated by Quick Start / Wireless Security for Device Onboarding (BYOD). - **Configuration** indicates that the record is a Network Access Configuration. - **Policy** indicates that the record is a Network Access Policy. - **Domain Admins** is the name of the Directory Group where the user must be a member. A corresponding Host group is created and hosts are placed in that group as they are registered by the user. - **[Windows,macOS,iOS,Android,RIM,Windows Phone]** is the list of operating systems selected in the SSID Mapping as a match for a connecting host. - **Production** is the name of the User Group/VLAN where the connecting host will be placed. - **XR4830 Secure** is the name of the SSID and the name of the port group where the SSID has been placed. The Network Access Configuration is configured as follows: - Name of the FortiNAC Access Group/VLAN where hosts should be placed when connected. The Access Group is the group selected in the SSID Mapping. The Network Access Policy is configured as follows: - Network Access Configuration created for the SSID Mapping. - User/Host Profile created for the SSID Mapping. Network Access Policy maps the Network Access Configuration to a corresponding User/Host Profile also created when SSID Mappings are added. Connecting users that match the User/Host Profile are placed in the Access Group or VLAN in the Network Access Configuration.
Endpoint Compliance Configuration Endpoint Compliance Policy		Endpoint Compliance Policies and Endpoint Compliance Configurations are created when a Device Onboarding SSID Mapping with a Supplicant Configuration is added on the Wireless Security View.

Data Type	Data	Notes
		Device Onboarding — An Endpoint Compliance Policy and Endpoint Compliance Configuration are created for each unique SSID, Directory Group, Host Operating System and Supplicant Configuration combination. **Example:** Endpoint Compliance Policy =XAM BYOD EPC Policy: AlansGroup [Windows,macOS,iOS,Android,Windows Phone] Isolation XR4830 Open Endpoint Compliance Configuration = XAM BYOD EPC Configuration: AlansGroup [Windows,macOS,iOS,Android,Windows Phone] Isolation XR4830 Open • **XAM BYOD** indicates that the User/Host Profile was generated by Quick Start / Wireless Security for Device Onboarding (BYOD). • **Policy** indicates that the record is an Endpoint Compliance Policy. • **Configuration** indicates that the record is an Endpoint Compliance Configuration. • **AlansGroup** is the name of the Directory Group where the user must be a member. A corresponding Host group is created and hosts are placed in that group as they are registered by the user. • **[Windows,macOS,iOS,Android, Windows Phone]** is the list of operating systems selected in the SSID Mapping as a match for a connecting host. • **Isolation** is the name of the User Group/VLAN where the connecting host will be placed. • **XR4830 Open** is the name of the SSID and the name of the port group where the SSID has been placed. The Endpoint Compliance Configuration is configured as follows: • Name of the Access Group/VLAN where hosts should be placed when connected. The Access Group is the group selected in the SSID Mapping. • Scan is set to the system scan "AgentNoScan" which does not scan for anything. • Agents are set to "Latest Dissolvable" for Windows, macOS and Linux and "Latest Mobile" for Android. All other operating systems are set to "None-Bypass". The Endpoint Compliance Policy is configured as follows: • Endpoint Compliance Configuration created for the SSID Mapping. • User/Host Profile created for the SSID Mapping.
Supplicant EasyConnect Policy		A Supplicant EasyConnect Policy is created when a Device Onboarding SSID Mapping with a Supplicant Configuration is added on the Wireless Security View view.

Data Type	Data	Notes
		Device Onboarding — A Supplicant EasyConnect Policy is created for each unique SSID, Directory Group, Host Operating System and Supplicant Configuration combination. **Example:** Supplicant EasyConnect Policy =XAM BYOD Supplicant Policy:AlansGroup [Windows,macOS,iOS,Android,Windows Phone] Isolation XR4830 Open Endpoint Compliance Configuration = XAM BYOD EPC Configuration: AlansGroup [Windows,macOS,iOS,Android,Windows Phone] Isolation XR4830 Open • **XAM BYOD** indicates that the Policy was generated by Quick Start / Wireless Security for Device Onboarding (BYOD). • **Supplicant Policy** indicates that the record is a Supplicant EasyConnect Policy. • **Configuration** indicates that the record is a Supplicant EasyConnect Configuration. • **AlansGroup** is the name of the Directory Group where the user must be a member. A corresponding Host group is created and hosts are placed in that group as they are registered by the user. • **[Windows,macOS,iOS,Android, Windows Phone]** is the list of operating systems selected in the SSID Mapping as a match for a connecting host. • **Isolation** is the name of the User Group/VLAN where the connecting host will be placed. • **XR4830 Open** is the name of the SSID and the name of the port group where the SSID has been placed. The Supplicant EasyConnect Policy is configured as follows: • Supplicant Configuration added to the SSID Mapping. • User/Host Profile created for the SSID Mapping.
Portal Policy		A Portal Policy is created if a portal other than the default portal is selected when adding an SSID Mapping on the Wireless Security View for either Guest Management or Device Onboarding. **Portal Policy** — A Portal Policy is created for each unique SSID, Directory Group, Host Operating System and Portal combination. **Example:** Portal Policy = XAM Portal Policy: -AlansGroup-[Windows,macOS,iOS,Android,RIM,Windows Phone] XAM-Access XirrusXMSOpen • **XAM Portal Policy** indicates that the policy was generated by Quick Start / Wireless Security to control the portal presented to the user when connecting to this SSID. • **AlansGroup** is the name of the Directory Group where the user must be a member. A corresponding Host group is created and hosts are placed in that group as they are registered by the user.

Data Type	Data	Notes
		- **[Windows,macOS,iOS,Android,RIM,Windows Phone]** is the list of operating systems selected in the SSID Mappings as a match for a connecting host. - **XAM-Access** is the name of the User Group/VLAN where the connecting host will be placed. - **XirrusXMSOpen** is the name of the SSID and the name of the port group where the SSID has been placed.
Quarantine VLAN Switching	Enable	If a Guest Template or administrative profile limits network access by time, Quarantine VLAN Switching must be enabled. This allows FortiNAC to mark Guests and Admin Users as "At Risk" for the GuestNoAccess admin scan during the times they are not allowed to access the network. If Login Availability is set to Always for Guests and Administrative users, the Quarantine VLAN Switching option is not enabled. Access this setting under **System > Settings > Control**.

SSID mappings

For supported wireless devices in the FortiNAC database you can configure Secure (802.1x) and Open SSIDs. The configuration is saved to the FortiNAC database. When configuring SSIDs, FortiNAC reads the existing configuration from the access point.

Supported wireless devices include: HP MSM Controllers, Ruckus Controllers and Xirrus Arrays.

The two primary functions for SSIDs configured through Wireless Security are to provide guest access and to allow network users to register devices on the network (Device Onboarding). Each of these functions can use either a Secure or an Open SSID and any given SSID can be used for more than one type of access.

Guest access

When Guest Management is selected, the Open SSID configuration includes access and isolation User Groups/VLANs, Guest Templates and the RADIUS secret. Existing Open SSIDs are read from the device by FortiNAC and they are displayed here.

The Secure SSID configuration for guest access includes access and isolation User Groups/VLANs, Guest Templates and RADIUS server information. These SSIDs are typically used by people with an 802.1x supplicant already installed on their wireless devices. Existing Secure SSIDs are read from the device by FortiNAC and they are displayed here. If a supplicant is required, this type of SSID may not be the best option for guests because the supplicant would need to be supplied separately.

Add or configure a Wireless Network (SSID) Mapping for each Guest Template. Guest Templates control the SSIDs to which guests or users can connect. A guest account is created using a Guest Template. That association with the Guest Template remains on the guest account and a guest can ONLY connect to this SSID if the template on the account matches the template on the SSID Mapping. The same SSID can have multiple configuration records with different Guest Templates. Multiple SSID Mappings can have the same Guest Template.

Device onboarding

When Device Onboarding is selected, the Open SSID Mapping can limit access to the SSID based on the operating system of the connecting device. If you are authenticating through LDAP, only users who are in the selected directory group with one of the approved operating systems can connect to this SSID. The Mapping also includes access and isolation User Groups/VLANs selected from the configuration on the device. The Open SSID can be leveraged to serve a Supplicant Configuration to the connecting host for one of your Secure SSIDs.

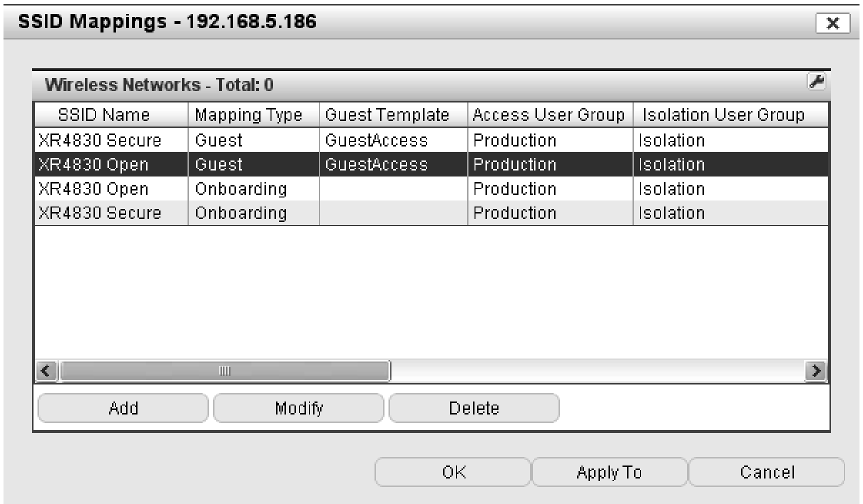
The Secure SSID Mapping for Device Onboarding can limit access to the SSID based on the operating system of the connecting host. If you are authenticating through LDAP, the selected Directory group also serves as criteria for connecting to this SSID. The Mapping includes RADIUS server information and access and isolation User Groups/VLANs selected from the configuration on the wireless device.

Supplicant configuration

Add or configure one or more Open SSIDs to serve supplicant configurations for Secure SSIDs, if needed. The supplicant configuration must be served via an Open SSID because it is the only SSID to which an unknown user can connect.

See Navigation on page 10 and Filters on page 15 for information on common navigation tools and data filters.

Titles of windows and field names may vary depending on the brand of the device being configured. For example, HP devices use VSC to represent the record for the SSID and its configuration details. Screen shots and Settings were done using a Xirrus Wireless Array.



Wireless Networks - Total: 0

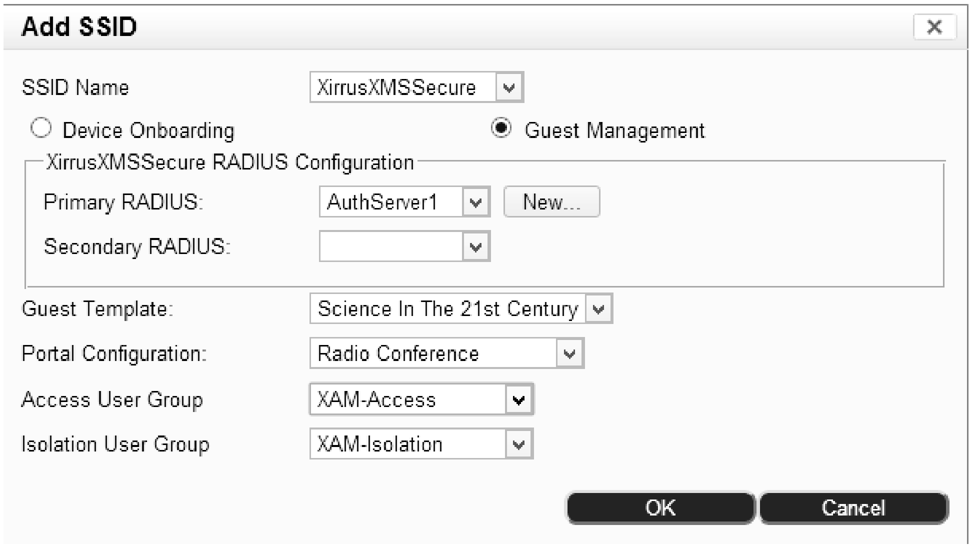
SSID Name	Mapping Type	Guest Template	Access User Group	Isolation User Group
XR4830 Secure	Guest	GuestAccess	Production	Isolation
XR4830 Open	Guest	GuestAccess	Production	Isolation
XR4830 Open	Onboarding		Production	Isolation
XR4830 Secure	Onboarding		Production	Isolation

Settings

Field	Definition
SSID Name	Network name of the SSID configuration that includes all of the settings for the SSID, such as User Group.
SSID	Broadcast SSID Name Typically this is read from the array..

Field	Definition
Mapping Type	Indicates whether this SSID Mapping is for Guest Management or Device Onboarding.
Guest Template	Guest Template associated with this SSID. Only guests whose accounts were created with this Guest Template can access the network via this SSID.
Access User Group	Name or number of the Network Access identifier where a known host or device will be placed, such as, User Group, VLAN ID or VLAN Name.
Isolation User Group	Name or number of the Network Access identifier, such as, User Group, VLAN ID or VLAN Name, for the Isolation VLAN where an unknown host or device will be placed.
Operating Systems	Allows or denies access to an SSID based on the operating system of the connecting host. Options include: • Windows • macOS • iOS • Android • RIM • Windows Mobile
Directory Group	Allows or denies access to an SSID based on the directory group of the connecting user. If you are authenticating through RADIUS instead of LDAP, this option is hidden.
Supplicant Configuration	Name of the Supplicant Configuration that will be served to hosts that connect to the selected SSID. Only Open SSIDs used for Device Onboarding can serve Supplicant Configurations.
Portal Configuration	Name of the Portal that will be applied to hosts connecting via this SSID.
Primary RADIUS Server	RADIUS server that will be used by FortiNAC for authentication.
Secondary RADIUS Server	Secondary RADIUS server that will be used by FortiNAC for authentication if the Primary RADIUS server cannot be reached.
RADIUS Secret	Encryption key used by the RADIUS server to send authentication information. The RADIUS secret must be the same in FortiNAC RADIUS settings, on the SSID configuration and on the access point itself.
Buttons	
Apply To	Copies SSID Mappings to selected device models in the database based on matching SSID Names. Configure SSIDs in an environment where roaming is used and SSIDs must have the same configuration across multiple access points.

Secure SSID for guest management



Add SSID

SSID Name: XirrusXMSSecure

○ Device Onboarding ● Guest Management

XirrusXMSSecure RADIUS Configuration

Primary RADIUS: AuthServer1

Secondary RADIUS:

Guest Template: Science In The 21st Century

Portal Configuration: Radio Conference

Access User Group: XAM-Access

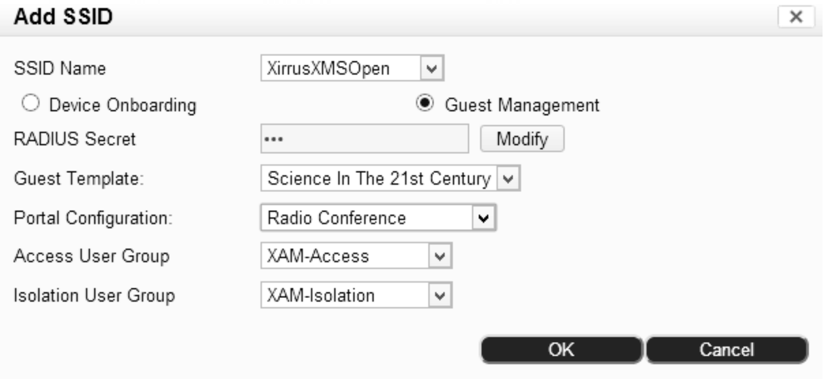
Isolation User Group: XAM-Isolation

1. Click **System > Quick Start**.
2. Select **Network Settings > Network Devices** from the steps on the left.
3. Select a device in the Network Devices window.
4. Click the **Wireless Security** button at the bottom.
5. On the SSID Mappings dialog, click the **Add** button.
6. Click the drop-down arrow in the **SSID Name** field and select the Name of the SSID to be mapped. These names are read from the wireless device and represent existing SSID configurations on the device.
7. Click the **Guest Management** radio button to select it.
8. In the **Primary RADIUS** field select the RADIUS server that FortiNAC should use for authentication. If no RADIUS servers are configured, click the **New** button to add one. See Configure profiles on page 104.
9. In the **Secondary RADIUS** field select the RADIUS server to be used in the event that the Primary RADIUS cannot be accessed. This field is optional.
10. In the **Guest Template** field select the template that is required for guest access using this SSID.
11. In the **Portal Configuration** field select the captive portal that should be presented to the user when the host connects to this SSID. If you are not using multiple portals or you do not have a specific portal for this group of guests, select **Use Default**.
12. In the **Access User Group** field select the production User Group to be used for hosts accessing the Secure SSID using a guest account. These are read from the wireless device and represent existing User Groups that have been configured on the wireless device.
13. In the **Isolation User Group** field select the User Group to be used to isolate unknown hosts. These User Groups are read from the wireless device and represent existing User Groups that have been configured on the wireless device.
14. Click **OK** to save the SSID configuration.

Settings

Field	Description
SSID Name	Network name of the SSID configuration that includes all of the settings for the SSID, such as encryption method or VLANs.
Mapping Type	**Device Onboarding**—Indicates that this SSID Mapping will be used by known network users to register devices. **Guest Management**—Indicates that this SSID Mapping will be used by guests to access the network via a guest account.
Primary RADIUS Server	RADIUS server that will be used by FortiNAC for authentication.
Secondary RADIUS Server	Secondary RADIUS server that will be used by FortiNAC for authentication if the Primary RADIUS server cannot be reached.
Guest Template	Guest template that must be associated with a guest account in order for the guest to connect on this SSID.
Portal Configuration	Name of the Portal that will be applied to hosts connecting via this SSID.
Access User Group	Name or number of the Network Access identifier where a known host or device will be placed, such as, User Group, VLAN ID or VLAN Name.
Isolation User Group	Name or number of the Network Access identifier, such as, User Group, VLAN ID or VLAN Name, for the Isolation VLAN where an unknown host or device will be placed.

Open SSID for guest management



Add SSID

SSID Name: XirrusXMSOpen

○ Device Onboarding ● Guest Management

RADIUS Secret: •••

Guest Template: Science In The 21st Century

Portal Configuration: Radio Conference

Access User Group: XAM-Access

Isolation User Group: XAM-Isolation

1. Click **System > Quick Start**.
2. Select **Network Settings > Network Devices** from the steps on the left.
3. Select a device in the Network Devices window.
4. Click the **Wireless Security** button at the bottom.
5. On the SSID Mappings dialog, click the **Add** button.
6. Click the drop-down arrow in the **SSID Name** field and select the Name of the SSID configuration to be added to the FortiNAC database. These names are read from the wireless device and represent existing SSID configurations.

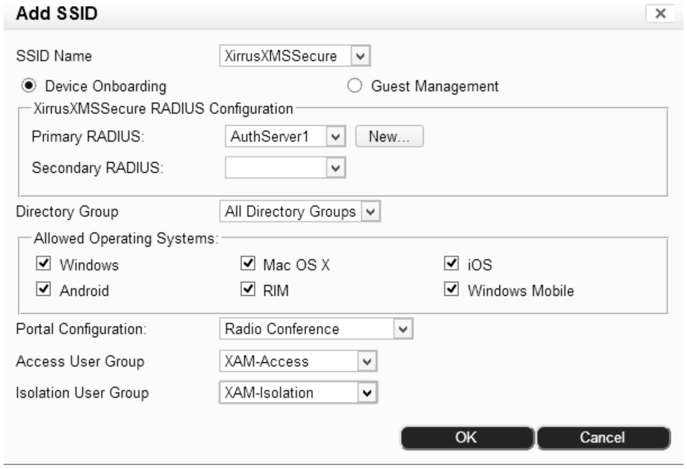
7. Click the **Guest Management** radio button to select it.
8. Click the **Modify** button next to the RADIUS Secret field. Enter the secret that is configured on the device.
9. In the **Guest Template** field select the template that is required for guest access using this SSID.
10. In the **Portal Configuration** field select the captive portal that should be presented to the user when the host connects to this SSID. If you are not using multiple portals or you do not have a specific portal for this group of guests, select Use Default.
11. In the **Access User Group** field select the production User Group to be used for hosts accessing the Secure SSID. These are read from the wireless device and represent existing User Groups that have been configured on the wireless device.
12. In the **Isolation User Group** field select the User Group to be used to isolate unknown hosts. These User Groups are read from the wireless device and represent existing User Groups that have been configured on the wireless device.
13. Click **OK** to save the SSID configuration.

Settings

Field	Definition
SSID Name	Network name of the SSID configuration that includes all of the settings for the SSID, such as encryption method or VLANs.
Mapping Type	**Device Onboarding**—Indicates that this SSID Mapping will be used by known network users to register devices. **Guest Management**—Indicates that this SSID Mapping will be used by guests to access the network via a guest account.
Guest Template	Guest template that must be associated with a guest account in order for the guest to connect on this SSID.
RADIUS Secret	Encryption key used by the RADIUS server to send authentication information. The RADIUS secret must be the same in FortiNAC RADIUS settings, on the SSID configuration and on the device itself.
Access User Group	Name or number of the Network Access identifier where a known host or device will be placed, such as, User Group, VLAN ID or VLAN Name.
Isolation User Group	Name or number of the Network Access identifier, such as, User Group, VLAN ID or VLAN Name, for the Isolation VLAN where an unknown host or device will be placed.

Secure SSID for device onboarding

If this SSID requires a supplicant configuration on the connecting host, the supplicant configuration can be served to the host through an Open SSID. Add the supplicant configuration to one of your Open SSIDs.



Add SSID

SSID Name: XirrusXMSSecure

● Device Onboarding ○ Guest Management

XirrusXMSSecure RADIUS Configuration

Primary RADIUS: AuthServer1 New...

Secondary RADIUS:

Directory Group: All Directory Groups

Allowed Operating Systems:

☑ Windows ☑ Mac OS X ☑ iOS

☑ Android ☑ RIM ☑ Windows Mobile

Portal Configuration: Radio Conference

Access User Group: XAM-Access

Isolation User Group: XAM-Isolation

1. Click **System > Quick Start**.
2. Select **Network Settings > Network Devices** from the steps on the left.
3. Select a device in the Network Devices window.
4. Click the **Wireless Security** button at the bottom.
5. On the SSID Mappings dialog, click the **Add** button.
6. Click the drop-down arrow in the **SSID Name** field and select the Name of the SSID to be mapped. These names are read from the wireless device and represent existing SSID configurations on the device.
7. Click the **Device Onboarding** radio button to select it.
8. In the **Primary RADIUS** field select the RADIUS server that FortiNAC should use for authentication. If no RADIUS servers are configured, click the **New** button to add one. See Configure profiles on page 104.
9. In the **Secondary RADIUS** field select the RADIUS server to be used in the event that the Primary RADIUS cannot be accessed. This field is optional.
10. In the **Directory Group** field select a Directory Group. The connecting user must be a member of this directory group to access the SSID. If you are authenticating through RADIUS instead of LDAP, this option is hidden.
11. In the **Allowed Operating Systems** section select one or more operating systems. The connecting host must have one of these operating systems installed to connect to this SSID.
12. In the **Portal Configuration** field select the captive portal that should be presented to the user when the host connects to this SSID. If you are not using multiple portals or you do not have a specific portal for this group of guests, select Use Default.
13. In the **Access User Group** field select the production User Group to be used for hosts accessing the Secure SSID. These are read from the wireless device and represent existing User Groups that have been configured on the wireless device.
14. In the **Isolation User Group** field select the User Group to be used to isolate unknown hosts. These User Groups are read from the wireless device and represent existing User Groups that have been configured on the wireless device.
15. Click **OK** to save the SSID configuration.

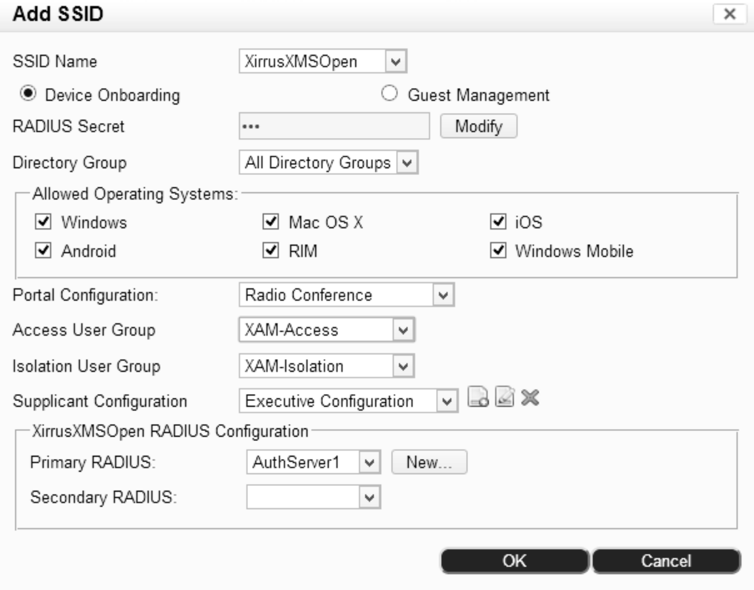
Settings

Field	Description
SSID Name	Network name of the SSID configuration that includes all of the settings for the SSID, such as encryption method or VLANs.

Field	Description
Mapping Type	**Device Onboarding**—Indicates that this SSID Mapping will be used by known network users to register devices. **Guest Management**—Indicates that this SSID Mapping will be used by guests to access the network via a guest account.
Primary RADIUS Server	RADIUS server that will be used by FortiNAC for authentication.
Secondary RADIUS Server	Secondary RADIUS server that will be used by FortiNAC for authentication if the Primary RADIUS server cannot be reached.
Directory Group	Connecting user must be a member of the selected directory group to access this SSID. If you are authenticating through RADIUS instead of LDAP, this option is hidden.
Allowed Operating Systems	Allows or denies access to an SSID based on the operating system of the connecting host. Options include: • Windows • macOS • iOS • Android • RIM • Windows Mobile
Portal Configuration	Name of the Portal that will be applied to hosts connecting via this SSID.
Access User Group	Name or number of the Network Access identifier where a known host or device will be placed, such as, User Group, VLAN ID or VLAN Name.
Isolation User Group	Name or number of the Network Access identifier, such as, User Group, VLAN ID or VLAN Name, for the Isolation VLAN where an unknown host or device will be placed.

Open SSID for device onboarding

If you have a Secure SSID that requires a supplicant configuration on the connecting host, the supplicant configuration can be served to the host through an Open SSID. Add the supplicant configuration to one of your Open SSIDs.



Add SSID

SSID Name: XirrusXMSOpen

● Device Onboarding ○ Guest Management

RADIUS Secret: ••• Modify

Directory Group: All Directory Groups

Allowed Operating Systems:

☑ Windows ☑ Mac OS X ☑ iOS

☑ Android ☑ RIM ☑ Windows Mobile

Portal Configuration: Radio Conference

Access User Group: XAM-Access

Isolation User Group: XAM-Isolation

Supplicant Configuration: Executive Configuration

XirrusXMSOpen RADIUS Configuration

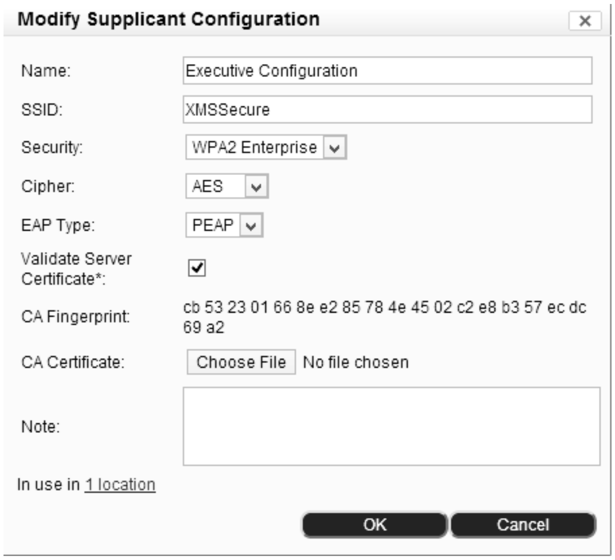
Primary RADIUS: AuthServer1 New...

Secondary RADIUS:

1. Click **System > Quick Start**.
2. Select **Network Settings > Network Devices** from the steps on the left.
3. Select a device in the Network Devices window.
4. Click the **Wireless Security** button at the bottom.
5. On the SSID Mappings dialog, click the **Add** button.
6. Click the drop-down arrow in the **SSID Name** field and select the Name of the SSID for which you are adding a configuration in the FortiNAC database. These names are read from the wireless device and represent existing SSIDs.
7. Click the **Device Onboarding** radio button to select it.
8. Click **Modify** next to the **RADIUS Secret field** and enter the RADIUS Secret configured on the device.
9. In the **Directory Group** field select a Directory Group. The connecting user must be a member of this directory group to access the SSID. If you are authenticating through RADIUS instead of LDAP, this option is hidden.
10. In the **Allowed Operating Systems** section select one or more operating systems. The connecting host must have one of these operating systems installed to connect to this SSID.
11. In the **Portal Configuration** field select the captive portal that should be presented to the user when the host connects to this SSID. If you are not using multiple portals or you do not have a specific portal for this group of guests, select Use Default.
12. In the **Access User Group** field select the production User Group to be used for hosts accessing the Secure SSID. These are read from the wireless device and represent existing User Groups that have been configured on the wireless device.
13. In the **Isolation User Group** field select the User Group to be used to isolate unknown hosts. These User Groups are read from the wireless device and represent existing User Groups that have been configured on the wireless device.

The Supplicant Configuration field is optional. If you select a Supplicant Configuration that configuration is installed on the connecting host, allowing the host to connect to a secure SSID. See the table below for settings and Supplicant configurations on page 476 for additional information.

14. Select a **Supplicant Configuration** from the drop-down menu. You can use the icons next to the Supplicant Configuration field to add a new configuration, delete a configuration or modify the configuration shown in the drop-down menu. Note that if you modify this configuration, it is modified for all features that make use of it.
15. To add a supplicant configuration, click the **Add** button next to the Supplicant Configuration field.



Modify Supplicant Configuration

Name: Executive Configuration

SSID: XMSSecure

Security: WPA2 Enterprise

Cipher: AES

EAP Type: PEAP

Validate Server Certificate*: ☑

CA Fingerprint: cb 53 23 01 66 8e e2 85 78 4e 45 02 c2 e8 b3 57 ec dc 69 a2

CA Certificate: Choose File No file chosen

Note:

In use in 1 location

16. In the **Name** field, enter a name for this Supplicant Configuration.
17. In the **SSID** field, select the SSID that requires that a Supplicant be installed and configured on the connecting host.
18. In the **Security** field select a type from the drop-down list. Options include: Open, WEP, WPA, WPA2, WEP Enterprise, WPA Enterprise, WPA2 Enterprise.
19. Click in the **Password** field to open the Password pop-up. This is the Pre-Shared Key. Enter the key twice to confirm that it is correct and click **OK**. The Password field does not display if Open, WPA2 Enterprise or WPA Enterprise is selected in the Security field.
20. Click in the **Cipher** field and select AES, NONE or TKIP.
21. In the **EAP Type** field PEAP is the only option. EAP type does not display when Open, WEP or WPA is selected in the Security field.
22. The **Validate Server Certificate** field applies only to Windows 7 and higher hosts:
    - If disabled, it disables the Validate Server Certificate setting on the host and any certificate will be accepted.
    - If enabled, the host validates the Certificate with the list of Trusted Root Certificate Authorities listed in the host's Certificate Manager. If the Certificate Authority is not listed on the host, the user may have to connect to the secure SSID manually.
23. If you have enabled WEP Enterprise, WPA Enterprise or WPA2 Enterprise the **CA Certificate** field is displayed. Browse to the CA or Root Certificate from the certificate authority that issued the SSL Certificate used on your RADIUS server. Select the file and click Open.
24. The **CA Fingerprint** field is displayed and automatically populated after a CA or Root Certificate is uploaded and the Supplicant Configuration is saved.
25. The **Note** field is optional.
26. Click **OK** to save the Supplicant Configuration.
27. In the **Primary RADIUS** field select the RADIUS server that FortiNAC should use for authentication. If no RADIUS servers are configured, click the **New** button to add one. Only displays if a Supplicant Configuration has been selected.

28. In the **Secondary RADIUS** field select the RADIUS server to be used in the event that the Primary RADIUS cannot be accessed. This field is optional.
29. Click **OK** to save the SSID configuration.

Open SSID settings

Field	Description
SSID Name	Network name of the SSID configuration that includes all of the settings for the SSID, such as encryption method or VLANs.
Mapping Type	• **Device Onboarding**—Indicates that this SSID Mapping will be used by known network users to register devices. • **Guest Management**—Indicates that this SSID Mapping will be used by guests to access the network via a guest account.
RADIUS Secret	Encryption key used by the RADIUS server to send authentication information. The RADIUS secret must be the same in FortiNAC RADIUS settings, on the SSID configuration and on the device itself.
Directory Group	Connecting user must be a member of the selected directory group to access this SSID. If you are authenticating through RADIUS instead of LDAP, this option is hidden.
Allowed Operating Systems	Allows or denies access to an SSID based on the operating system of the connecting host. Options include: • Windows • macOS • iOS • Android • RIM • Windows Mobile
Portal Configuration	Name of the Portal that will be applied to hosts connecting via this SSID.
Access User Group	Name or number of the Network Access identifier where a known host or device will be placed, such as, User Group, VLAN ID or VLAN Name.
Isolation User Group	Name or number of the Network Access identifier, such as, User Group, VLAN ID or VLAN Name, for the Isolation VLAN where an unknown host or device will be placed.
Supplicant Configuration	Contains the configuration for the SSID, Security Settings and password if required. This is optional. See the table below and Supplicant configurations on page 476.
Primary RADIUS Server	RADIUS server that will be used by FortiNAC for authentication. Only displays if a Supplicant Configuration has been selected.
Secondary RADIUS Server	Secondary RADIUS server that will be used by FortiNAC for authentication if the Primary RADIUS server cannot be reached.

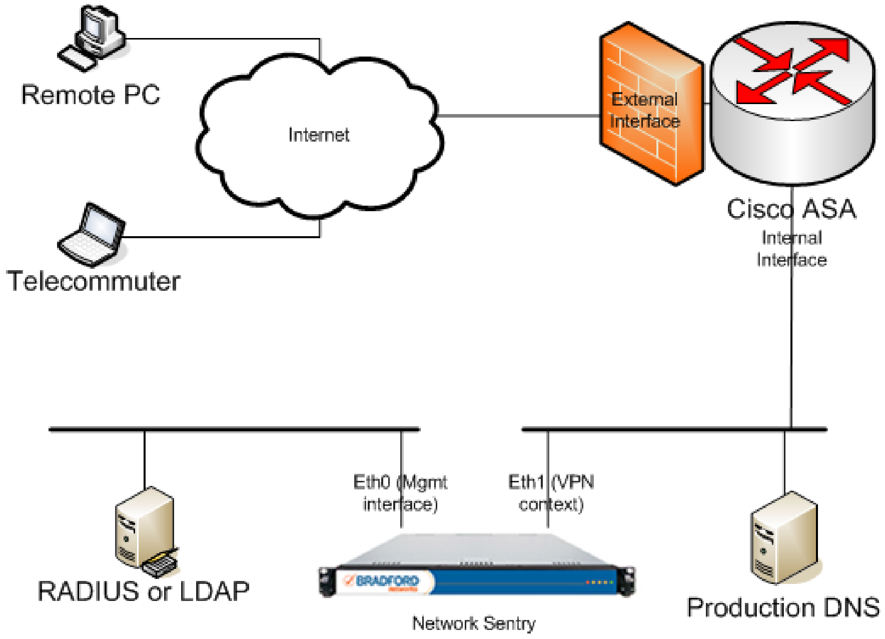
Supplicant configuration settings

Field	Definition
Name	User defined name for the Configuration.
SSID	Name of the SSID being configured. This is not necessarily the SSID to which the host is connected. However, the agent will attempt to move the host to this SSID when the configuration is applied. A host can have Supplicant Configurations stored for multiple SSIDs.
Security	Indicates the type of encryption that will be used for connections to this SSID. Options include: • Open • WEP (PSK) • WPA (PSK) • WPA2 (PSK) • WEP Enterprise (PEAP) • WPA Enterprise (PEAP) • WPA2 Enterprise (PEAP) WPA Enterprise and WPA2 Enterprise are limited to PEAP-MSCHAPv2.
Password	Opens the Password pop-up. This is the Pre-Shared Key. Enter the key twice to confirm that it is correct and click **OK**. The Password field does not display if Open, WPA2 Enterprise or WPA Enterprise is selected in the Security field. The XML predefined characters **' " < > &** are not supported.
Cipher	Encryption/decryption method used in conjunction with the information in the Security field to secure this connection. Options include: • AES • NONE • TKIP
EAP Type	Currently only PEAP is supported.

Field	Definition
Validate Server Certificate	Applies only to Windows 7 and higher hosts. Default = Disabled. If disabled, it disables the Validate Server Certificate setting on the host and any certificate will be accepted. If enabled, the host validates the Certificate with the list of Trusted Root Certificate Authorities listed in the host's Certificate Manager. If the Certificate Authority is not listed on the host, the user may have to connect to the secure SSID manually.
CA Fingerprint	Fingerprint parsed from the CA or Root Certificate from the certificate authority that issued the SSL Certificate used to secure the RADIUS server. This field does not display until after the certificate has been uploaded and the Supplicant Configuration has been saved.
CA Certificate	This field is only displayed if you select WEP Enterprise, WPA Enterprise or WPA2 Enterprise in the Security field. Use the **Choose File** button to browse to and select the CA or Root certificate from the certificate authority that issued the SSL Certificate used to secure the RADIUS server. CA or Root certificates can be downloaded from the certificate authority web site. Either PEM or binary format can be used.
Note	User specified note field.

VPN integration

VPN technologies allow you to securely extend your private network into the public domain. Network users can connect to your network from anywhere on the Internet. FortiNAC can identify and control access for users who connect to your network through a VPN. Once a user has connected to the network and been authenticated, that user can work on the network as if he were inside one of your buildings.



Requirements

This solution does not work in an environment using Cisco Dynamic Access Policies (DAP).

A FortiNAC agent (Persistent or Dissolvable) must be used when enforcing access policies on VPN clients.

If you plan to use a VPN device to allow users to connect to your network, the following requirements must be met:

VPN requirements

- Remote clients connecting to the network through a FortiNAC-managed VPN cannot be connected to a local network that is also being managed by FortiNAC within the same management domain.
- The VPN access device must be a Cisco ASA running firmware version 8.0(4) or higher.
- The VPN connection can be either IPsec or SSL. FortiNAC supports IPsec or SSL tunnel types with the condition that the host receives an IP address from a pool defined on the VPN device.
- The VPN users that you choose to manage with FortiNAC must be authenticated by the VPN using RADIUS or LDAP. FortiNAC must be configured as the RADIUS Server to authenticate those users.
- If you are setting up FortiNAC as the RADIUS server for a device in a Fortinet High Availability environment, you must use the actual IP address of the primary control server, not the Shared IP address. Set up the secondary control server as a secondary RADIUS server using its actual IP address. Regardless of the environment, you may also want to set up your actual RADIUS server to be used in the event that none of your FortiNAC appliances can be reached. This would allow users to access the network, but they would not be controlled by FortiNAC.
- The RADIUS secret must be the same in the VPN configuration, in the FortiNAC RADIUS Server configuration and in the FortiNAC VPN model configuration.

For detailed requirements,

> If you are using Cisco AnyConnect VPN software and a MacOS client with FortiNAC, make sure that the Web Security and Posture settings are both disabled. Otherwise, the AnyConnect software will not work with FortiNAC.

FortiNAC requirements

- In the Configuration Wizard you must configure the VPN context. Assign the VPN context an IP address and relevant subnet mask. The VPN DHCP scope(s) must match the IP Pools that are configured on the VPN. See the *Appliance Installation Guide* for instructions on running the Configuration Wizard.
- To authenticate VPN network users, FortiNAC must have either a RADIUS server or a directory configured. See RADIUS on page 102 or Configuration on page 82.
- Create a default VPN policy that will assign the appropriate agent to the VPN user.
- The VPN device must be modeled and correctly configured in FortiNAC.
- Security scans used for hosts that connect through VPN must not have Force DHCP enabled under the detailed settings for specific operating systems. For example, if you have modified the settings associated with Windows 2000 and you have enabled Force DHCP in the profile for Windows 2000, VPN clients will not be able to maintain their VPN connection.
- (Optional) Users connecting to the network through the VPN device are assigned a Tunnel Group Policy that controls network access. You can use FortiNAC Network Access Policies to assign a group policy as long as the new IP address is part of the same IP Pool as the one assigned by the original group policy. See Network access policies on page 407 for additional information.

Host requirements

- The host must have a FortiNAC agent installed when connecting via a VPN. Users can either have the Persistent Agent installed on their hosts or they can download and run the Dissolvable Agent each time they connect to the network using the VPN device. Mobile devices can install the Mobile Agent. The FortiNAC administrator determines which agent to provide and creates a Security Policy to distribute that agent.

If you choose to provide the Dissolvable Agent to your users, it is recommended that you disable split-tunneling for the tunnel group policy used to govern connected users. This ensures that the user’s browser is automatically redirected to the URL where they can download the run-once agent.

Operating systems that cannot run an agent cannot connect via a VPN when that connection is managed by FortiNAC. Operating systems such as Windows (not Windows CE), MAC OS and Linux can run an agent. Mobile devices running Android can run the Mobile Agent and connect via VPN. Typically smart phones and hand held devices cannot run agents and therefore are not allowed to connect via a VPN tunnel managed by FortiNAC. Refer to the release notes for additional information on specific versions of operating systems that are supported.

Due to unsupported features by the vendor, mobile devices running iOS cannot connect through VPN.

Configuration

FortiNAC has several configuration requirements when integrating with a VPN device.

Device integration

The VPN device must be added to the Topology View and must be modeled and configured. See Add or modify a pingable device on page 725 to add the VPN device to Topology.

Agent

FortiNAC identifies the remote PC through the agent running on that PC at connection time. If no agent is running, FortiNAC cannot identify the PC. Users can run the Persistent Agent, the Mobile Agent or the Dissolvable Agent, depending on which one the FortiNAC administrator has chosen. The Persistent Agent is installed on the user's PC and remains there, communicating with FortiNAC whenever the PC is on the network.

The Mobile Agent is installed on a handheld device running Android and remains there, communicating with FortiNAC whenever the device is on the network.

Due to unsupported features by the vendor, mobile devices running iOS cannot connect through VPN.

The Dissolvable Agent must be downloaded and installed every time the user connects to the network. After scanning the user's PC and reporting results to FortiNAC, the agent removes itself. If you choose to use the Dissolvable Agent, it is recommended that you send users to the download location through DNS and URL redirection.

Endpoint compliance policy

Endpoint Compliance Policies are used to deliver agents and scan hosts when they connect to the network. You must set up at least one default policy for VPN connections and indicate which agent should be presented to the user for download. Users who have an agent permanently installed on their hosts, would not have to download another agent, but would simply be scanned based on the rules of the VPN Endpoint Compliance Policy. See Endpoint compliance policies on page 415.

Network access policy (optional)

Using Network Access Policies with the VPN device is optional. The VPN connection profile configured on the user's PC refers to a specific Tunnel Group. The Group Policy associated with that Tunnel Group controls network access for the user. All users with the same VPN connection profile will have the same level of access. In order to provide different levels of access for different users, you either must provide separate VPN profiles or you must use Network Access Policies.

If you choose to use Network Access Policies, you would set it up as follows:

- Create multiple Tunnel Group Policies on the VPN device with the levels of network access required.
- Place the VPN device in a Device Group in FortiNAC.
- In Network Access Policies create a separate User/Host Profile for each level of access, such as Staff and Executives and use the VPN Device Group as the connection location.
- Create a separate Network Access Configuration for each VPN Tunnel Group Policy and place the appropriate Group Policy name in the Access Value/VLAN field.
- Create Network Access Policies to Map User/Host Profiles to Network Access Configurations
- The IP Pool for the group policy associated with the role must be the same as the IP Pool for the default group policy.
- Make sure each user and associated host are will match one of the User/Host Profiles.

When a user connects to the VPN device and the authentication request is sent to FortiNAC, FortiNAC returns the appropriate Group Policy in the response to the authentication request based on the User/Host Profile. See Network access policies on page 407.

Address VPN connection delays

If the VPN user's session has been set up, and the user opens a browser and gets the wrong portal page (e.g., the normal Registration page rather than the VPN portal page), follow this process. Also use this process to improve the host experience, where SSL VPN could cause a significant delay (from the time a VPN client connects, and downloads and installs the AnyConnect VPN Client).

The remoteAccessDB.properties file on the FortiNAC appliance contains the configuration for controlling remote access to your network. The remoteAccessDB.properties file is located in the following directory on your FortiNAC Server or Control Server: /bsc/campusMgr/master_loader/properties_plugin

Properties files stored in the properties_plugin directory are overwritten during upgrades. Therefore, modifications to those files should be done in .masterPropertyFile which is never overwritten. Entries in the .masterPropertyFile file are written to the appropriate properties files when the FortiNAC software is restarted.

1. Go to the CLI on your FortiNAC Server or Control Server.
2. Navigate to the `/bsc/campusMgr/master_loader directory`.

3. Use an editor such as VI to open the .masterPropertyFile file.
4. At the top of the file there is a sample entry that is commented out. Follow the syntax of the sample entry to create your own changes. There are two attributes that can be modified, Idle time and read attempts. The example shown below contains the defaults. Increase the values as needed.

   ```
   FILE_NAME=./properties_plugin/remoteAccessDB.properties
   {
   com.bsc.plugin.remote.RemoteAccessServer.remoteArpIdleTime=10
   com.bsc.plugin.remote.RemoteAccessServer.maxReadAttempts=12
   }
   ```

   `remoteArpIdleTime` sets the time (in sec) to wait before processing an ARP request from the ASA looking for an IP address assignment for a newly authenticated user. The time between user authentication and IP address assignment can vary on the ASA depending on the type of VPN software being used on the remote client.

   `maxReadAttempts` - Because the time it takes for a remote client to receive an IP from the ASA after authentication can be variable, it may exceed the configured `remoteArpIdleTime`. This value indicates how many subsequent attempts will be made to read the IP address from the device.
5. Save the changes to the file.
6. Restart FortiNAC using the following command: `restartCampusMgr`
7. From the CLI navigate to: `/bsc/campusMgr/master_loader/properties_plugin`
8. Display the contents of the `remoteAccessDB.properties` file to make sure the changes have been written correctly.

Troubleshooting

If you are experiencing problems with the VPN device and users managed by FortiNAC, check the following:

1. Make sure that an IP pool has been configured on the VPN. This pool represents the scope set up in the Configuration Wizard and used by FortiNAC to control users access levels.
2. Ensure static route is defined to send traffic to FortiNAC from the VPN device.
3. The FortiNAC Application server should always be able to communicate via SSH or Telnet to control connecting hosts.

> The ACLs and routes must be defined to enable users on that network to access the FortiNAC VPN interface.

4. Ensure that SNMP read/write community strings are setup on the VPN device to facilitate device discovery.
5. Ensure that telnet or SSH is enabled on the VPN device.
6. Ensure that the RADIUS secret is the same on the VPN device, the FortiNAC RADIUS server configuration and the FortiNAC model configuration for the VPN device.
7. Make sure to use a privileged administrator account when creating the device model in FortiNAC. The VPN device restricts command line access to all other accounts.

View hosts

When hosts connect through a VPN device managed by FortiNAC, they may or may not be modeled as FortiNAC hosts. If a FortiNAC agent running on the remote host has not identified the host to FortiNAC, then that host cannot be identified as a host in FortiNAC. You can view the connected hosts by selecting the VPN User Table option available from the device specific menu. Enter information into the filter fields to narrow the results and locate specific hosts.

1. Click **Network Devices > Topology**.
2. Expand the container icon where the VPN device is modeled and double-click the VPN device.
3. Select the device specific name, then click the **VPN User Table** option.
4. A list of the connected VPN hosts is displayed.

You can filter the list of hosts by entering information into the filter parameters. Single characters or partial strings may be used as wildcards. For example, entering Bob in the User Name field returns records with Bob Smith, Bobby Jones, Bob Johnson, etc.

VPN users can be filtered by any combination the following fields: User Name, MAC Address, IP address, Session ID, Group or Protocol.

REST API

FortiNAC's REST API provides a powerful yet standardized method for other systems to interact with FortiNAC, leverage data from the FortiNAC database and add or remove users and hosts. Each resource in the REST API is identified by a named URL, and is accessed using standard HTTP methods (HEAD, GET, POST, PATCH, DELETE). Using REST API you can:

- Retrieve detailed information about an element such as a Host or a User.
- Query the database for a list of items.
- Update User or Host records.
- Block a host's access to the network or unblock access to the network.

Request parameters and response values are case sensitive.

Overview

- Requires firmware version 3.x or higher (CentOS).
- Connect to the FortiNAC Server or Control Server using a browser.
- Authenticate using an Admin User account. This should be set up in advance through the Admin User Interface. See Admin users on page 683.
- Currently only XML is supported.
- Review the list of API URLs that can be accessed. See API URLs on page 1009.

Authentication

1. To use the API you must connect to the FortiNAC Server or Control Server and authenticate. Open a browser and type the following: `https://<servername>:8443/api`

   Example: `https://qa228:8443/api`
2. A warning is displayed indicating that the site's security certificate is not trusted. This is because a self-signed certificate is being used. Click Proceed anyway to continue.
3. An authentication dialog is displayed. Enter the user name and password for the Admin you configured under Admin Users and click OK to continue.
4. The service document is displayed. You are now authenticated and connected to the FortiNAC REST API. From here you can do queries.

   To add or delete record you must use an API tool, such as RESTClient.

API URLs

Below is a list of the API URLs that can be accessed for FortiNAC.

Function	Method	API URL
Alarm details		
Alarm Information	GET	https://<servername>:8443/api/alarm?tag={tag}
Alarm Information by ID	GET	https://<servername>:8443api/alarm/{id}
Alarm actions		
Acknowledge Alarm	POST	https://<servername>:8443/api/alarm/acknowledge/{dbid}
Control details		
Get Control Tasks	GET	https://<servername>:8443/api/control
Control Information – by ID	GET	https://<servername>:8443/api/control/{dbid}
Control Information – by Host	GET	https://<servername>:8443/api/control/host/{hostId}
Control Information – by IP	GET	https://<servername>:8443/api/control/ipaddress/{ip}
Active Control Information	GET	https://<servername>:8443/api/control/active
Active Control Info - by IP	GET	https://<servername>:8443/api/control/active/ipaddress/{ip}
Active Control Info - by Host	GET	https://<servername>:8443/api/control/active/host/{hostId}
Inactive Control Information	GET	https://<servername>:8443/api/control/inactive

Function	Method	API URL
Inactive Control Information - by IP	GET	https://<servername>:8443/api/control/inactive/ipaddress/{ip}
Inactive Control Information - by Host	GET	https://<servername>:8443/api/control/inactive/host/{hostId}
Control Task Information	GET	https://<servername>:8443/api/control/{dbid}tasks
Control actions		
Add Control Task by IP	POST	https://<servername>:8443/api/control/ipaddress **Accepted Content-type:** application/x-www-form-urlencoded **Form Parameters:** IP address: ip Control Action: action Duration: duration
Add Control Task by MAC Address	POST	https://<servername>:8443/api/control/macaddress **Accepted Content-type:** application/x-www-form-urlencoded **Form Parameters:** MAC Address: mac Control Action: action Duration: duration
Add Control Task by Endpoint	POST	https://<servername>:8443/api/control/endpoint **Accepted Content-type:** application/x-www-form-urlencoded **Form Parameters:** ID: id Control Action: action Duration: duration
Undo Control Task	POST	https://<servername>:8443/api/control/undo/{dbid} **Accepted Content-type:** application/x-www-form-urlencoded **Form Parameters:** IP address: ip Control Action: action Duration: duration

Function	Method	API URL
Delete Control Task	DELETE	https://<servername>:8443/api/control/{id}
Scan Control Task	POST	https://<servername>:8443/api/control/scan/{id}
Device profile actions		
Register Profiled Devices	POST	https://<servername>:8443/api/deviceprofiler/profiled/register/{id}
Delete Profiled Device	DELETE	https://<servername>:8443/api/deviceprofiler/profiled/{id}
Device profile details		
Profiled Devices	GET	https://<servername>:8443/api/deviceprofiler/profiled
Profile Device Identity	GET	https://<servername>:8443/api/deviceprofiler/identity/{id}
Device Profiling Rules	GET	https://<servername>:8443/api/deviceprofiler/rule
Device Profiling Rules by ID	GET	https://<servername>:8443/api/deviceprofiler/rule/{id}
Endpoint details		
Endpoint Information	GET	https://<servername>:8443/api/host/?offset={offset}&limit={limit} Default offset = 0 Default limit = 25 The following values can be appended to the end of the URL to further filter the results: id, createTime, hardwareType, hostName, owner, loggedOnUserId, os, connected, notes, ipAddress, macAddress, location, orderby, direction, role, atRisk, enabled, deviceType, serialNumber, limit, offset **Example:** https://<servername>:8443/api/host/?hardwareType=mobile&connected=true
Endpoint Information - by ID	GET	https://<servername>:8443/api/host/{id} The following values can be appended to the end of the URL to further filter the results: role, atRisk, enabled, deviceType, serialNumber **Example:**

Function	Method	API URL
		https://<servername>:8443/api/host/3717/"enabled":true,"role":null,"atRisk": false,"deviceType":"Rogue","serialNumber":null
Endpoint Information - by IP	GET	https://<servername>:8443/api/host/ipaddress/{ip}
Endpoint Information - by MAC	GET	https://<servername>:8443/api/host/macaddress/{mac}
Endpoint Adapters Information	GET	https://<servername>:8443/api/host/{dbid}/adapters
Endpoint Adapter Information - by Adapter	GET	https://<servername>:8443/api/host/adapter/{adapterID}
Network Port Information - by Adapter	GET	https://<servername>:8443/api/host/adapter/{adapterID}/port
Network Device Information - by Endpoint	GET	https://<servername>:8443/api/host/dbid/device
Endpoint actions		
Add Modify Endpoint	POST	https://<servername>:8443/api/host/update **Accepted Content-type:** application/x-www-form-urlencoded **Form Parameters:** Username: userID Hostname: hName Operating System: os IP address: ip MAC Address: mac MAC Address is required to uniquely identify the endpoint. If the MAC Address exists in the database, the record is updated. If the MAC Address does not exist in the database a new endpoint record is created. The following values can be appended to the end of the URL to further filter the results: notes, hwType, role, enabled, serialNumber Example: https://&lt;servername&gt;:8443/api/host/update/"hardwareType":null, "connected":false,"enabled":false,"role":"MyNewRole","serialNumber":null

Function	Method	API URL
Bulk Add Modify Endpoint	POST	https://<servername>:8443/api/host/bulkupdate
Delete Endpoint	DELETE	https://<servername>:8443/api/host/{id}
Event details		
Retrieve Events	GET	https://<servername>:8443/api/event
Group details		
Retrieve Groups	GET	https://<servername>:8443/api/group
Group actions		
Update Group	POST	https://<servername>:8443/api/group
Delete Group	DELETE	https://<servername>:8443/api/group/{id}
Network details		
Network Device Information	GET	https://<servername>:8443/api/network/device/?offset={offset}&limit={limit} Default offset = 0 Default limit = 25 The following values can be appended to the end of the URL to further filter the results: id, name, hardwareType, ipAddress, description, sysOid, orderby, direction **Example:** https://<servername>:8443/api/network/device/?hardwareType=mobile&connected=true
Network Device Information - by ID	GET	https://<servername>:8443/api/network/device/{dbid}
Network Device Ports Information	GET	https://<servername>:8443/api/network/device/{dbid}/ports
Network Device Port Information - by ID	GET	https://<servername>:8443/api/network/device/port/{dbid}

Function	Method	API URL
Endpoint Information - by Port	GET	https://<servername>:8443/api/network/device/port/{dbid}/hosts
Endpoint Information - by Device	GET	https://<servername>:8443/api/network/device/{dbid}/hosts
Scheduler details		
Scheduled Tasks	GET	https://<servername>:8443/api/scheduler
Scheduled Task by ID	GET	https://<servername>:8443/api/scheduler/{id}
Scheduler actions		
Run Scheduled Tasks	POST	https://<servername>:8443/api/scheduler/run/{id}
User details		
User Information	GET	https://<servername>:8443/api/user/?offset={offset}&limit={limit} Default offset = 0 Default limit = 25 The following values can be appended to the end of the URL to further filter the results: id, userid, firstName, lastName, address, city, state, zipcode, phone, email, mobilephone, mobileprovider, orderby, direction, role **Example:** https://<servername>:8443/api/user?city=concord&state=nh
User Information - by ID	GET	https://<servername>:8443/api/user/{dbid} The following values can be appended to the end of the URL to further filter the results: id, userid, firstName, lastName, address, city, state, zipcode, phone, email, mobilephone, mobileprovider, orderby, direction, role
User Information - by User ID	GET	https://<servername>:8443/api/user/userid/{userid} id, userid, firstName, lastName, address, city, state, zipcode, phone, email, mobilephone, mobileprovider, orderby, direction, role
User actions		
Add Modify User	POST	https://<servername>:8443/api/user/update **Accepted Content-type:** application/x-www-form-urlencoded **Form Parameters:** Username: userID

Function	Method	API URL
		First Name: fName Last Name: lName User Type: type (values are User or Administrative, with User being the default) Email Address: email Admin Profile: adminProfile (enter the name of the admin profile) The userID parameter is required to uniquely identify the User. If the userID exists in the database, the record is updated. If the userID does not exist in the database a new User record is created. Role: role
Delete User	DELETE	https://<servername>:8443/api/user/{id}
Network containers		
Container Information	GET	https://<servername>:8443/api/network/domain?offset={offset}&limit={limit} Default offset = 0 Default limit = 25
Container Information - by ID	GET	https://<servername>:8443/api/network/domain/{dbid}
Container Information - by Name	GET	https://<servername>:8443/api/network/domain/name/{name}
Network Devices by Container ID	GET	https://<servername>:8443/api/network/domain/{dbid}/devices
Network container actions		
Add Container	POST	https://<servername>:8443/api/network/domain/update **Accepted Content-type:** application/x-www-form-urlencoded **Form Parameters:** Name: name The name parameter is required to uniquely identify the container. If the name does not exist in the database a new Container record is created.
SNMPv1 Discovery	POST	https://<servername>:8443/api/network/domain/ discovery/snmpV1 **Accepted Content-type:** application/x-www-form-urlencoded **Form Parameters:** Name: name Starting IP address: startIP Ending IP address: endIP Security String: security

Function	Method	API URL
		The name parameter is required to uniquely identify the container where discovery should be run. If the name exists in the database discovery is done for the selected container.
SNMPv1 CDP Discovery	POST	https://<servername>:8443/api/network/domain/ discovery/snmpV1/cdp **Accepted Content-type:** application/x-www-form-urlencoded **Form Parameters:** Name: name Starting IP address: startIP Security String: security The name parameter is required to uniquely identify the container where discovery should be run. If the name exists in the database discovery is done for the selected container. When using CDP discovery it is recommended that you set the Maximum Cisco Discovery Depth in the FortiNAC Admin UI to limit the number of levels searched from the starting IP address. If this setting is not enabled, discovery may take an extensive amount of time.
SNMPv3 Discovery	POST	https://<servername>:8443/api/network/domain/ discovery/snmpV3 **Accepted Content-type:** application/x-www-form-urlencoded **Form Parameters:** Name: name Starting IP address: startIP Ending IP address: endIP User name: user Authentication Password: password Privacy Password: privacy Authentication Protocol: authProto Privacy Protocol: privProto The name parameter is required to uniquely identify the container where discovery should be run. If the name exists in the database discovery is done for the selected container.
SNMPv3 CDP Discovery	POST	https://<servername>:8443/api/network/domain/ discovery/snmpV3/cdp **Accepted Content-type:** application/x-www-form-urlencoded **Form Parameters:** Name: name Starting IP address: startIP User name: user Authentication Password: password Privacy Password: privacy Authentication Protocol: authProto Privacy Protocol: privProto

Function	Method	API URL
		The name parameter is required to uniquely identify the container where discovery should be run. If the name exists in the database discovery is done for the selected container. When using CDP discovery it is recommended that you set the Maximum Cisco Discovery Depth in the FortiNAC Admin UI to limit the number of levels searched from the starting IP address. If this setting is not enabled, discovery may take an extensive amount of time.
Vendor OUI details		
Vendor OUIs	GET	https://<servername>:8443/api/vendoroui
Vendor OUI by ID	GET	https://<servername>:8443/api/vendoroui/{id}

Alarms

Retrieve alarms.

```
https://<servername>:8443/api/alarmhttps://<servername>:8443/api/alarm?tag={tag}
```

Return Value	Type	Description
id	Integer	Alarm record ID
acknowledgedTime	Integer	Time of acknowledgement (zero if not acknowledged)
creationTime	Integer	Time alarm was created
name	String	Alarm severity
tag	String	Alarm tag
Element		
id	Integer	Element ID
Name	String	Element Name
Type	Integer	Element Type

Example Request

```
curl -k -u 'username:password' -H "accept: application/xml" -X GET
https://localhost:8443/api/alarm?limit=1\&tag=READ_CLIENTS_FAILURE
```

Example XML Format

```
<alarmSearchResult>
   <status>success</status>
   <limit>1</limit>
   <nextOffset>1</nextOffset>
   <offset>0</offset>
   <total>61</total>
   <alarms>
      <alarm>
         <acknowledgedTime>0</acknowledgedTime>
         <creationTime>1484546536473</creationTime>
         <element>
            <id>2886</id>
            <name>Aruba5000</name>
            <type>1</type>
         </element>
         <id>33757</id>
         <name>L2 Poll Failed</name>
         <severity>Critical</severity>
         <tag>READ_CLIENTS_FAILURE</tag>
      </alarm>
   </alarms>
</alarmSearchResult>
```

Specific alarm

Retrieve a specific alarm.

```
https://<servername>:8443/api/alarm/{id}
```

Return Value	Type	Description
id	Integer	Alarm record ID
acknowledgedTime	Integer	Time of acknowledgement (zero if not acknowledged)
creationTime	Integer	Time alarm was created
name	String	Alarm severity
tag	String	Alarm tag
Element		
id	Integer	Element ID
Name	String	Element Name
Type	Integer	Element Type

Example Request

```
curl -k -u 'username:password' -H "accept: application/xml" -X GET
https://localhost:8443/api/alarm/33757
```

Example XML Format

```
<alarmResult>
   <status>success</status>
   <alarm>
      <acknowledgedTime>0</acknowledgedTime>
```

```
        <creationTime>1484546536473</creationTime>
        <element>
           <id>2886</id>
           <name>Aruba5000</name>
           <type>1</type>
        </element>
        <id>33757</id>
        <name>L2 Poll Failed</name>
        <severity>Critical</severity>
        <tag>READ_CLIENTS_FAILURE</tag>
     </alarm>
  </alarmResult>
```

Acknowledge alarm

Acknowledges an alarm.

`https://<servername>:8443/api/alarm/acknowledge/{id}`

- Return Value: status

Example Request

```
curl -k -i -u '<username>:<password>' -X POST https://<servername>:8443/api/alarm
/acknowledge/29641
```

Example Response

```
SUCCESS
```

Containers - bulk

Displays a list of Containers.

`URL = https://<servername>:8443/api/network/domain?offset={offset}&limit={limit}`

Return Value	Type	Description
ID	Integer	ID that uniquely identifies the container.
Name	String	Name of the container.

Example XML format:

```
<networkDomainSearchResult>
<status>success</status>
<limit>25</limit>
    <networkDomains>
      <id>29</id>
      <name>qa</name>
```

```
   </networkDomains>
    <networkDomains>
      <id>619</id>
      <name>test</name>
   </networkDomains>
<nextOffset>0</nextOffset>
<offset>0</offset>
<total>2</total>
</networkDomainSearchResult>
```

Specific container

Display a specific container

`URL = https://<servername>:8443/api/network/domain/{dbid}`

`URL = https://<servername>:8443/api/network/domain/name/{name}`

Return Value	Type	Description
ID	Integer	ID that uniquely identifies the container.
Name	String	Name of the container.

Example XML format:

```
<networkDomainResult>
<status>success</status>
   <networkDomains>
      <id>1362</id>
      <name>Pingables</name>
   </networkDomains>
</networkDomainResult>
```

Control tasks

Perform tasks that modify port state or host network access.

`URL = https://<servername>:8443/api/control`

`URL = https://<servername>:8443/api/control/{taskid}`

`URL = https://<servername>:8443/api/control/host/{hostid}`

`URL = https://<servername>:8443/api/control/ipaddress/{ip}`

`URL = https://<servername>:8443/api/control/macaddress/{mac}`

`URL = https://<servername>:8443/api/control/active`

`URL = https://<servername>:8443/api/control/active/ipaddress/{ip}`

`URL = https://<servername>:8443/api/control/active/host/{hostid}`

```
URL = https://<servername>:8443/api/control/inactive
URL = https://<servername>:8443/api/control/inactive/ipaddress/{ip}
URL = https://<servername>:8443/api/control/inactive/host/{hostid}
```

Return value	Type	Description
action	String	The control action to take • Port – Port State • Access – Host Denied
createTime	Time	Date and time that this task was created.
duration	Integer	Time in seconds to perform the task. 0 indicates an unlimited duration, and requires manual intervention to undo.
endpointId	Integer	ID that uniquely identifies the host.
id	Integer	ID that uniquely identifies the task.
Inactive Time	Time	Date and time that this task was made inactive.
ipaddress	String	IP address of the host, such as “192.168.1.1”.
status	String	Status of the task: • active -Task is accepted. • undo - Undo the task. • noHost - No host found. • invalidAction - Action is not recognized by FortiNAC. • systemError - FortiNAC cannot process the task. • taskExists - The same task has already been sent.

Example request

```
curl -k -u '<username>:<password>' -H "accept: application/xml" -X POST -d
'ip=192.168.10.182' -d'action=atrisk' -d'duration=60'
https://<servername>:8443/api/control/ipaddress
```

Example XML format:

```
<controlTaskResult>
<status>success</status>
   <controlTasks>
      <id>24</id>
      <action>atrisk</action>
      <createTime>2017-01-26T11:42:19-05:00</createTime>
      <duration>60</duration>
      <endpointId>1274</endpointId>
      <status>active</status>
   </controlTasks>
</controlTaskResult>
```

Control task items

Change VLANs, turn a port on or off, control port security, send a CLI command on a device.

`URL = https://<servername>:8443/api/control/{id}/tasks`

Return value	Type	Description
Action	String	The control action to take • VLAN– VLAN Change • Port State – ON / OFF • Port Security • CLI
Create Time	Time	Date and time that this task was created.
Element Name	String	Element description
Element Type	String	Type of connection: • Wired • Wireless
ID	Integer	ID that uniquely identifies the network element.
DBID	Integer	ID that uniquely identifies the task.
Inactive Time	Time	Date and time that this action was undone.
IP address	String	IP address of the network element, such as “192.168.1.1”.
Status	String	Status of the task: • NotBlocking • BlockingByVLAN • BlockingByMacFiltering • BlockingByPortCLI • BlockingByIPCLI • BlockingByWireless • unDo

Example XML format:

```
<controlTaskItemResult>
<status>success</status>
   <controlTaskItems>
      <action>BlockByVLAN</action>
      <createTime>2013-07-02T10:49:21-04:00</createTime>
      <elementName>Concord-3750 Fa4/0/34</elementName>
      <elementType>Wired</elementType>
      <id>5</id>
      <inactiveTime>2013-07-02T11:11:19-04:00</inactiveTime>
      <ipAddress>192.168.10.1</ipAddress>
      <networkPortId>535</networkPortId>
      <status>unDo</status>
   </controlTaskItems>
</controlTaskItemResult>
```

Control task - scan by endpoint ID

Scan by endpoint ID.

`URL = https://<servername>:8443/api/control/scan/{id}`

Return values:

- Status: status
- Message: errorMessage

Example request

```
curl -k -u '<username>:<password>' -H "accept: application/xml" -X POST
https://<servername>:8443/api/control/scan/18
```

Example XML format

```
<scanResult>
   <status>success</status>
   <errorMessage></errorMessage>
</scanResult>
```

Device identities

Retrieve device identities.

`https://<servername>:8443/api/deviceprofiler/identity`

`https://<servername>:8443/api/deviceprofiler/identity?macAddress={mac}`

Return value	Type	Description
id	Integer	Device Identity record ID
createTime	Integer	Time fingerprint was created
lastHeardTime	Integer	Time fingerprint was last heard
messageType	String	Message Type
parameterList	String	List of DHCP Parameters
optionList	String	DHCP Option List
physAddress	String	MAC Address
operatingSystem	String	Operating System
timeToLive	String	Time To Live
deviceIdentity	String	Device Identity

Example request

```
curl -k -u 'username:password' -H "accept: application/xml" -X GET
https://localhost:8443/api/deviceprofiler/identity?macAddress=00:0B:86:C0:1A:76
```

Example XML format

```
<fingerprintSearchResult>
   <status>success</status>
   <limit>1</limit>
   <nextOffset>1</nextOffset>
   <offset>0</offset>
   <total>917</total>
   <fingerprints>
      <fingerprint>
         <createTime><nanos>0</nanos></createTime>
         <deviceIdentity>
            <name>Wireless Access Point</name>
            <tag>WAP</tag>
         </deviceIdentity>
         <ID>1</ID>
         <lastHeardTime><nanos>0</nanos></lastHeardTime>
         <messageType>
            <id>1</id>
            <name>DHCP Fingerprinting</name>
            <shortName>DISCOVER</shortName>
         </messageType>
         <operatingSystem>Aruba</operatingSystem>
         <optionList>53,57,55</optionList>
         <parameterList>1,3,6,15</parameterList>
         <physAddress>00:0B:86:C0:1A:76</physAddress>
         <timeToLive>255</timeToLive>
      </fingerprint>
   </fingerprints>
</fingerprintSearchResult>
```

Specific device identity

Retrieve a specific device identity.

`https://<servername>:8443/api/deviceprofiler/identity/{id}`

Return value	Type	Description
id	Integer	Device Identity record ID
createTime	Integer	Time fingerprint was created
lastHeardTime	Integer	Time fingerprint was last heard
messageType	String	Message Type
parameterList	String	List of DHCP Parameters

Return value	Type	Description
optionList	String	DHCP Option List
physAddress	String	MAC Address
operatingSystem	String	Operating System
timeToLive	String	Time To Live
deviceIdentity	String	Device Identity

Example request

```
curl -k -u 'username:password' -H "accept: application/xml" -X GET
https://localhost:8443/api/deviceprofiler/identity/1
```

Example XML format

```
<fingerprintResult>
   <status>success</status>
   <fingerprint>
      <createTime><nanos>0</nanos></createTime>
      <deviceIdentity>
      <name>Wireless Access Point</name>
      <tag>WAP</tag>
      </deviceIdentity>
      <ID>1</ID>
      <lastHeardTime><nanos>0</nanos></lastHeardTime>
      <messageType>
         <id>1</id>
         <name>DHCP Fingerprinting</name>
         <shortName>DISCOVER</shortName>
      </messageType>
      <operatingSystem>Aruba</operatingSystem>
      <optionList>53,57,55</optionList>
      <parameterList>1,3,6,15</parameterList>
      <physAddress>00:0B:86:C0:1A:76</physAddress>
      <timeToLive>255</timeToLive>
   </fingerprint>
</fingerprintResult>
```

Profiled devices

Retrieve profiled devices.

```
https://<servername>:8443/api/deviceprofiler/profiled
```

Return value	Type	Description
deviceType	String	The type of the device determined by the profiling rule.

Return value	Type	Description
id	Long	The record ID
ipAddress	String	Primary IP address
ipAddresses	String	Alternate IP addresses
location	String	Location
macAddress	String	MAC Address
name	String	Host name
role	String	Role
rule		Matched Device Profiling Rule

Example request

```
curl -k -u 'username:password' -H "accept: application/xml" -X GET
https://localhost:8443/api/deviceprofiler/profiled?macAddress=08:00:27:2F:27:00
```

Example XML format

```
<profiledDevicesSearchResult>
   <status>success</status>
   <limit>25</limit>
   <nextOffset>1</nextOffset>
   <offset>0</offset>
   <total>1</total>
   <profiledDevices>
      <profiledDevice>
         <deviceType>Registered Host</deviceType>
         <id>3602</id>
         <ipAddress>192.168.35.55</ipAddress>
         <ipAddresses>192.168.35.55 (IPv4)</ipAddresses>
         <location>Dell-3324 Port 15</location>
         <macAddress>08:00:27:2F:27:00</macAddress>
         <name>Win7QA</name>
         <role>NAC-Default</role>
         <rule>
            <id>2</id>
            <name>Windows (DHCP)</name>
         </rule>
      </profiledDevice>
   </profiledDevices>
</profiledDevicesSearchResult>
```

Specific profiled devices

Retrieve a specific profiled device.

```
https://<servername>:8443api/deviceprofiler/profiled/{id}
```

Return value	Type	Description
deviceType	String	The type of the device determined by the profiling rule.
id	Long	The record ID
ipAddress	String	Primary IP address
ipAddresses	String	Alternate IP addresses
location	String	Location
macAddress	String	MAC Address
name	String	Host name
role	String	Role
rule		Matched Device Profiling Rule

Example request

```
curl -k -u 'username:password' -H "accept: application/xml" -X GET
https://localhost:8443/api/deviceprofiler/profiled/3602
```

Example XML format

```
<profiledDeviceResult>
   <status>success</status>
   <profiledDevice>
      <deviceType>Registered Host</deviceType>
      <id>3602</id>
      <ipAddress>192.168.35.55</ipAddress>
      <ipAddresses>192.168.35.55 (IPv4)</ipAddresses>
      <location>Dell-3324 Port 15</location>
      <macAddress>08:00:27:2F:27:00</macAddress>
      <name>Win7QA</name>
      <role>NAC-Default</role>
      <rule>
         <id>2</id>
         <name>Windows (DHCP)</name>
      </rule>
   </profiledDevice>
</profiledDeviceResult>
```

Register a profiled device

Registers a profiled device.

```
https://<servername>:8443/api/deviceprofiler/profiled/register/{id}
```

- Return value: status

Example request

```
curl -k -u '<username>:<password>' -X POST
https://<servername>:8443/api/deviceprofiler/profiled/register/3602
```

Example response

```
SUCCESS
```

Device profiling rules

Retrieve device profiling rules.

```
https://<servername>:8443/api/deviceprofiler/rule
```

Return value	Type	Description
type	String	The type to assign to hosts that match rule
notify	boolean	If true, notify sponsors
registerAutomatically	boolean	if true, automatically registers matched hosts
registerClient	boolean	if true, adds matched hosts to the Host View
registerToLoggedInUser	boolean	if true, register matched hosts to logged in user
role	String	The role to set when registering hosts that match rule
addToGroup	boolean	If true, adds matched hosts to a group
groupName	String	Group to add matched hosts to if addToGroup is true
addToContainer	boolean	If true, adds matched hosts to a domain
containerName	String	Container to add matched hosts to if addToContainer is true
enabled	boolean	
methods		Methods used to match rule
description	String	Description of the rule
sponsorNote	String	
weeklySchedule		Schedule for when rule should be enabled
reValidation	boolean	If true, Device Profiler confirms previously profiled devices still match rule
reValidationInterval	Integer	If set, Device Profiler confirms previously profiled devices still match rule at an interval
failedValidationAction		If set, action to take if profile devices no longer match rule

Example request

```
curl -k -u '<username>:<password>' -H "accept: application/xml" -X GET
https://localhost:8443/api/deviceprofiler/rule?limit=1
```

Example XML format

```
<deviceProfilingRuleSearchResult>
   <status>success</status>
   <limit>1</limit>
   <nextOffset>1</nextOffset>
   <offset>0</offset>
   <total>20</total>
   <rules>
      <rule>
         <id>1</id>
         <name>Mobile Device (DHCP)</name>
         <type>Mobile</type>
         <notify>false</notify>
         <registerAutomatically>false</registerAutomatically>
         <registerClient>false</registerClient>
         <registerToLoggedInUser>false</registerToLoggedInUser>
         <role>NAC-Default</role>
         <addToGroup>false</addToGroup>
         <groupName/>
         <addToDomain>false</addToDomain>
         <domainName/>
         <enabled>false</enabled>
         <methods>
            <dhcpMethodData>
               <enabled>true</enabled>
            </dhcpMethodData>
         </methods>
         <description></description>
         <sponsorNote></sponsorNote>
         <weeklySchedule>
            <alwaysOn>true</alwaysOn>
            <daysOfWeek>-1</daysOfWeek>
            <endTimeOfDay>-1</endTimeOfDay>
            <startTimeOfDay>-1</startTimeOfDay>
         </weeklySchedule>
         <reValidation>false</reValidation>
         <reValidationInterval>0</reValidationInterval>
         <failedValidationAction><disable>false</disable></failedValidationAction>
      </rule>
   </rules>
</deviceProfilingRuleSearchResult>
```

Specific device profiling rule

Retrieve specific device profiling rule.

```
https://<servername>:8443/api/deviceprofiler/rule/{id}
```

Return value	Type	Description
id	Integer	Device Profiling Rule record ID
name	String	User specified name for this rule
type	String	The type to assign to hosts that match rule
notify	boolean	If true, notify sponsors
registerAutomatically	boolean	if true, automatically registers matched hosts
registerClient	boolean	if true, adds matched hosts to the Host View
registerToLoggedInUser	boolean	if true, register matched hosts to logged in user
role	String	The role to set when registering hosts that match rule
addToGroup	boolean	If true, adds matched hosts to a group
groupName	String	Group to add matched hosts to if addToGroup is true
addToContainer	boolean	If true, adds matched hosts to a domain
containerName	String	Container to add matched hosts to if addToContainer is true
enabled	boolean	
methods		Methods used to match rule
description	String	Description of the rule
sponsorNote	String	
weeklySchedule		Schedule for when rule should be enabled
reValidation	boolean	If true, Device Profiler confirms previously profiled devices still match rule
reValidationInterval	Integer	If set, Device Profiler confirms previously profiled devices still match rule at an interval
failedValidationAction		If set, action to take if profile devices no longer match rule

Example request

```
curl -k -u '<username>:<password>' -H "accept: application/xml" -X GET
https://localhost:8443/api/deviceprofiler/rule/1
```

Example XML format

```
<deviceProfilingRuleResult>
   <status>success</status>
   <rule>
      <id>1</id>
      <name>Mobile Device (DHCP)</name>
      <type>Mobile</type>
      <notify>false</notify>
      <registerAutomatically>false</registerAutomatically>
      <registerClient>false</registerClient>
      <registerToLoggedInUser>false</registerToLoggedInUser>
      <role>NAC-Default</role>
      <addToGroup>false</addToGroup>
      <groupName/>
      <addToDomain>false</addToDomain>
      <domainName/>
      <enabled>false</enabled>
      <methods>
         <dhcpMethodData>
            <enabled>true</enabled>
         </dhcpMethodData>
      </methods>
      <description></description>
      <sponsorNote></sponsorNote>
      <weeklySchedule>
         <alwaysOn>true</alwaysOn>
         <daysOfWeek>-1</daysOfWeek>
         <endTimeOfDay>-1</endTimeOfDay>
         <startTimeOfDay>-1</startTimeOfDay>
      </weeklySchedule>
      <reValidation>false</reValidation>
      <reValidationInterval>0</reValidationInterval>
      <failedValidationAction><disable>false</disable></failedValidationAction>
   </rule>
</deviceProfilingRuleResult>
```

Endpoint

Retrieve endpoints.

`https://<servername>:8443/api/endpoint`

Return value	Type	Description
id	Integer	ID that uniquely identifies the endpoint.
createTime	Time	Date and time that this endpoint was created.
atRisk	Boolean	If true, endpoint has been marked at risk.
connected	Boolean	If true, Endpoint is connected.
enabled	Boolean	If true, endpoint is enabled
deviceType	String	Type of the endpoint, such as, an IP Phone.
ipAddress	String	List of IP addresses assigned to the interfaces on the endpoint separated by commas
macAddress	String	List of MAC addresses on the endpoint separated by commas
location	String	Name of the connection location, such as a port name.
hardwareType	String	Type of hardware, such as, a PC .
hostName	String	Host name of the endpoint.

Return value	Type	Description
loggedOnUser	String	User ID of the logged on user.
owner	String	User ID of the user to whom this endpoint is registered.
notes	String	Notes entered on the host record.
os	String	Operating System on the endpoint.
serialNumber	String	Serial Number of the endpoint.

Example request

```
curl -k -u '<username>:<password>' -H "accept: application/xml" -X GET
https://<servername>:8443/api/host?limit=1
```

Example XML format

```
<endpointSearchResult>
   <status>success</status>
   <limit>25</limit>
   <nextOffset>0</nextOffset>
   <offset>0</offset>
   <total>1</total>
   <endpoints>
      <endpoint>
         <atRisk>false</atRisk>
         <connected>true</connected>
         <createTime>2017-01-25T16:59:49.103-05:00</createTime>
         <deviceType>IP-Phone</deviceType>
         <enabled>true</enabled>
         <hardwareType></hardwareType>
         <hostName>host-1</hostName>
         <id>4218</id>
         <ipAddress>192.168.99.170</ipAddress>
         <location>Concord-3750 Fa2/0/29</location>
         <macAddress>00:22:90:59:CD:DF</macAddress>
         <notes>the quick brown fox</notes>
         <os>OS 1.2</os>
         <owner>Moe</owner>
         <role>Concord</role>
         <serialNumber>123456789</serialNumber>
      </endpoint>
   </endpoints>
</endpointSearchResult>
```

Specific endpoint

Display a specific endpoint.

`URL=https://<servername>:8443/api/endpoint/{id}`

`URL=https://<servername>:8443/api/endpoint/macaddress/{mac}`

```
URL=https://<servername>:8443/api/endpoint/ipaddress/{ip}
URL=https://<servername>:8443/api/network/device/port/{id}/hosts
URL=https://<servername>:8443/api/network/device/{id}/hosts
```

Return value	Type	Description
id	Integer	ID that uniquely identifies the endpoint.
createTime	Time	Date and time that this endpoint was created.
atRisk	Boolean	If true, endpoint has been marked at risk.
connected	Boolean	If true, endpoint is connected.
enabled	Boolean	If true, endpoint is enabled
deviceType	String	Type of the endpoint, such as, an IP Phone.
ipAddress	String	List of IP addresses assigned to the interfaces on the endpoint separated by commas
macAddress	String	List of MAC addresses on the endpoint separated by commas
location	String	Name of the connection location, such as a port name.
hardwareType	String	Type of hardware, such as, a PC .
hostName	String	Host name of the endpoint.
loggedOnUser	String	User ID of the logged on user.
owner	String	User ID of the user to whom this endpoint is registered.
notes	String	Notes entered on the host record.
os	String	Operating System on the endpoint.
serialNumber	String	Serial Number of the endpoint.

Example request

```
curl -k -u '<username>:<password>' -H "accept: application/xml" -X GET
https://<servername>:8443/api/host/4218
```

Example XML format:

```
<endpointSearchResults>
   <status>success</status>
   <limit>25</limit>
   <nextOffset>0</nextOffset>
   <offset>0</offset>
   <total>1</total>
   <endpoints>
      <endpoint>
         <atRisk>false</atRisk>
         <connected>true</connected>
         <createTime>2017-01-25T16:59:49.103-05:00</createTime>
         <deviceType>IP-Phone</deviceType>
```

```
            <enabled>true</enabled>
            <hardwareType></hardwareType>
            <hostName>host-1</hostName>
            <id>4218</id>
            <ipAddress>192.168.99.170</ipAddress>
            <location>Concord-3750 Fa2/0/29</location>
            <macAddress>00:22:90:59:CD:DF</macAddress>
            <notes>the quick brown fox</notes>
            <os>OS 1.2</os>
            <owner>Moe</owner>
            <role>Concord</role>
            <serialNumber>123456789</serialNumber>
         </endpoint>
      </endpoints>
   </endpointResult>
```

Endpoints - bulk

Display a list of endpoints.

`URL = https://<servername>:8443/api/endpoint`

Return value	Type	Description
Connected	Boolean	If true, endpoint is connected.
Create Time	Time	Date and time that this endpoint was created.
Hardware Type	String	Type of hardware, such as, a PC .
Host Name	String	Host name of the endpoint.
id	Integer	ID that uniquely identifies the endpoint.
IP address	String	List of IP addresses assigned to the interfaces on the endpoint separated by commas
Location	String	Name of the connection location, such as a port name.
Logged On User	String	User ID of the logged on user.
MAC Address	String	List of MAC addresses on the endpoint separated by commas
Notes	String	Notes entered on the host record.
OS	String	Operating System on the endpoint.
Owner	String	User ID of the user to whom this endpoint is registered.

Example XML format:

```
<endpointSearchResult>
   <status>success</status>
   <limit>25</limit>
   <nextOffset>25</nextOffset>
   <offset>0</offset>
```

```
    <total>2</total>
    <endpoints>
       <endpoint>
          <atRisk>false</atRisk>
          <connected>false</connected>
          <createTime>2017-02-04T10:35:35.653-05:00</createTime>
          <deviceType>Rogue</deviceType>
          <enabled>true</enabled>
          <hostName>Franks-Mac-mini</hostName>
          <id>5688</id>
          <ipAddress>192.168.6.232</ipAddress>
          <location/>
          <macAddress>0C:4D:E9:A2:90:75</macAddress>
          <os>Mac OS X OS X</os>
          <role>TEST</role>
       </endpoint>
       <endpoint>
          <atRisk>false</atRisk>
          <connected>false</connected>
          <createTime>2017-02-10T16:32:54.137-05:00</createTime>
          <deviceType>Rogue</deviceType>
          <enabled>true</enabled>
          <id>5714</id>
          <ipAddress/>
          <location>XirrusLabQA-1 ROLE -Configured-</location>
          <macAddress>DA:4B:46:55:C2:CD</macAddress>
          <role>TEST</role>
       </endpoint>
    <endpoints>
</endpointSearchResult>
```

Specific endpoint adapter

Display a specific adapter on an endpoint.

`URL = https://<servername>:8443/api/host/{id}/adapters`

`URL = https://<servername>:8443/api/host/ adapter/{adapterID}`

Return value	Type	Description
Connected	Boolean	True = Endpoint is connected.
EndpointID	Integer	ID that uniquely identifies the endpoint.
id	Integer	ID that uniquely identifies the adapter.
IP address	String	IP address of the adapter, such as "192.168.1.1".
Location	String	Connection location of the adapter.
MAC Address	String	MAC address of the adapter.

Return value	Type	Description
		MAC address values are case sensitive and are stored as uppercase values.

Example XML format:

```
<endpointAdapterResult>
<status>success</status>
   <endpointAdapters>
      <connected>true</connected>
      <endpointId>2831</endpointId>
      <id>2847</id>
      <ipAddress>172.16.49.147</ipAddress>
      <location>Stk Master 1/7</location>
      <macAddress>00:21:70:9A:38:AC</macAddress>
   </endpointAdapters>
</endpointAdapterResult>
```

Add or update an endpoint - FORM

Add or update a host with form parameters.

```
https://<servername>:8443/api/host/update
```

Return value	Type	Description
id	Integer	ID that uniquely identifies the endpoint.
createTime	Time	Date and time that this endpoint was created.
atRisk	Boolean	If true, endpoint has been marked at risk.
connected	Boolean	True = Endpoint is connected.
enabled	Boolean	If true, endpoint is enabled.
deviceType	String	Type of the endpoint, such as, an IP Phone.
ipAddress	String	List of IP addresses assigned to the interfaces on the endpoint separated by commas.
macAddress	String	List of MAC addresses on the endpoint separated by commas. MAC address values are case sensitive and are stored as uppercase values.
location	String	Name of the connection location, such as a port name.

Return value	Type	Description
hardwareType	String	Type of hardware, such as, a PC .
hostName	String	Host name of the endpoint.
loggedOnUser	String	User ID of the logged on user.
owner	String	User ID of the user to whom this endpoint is registered.
notes	String	Notes entered on the host record.
os	String	Operating System on the endpoint.
serialNumber	String	Serial Number of the endpoint.

Example request

```
curl -k -u '<username>:<password>' -H "accept: application/xml" -X POST -d
'macAddress=00:0C:29:3D:9B:4D' -d'role=MyNewRole'
https://<servername>:8443/api/host/update
```

Example XML format

```
<endpointResult>
   <status>success</status>
   <endpoints>
      <endpoint>
         <atRisk>false</atRisk>
         <connected>false</connected>
         <createTime>2017-01-25T10:20:50.533-05:00</createTime>
         <enabled>false</enabled>
         <id>3717</id>
         <macAddress>00:0C:29:3D:9B:4D</macAddress>
         <role>MyNewRole</role>
      </endpoint>
   </endpoints>
</endpointResult>
```

Add or update an dndpoint - JSON/XML

Add or update a host with a JSON object {Endpoint}.

`https://<servername>:8443/api/host`

Return value	Type	Description
id	Integer	ID that uniquely identifies the endpoint.
createTime	Time	Date and time that this endpoint was created.
atRisk	Boolean	If true, endpoint has been marked at risk.

Return value	Type	Description
connected	Boolean	True = Endpoint is connected.
enabled	Boolean	If true, endpoint is enabled
deviceType	String	Type of the endpoint, such as, an IP Phone.
ipAddress	String	List of IP addresses assigned to the interfaces on the endpoint separated by commas.
macAddress	String	List of MAC addresses on the endpoint separated by commas. MAC address values are case sensitive and are stored as uppercase values.
location	String	Name of the connection location, such as a port name.
hardwareType	String	Type of hardware, such as, a PC .
hostName	String	Host name of the endpoint.
loggedOnUser	String	User ID of the logged on user.
owner	String	User ID of the user to whom this endpoint is registered.
notes	String	Notes entered on the host record.
os	String	Operating System on the endpoint.
serialNumber	String	Serial Number of the endpoint.

Example request

```
curl -k -u '<username>:<password>' -H "accept: application/json" -H "content-type:
application/json" -X POST -d '
{"id":3691,"role":"MyNewRole","deviceType":"Registered Host"}'
https://<servername>:8443/api/host
```

```
curl -k -u '<username>:<password>' -H "accept: application/xml" -H "content-type:
application/xml" -X POST -d
'<endpoint><id>3691</id><role>MyNewRole</role></endpoint>'
https://<servername>:8443/api/host
```

Example XML format

```
<endpointResult>
   <status>success</status>
   <errorMessage></errorMessage>
   <endpoints>
      <endpoint>
         <atRisk>false</atRisk>
         <connected>false</connected>
         <createTime>2017-01-25T10:22:57.121-05:00</createTime>
         <deviceType>Registered Host</deviceType>
         <enabled>true</enabled>
```

```
        <id>3691</id>
        <macAddress>00:30:48:92:86:32</macAddress>
        <role>MyNewRole</role>
     </endpoint>
   </endpoints>
</endpointResult>
```

Bulk add or update endpoints - JSON/XML

Add or update hosts with a JSON object {Endpoint}.

`URL = https://<servername>:8443/api/host/bulkupdate`

Return value	Type	Description
id	Integer	ID that uniquely identifies the endpoint.
createTime	Time	Date and time that this endpoint was created.
atRisk	Boolean	If true, endpoint has been marked at risk.
connected	Boolean	True = Endpoint is connected.
enabled	Boolean	If true, endpoint is enabled
deviceType	String	Type of the endpoint, such as, an IP Phone.
ipAddress	String	List of IP addresses assigned to the interfaces on the endpoint separated by commas
macAddress	String	List of MAC addresses on the endpoint separated by commas
location	String	Name of the connection location, such as a port name.
hardwareType	String	Type of hardware, such as, a PC .
hostName	String	Host name of the endpoint.
loggedOnUser	String	User ID of the logged on user.
owner	String	User ID of the user to whom this endpoint is registered.
notes	String	Notes entered on the host record.
os	String	Operating System on the endpoint.
serialNumber	String	Serial Number of the endpoint.

Example request

```
curl -k -u '<username>:<password>' -H "accept: application/xml" -H "content-type:
application/json" -X POST -d '{"endpoints":
[{"id":3691,"role":"MyNewRole","deviceType":"Registered Host"}]}'
https://<servername>:8443/api/host/bulkupdate
```

Example XML format

```
<bulkEndpointResult>
   <status>success</status>
   <errorMessage></errorMessage>
   <endpointResults>
      <endpointResult>
         <status>success</status>
         <errorMessage></errorMessage>
         <endpoints>
            <endpoint>
               <atRisk>false</atRisk>
               <connected>false</connected>
               <createTime>2017-01-26T09:14:13.548-05:00</createTime>
               <deviceType>Registered Host</deviceType>
               <enabled>true</enabled>
               <id>3691</id>
               <macAddress>00:30:48:92:86:32</macAddress>
               <role>MyNewRole</role>
            </endpoint>
         </endpoints>
      </endpointResult>
   </endpointResults>
</bulkEndpointResult>
```

Events

Retrieve events.

```
https://<servername>:8443/api/event
```

```
https://<servername>:8443/api/event?tag={tag}
```

Return value	Type	Description
id	Integer	Event record ID
creationTime	Integer	Time alarm was created
name	String	Description of alarm
message	String	Event Detail
tag	String	Event tag
element		
id	Integer	Element ID
name	String	Element Name
type	Integer	Element Type

Example request

```
curl -k -u '<username>:<password>' -H "accept: application/xml" -X GET
https://<servername>:8443/api/event?limit=1
```

Example XML format

```
<eventSearchResult>
   <status>success</status>
   <limit>1</limit>
   <nextOffset>1</nextOffset>
   <offset>0</offset>
   <total>50724</total>
   <events>
      <event>
         <creationTime>1484546536470</creationTime>
         <element>
            <id>2886</id>
            <name>Aruba5000</name>
            <type>1</type>
         </element>
         <id>2956873</id>
         <message>SNMP error 2 occurred for device Aruba5000</message>
         <name>SNMP Read Error</name>
         <tag>SNMP_READ_ERROR</tag>
      </event>
   </events>
</eventSearchResult>
```

Specific event

Retrieve a specific event.

```
https://<servername>:8443/api/event/{id}
```

Return value	Type	Description
id	Integer	Event record ID
creationTime	Integer	Time alarm was created
name	String	Description of alarm
message	String	Event Detail
tag	String	Event tag
element		
id	Integer	Element ID
name	String	Element Name
type	Integer	Element Type

Example request

```
curl -k -u '<username>:<password>' -H "accept: application/xml" -X GET
https://<servername>:8443/api/event/33757
```

Example XML format

```
<eventResult>
   <status>success</status>
   <errorMessage></errorMessage>
   <event>
      <creationTime>1484546536470</creationTime>
      <element>
         <id>2886</id>
         <name>Aruba5000</name>
         <type>1</type>
      </element>
      <id>2956873</id>
      <message>SNMP error 2 occurred for device Aruba5000</message>
      <name>SNMP Read Error</name>
      <tag>SNMP_READ_ERROR</tag>
   </event>
</eventResult>
```

Group

Retrieve groups.

`https://<servername>:8443/api/group`

`https://<servername>:8443/api/group?name={name}`

Return value	Type	Description
id	Integer	
name	String	
daysInactive	Integer	
daysValid	Integer	
description	String	
owner	String	
type	String	
members		List of group members with record id and name
childGroups		List of groups that are members of this group with record id and name

Example request

```
curl -k -u '<username>:<password>' -H "accept: application/xml" -X GET
https://<servername>:8443/api/group?name=All%20Management%20Group
```

Example XML format

```
<groupSearchResult>
   <status>success</status>
   <limit>0</limit>
   <nextOffset>31</nextOffset>
   <offset>0</offset>
   <total>31</total>
   <groups>
      <group>
         <daysInactive>0</daysInactive>
         <daysValid>0</daysValid>
         <description>Administrative users with all management access rights.</ description>
         <id>1</id>
         <members>
            <member><id>1</id><name>root</name></member>
            <member><id>6</id><name>helpdesk, helpdesk</name></member>
            <member><id>22</id><name>admin, </name></member>
            <member><id>21</id><name>operator, operator</name></member>
            <member><id>33</id><name>Howard, Moe</name></member>
         </members>
         <childGroups></childGroups>
         <name>All Management Group</name>
         <owner>System</owner>
         <type>Administrator</type>
      </group>
   </groups>
</groupSearchResult>
```

Specific group

Retrieve a specific group.

```
https://<servername>:8443/api/group/{id}
```

Return value	Type	Description
id	Integer	
name	String	
daysInactive	Integer	
daysValid	Integer	
description	String	
owner	String	

Return value	Type	Description
type	String	
members		List of group members with record id and name
childGroups		List of groups that are members of this group with record id and name

Example request

```
curl -k -u '<username>:<password>' -H "accept: application/xml" -X GET
https://<servername>:8443/api/group/1
```

Example XML format

```
<groupResult>
   <status>success</status>
   <errorMessage></errorMessage>
   <group>
      <daysInactive>0</daysInactive>
      <daysValid>0</daysValid>
      <description>Administrative users with all management access rights. </description>
      <id>1</id>
      <members>
         <member><id>1</id><name>root</name></member>
         <member><id>6</id><name>helpdesk, helpdesk</name></member>
         <member><id>22</id><name>admin, </name></member>
         <member><id>21</id><name>operator, operator</name></member>
         <member><id>33</id><name>Howard, Moe</name></member>
      </members>
      <childGroups></childGroups>
      <name>All Management Group</name>
      <owner>System</owner>
      <type>Administrator</type>
   </group>
</groupResult>
```

Add or update a group

Add or updates a group.

```
https://<servername>:8443/api/group
```

Return Value: status

Example Request

```
curl -k -u '<username>:<password>' -H "content-type: application/json" -X POST -d '
{"id":1,"members":[{"id":1},{"id":6},{"id":17},{"id":22},{"id":21}],"childGroups":
[]}' https://<servername>:8443/api/group
```

Example Response

```
SUCCESS
```

Delete a group

Deletes a group.

```
https://<servername>:8443/api/group/{id}
```

Return Value: status

Example request

```
curl -k -u '<username>:<password>' -X DELETE https://<servername>:8443/api/group/1
```

Example response

```
SUCCESS
```

Specific network device

Display a specific network device.

```
URL = https://<servername>:8443/api/host/{dbid}/device
```

```
URL = https://<servername>:8443/api/network/device/{dbid}
```

```
URL = https://<servername>:8443/api/network/domain/{dbid}/devices
```

Return value	Type	Description
Description	String	System description of the device.
Direction		
Hardware Type	String	Type of network device: Switch Wswitch Printer server
ID	Integer	ID that uniquely identifies the network device.
IP address	String	IP address of the network device, such as "192.168.1.1".
Name	String	System name of the device
Orderby		
SysOID	String	OID of the device, such as 1.3.6.1.4.1.14823.1.1.32.

Example XML format:

```
<networkDeviceResult>
<status>success</status>
   <networkDevices>
      <description>Summit300-24 - Version 7.6e.1 (Build 4) by Release_Master 03/13/06
            11:53:13</description>
      <hardwareType>switch</hardwareType>
      <id>943</id>
      <ipAddress>192.168.5.100</ipAddress>
      <name>Stk Master</name>
      <sysOid>1.3.6.1.4.1.1916.2.67</sysOid>
   </networkDevices>
</networkDeviceResult>
```

Network devices - bulk

Display all network devices.

`URL = https://<servername>:8443/api/network/device/`

Return value	Type	Description
Description	String	System description of the device.
Hardware Type	String	Type of network device: Switch Wswitch Printer server
ID	Integer	ID that uniquely identifies the network device.
IP address	String	IP address of the network device, such as "192.168.1.1".
Name	String	System name of the device
SysOID	String	OID of the device, such as 1.3.6.1.4.1.14823.1.1.32.

Example XML format:

```
<networkDeviceSearchResult>
<status>success</status>
<limit>25</limit>
   <networkDevices>
      <description>Summit300-24 - Version 7.6e.1 (Build 4) by Release_Master 03/13/06
            11:53:13</description>
      <hardwareType>switch</hardwareType>
      <id>943</id>
      <ipAddress>192.168.5.100</ipAddress>
      <name>Stk Master</name>
      <sysOid>1.3.6.1.4.1.1916.2.67</sysOid>
   </networkDevices>
<nextOffset>0</nextOffset>
```

```
<offset>0</offset>
<total>1</total>
</networkDeviceSearchResult>
```

Specific network port

Display a specific network port.

URL = https://<servername>:8443/api/host/adapter/{dbid}/port

URL = https://<servername>:8443/api/network/device/{dbid}/ports

URL = https://<servername>:8443/api/network/device/port/{dbid}

Return value	Type	Description
Description	String	Port Description
Device ID	Integer	ID that uniquely identifies the network device.
Hosts Connected	Boolean	True = Host is connected.
ID	Integer	ID that uniquely identifies the port.
MAC Address	String	MAC Address of the port.
Name	String	Port name

Example XML format:

```
<networkPortResult>
<status>success</status>
   <networkPorts>
      <description>Stk Master 1/7</description>
      <deviceId>943</deviceId>
      <hostsConnected>true</hostsConnected>
      <id>944</id>
      <macAddress>00:04:96:1F:89:C4</macAddress>
      <name>1007</name>
   </networkPorts>
</networkPortResult>
```

Service

Request a service document located at the entry point of the API application.

URL=https://<servername>:8443/api/

Return value	Type	Description
status	String	Status of the connection.

Return value	Type	Description
apiVersion	String	Version of the FortiNAC api software.
productCopyright	String	Fortinet copyright information for the REST api module.
productName	String	FortiNAC official product name.
productVersion	String	FortiNAC software version number.

Example XML format:

```
<serviceDocument>
   <status>success</status>
   <apiVersion>1.0</apiVersion>
   <productCopyright>© 1999-2013 Fortinet. All rights reserved.</productCopyright>
   <productName>FortiNAC Server</productName>
   <productVersion>6.2.3.56</productVersion>
</serviceDocument>
```

Scheduled tasks

Retrieve scheduled tasks.

```
https://<servername>:8443/api/scheduler
```

Return value	Type	Description
id	Integer	Scheduled task record ID
hidden	boolean	Is task for internal use only.
paused	boolean	Is task paused.
previousScheduledTime	String	Last time task ran.
scheduledTime	String	Next time task scheduled to run
name	String	Name of scheduled task.

Example request

```
curl -k -u '<username>:<password>' -H "accept: application/xml" -X GET
https://<servername>:8443/api/scheduler?limit=1
```

Example XML format

```
<schedulerSearchResult>
   <status>success</status>
   <limit>1</limit>
   <nextOffset>1</nextOffset>
   <offset>0</offset>
   <total>11</total>
   <schedules>
```

```
      <schedule>
         <hidden>false</hidden>
         <id>1</id>
         <name>Auto-Definition Synchronizer</name>
         <paused>false</paused>
         <previousScheduledTime>2017-01-23T10:45:22.326-05:00 </previousScheduledTime>
         <scheduledTime>2017-01-30T10:45:33.393-05:00</scheduledTime>
      </schedule>
   </schedules>
</schedulerSearchResult>
```

Run a scheduled task

Run scheduled tasks.

`https://<servername>:8443/api/scheduler/run/{id}`

- Return Value: status

Example request

```
curl -k -u '<username>:<password>' -X POST
https://<servername>:8443/api/scheduler/run/3
```

Example response

```
SUCCESS
```

Specific scheduled task

Retrieve a specific scheduled task.

`https://<servername>:8443/api/scheduler/{id}`

Return value	Type	Description
id	Integer	Scheduled task record ID
hidden	boolean	Is task for internal use only.
paused	boolean	Is task paused.
previousScheduledTime	String	Last time task ran.
scheduledTime	String	Next time task scheduled to run
name	String	Name of scheduled task.

Example request

```
curl -k -u '<username>:<password>' -H "accept: application/xml" -X GET
https://<servername>:8443/api/scheduler/1
```

Example XML format

```
<schedulerResult>
   <status>success</status>
   <errorMessage></errorMessage>
   <schedule>
      <hidden>false</hidden>
      <id>1</id>
      <name>Auto-Definition Synchronizer</name>
      <paused>false</paused>
      <previousScheduledTime>2017-01-23T10:45:22.326-05:00</previousScheduledTime>
      <scheduledTime>2017-01-30T10:45:59.681-05:00</scheduledTime>
   </schedule>
</schedulerResult>
```

Users

Retrieve users.

```
https://<servername>:8443/api/user
```

Return value	Type	Description
Id	Integer	User record ID
adminProfile	String	User's admin profile
address	String	User's street address
city	String	User's city
email	String	Email address
firstName	String	First name
lastName	String	Last name
mobileNumber	String	Mobile phone number
mobileProvider	String	Mobile phone service provider
phone	String	Phone number
role	String	User's role
type	String	User Record Type (possible values: User or Administrative)
userId	String	User name
zipCode	String	User's zip code

Example request

```
curl -k -u '<username>:<password>' -H "accept: application/xml" -X GET
https://<servername>:8443/api/user?lastName=Howard
```

Example XML format

```
<userSearchResult>
   <status>success</status>
   <limit>1</limit>
   <nextOffset>0</nextOffset>
   <offset>0</offset>
   <total>1</total>
   <users>
      <user>
         <id>32</id>
         <address>123 Main Str</address>
         <city>Concord</city>
         <email>Shemp@example.com</email>
         <firstName>Shemp</firstName>
         <lastName>Howard</lastName>
         <mobilePhone>555-555-6789</mobilePhone>
         <mobileProvider>AT&amp;T</mobileProvider>
         <phone>555-555-1234</phone>
         <role>Employee</role>
         <state>NH</state>
         <type>User</type>
         <userId>Shemp</userId>
         <zipCode>12345</zipCode>
         <notes>the quick brown fox</notes>
      </user>
   </users>
</userSearchResult>
```

Add or update a user

Add or update a user.

`https://<servername>:8443/api/user/update`

Return value	Type	Description
Id	Integer	User record ID
adminProfile	String	User's admin profile
address	String	User's street address
city	String	User's city
email	String	Email address
firstName	String	First name
lastName	String	Last name
mobileNumber	String	Mobile phone number
mobileProvider	String	Mobile phone service provider

Return value	Type	Description
phone	String	Phone number
role	String	User's role
type	String	User Record Type (possible values: User or Administrative)
userId	String	User name
zipCode	String	User's zip code

Example Request

```
curl -k -u '<username>:<password>' -H "accept: application/xml" -X POST -d
'userID=moe' -d'role=MyNewRole’ https://<servername>:8443/api/user/update
```

Example XML format

```
<userResult>
   <status>success</status>
   <users>
      <user>
         <id>32</id>
         <address>123 Main Str</address>
         <city>Concord</city>
         <email>Shemp@example.com</email>
         <firstName>Shemp</firstName>
         <lastName>Howard</lastName>
         <mobilePhone>555-555-6789</mobilePhone>
         <mobileProvider>AT&amp;T</mobileProvider>
         <phone>555-555-1234</phone>
         <role>Employee</role>
         <state>NH</state>
         <type>User</type>
         <userId>Shemp</userId>
         <zipCode>12345</zipCode>
         <notes>the quick brown fox</notes>
      </user>
   </users>
</userResult>
```

Add or update a user - FORM

Display a specific user.

`URL = https://<servername>:8443/api/user/{id}`

`URL = https://<servername>:8443/api/user/userid/{userid}`

Return value	Type	Description
Id	Integer	User record ID

Return value	Type	Description
adminProfile	String	User's admin profile
address	String	User's street address
city	String	User's city
email	String	Email address
firstName	String	First name
lastName	String	Last name
mobileNumber	String	Mobile phone number
mobileProvider	String	Mobile phone service provider
phone	String	Phone number
role	String	User's role
type	String	User Record Type (possible values: User or Administrative)
userId	String	User name
zipCode	String	User's zip code

Example request

```
curl -k -u '<username>:<password>' -H "accept: application/xml" -X GET
https://<servername>:8443/api/user/31
```

Example XML format:

```
<userResult>
   <status>success</status>
   <users>
      <user>
         <id>32</id>
         <address>123 Main Str</address>
         <city>Concord</city>
         <email>Shemp@example.com</email>
         <firstName>Shemp</firstName>
         <lastName>Howard</lastName>
         <mobilePhone>555-555-6789</mobilePhone>
         <mobileProvider>AT&amp;T</mobileProvider>
         <phone>555-555-1234</phone>
         <role>Employee</role>
         <state>NH</state>
         <type>User</type>
         <userId>Shemp</userId>
         <zipCode>12345</zipCode>
         <notes>the quick brown fox</notes>
      </user>
   </users>
</userResult>
```

Add or update a user - JSON/XML

Add or update a user.

`https://<servername>:8443/api/user/`

Return value	Type	Description
Id	Integer	User record ID
adminProfile	String	User's admin profile
address	String	User's street address
city	String	User's city
email	String	Email address
firstName	String	First name
lastName	String	Last name
mobileNumber	String	Mobile phone number
mobileProvider	String	Mobile phone service provider
phone	String	Phone number
role	String	User's role
type	String	User Record Type (possible values: User or Administrative)
userId	String	User name
zipCode	String	User's zip code

Example request

```
curl -k -u '<userId>:<password>' -H "accept: application/json" -H "content-type:
application/json" -X POST -d '{"userId":"bigT","lastName":"Tutone"}'
https://<servername>/api/user
```

```
curl -k -u '<userId>:<password>' -H "accept: application/xml" -H "content-type:
application/xml" -X POST -d '<user><lastName>Tutone</lastName><role>NAC-
Default</role><userId>bigT</userId></user>' https://<servername>/api/user
```

Example XML format:

```
<userResult>
   <status>success</status>
   <users>
      <user>
         <id>45</id>
         <lastName>Tutone</lastName>
         <role>NAC-Default</role>
         <userId>bigT</userId>
      </user>
   </users>
```

```
</userResult>
```

Vendor OUIs

Retrieve vendor OUIs.

```
URL = https://<servername>:8443/api/vendoroui
```

Return value	Type	Description
id	Integer	Vendor OUI record ID
oui	String	Organizationally unique identifier
name	String	Vendor name
alias	String	Alternate name
description	String	Description
registration type	Integer	Type of device registration that is specified through the AutoDef Synchronization. Assigned to devices registered via the Portal page.
userRegistrationType	Integer	Overrides the type of device registration that is specified through the AutoDef Synchronization. Assigned to devices registered via the Portal page
role	String	Role assigned to devices registered via the Portal page.

Example request

```
curl -k -u '<username>:<password>' -H "accept: application/xml" -X GET
https://<servername>:8443/api/vendoroui?oui=00:00:1d
```

Example XML format

```
<vendorOuiSearchResult>
   <status>success</status>
   <limit>25</limit>
   <nextOffset>1</nextOffset>
   <offset>0</offset>
   <total>1</total>
   <vendorOuis>
      <vendorOui>
         <id>30</id>
         <oui>00:00:1D</oui>
         <name>Cabletron Systems, Inc.</name>
         <alias>ctron</alias>
         <description>Cabletron/Enterasys</description>
         <role>NAC-Default</role>
         <registrationType>0</registrationType>
         <userRegistrationType>0</userRegistrationType>
      </vendorOui>
   </vendorOuis>
```

```
</vendorOuiSearchResult>
```

Specific vendor OUI

Retrieve a specific vendor OUI.

`URL = https://<servername>:8443/api/vendoroui/{id}`

Return value	Type	Description
id	Integer	Vendor OUI record ID
oui	String	Organizationally unique identifier
name	String	Vendor name
alias	String	Alternate name
description	String	Description
registration type	Integer	Type of device registration that is specified through the AutoDef Synchronization. Assigned to devices registered via the Portal page.
userRegistrationType	Integer	Overrides the type of device registration that is specified through the AutoDef Synchronization. Assigned to devices registered via the Portal page
role	String	Role assigned to devices registered via the Portal page.

Example request

```
curl -k -u '<username>:<password>' -H "accept: application/xml" -X GET
https://<servername>:8443/api/vendoroui/1
```

Example XML format

```
<vendorOuiResult>
   <status>success</status>
   <errorMessage></errorMessage>
   <vendorOui>
      <id>30</id>
      <oui>00:00:1D</oui>
      <name>Cabletron Systems, Inc.</name>
      <alias>ctron</alias>
      <description>Cabletron/Enterasys</description>
      <role>NAC-Default</role>
      <registrationType>0</registrationType>
      <userRegistrationType>0</userRegistrationType>
   </vendorOui>
</vendorOuiResult>
```

Troubleshooting REST API

Test from Linux

Use your browser or another REST tool to test querying, deleting or updating using REST API. Below are some sample commands.

```
curl -k -i -u <uname>:<passwd> -H "Accept: application/xml" -X GET
https://<servername>:8443/api
```

```
curl -k -i -u <uname>:<passwd> -H "Accept: application/xml" -X GET
https://<servername>:8443/api/host
```

```
curl -k -i -u <uname>:<passwd> -H "Accept: application/xml" -X GET
https://<servername>:8443/api/host/320
```

```
curl -k -i -u <uname>:<passwd> -H "Accept: application/xml" -X DELETE
https://<servername>:8443/api/host/320
```

```
curl -k -i -u <uname>:<passwd> -H "Accept: application/xml" -X POST -d
"mac=00:00:1D:33:44:55" -d "os=Windows" https://<servername>:8443/api/host/update
```

Enable debug

To enable debug, uncomment the following in the jersey servlet configuration in `/bsc/campusMgr/ui/ROOT/WEB-INF/web.xml`:

```
<!--
<init-param>
<param-name>com.sun.jersey.config.feature.Trace</param-name>
<param-value>true</param-value>
</init-param>
<init-param>
<param-name>com.sun.jersey.spi.container.ContainerRequestFilters</param-name>
<param-value>com.sun.jersey.api.container.filter.LoggingFilter</param-value>
</init-param>
<init-param>
<param-name>com.sun.jersey.spi.container.ContainerResponseFilters</param-name>
<param-value>com.sun.jersey.api.container.filter.LoggingFilter</param-value>
</init-param>
-->
```

To restart tomcat-admin, run `service tomcat-admin restart`.

The debug file can be found in `/bsc/logs/tomcat-admin/catalina.out`.

Appendix A - Appendix A: Scan parameters

Endpoint Compliance Policies used to scan your hosts for compliance, have many variables for which the host can be scanned. For the anti-virus and operating system variables, you can narrow the scan by setting custom parameters. For example, when scanning for a particular operating system you can require that the operating system be at Service Pack 4 or higher.

Any parameter that you modify will no longer be updated by the Auto-Def Updates scheduled task. That task updates the list of anti-virus and operating systems for which you can scan. It also modifies parameters associated with each of those items to force hosts to use the most recent definitions for anti-virus and to have installed the latest updates to the operating system.

This section provides details about each type of variable and the detailed parameters within that can be set to narrow your scan further.

Anti-Virus parameters - Windows

The table below provides an alphabetical list all of the possible parameters that can be configured for anti-virus software for Windows. Only some of these parameters are used for any given anti-virus program.

Check with your vendor for the required format. Formats for dates, version numbers, .dat files, etc. change frequently and vary by product.

Default parameter values are entered and updated automatically by the scheduled Auto-Def Updates. If the values have been manually edited, the Auto-Def Updates will not override those changes.

Settings

Parameter	Description	Typical options
AntiVirus definition Date	The date of the required AntiVirus definition files.	YYYY-MM-DD
AntiVirus Engine	The version number of the required AntiVirus Engine. Select the operator that will apply to the definition value found on the host: greater than, equal to, or both.	** > = >=

Parameter	Description	Typical options
Client Security Antimalware Service must be running	Select a setting.	Enabled or Disabled
Client Security State Assessment Service must be running	Select a setting.	Enabled or Disabled
Custom Scans	Select the custom scans that you want to implement for the product.	Custom Scans
Daily Virus Definition	The version of the required daily definition files. Select the operator that will apply to the definition value found on the host: greater than, equal to, or both.	** > = >=
Definitions Label	Enter the label for the Definitions Web Address.	Text entry
Definitions Web Address	Enter the URL for the web page where the updated definitions for the selected product can be located and downloaded. When a host fails the scan this URL appears in the Failed Policy Results view.	URL
Definitions Version	The version of the required definition files. Select the operator that will apply to the definition value found on the host: greater than, equal to, or both.	** > = >=
Engine Version	The number of the required engine version. Select the operator that will apply to the definition value found on the host: greater than, equal to, or both.	** > = >=
Engine Version Label	Enter the label for the Engine Version Web Address.	Text entry
Engine Version Web Address	Enter the URL for the web page where the updated engine version for the selected product can be located and downloaded. When a host fails the scan this URL appears in the Failed Policy Results view.	URL
Label	Enter a label. This label will appear on the Results panel to identify which scan the host failed.	Text entry
Macro Definition	The date of the required macro definition files.	YYYY-MM-DD

Parameter	Description	Typical options
	Select the operator that will apply to the definition value found on the host: greater than, equal to, or both.	> = >=
Main Virus Definition	The version of the required main definition files. Select the operator that will apply to the definition value found on the host: greater than, equal to, or both.	** > = >=
Minimum Engine Version	Minimum engine version required to pass the scan.	**
Operational Label	Enter a label. This label will appear on the Results panel to identify that an operational state did not meet the requirement.	Text entry
Operational Web Address	Enter the URL of the web page that displays information about the product when the host fails the scan because the Client Security State Assessment or Antimalware Service operational state did not meet the requirement.	URL
Operator (applies to all)	The Engine version and definition (Virus and Spyware) values found on the host must be either greater than, equal to, or both than the value(s) entered.	> = >=
Products to Detect	Select which products you wish to include in the scan. All products are selected by default. Scan results show the group name (label) only, not the specific AV/AS product. The scan will either pass or fail for the group (label).	
Program Version	The version number of the program. Select the operator that will apply to the definition value found on the host: greater than, equal to, or both.	** > = >=
Program Version Label	Enter the label for the Program Version Web Address.	Text entry
Program Version Web Address	Enter the URL for the web page where the required version can be located and downloaded. When a host fails the scan this URL appears in the Failed Policy Results view.	URL

Parameter	Description	Typical options
Prohibit this Product	Set this option to true if you want to prohibit the installation of this product. If this product is installed, the scan fails.	true or false
Protection Updates	The date of the required Protection Updates file. Select the operator that will apply to the definition value found on the host: greater than, equal to, or both.	YYYYMMDD > = >+
Protection Updates Label	Enter the label for the Protection Updates Web Address.	Text entry
Protection Updates Web Address	Enter the URL for the web page where the Production Updates can be located and downloaded. When a host fails the scan this URL appears in the Failed Policy Results view.	URL
Signature Version	The build number or date and build number of the required signature file. Select the operator that will apply to the definition value found on the host: greater than, equal to, or both.	** > = >=
Signature Version Label	Label for the Signature Version Web Address.	Text entry
Signature Version Web Address	Enter the URL for the web page where the required signature version can be located and downloaded. When a host fails the scan this URL appears in the Failed Policy Results view.	URL
Spyware Definition	Number of the required spyware definition file.	**
Version	The number of the required virus definition file. Select the operator that will apply to the definition value found on the host: greater than, equal to, or both.	** > = >=
Version Label	Enter the label for the Version Web Address.	Text entry
Version Web Address	Enter the URL for the web page where the required version can be located and downloaded. When a host fails the scan this URL appears in the Failed Policy Results view.	URL

Parameter	Description	Typical options
Virus Definition	Used to identify the virus definition version installed. May be the name of the definition file, the date of the file, a version number,etc. Select the operator that will apply to the definition value found on the host: greater than, equal to, or both.	** > = >=
Virus Definition VDF Label	The label for the VDF web address.	Text entry
Virus Definition VDF Web Address	The URL for the web page where updated definitions can be located and downloaded. Supply a local or Internet URL. This URL will be displayed on the Failed Policy Results view if the host fails the scan.	URL
Virus Signature	The date of the required virus signature.	YYYY-MM-DD
Web Address	Enter the URL of the web page that displays information about the product if the host fails the scan.	URL
Windows Operating System	Select any or all Windows Operating Systems required for the selected product.	
Software specific parameters		
Eset-NOD32 Minimum Scanner Version (nod32.exe)	The number of the required scanner version of the file nod32.exe.	**

Anti-Virus parameters - macOS

The table below provides an alphabetical list all of the possible parameters that can be configured for anti-virus software for macOS. Only some of these parameters are used for any given anti-virus program.

Check with your vendor for the required format. Formats for dates, version numbers, .dat files, etc. change frequently and vary by product.

Default parameter values are entered and updated automatically by the scheduled Auto-Def Updates. If the values have been manually edited, the Auto-Def Updates will not override those changes.

Settings

Parameter	Description	Typical options
Definitions Label	Enter the label for the Definitions Web Address.	Text entry
Definitions Web Address	Enter the URL for the web page where the updated definitions for the selected product can be located and downloaded. When a host fails the scan this URL appears in the Failed Policy Results view.	URL
Engine Version Web Address	Enter the URL of the web page where information about the engine version is displayed if the host fails the scan.	URL
Engine Version Label	Enter the label for the Engine Version Web Address.	Text entry
Label	Enter a label. This label appears in the Results page information to identify which scan the host failed.	Text entry
Program Version	The number of the required version. Select the Operator to apply to the definition value found on the host: greater than, equal to, or both.	** > = >=
Program Version Label	Enter the label for the Program Version Web Address.	Text entry
Program Version Web Address	Enter the URL for the web page where the required program version can be located and downloaded. When a host fails the scan this URL appears in the Failed Policy Results view.	URL
Prohibit this Product	Set this option to true if you want to prohibit the installation of this product. If this product is installed, the scan fails.	true or false
Version Label	Enter the label for the Version Web Address.	Text entry
Virus Definition	Used to identify the virus definition version installed. May be the name of the definition file, the date of the file, a version number,etc. Select the operator to apply to the definition value found on the host: greater than, equal to, or both.	** > = >=
Version Web Address	Enter the URL for the web page where information about the version is displayed when the scan is failed. When a host fails the scan this URL appears in the Failed Policy Results view.	URL
Web Address	Enter the URL of the web page where information about the product is displayed in case the scan fails.	URL

Parameter	Description	Typical options
Software specific parameters		
Clam Engine Version	The number of the required engine version. Select the Operator to apply to the definition value found on the host: greater than, equal to, or both.	** > = >=

Operating system parameters - Windows

The table below contains an alphabetical list of possible Configuration Parameters that can be used when setting up scans for Windows Operating Systems. A subset of these parameters is available for each version of this operating system.

Default parameter values are entered and updated automatically by the scheduled Auto-Def Updates. If the values have been manually edited, the Auto-Def Updates will not override those changes.

Settings

Parameter	Description
Allowed Editions	Select the allowed editions. Options are Home Basic, Home Premium, Business, Enterprise, Ultimate, and Starter.
Critical / Security Updates Label	The Critical / Security Updates Label that displays on the results page.
Critical / Security Updates Web Address	The URL for the web page where Windows-Server-2008 Critical / Security Updates information can be located and downloaded. Supply a local or Internet URL to display in the Failed Policy Results window if the host fails the scan.
Custom Scans	Any custom scans that have been created are shown.
Disable Bridging	When selected, disables bridging on the host.
Disable Internet Connection Sharing	When selected Internet Connection Sharing is disabled on the host.
Edition Label	Enter a label. This label appears in the Results page information to identify which scan the host failed.
Edition Web Address	The URL for the web page where the specific edition information can be located and downloaded. Supply a local or Internet URL to display in the Failed Policy Results window if the host fails the scan.
Enable Automatic Updates	See the enable automatic updates parameters table below.

Parameter	Description
Enable Windows Firewall	When selected, the Windows Firewall is enabled.
Force DHCP	Requires write access to the registry if done through the dissolvable agent. Do not enable Force DHCP on policies that will be used for VPN clients. Enabling this setting can cause the host to continuously lose its VPN connection.
Label	Enter a label. This label appears in the Results page information to identify which scan the host failed.
Prohibit Home Edition	When selected, prohibits Windows-XP Home Edition.
Require All Critical Updates	When selected, all Critical Updates are required for the host.
Require Critical Updates	When selected, Require Critical Updates must be enabled on the host.
FortiNAC leverages the Windows Update tool to check for Critical Updates and Security Updates during an operating system scan. The host must be able to connect to the Microsoft Windows Update web site and any other associated sites.	
In the event that the local WSUS server is unreachable, FortiNAC does not revert to using the Microsoft update servers. FortiNAC will not generate events when a host fails to contact the WSUS server because it occurs on the endpoints and not on FortiNAC. However, a local event log entry is created for hosts that fail to connect to the WSUS server.	
Require Security Updates	When selected will Require Security Updates to be enabled on the host.
Require Service Pack	When the checkbox labeled "Require Service Pack" is selected a text field displays. Enter the numeric value for the Service Pack Level.
SCCM Evaluation Label	The SCCM Evaluation label that is displayed in scan results to indicate that the SCCM Evaluation was triggered for the host.
Service Pack Label	The Service Pack Label that displays on the results page.
Service Pack Level	The required Service Pack Level. Enter the numeric value. Select the Operator to apply to the definition value found on the host: greater than, equal to, or both.
Service Pack Web Address	URL for the web page where Service Pack information can be located and downloaded. Supply either a local or Internet URL. This URL is displayed in the Failed Policy Results window if the host fails the scan.
Trigger SCCM Evaluation	When selected, an upgrade is forced on the host from the SCCM controller. This ensures all hosts on the network are up-to-date. Requires Agent Version 4.0.3 or greater.

Parameter	Description
	This option is available for Windows 7, 8, 10, Windows-Server-2012, Windows-Server-2008-R2, and Windows-Server-2012-R2.
Edition Label	The Updates Label that displays on the results page.
Validate Edition	When enabled, only those editions of Windows that are selected in FortiNAC are permitted. When disabled, all/any edition of the selected Windows operating systems will be allowed, such as Windows Vista N or Windows Vista K.
Web Address	The URL for the web page where Windows operating system information can be located and downloaded. Supply either a local or Internet URL. This URL is displayed in the Failed Policy Results window if the host fails the scan.

Enable automatic updates parameters

When this option is checked for the selected operating system, it enables Automatic Updates on the host by modifying the registry. Additional configuration options appear once the box is selected. Use CAUTION when changing any of the Auto Update Settings. It is recommended that you are familiar with these options before you make any changes.

Parameter	Description
Auto Update Web Address	Web address used for Windows update. The default is sma/windowsupdates.jsp.

Apply as a Policy
(users can't modify)
	Select True or False. Default = True.
	If this option is enabled, users of hosts running the selected version of Windows can no longer set Windows Update Parameters for their own hosts. Registry keys for those settings are set by FortiNAC and are locked. Changing this option to False does not remove the lock from the registry keys. The keys must be deleted to restore user access to Windows Update settings. Keys are as follows:
	`SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate`
	`SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU`

RescheduleWaitTime	Time to wait between the time Automatic Updates starts and the time it begins installations, where the scheduled times have passed. The time is set in minutes from 1 to 60, representing 1 minute to 60 minutes). This setting only affects host behavior after the hosts have updated to the SUS SP1 client version or later.
NoAuto RebootWithLoggedOnUsers	Select True or False. Default = False. If set to true, Automatic Updates does not automatically restart a computer while users are logged on. Note: This setting affects host behavior after the hosts have updated to the SUS SP1 host version or later.
NoAutoUpdate	0 = Automatic Updates is enabled. 1 = Automatic Updates is disabled.

Parameter	Description
	Default = 0
AUOptions	1 = Keep my computer up to date has been disabled in Automatic Updates. 2 = Notify of download and installation. 3 =Automatically download and notify of installation. 4 = Automatically download and schedule installation.
AUState	0 = Initial 24-hour timeout (Automatic Updates doesn't run until 24 hours after it first detects an Internet connection.) 1 = Waiting for the user to run Automatic Updates 2 = Detection pending 3 = Download pending (Automatic Updates is waiting for the user to accept the pre-downloaded prompt.) 4 = Download in progress 5 = Install pending 6 = Install complete 7 = Disabled 8 = Reboot pending (Updates that require a reboot were installed, but the reboot was declined. Automatic Updates will not do anything until this value is cleared and a reboot occurs.)
ScheduledInstallDay	0 = Every day. 1 - 7 = The days of the week from Sunday (1) to Saturday (7).
ScheduledInstallTime	The time of day in a 24-hour format (0-23).
UseWUServer	Select True or False Use or not use a server that is running Software Update Services instead of Windows Update.
WUServer	http://<server> This value sets the SUS server by HTTP name (for example, http://IntranetSUS).
WUStatusServer	http://<server> This value sets the SUS statistics server by HTTP name (for example, http://IntranetSUS).

If you configure the scan to enable Automatic Updates and an error occurs (for example, a network or permission error) so that the scan cannot perform the update, then the scan might fail.

Operating systems parameters - macOS

The table below contains an alphabetical list of possible Configuration Parameters for Mac Operating Systems. A subset of these parameters is available for each operating system.

Default parameter values are entered and updated automatically by the scheduled Auto-Def Updates. If the values have been manually edited, the Auto-Def Updates will not override those changes.

Settings

Parameter	Description	Typical options
Label	Enter a label. This label appears in the Results page information to identify which scan the host failed.	Text entry
Web Address	The URL for the web page where Mac information can be located and downloaded. Supply a URL to display in the Failed Policy Results window if the host fails the scan.	URL
Label for Update Version	Enter a label.	Text entry
Update Version Web Address	The URL for the web page where Mac update information can be located and downloaded. Supply either a local or Internet URL.	URL
Require at least Version 10.x.	Numerical entry for x in the version 10.1.x	Number
Custom Scans	Any custom scans that have been created will be shown.	Select a custom scan.

Appendix B: Security event severity level mappings

Each vendor defines its own severity levels for syslog messages. These severity levels are normalized within FortiNAC to provide additional filtering options for incoming security events. The following table provides severity level mappings between the vendor and FortiNAC.

You must have ATR enabled in your licensing package in order to use ATR features.

Vendor	Vendor Severity Level	FortiNAC Severity Level
CheckPoint	1	1
	2	2
	3	3
	4	4
	5	5
	6	6
	7	7
	8	8
	9	9
	10	10
Stonegate	0	1
	1	2
	2	3
	3	4
	4	5
	5	6
	6	7
	7	8
	8	9
	9	10

Vendor	Vendor Severity Level	FortiNAC Severity Level
TippingPointSMS	0	1
	1	3
	2	5
	3	7
	4	9
FireEye	0	1
	1	2
	2	3
	3	4
	4	5
	5	6
	6	7
	7	8
	8	9
	9	10
FortiOS4	INFORMATION	1
	NOTICE	3
	WARNING	5
	ALERT	7
	CRITICAL	8
	ERROR	9
	EMERGENCY	10
FortiOS5	INFORMATION	1
	NOTICE	3
	WARNING	5
	ALERT	7
	CRITICAL	8
	ERROR	9
	EMERGENCY	10

Vendor	Vendor Severity Level	FortiNAC Severity Level
PaloAlto	INFORMATIONAL	1
	LOW	3
	MEDIUM	5
	HIGH	7
	CRITICAL	9
RSA	0	1
	1	2
	2	3
	3	4
	4	5
	5	6
	6	7
	7	8
	8	9
	9	10

FORTINET®

Copyright© 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.