FortiNAC

FortiGate
Endpoint Management
Integration

Version: 8.5, 8.6, 8.7, 8.8

Date: March 25, 2022

Rev: R

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

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

FORTINET KNOWLEDGE BASE
https://community.fortinet.com/t5/Knowledge-Base/ct-p/knowledgebase

FORTINET BLOG
http://blog.fortinet.com

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

FORTINET COOKBOOK
http://cookbook.fortinet.com

NSE INSTITUTE
http://training.fortinet.com

FORTIGUARD CENTER
http://fortiguard.com

FORTICAST
http://forticast.fortinet.com

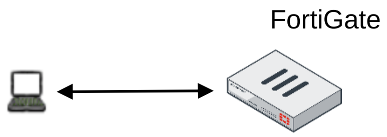
END USER LICENSE AGREEMENT
http://www.fortinet.com/doc/legal/EULA.pdf

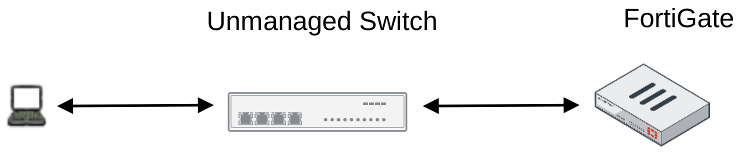
Contents

Overview

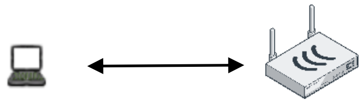
The information in this document provides guidance to integrate FortiNAC with FortiGate in order to provide visibility and control for the following connectivity:

- Ethernet access ports on the FortiGate (directly connected endpoints or unmanaged switches where endpoints connect).





- Wireless via built-in access point on a FortiWiFi unit



For all other FortiGate related connections to be managed by FortiNAC, do not use this document. Refer to one of the following in the Document Library:

- Clients connecting to a FortiSwitch: FortiSwitch Integration
- Clients connecting to a FortiAP: FortiAP Integration Guide
- Clients connecting through FortiGate VPN tunnel: FortiGate VPN Device Integration

What it Does

FortiNAC provides network visibility (where endpoints connect) and manages network access at the point of connection at the FortiGate for the endpoint. This is accomplished by sending the appropriate configuration commands to the device.

How it Works

Visibility
FortiNAC learns where endpoints are connected on the network using the following methods:

- RADIUS communication
- Device Detection SNMP traps
- L2 Polling (MAC address table read)
- L3 Polling (ARP cache read)

Control FortiWiFi Connections: FortiNAC provisions a wireless device's network access by assigning VLANs during RADIUS authentication. In addition, firewall policies can be applied to the connected device's session.

Control Wired Interfaces: FortiNAC provisions a wired device's network access by applying a firewall policy to the connected device's session. VLANs are not assigned.

FortiGates/FortiSwitches managed by FortiManager: When FortiNAC makes any changes to the FortiGate or FortiSwitch, the Fortigate/FortiSwitch updates FortiManager. This keeps FortiManager in sync.

Device Support Methods - FortiWiFi

Device Support Method	Protocol
Network Device Management/Device Discovery	SNMP (UDP 161) SSH (TCP 22)
Dynamic Connection Status	RADIUS 802.1x or MAC-auth (UDP 1812) RADIUS Accounting (UDP 1813)
L2 Poll (Collect MAC Address information)	SSH (TCP 22) REST API (TCP 443 or as defined on FortiGate)
L3 Poll (Collect IP to MAC address information)	SNMP (UDP 161) SSH (TCP 22) REST API (TCP 443 or as defined on FortiGate)
Provision Network Access/VLAN Assignment	VLANs: RADIUS 802.1x or MAC-auth (UDP 1812) Firewall policies: • Fortinet Security Fabric (FSSO) (TCP 8000 (Private Protocol)) • CLI (SSH TCP 22)
De-auth	RADIUS Disconnect (UDP 3799) RADIUS Change of Authentication (CoA) (UDP 3799)

Device Support Methods – Wired Interfaces

Device Support Method	Protocol
Network Device Management/Device Discovery	SNMP (UDP 161) SSH (TCP 22)
Dynamic Connection Status	RADIUS 802.1x or MAC-auth (UDP 1812) RADIUS Accounting (UDP 1813) Device Detection SNMP Trap
L2 Poll (Collect MAC Address information)	SSH (TCP 22) REST API (TCP 443 default)
L3 Poll (Collect IP to MAC address information)	SNMP (UDP 161) SSH (TCP 22) REST API (TCP 443 default)
Provision Network Access/VLAN Assignment	Firewall policies: • Fortinet Security Fabric (FSSO) (TCP 8000 (Private Protocol)) • CLI (SSH TCP 22)

Requirements

FortiNAC

- Supported Engine Version: 8.5 or greater
- Recommended Engine Version: 8.8.5 or greater
- Multiple VDOM/Split-Task VDOM support: Version 8.8.8, 9.1.2 or greater

FortiGate

- Support Firmware Version: 6.0.5 or greater.
- Recommended Firmware Version:
  - 6.2: 6.2.8 or greater
  - 7.0: (if using post-login banner) Requires FortiNAC 8.8.8 or greater. See KB article 193514 for details
- Enable FortiGate admin-https-ssl-versions tlsv1-2. Tlsv1-3 is not supported.
- SNMP community or account
- Administrator account
  - Visibility only: System read access to all VDOMs
  - Control: System read/write access to all VDOMs

Considerations

- As of version 8.7.6 and 8.8.2, the use of Syslog is no longer recommended due to performance and scalability issues. Configure Device Detection traps instead. Syslog configuration information has been moved to the Appendix for reference.
- FortiGate versions 6.2.1 and below: FortiGate does not respond to RADIUS CoA unless the root VDOM is used (Bug ID 562861).

- FortiGate can only support one FSSO agent sending tags for a specific endpoint IP address. If there are multiple agents, the FortiGate entries will be overwritten when other FSSO agents send information for the same endpoint IP. Therefore, the following should be done prior to integration:
  - Identify any other FSSO agents that provide logon information for the same endpoints FortiNAC would be managing through the FortiGate. For additional information, see section **Agent-based FSSO** in the FortiOS 6.0.0 Handbook:

    https://docs2.fortinet.com/document/fortigate/6.0.0/handbook/482937/agent-based-fsso

  - For those agents, logon events must be blocked. See related KB article

    Excluding IP addresses from FSSO logon events

    https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD45566

  - Develop a plan to make the appropriate modifications to existing firewall policies to accommodate FortiNAC as the FSSO agent for the managed endpoint IP address scope.

General Configuration

Configure FortiGate

SNMP (System Level)

SNMP is required for communication with FortiNAC and must be configured. SNMP versions 1, 2c and 3 are supported.

1. In the FortiGate UI, navigate to **System > SNMP.**
2. Enable **SNMP Agent.**
3. Under the appropriate SNMP Protocol (v1/v2c or v3), click **Create New** to create a new Community to use with FortiNAC or verify the following are already configured in an existing Community.
4. Click **OK** to save any modifications.

SNMP Settings (v1/v2c)

Community Name	Community Name
Enabled	Selected
Hosts	**IP Address**: <eth0 IP address of FortiNAC Control Server> **Host Type**: Accept Queries Only
Queries	V1 or v2 enabled **Port:** 161
Traps	V1 or v2 enabled **Port:** 162
SNMP Events	<all disabled>

SNMP Settings (v3)

User Name	User Name
Enabled	Selected
Security Level	Authentication (No Private) • **Authentication Algorithm**: SHA1 or MD5 • **Password** Authentication (Private) • **Authentication Algorithm**: SHA1 or MD5 • **Password** • **Encryption Algorithm**: DES or AES256
Hosts	**IP Address**: <eth0 IP address of FortiNAC Control Server> **Host Type**: Accept Queries Only
Queries	Enabled **Port:** 161
Traps	Enabled **Port:** 162
SNMP Events	<all disabled>

Management Interface

Configure the interface used to communicate with FortiNAC to allow the required protocols.

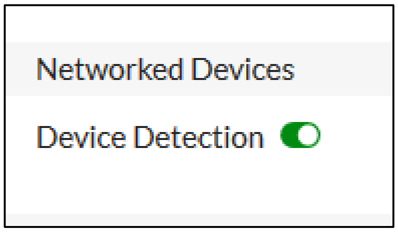
1. In the FortiGate UI, navigate to **Network > Interfaces.**
2. Double click the interface whose IP address will be used to communicate with FortiNAC**.**
3. Under **Administrative Access**, enable the following protocols: HTTPS, HTTP, SNMP and RADIUS Accounting.
4. Click **OK** to save any modifications.

General Interface

FortiNAC requires device identification enabled in order to process connection information for the interface. This can be configured using either the FortiGate UI or CLI.

FortiGate UI

1. In UI navigate to **Network > Interfaces**
2. Select the interface, right-click and select **Edit**
3. Enable **Device Detection** and click **OK**



Networked Devices

Device Detection ●

FortiGate CLI

config system interface
edit "<*name*>"
set device-identification enable
set device-identification-active-scan enable
next

Example

```
config system interface
    edit "Managed Ports"
        set vdom "root"
        set ip 172.28.10.1 255.255.255.0
        set allowaccess ping snmp radius-acct
        set type hard-switch
        set security-mode 802.1X
        set security-mac-auth-bypass enable
        set security-groups "Radius Servers"
        set device-identification enable
        set device-identification-active-scan enable
        set role lan
        set snmp-index 8
    next
    edit "lan 100"
        set vdom "root"
        set ip 172.17.100.1 255.255.255.0
        set allowaccess ping snmp capwap
        set device-identification enable
        set device-identification-active-scan enable
        set role lan
        set snmp-index 14
        set interface "lan"
        set vlanid 100
    next
end
```

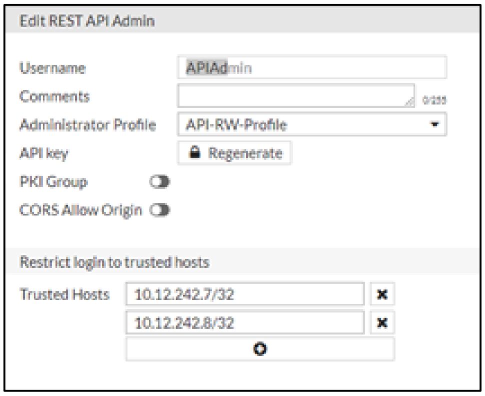
System Administrator Account

A System Administrator account is used for SSH and REST API access on the FortiGate. To create or view user accounts, navigate to **System > Administrators**.

REST API Administrator Account (Optional)

In FortiNAC version 8.8.3 and higher, a FortiGate REST API Administrator key can be used in addition to the System Administrator Account. The API key allows FortiNAC to bypass the need to authenticate every time it connects, improving performance.

1. Navigate to **System > Administrators**
2. Click **Create New > REST API Admin**.
3. Configure the settings as needed.



Edit REST API Admin

Username	APIAdmin
Comments	0/255
Administrator Profile	API-RW-Profile
API key	Regenerate
PKI Group	
CORS Allow Origin	

Restrict login to trusted hosts

Trusted Hosts	10.12.242.7/32 ✖ 10.12.242.8/32 ✖

4. Click **OK**. The New API key window opens.
5. Copy the key to the clipboard and click **Close**.

6. Click **OK**.

Save the key for use in the FortiNAC configuration section.

REST API

REST API is required for communication with FortiNAC and must be configured. Verify the appropriate port is configured:

1. In the FortiGate UI, navigate to **System > Settings.**
2. Under **Administration Settings**, modify the **HTTPS port** as necessary (another service may already use 443).
3. Click **Apply** to save any modifications.

Configure FortiNAC

Add Device Model

1. In the FortiNAC Administration UI, navigate to **Network Device > Topology.**

2. Discover or add the FortiGate. Include the following:

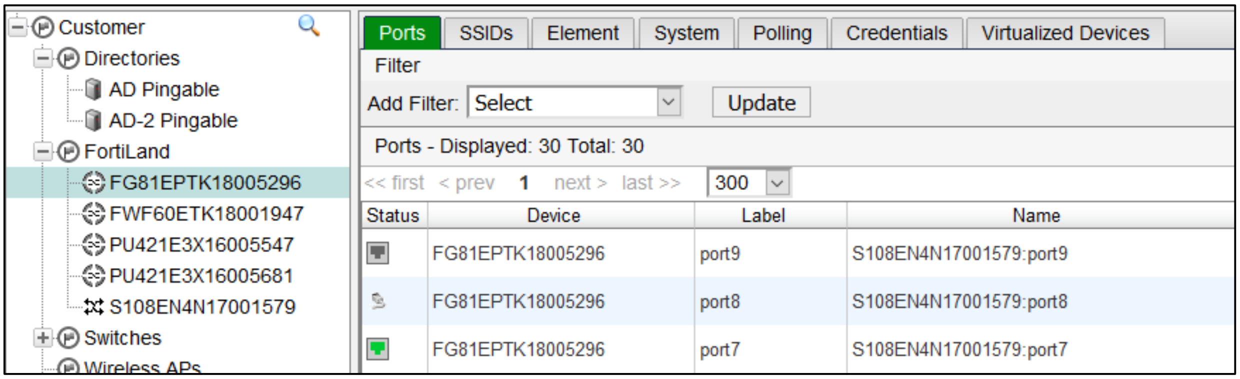
   SNMP Settings: SNMP v1 or v3 credentials used for device discovery and ARP collection/L3 polling

   CLI Settings: Administrator account credentials used for API access.

   Instructions in the Administration Guide (Tip: Open in New Tab)
   Single device: **Add or modify a device**
   Multiple devices: **Discovery**

   Note: If a "?" appears as the icon, then support needs to be added for that device. See KB article Options for Devices Unable to Be Modeled in Topology for instructions.

The FortiGate will display in Topology as a wireless device since it can act as a wireless controller. Device Type will show the part number.

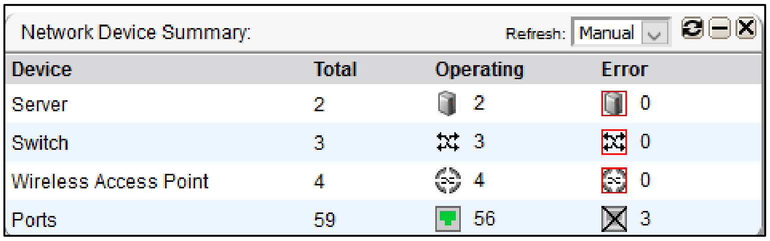


Add Filter: Select

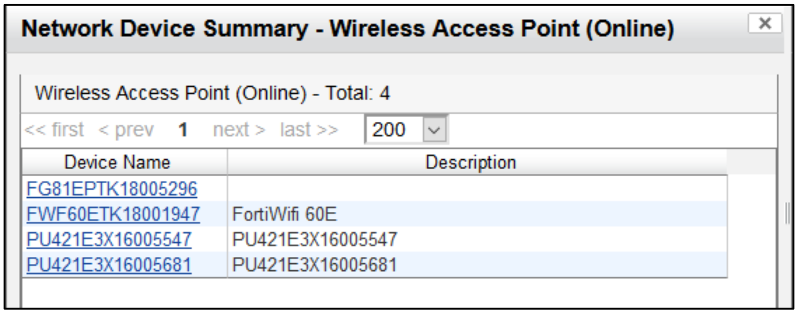
Ports - Displayed: 30 Total: 30

Status	Device	Label	Name
▪	FG81EPTK18005296	port9	S108EN4N17001579:port9
	FG81EPTK18005296	port8	S108EN4N17001579:port8
🟩	FG81EPTK18005296	port7	S108EN4N17001579:port7

Since the FortiGate displays as a wireless device, the Network Device Summary panel under **Bookmarks > Dashboard** lists FortiGate models as Wireless Access Points. Clicking on the ⊗ icon lists the devices.



Device	Total	Operating	Error
Server	2	2	0
Switch	3	3	0
Wireless Access Point	4	4	0
Ports	59	56	3


Network Device Summary - Wireless Access Point (Online)
<< first < prev 1 next > last >>
200

Wireless Access Point (Online) - Total: 4

Device Name	Description
FG81EPTK18005296	
FWF60ETK18001947	FortiWifi 60E
PU421E3X16005547	PU421E3X16005547
PU421E3X16005681	PU421E3X16005681

3. Once added, right click on the model and select **Resync Interfaces**. The ports will be listed under the **Ports** tab.

4. Enable L3 Polling. Right click on the model in the left panel and select **Group Membership**.

5. Check the box next to **L3 Polling (IP→MAC)** and click **OK.**

6. Click the **Polling** tab.
   a. Check the box next to **L2 Hosts Polling**. If configuring Device Detection traps, set the **L2 (Hosts) Polling** value for 15 minutes.
   b. Check the box next to **L3 (IP→MAC) Polling**.
   c. Click **Save**.

7. If utilizing the FortiGate API key (FortiNAC versions 8.8.3 and greater), login to the FortiNAC CLI as root and enter the following:

   ```
   Device -ip <FortiGate model IP> -SetAttr -name APIToken -value <API Key>
   logout
   ```

Proceed to one of the following sections:
WiFi Configuration
Wired Port Configuration

WiFi Configuration

RADIUS Authentication

When a wireless client attempts to connect, the FortiWiFi sends a RADIUS request to FortiNAC. Accounting messages inform FortiNAC of any hosts that have disconnected.

- **MAC-based Authentication**: Endpoints are authenticated based on the MAC address. This requires no configuration on the endpoint.

- **802.1x Authentication**: Endpoints are authenticated based on user information.

Network Requirements

- 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.
- **Important:** 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 FortiNAC is going to be installed in an environment where it is expected to receive more than 60 RADIUS requests per second, an additional FortiNAC appliance may be required to handle the load.

802.1x RADIUS Server

In 802.1X environments, 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.

Controllers/APs Requirements

- 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 to throttle the rate of connection requests accepted from any individual host using the rate-limiting features available on the wireless device.
- 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.

- 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.
- Do not set FortiNAC as the trap receiver on any wireless devices. FortiNAC does not process traps from wireless devices.
- 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.

Configure FortiGate

General Configuration

Define FortiNAC as RADIUS Server

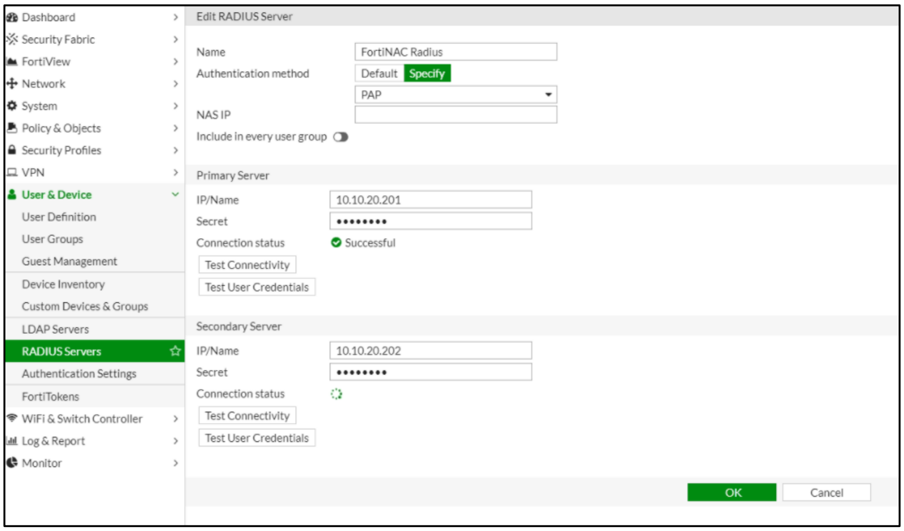
1. In the FortiGate UI, navigate to **User & Device > RADIUS Servers**
2. Click **Create New**
3. Configure using the chart below
4. Click **OK** to save

RADIUS Settings

Name	Name of FortiNAC Server
Authentication Method	PAP (required for MAC-Authentication only)
Primary Server	FortiNAC Server/Control server eth0 interface IP Address **High Availability:** IP address of primary control server (Do not use Shared IP address)
Secret	**Important:** must be exactly the same on the FortiWiFi device and in the FortiNAC software in the FortiWiFi Model Configuration.
Secondary Server	**High Availability:** IP address of secondary control server (Do not use Shared IP address)
Change of Authorization (CoA)	Enabled (Disabled by default) Note: This setting can only be enabled via CLI
Authentication port	UDP 1812
Accounting	Enabled (Disabled by default) Note: This setting can only be configured via CLI

Note the following:

- Multiple VDOM/Split-Task VDOMs: RADIUS settings must be configured for each VDOM sending RADIUS requests to FortiNAC.
- RADIUS timeouts should be large enough to allow some transaction delays. Many devices use default timeout values under 10 seconds. It is recommended to use larger values for busy environments, though experimentation to find the optimal value may be needed.
- Regardless of the environment, consider setting up the actual RADIUS server as a backup to be used in the event that none of the FortiNAC appliances can be reached. This would allow users to access the network, but they would not be controlled by FortiNAC.



Edit RADIUS Server

Name: FortiNAC Radius
Authentication method: Default [✓ Specify]
PAP
NAS IP
Include in every user group ○

Primary Server
IP/Name: 10.10.20.201
Secret: ••••••••
Connection status: ✓ Successful
Test Connectivity
Test User Credentials

Secondary Server
IP/Name: 10.10.20.202
Secret: ••••••••
Connection status
Test Connectivity
Test User Credentials

5. Configure COA and Accounting. Login as admin and use the following commands in sequence:

```
config user radius
edit "<name>"
set radius-coa enable
set acct-all-servers enable

config accounting-server
edit 1
set status enable
set server "<FortiNAC eth0 IP>"
set secret <secret value used previously>
next
end
next
end
```

FortiGate CLI Configuration Example

```
config user radius
    edit "FortiNAC Radius"
        set server "10.10.20.201"
        set secret ENC
UjjrEu9QWWaRs3IhyicgkvU9bFTAn17DKgyZa/ZVmJPS8gHZNZysw/XRSRBlZmw1CYs36F
91stvX
        set acct-all-servers enable
        set radius-coa enable
        set auth-type pap
        set secondary-server "10.10.20.202"
        set secondary-secret ENC
jbBET+y1KNbd28Q+7kebzySPohXC7UGRqkgrU2EW5yD8kSXwyqzNcJlLxh9SbGD0EapJTN
EMzD0p
```

```
config accounting-server
    edit 1
        set status enable
        set server "10.10.20.201"
        set secret ENC
```

Proceed to one of the following sections:
WiFi Using VLANs
WiFi without VLANs

WiFi Using VLANs

SSID

When a host connects to a SSID on the FortiGate, VLANs are assigned to provision network access. DHCP addressing is provided to isolated hosts by FortiNAC. DHCP addressing is provided to registered hosts by the production DHCP server.

Configure the SSID's that will be placed under enforcement:

1. Navigate to **Network > Interfaces**
2. Click **Create New > Interface**
3. Configure using the chart below
4. Click **OK** to save

Interface Settings (Using VLANs)

Interface Name	Wifi SSID interface name (must be unique). FortiNAC creates the interface models using these names.
Type	WiFi SSID
IP/Network Mask	IP address and mask for the SSID interface
Administrative Access	Select the following: • RADIUS Accounting • PING
DHCP Server	Disabled
WiFi Settings	**SSID:** Same as interface name or another name of choice **Security Mode:** WPA2 Enterprise **Broadcast SSID:** enabled **Authentication**: 1. Click RADIUS Server tab 2. Use the drop down to select RADIUS server configured above **Dynamic VLAN Assignment:** Enabled - Allows FortiNAC to assign a VLAN from the authentication response. **Note:** Since Dynamic VLAN assignment is enabled, it is not necessary to assign an IP address to the SSID interface.

VLANs

Ensure VLANs are configured and working on the FortiGate for all FortiNAC states desired to be enforced (Registration, Remediation, etc).

1. Navigate to **Network > Interfaces**

   Note: The newly created Wifi Interfaces should display under the **WiFi** section at the bottom of the view.
2. Select **Create New > Interface**
3. Configure using the parameters below
4. Click **OK**.

Required “Isolation” VLAN Settings

Interface Name	VLAN Interface name
Type	VLAN
Interface	WiFi SSID interface name
VLAN ID	VLAN number
Role	LAN
DHCP Server	Enabled
DHCP Server Mode (Expand **Advanced** to expose this option)	Relay
DHCP Server IP	FortiNAC eth1 IP address

Required “Production” VLAN Settings

Interface Name	VLAN Interface name
Type	VLAN
Interface	WiFi SSID interface name
VLAN ID	VLAN number
Role	LAN
DHCP Server	Optional
DHCP Server Mode	Optional
DHCP Server IP	Optional

Proceed to Configure FortiNAC.

WiFi without VLANs

SSID

When a host connects to a SSID on the FortiGate, firewall policies are used to provision network access. The host's IP address does not change when network access changes.

When managing FortiGate SSID's, FortiGate acts as the DHCP server. The DNS server list provided by DHCP must contain:

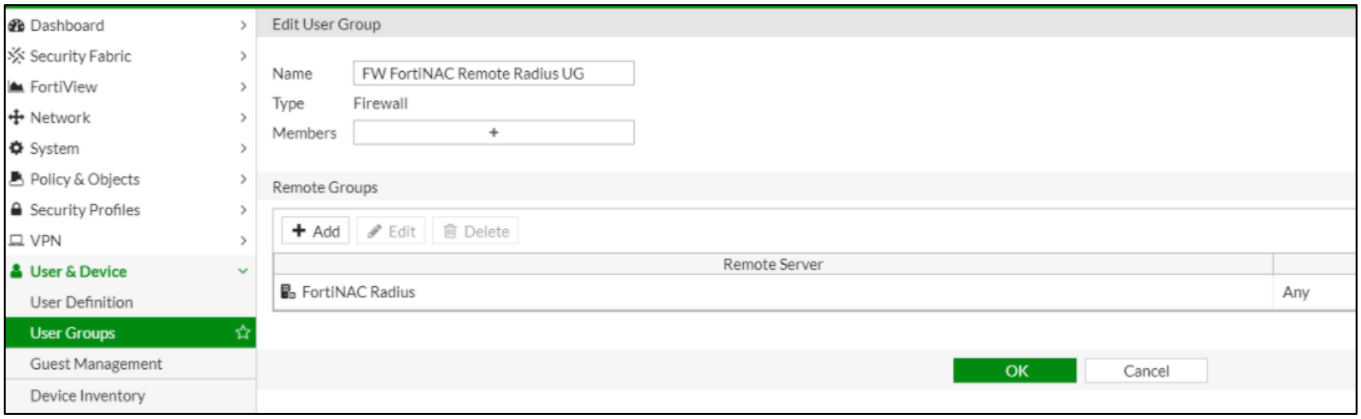
- FortiNAC Server/Application Server eth1 IP address
- Production DNS server(s)

Interface Settings (Not Using VLANs)

Interface Name	Wifi SSID interface name (must be unique). FortiNAC creates the interface models using these names.
Type	WiFi SSID
IP/Network Mask	IP address and mask for the SSID interface
Administrative Access	Select the following: • RADIUS Accounting • PING
DHCP Server	Enabled Under Address Range click **Create New** • Specify IP range and mask • Default Gateway • DNS Server: Specify <Application Server eth1 IP, Production DNS IP>
WiFi Settings (example)	**SSID:** Same as interface name or another name of choice **Security Mode:** WPA2 Personal **Pre-Shared Key**: <if WPA2 Personal> **Broadcast SSID**: enabled **Filter clients by MAC Address:** enabled **RADIUS server:** 1. Toggle to Enable 2. Use the drop down to select RADIUS server configured above

User Group for RADIUS

1. In FortiGate UI, navigate to **User & Device > User Groups**
2. Click **Create new**
3. Name the Group
4. Select Type: **Firewall**
5. Under Remote Groups click **Add**
6. Click the drop down menu and select the RADIUS server(s) configured in previous step
7. Click **OK**
8. Click **OK** again



Edit User Group

Name: FW FortiNAC Remote Radius UG

Type: Firewall

Members: +

Remote Groups

Remote Server	
FortiNAC Radius	Any

Proceed to Configure FortiNAC

Configure FortiNAC

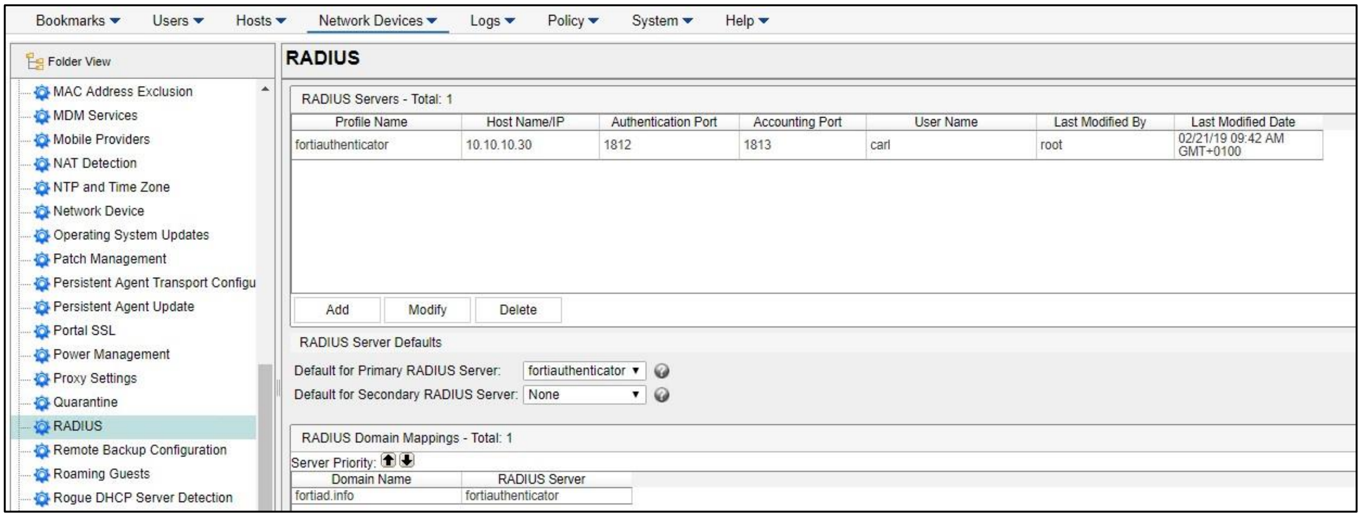
General Configuration

802.1x RADIUS Server (Optional)

Required for 802.1x authentication configurations.

FortiNAC acts as a proxy for 802.1X requests. Add a RADIUS server (such as FortiAuthenticator) to FortiNAC in order to proxy the 802.1X packets to the correct server. See **Configure RADIUS Server Profiles** in the Online Help or Administration and Operation guide for instructions.

Important: The RADIUS Secret used must be exactly the same on the RADIUS server.



RADIUS

RADIUS Servers - Total: 1

Profile Name	Host Name/IP	Authentication Port	Accounting Port	User Name	Last Modified By	Last Modified Date
fortiauthenticator	10.10.10.30	1812	1813	carl	root	02/21/19 09:42 AM GMT+0100

RADIUS Server Defaults

Default for Primary RADIUS Server: fortiauthenticator

Default for Secondary RADIUS Server: None

RADIUS Domain Mappings - Total: 1

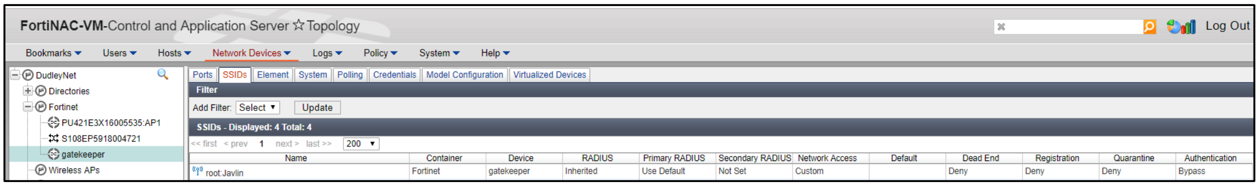
Server Priority:

Domain Name	RADIUS Server
fortiad.info	fortiauthenticator

Note: FortiNAC does not proxy RADIUS requests when using MAC authentication.

Validate SSID Visibility

1. In the FortiNAC Administration UI, navigate to **Network Devices > Topology**.
2. Click on the FortiGate model in the left column then click the **SSIDs** tab.
3. Verify the new SSID is listed. If not, right click on the model name in left column and select **Resync Interfaces**. The view may need to be refreshed in order for the new SSID(s) to appear.



Add Filter: Select

SSIDs - Displayed: 4 Total: 4

Name	Container	Device	RADIUS	Primary RADIUS	Secondary RADIUS	Network Access	Default	Dead End	Registration	Quarantine	Authentication
root:Javlin	Fortinet	gatekeeper	Inherited	Use Default	Not Set	Custom		Deny	Deny	Deny	Bypass

4. Click on the **Ports** tab of the FortiGate.
5. Poll the FortiGate to read the MAC address table (L2 Poll) and ARP cache (L3 Poll). Click the **Polling** tab in the right panel of the FortiGate model.
   - Click **Poll Now** next to **L2 (Hosts) Polling**
   - Click **Poll Now** next to **L3 (IP → MAC) Polling**

Define 802.1x RADIUS Server in FortiGate Model (Optional)

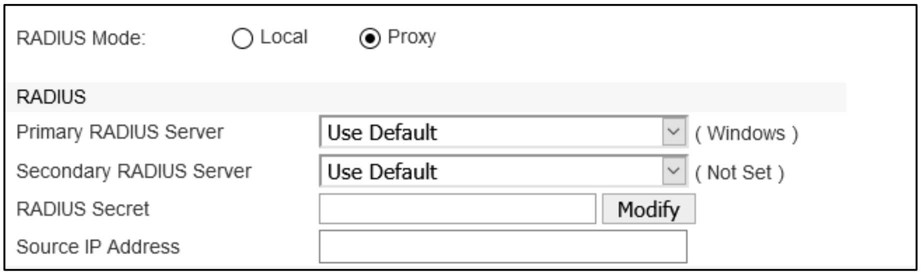
Required for 802.1x authentication.

The RADIUS server(s) FortiNAC uses to proxy the requests can be configured at the model or SSID level. Must be configured for each VDOM sending RADIUS to FortiNAC (Multiple VDOM/Split-Task VDOM support requires FortiNAC version 8.8.8, 9.1.2 or greater).

1. Right click the FortiGate model and select **Model Configuration**.

2. Configure per the chart below then click **Apply**.

RADIUS Mode	Select Proxy or Local see RADIUS in the Administration Guide for details
Primary RADIUS Server (Proxy Mode)	RADIUS servers FortiNAC will proxy the RADIUS requests
Secondary RADIUS Server (Proxy Mode)	RADIUS servers FortiNAC will proxy the RADIUS requests if Primary is not available
RADIUS Secret	**Important:** The RADIUS Secret used must be exactly the same on the FortiGate device, the RADIUS server (if 802.1X is used) and FortiNAC software under RADIUS Settings and FortiGate Model Configuration
Source IP Address	FortiGate IP address sending RADIUS



RADIUS Mode: ○ Local ● Proxy

RADIUS

Primary RADIUS Server: Use Default (Windows)

Secondary RADIUS Server: Use Default (Not Set)

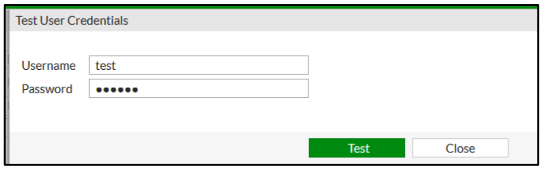
RADIUS Secret:

Source IP Address:

Validate RADIUS Connectivity

Verify FortiGate can successfully validate user credentials with FortiNAC using RADIUS. This tests the connection between the FortiGate and FortiNAC only. The credentials entered are validated against the FortiNAC database and does not test 802.1x proxy.

1. In the FortiGate UI, navigate to **User & Device > RADIUS Servers**
2. Double click on the RADIUS server for FortiNAC created previously.
3. Click **Test User Credentials**
4. Enter the user ID of a user present in FortiNAC database (to view user records, navigate to **Users > User View** in the FortiNAC UI).
5. Click **Test**



Test User Credentials

Username: test

Password: ••••••

Proceed to one of the following sections:
WiFi Using VLANs
WiFi Using Policies

WiFi Using VLANs

Review Enforcement Checklist

Before enabling enforcement, verify the following:

- There are no rogue MAC addresses connected to the SSID.
  Important: Rogue MAC addresses detected on enforced interfaces will be isolated.
- Isolation VLANS are working.

Network Access Policies

Network Access Policies can be created to provide flexible network assignments based on different host and user criteria.

Location based policies can be created based on SSID. Assign SSID models to port groups and include the port groups within the User/Host Profile.

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.

For more information on policy configuration, refer to Network Access Policies in the Administration Guide in the Fortinet Document Library.

Enable Enforcement

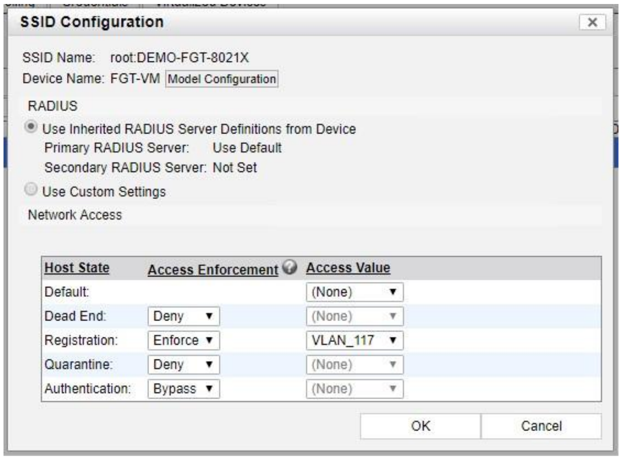
To place SSIDs under FortiNAC's control, assign VLANs and enable enforcement for the various host states in the SSID model of the FortiGate.

Important: Always validate behavior on a test SSID first.

1. With the FortiGate's model selected in the left panel, click the **SSIDs** tab in the right panel.

2. Click the desired SSID, right click and select **SSID Configuration**.

3. (Optional) Click **Use Custom Settings** to configure a RADIUS server different than the FortiGate's RADIUS configuration.



SSID Name: root:DEMO-FGT-8021X

Device Name: FGT-VM Model Configuration

RADIUS

● Use Inherited RADIUS Server Definitions from Device

Primary RADIUS Server: Use Default

Secondary RADIUS Server: Not Set

○ Use Custom Settings

Network Access

Host State	Access Enforcement	Access Value
Default:		(None)
Dead End:	Deny	(None)
Registration:	Enforce	VLAN_117
Quarantine:	Deny	(None)
Authentication:	Bypass	(None)

4. Under **Network Access**, fill in the following fields as they apply. See **Model Configuration** in the Online Help or Administration and Operations guide for definitions of Host State, Access Enforcement and Access Value.
   - VLAN ID for each state (Registration, Remediation, Authentication, Deadend)
   - VLAN ID Default (the "catch all" VLAN for registered endpoints).

5. Click **OK** to save changes.

Validate Enforcement

1. Connect a rogue host to the newly enforced SSID.
2. Verify the following:
   - Host is moved to the Isolation VLAN
   - Host is able to access the captive portal (if configured)
   - Register the system and make sure it gets moved to the appropriate VLAN.

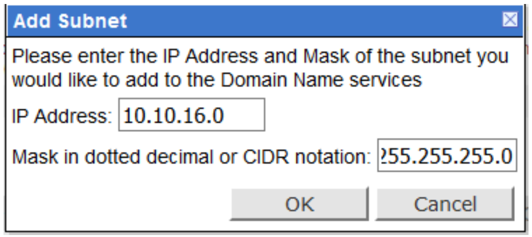
If any of the above do not work as expected, refer to the Troubleshooting section of this document.

WiFi Using Policies

Configure NAC DNS to Respond to FortiGate Isolation Scope

By default, FortiNAC only accepts DNS requests from the subnet or subnets defined by the Isolation scopes. Using Configuration Wizard, configure FortiNAC to accept DNS requests from the address range provided by FortiGate DHCP.

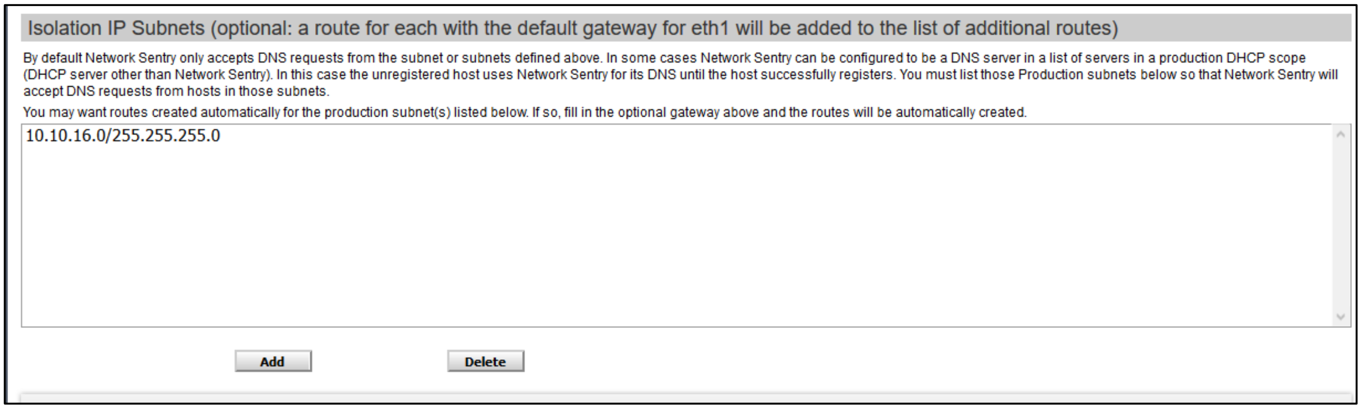
1. Navigate to **https://<FortiNAC Control Server IP or name>:8443/configWizard/**
2. Click **OK** twice to pass by the License Key and documentation pages and reach the Basic Network page
3. In the left hand column, click Isolation
4. Under Isolation IP Subnets, click **Add**
5. Ender the subnet(s) defined in the DHCP IP address range configured in section Configure SSID(s).



Please enter the IP Address and Mask of the subnet you would like to add to the Domain Name services

IP Address: 10.10.16.0

Mask in dotted decimal or CIDR notation: 255.255.255.0



Isolation IP Subnets (optional: a route for each with the default gateway for eth1 will be added to the list of additional routes)

By default Network Sentry only accepts DNS requests from the subnet or subnets defined above. In some cases Network Sentry can be configured to be a DNS server in a list of servers in a production DHCP scope (DHCP server other than Network Sentry). In this case the unregistered host uses Network Sentry for its DNS until the host successfully registers. You must list those Production subnets below so that Network Sentry will accept DNS requests from hosts in those subnets.

You may want routes created automatically for the production subnet(s) listed below. If so, fill in the optional gateway above and the routes will be automatically created.

10.10.16.0/255.255.255.0

Configure Security Fabric Connection and Policies

Refer to **Fortinet Security Fabric Integration Guide** in the Fortinet Library to complete the following steps:

- Create FortiNAC Network Access Policies
- Create FortiGate Firewall Policies
- Establish Security Fabric Connection between FortiNAC and FortiGate

Review Enforcement Checklist

Before enabling enforcement, verify the following:

- There are no rogue MAC addresses connected to the SSID.
  Important: Rogue MAC addresses detected on enforced interfaces will be isolated.
- Isolation VLANS are working.

Enable Enforcement

To place SSIDs under FortiNAC's control, enable enforcement for the various host states in the SSID model of the Fortigate.

Important: Always validate behavior on a test SSID first.

1. With the FortiGate's model selected in the left panel, click the **SSIDs** tab in the right panel.

2. Click the desired SSID, right click and select **SSID Configuration**.

3. (Optional) Click **Use Custom Settings** to configure a RADIUS server different than the FortiGate's RADIUS configuration.

4. Under Network Access, set the Access Enforcement for each Host State to be enforced to **Bypass**. Setting the Network Access to Bypass allows FortiNAC respond to RADIUS requests for hosts in those states without including any VLAN or role information in the response packet. The Network Access values will be assigned via FSSO once the host is authenticated via RADIUS.

5. Click **OK** to save changes.

Validate Enforcement

1. Connect a rogue host to one of the ports added to the interface
2. Host receives IP address from FortiGate
3. Host is able to access the captive portal (if configured)

   The FortiGate CLI can be used to verify FortiGate received and processed the Group or Firewall Tag information from FortiNAC:
   diagnose debug authd fsso list

   The results should show the IP, user ID and Group Membership.

4. Register the host and verify the correct network access is provisioned. Use the FortiGate CLI command above to view the IP, user ID and Group Membership.

   Example output:

   ```
   ----FSSO logons----
   IP: 10.10.79.51  User: BOBBYO  Groups: REGISTERED HOSTS
   Workstation:  MemberOf: Authorized Assets
   Total number of logons listed: 1, filtered: 0
   ----end of FSSO logons----
   ```

If any of the above do not work as expected, refer to the Troubleshooting section of this document.

Wired Port Configuration

Determine the Appropriate Dynamic Connection Status Method

In addition to scheduled L2 polls, FortiNAC learns of endpoints connecting and disconnecting from the Ethernet interfaces using the below dynamic methods. Choose the method that is most appropriate for the environment (only one method must be used).

Device Detection SNMP Trap (FortiNAC version 8.7.6, 8.8.2 or higher): When a host connects, the FortiGate updates its Device Inventory and sends a SNMP trap to FortiNAC. **Note:** FortiGate does not send a message when hosts disconnect. Host continues to show online in FortiNAC until the next L2 poll of the FortiGate. See Determining Offline Status in Appendix for details.

Use Cases:

- Endpoints directly connected to FortiGate ports.
- Endpoints whose traffic is managed by the FortiGate but directly connected network infrastructure is not modeled in FortiNAC. Note that in this network design, FortiNAC will show these host record locations as connecting to the FortiGate.

RADIUS Authentication: When a host attempts to connect, the FortiWiFi sends a RADIUS request to FortiNAC. Accounting messages inform FortiNAC of any hosts that have disconnected. Both MAC-based and 802.1x Authentication are supported.

- Network Requirements: 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.
- 802.1x RADIUS Server: In 802.1X environments, 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.

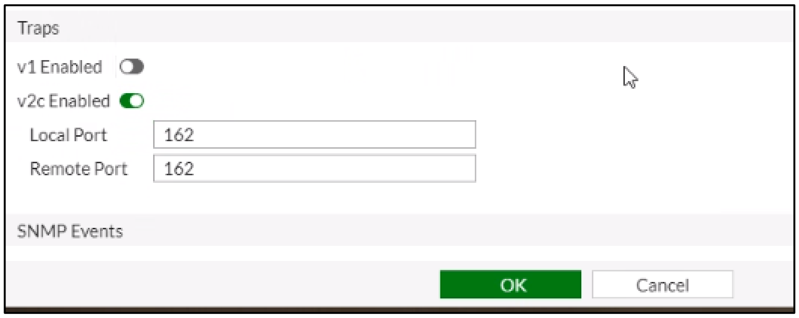
Click on the appropriate link below to continue FortiGate configuration:
Device Detection SNMP Trap
RADIUS

Configure FortiGate

Device Detection Traps

1. Navigate to **System > SNMP**.
2. Modify the SNMP Community created previously.
3. Under the **Traps** section, toggle (enable) **v2c Enabled**

   Note: v1 traps currently not supported.



Traps

v1 Enabled ○

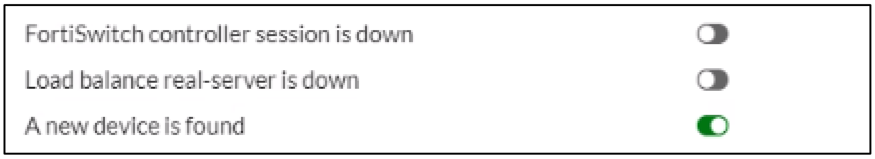
v2c Enabled ●

Local Port 162

Remote Port 162

SNMP Events

4. Under **SNMP Events**, toggle (enable) **A new device is found**.
5. Click **OK** to save.



FortiSwitch controller session is down ○

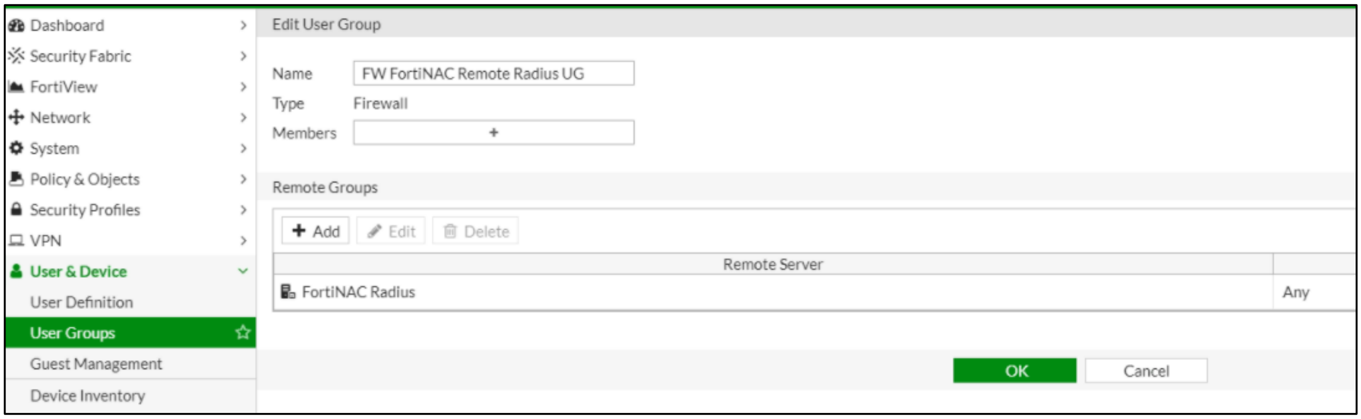
Load balance real-server is down ○

A new device is found ●

Proceed to Port Interfaces.

User group for RADIUS

1. In FortiGate UI, navigate to **User & Device > User Groups**
2. Click **Create new**
3. Name the Group
4. Select Type: **Firewall**
5. Under Remote Groups click **Add**
6. Click the drop down menu and select the RADIUS server(s) configured in previous step
7. Click **OK**
8. Click **OK** again



Edit User Group

Name: FW FortiNAC Remote Radius UG
Type: Firewall
Members: +

Remote Groups

Remote Server	
FortiNAC Radius	Any

Proceed to Port Interfaces.

Port Interfaces

When a host connects to a port on the Fortigate, firewall policies are used to provision network access. The host's IP address does not change when network access changes.

When managing FortiGate ports, FortiGate acts as the DHCP server. The DNS server list provided by DHCP must contain:

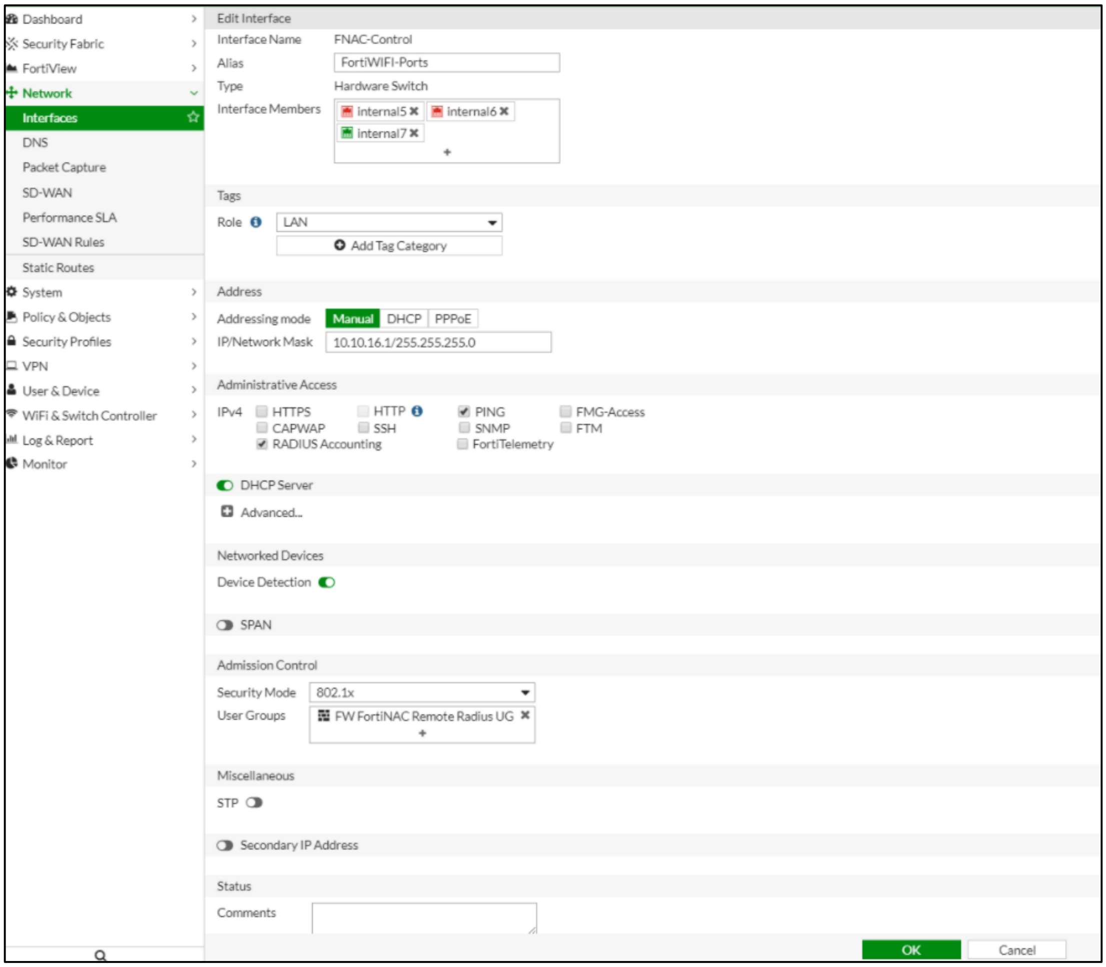
- FortiNAC Server/Application Server eth1 IP address
- Production DNS server(s)

Configure the ports that will be placed under enforcement:

1. Navigate to **Network > Interfaces**
2. Click **Create New > Interface**
3. Configure using the chart below
4. Click **OK** to save

Interface Settings

Interface Name	Name of Interface (example: FNAC-Control)
Type	Hardware Switch
Interface Members	Select ports to be managed by FortiNAC **Note:** It is recommended to add a minimal number of ports during initial configuration for testing purposes.
Addressing Mode	Manual
IP/Network Mask	IP address and mask for the interface
Administrative Access	Select the following: RADIUS Accounting PING
DHCP Server	Enabled Under Address Range click **Create New** • Specify IP range and mask • Default Gateway: • DNS Server: Specify <Application Server eth1 IP, Production DNS IP>
Security Mode	802.1x
User Groups	Select newly created Remote Group
Security mac authentication bypass	Enabled (disabled by default). When enabled, FortiGate will send a MAC authentication request if there is no supplicant included. Note: This setting can only be configured via CLI



Edit Interface

Interface Name FNAC-Control

Alias FortiWIFI-Ports

Type Hardware Switch

Interface Members internal5 ✖ internal6 ✖ internal7 ✖ +

Tags

Role LAN

Add Tag Category

Address

Addressing mode Manual DHCP PPPoE

IP/Network Mask 10.10.16.1/255.255.255.0

Administrative Access

IPv4 □ HTTPS □ HTTP ☑ PING □ FMG-Access
□ CAPWAP □ SSH □ SNMP □ FTM
☑ RADIUS Accounting □ FortiTelemetry

DHCP Server

Advanced...

Networked Devices

Device Detection

SPAN

Admission Control

Security Mode 802.1x

User Groups FW FortiNAC Remote Radius UG ✖ +

Miscellaneous

STP

Secondary IP Address

Status

Comments

OK Cancel

5. Login as admin and use the following commands in sequence:
   config system interface
   edit “<interface name>”
   set security-mac-auth-bypass enable
   next
   end

Note: A warning may display. Acknowledge warning to continue.

Example

```
config system interface
    edit "FNAC-Control"
        set vdom "root"
        set ip 10.10.16.1 255.255.255.0
        set allowaccess ping radius-acct
        set type hard-switch
        set alias "FortiWIFI-Ports"
        set security-mode 802.1X
        set security-mac-auth-bypass enable
        set security-groups "FW FortiNAC Remote Radius UG"
        set device-identification enable
        set role lan
        set snmp-index 8
    next
end
```

Configure FortiNAC

Validate Port Visibility

1. In the FortiNAC UI, poll the FortiGate to read the MAC address table (L2 Poll) and ARP cache (L3 Poll). Click the **Polling** tab in the right panel of the FortiGate model.
   a. Click **Poll Now** next to **L2 (Hosts) Polling**
   b. Click **Poll Now** next to **L3 (IP → MAC) Polling**

2. Click on the **Ports** tab of the FortiGate.

3. Review the values populated for each port (Label, Connection State, etc) and verify they are accurate.

4. If the **Adapter** tab is not already visible, click the **Show Details Panel** button at the bottom of the window.

5. Verify connection information for hosts currently connected to those is accurate by clicking on one of the ports showing a connection. The adapter tab below should reflect the correct Adapter Status, Host Status, IP Address, Physical (MAC) Address and Location. If connection information is not correct, see Inaccurate Port Connection Information in the Troubleshooting section.

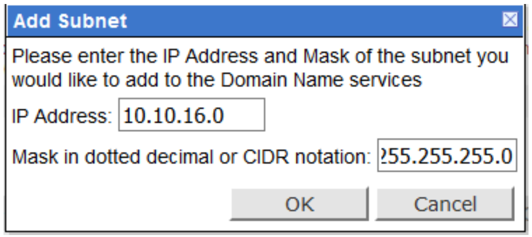
6. Connect a host to one of the wired ports and verify the view updates.

7. Disconnect the host and verify the port view updates:
   a. **Device Detection Trap**: View should update upon the next L2 poll. Alternatively, force the poll by selecting the **Polling** tab and click **Poll Now** for L2 Polling.
   b. **RADIUS**: view should update upon receipt of accounting message from FortiGate (which occurs immediately after disconnect).

Configure NAC DNS to Respond to FortiGate Isolation Scope

By default, FortiNAC only accepts DNS requests from the subnet or subnets defined by the Isolation scopes. Using Configuration Wizard, configure FortiNAC to accept DNS requests from the address range provided by FortiGate DHCP.

1. Navigate to **https://<FortiNAC Control Server IP or name>:8443/configWizard/**
2. Click **OK** twice to pass by the License Key and documentation pages and reach the Basic Network page
3. In the left hand column, click Isolation
4. Under Isolation IP Subnets, click **Add**
5. Ender the subnet(s) defined in the DHCP IP address range configured in section Create Port Interfaces in FortiGate.

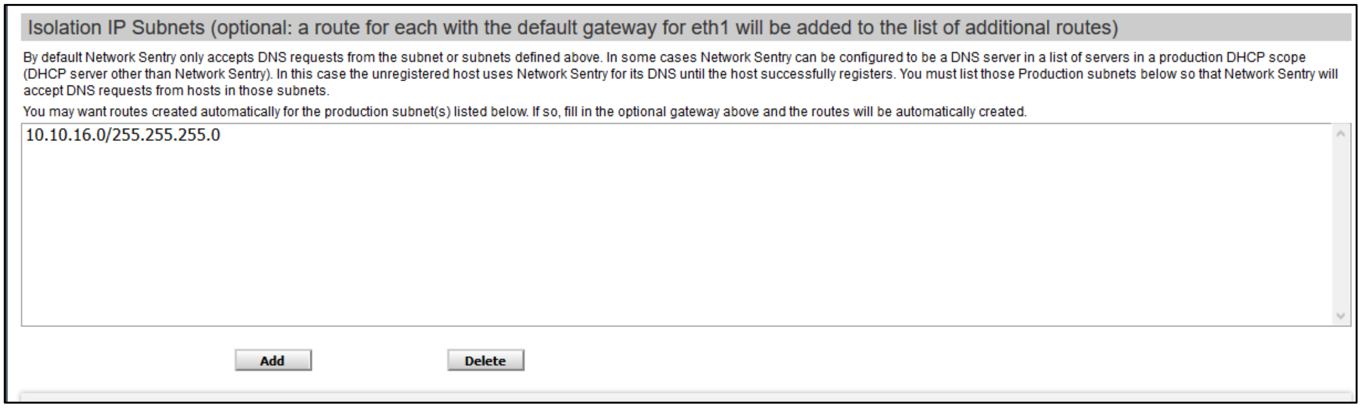


Add Subnet

Please enter the IP Address and Mask of the subnet you would like to add to the Domain Name services

IP Address: 10.10.16.0

Mask in dotted decimal or CIDR notation: 255.255.255.0



Isolation IP Subnets (optional: a route for each with the default gateway for eth1 will be added to the list of additional routes)

By default Network Sentry only accepts DNS requests from the subnet or subnets defined above. In some cases Network Sentry can be configured to be a DNS server in a list of servers in a production DHCP scope (DHCP server other than Network Sentry). In this case the unregistered host uses Network Sentry for its DNS until the host successfully registers. You must list those Production subnets below so that Network Sentry will accept DNS requests from hosts in those subnets.

You may want routes created automatically for the production subnet(s) listed below. If so, fill in the optional gateway above and the routes will be automatically created.

10.10.16.0/255.255.255.0

Configure Security Fabric Connection and Policies

Refer to **Fortinet Security Fabric Integration** reference manual in the Fortinet Document Library to complete the following steps:

- Create FortiNAC Network Access Policies
- Create FortiGate Firewall Policies
- Establish Security Fabric Connection between FortiNAC and FortiGate

Validate Enforcement

1. Connect a rogue host to one of the managed ports
2. Host receives IP address from FortiGate
3. Upon bringing up browser, the captive portal is displayed (if configured). If portal page is slow to build, certain domains may need to be whitelisted. See KB article Captive Portal Slow to Build.
4. Register the system
5. Once registered, verify the correct Network Access Policy matches in FortiNAC
    a. In FortiNAC UI, navigate to **Hosts > Host View**
    b. Search on host record, right click and select **Policy Details**
6. Verify the correct IPv4 Policy matches in the FortiGate
    a. In FortiGate UI, navigate to **FortiView > Sources**
    b. Double click on host entry
    c. Click **Policies** tab
    d. Hover over policy to verify time last used

If any of the above do not work as expected, refer to the **Troubleshooting** section of this document.

Troubleshooting

Unable to Connect Using SNMP

Refer to KB article Troubleshooting SNMP Communication Issues.

Inaccurate Host Connection Information

1. Click the **Polling** tab and verify **L2 (Hosts) Polling** and **L3 (IP-->MAC) Polling** completed. The timestamps for **Last Successful Poll** and **Last Attempted Poll** should be the same.

2. If Last Successful Poll is not current, see KB article Troubleshooting Poll Failures.

If host connection information does not update dynamically, refer to the applicable KB article:
Troubleshooting RADIUS clients not connecting
Troubleshooting Device Detection traps

Related KB Articles

Refer to the applicable KB article(s):
Rogue Wireless Clients Cannot Connect to SSID
Troubleshooting Wireless Clients Moved to the Wrong VLAN

Debugging

FortiGate Commands

Enable debugging feature

```
diagnose debug enable
```

Run the applicable debug
“:” MAC Address filtering

```
diagnose wireless-controller wlac sta_filter <STA MAC>255 diagnose
```

MAC Authentication / PSK

```
debug application wpad 8 (WPA deamon)
```

802.1X

```
diagnose debug app eap_proxy 31 (EAP deamon)
```

RADIUS Disconnect

```
diag debug app radius-das 8
```

Disable debugging feature

```
diagnose debug disable
```

List currently connected hosts:

```
diagnose debug authd fsso list
```

Example output:

```
----FSSO logons----
IP: 172.28.10.2  User: 00:21:70:D1:92:77  Groups: REGISTERED
Workstation:  MemberOf: Registered
Total number of logons listed: 1, filtered: 0
----end of FSSO logons----
```

FortiNAC Commands

Use the following KB article to gather the appropriate logs using the debugs below.
Gather logs for debugging and troubleshooting

Note: Debugs disable automatically upon restart of FortiNAC control and management processes.

Function	Syntax	Log File
FortiNAC Server (Proxy RADIUS)	`nacdebug -name RadiusManager true`	/bsc/logs/output.master
FortiNAC Server (Local RADIUS)*	`nacdebug -name RadiusAccess true`	/bsc/logs/output.master
RADIUS Service (Local RADIUS)	`radiusd -X -l /var/log/radius/radius.log` Stop logging: Ctrl-C	/var/log/radius/radius.log
L2 related activity	`nacdebug -name BridgeManager true`	/bsc/logs/output.master
FortiGate wired port specific	`nacdebug -name Fortinet true`	/bsc/logs/output.master
FortiGate wireless specific	`nacdebug -name FortiAP true`	
SSO activity**	`nacdebug -name SSOManager true`	/bsc/logs/output.master
SNMP activity	`nacdebug -name SnmpV1 true`	/bsc/logs/output.master

Device Detection Trap processing	`nacdebug -name DeviceInterface true`
	`nacdebug -name BridgeManager true`
	`nacdebug -name SnmpV1 true`
		/bsc/logs/output.master

Disable debug	`nacdebug -name <debug name> false`	N/A

Note: If not using VLANs, will always return policy value “NativePolicy” in RADIUS response. Otherwise, a VLAN value is returned.

*Enables logging for a given MAC Address:

```
nacdebug -logger 'yams.RadiusAccess.RadiusAccessEngine.00:11:22:33:44:55' -level
FINEST
```

**SSO communication:
As of version 8.8.5, logon and logoff messages are written to **/bsc/logs/output.master** in the FortiNAC CLI by default without debug enabled.

Logon Sample message:
FortiGate IP: 10.0.0.1
Client IP address: 10.0.0.10
Client MAC address = 00:09:B0:DA:40:C9
SSO Tag = Production

```
yams.SSOManager INFO :: 2021-02-23 07:33:25:003 ::
SSOManager.sendMessage sending message to 10.0.0.1 for client
00:09:B0:DA:40:C9
com.bsc.plugin.manager.SSOManager$DeviceMessage[logon,
mac=00:09:B0:DA:40:C9, ip=10.0.0.10, tags=[Production]]
```

Other Tools

Send a RADIUS Disconnect:

```
SendCoA -ip <devip> -mac <clientmac> -dis
```

Example:

```
SendCoA -ip 10.1.0.25 -mac 00:1B:77:11:CE:2F -dis
```

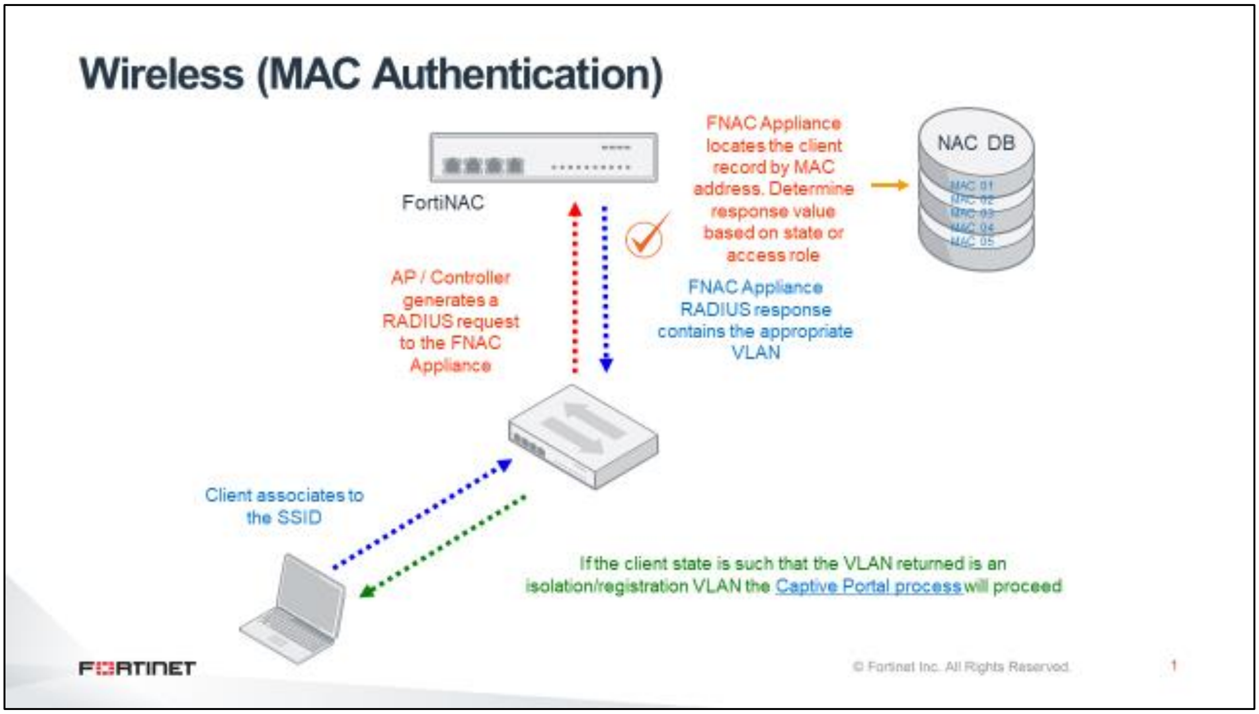
Appendix

RADIUS Authentication

MAC Authentication

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)

FNAC Appliance locates the client record by MAC address. Determine response value based on state or access role

AP / Controller generates a RADIUS request to the FNAC Appliance

FNAC Appliance RADIUS response contains the appropriate VLAN

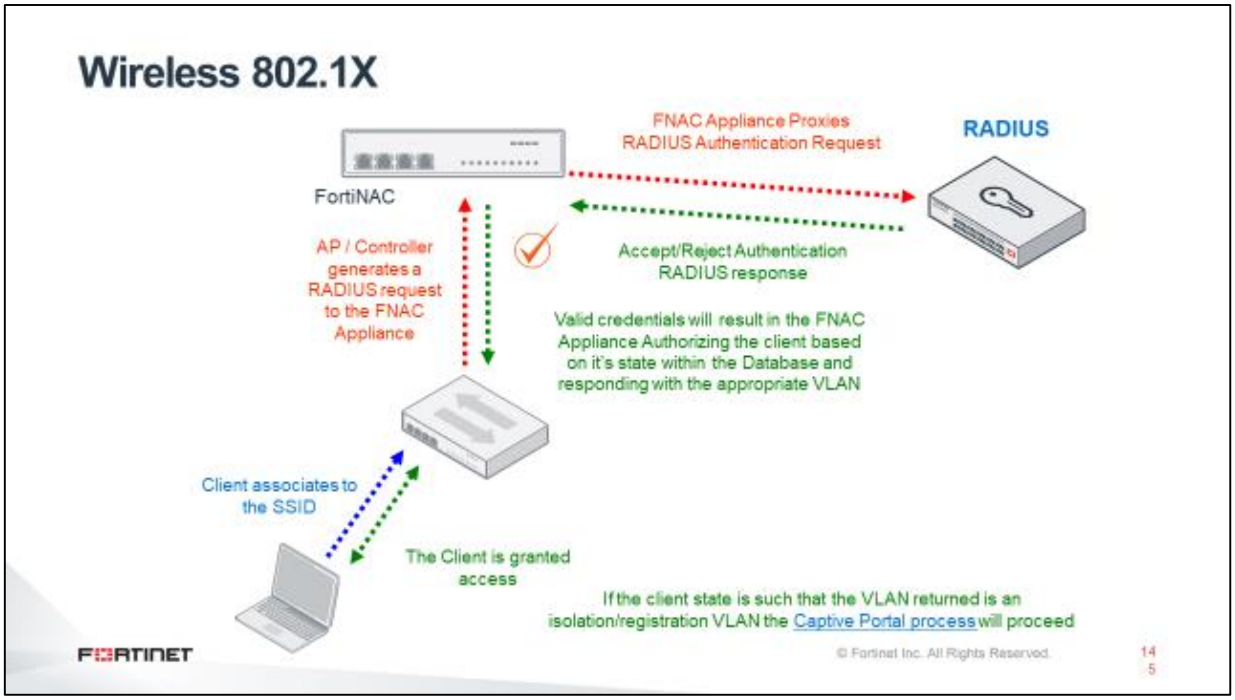
Client associates to the SSID

If the client state is such that the VLAN returned is an isolation/registration VLAN the Captive Portal process will proceed

© Fortinet Inc. All Rights Reserved. 1

802.1X Authentication

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.



Wireless 802.1X

FortiNAC
RADIUS
FNAC Appliance Proxies RADIUS Authentication Request
Accept/Reject Authentication RADIUS response
AP / Controller generates a RADIUS request to the FNAC Appliance
Valid credentials will result in the FNAC Appliance Authorizing the client based on it's state within the Database and responding with the appropriate VLAN
Client associates to the SSID
The Client is granted access
If the client state is such that the VLAN returned is an isolation/registration VLAN the Captive Portal process will proceed
FORTINET
© Fortinet Inc. All Rights Reserved.
14
5

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

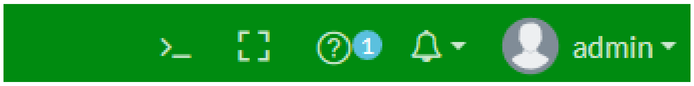
The following EAP types have not yet been tested with FortiNAC:

- EAP-MD-5
- EAP-Fast
- Cisco LEAP

FortiGate CLI Access

From FortiGate CLI:

The FortiGate UI can be used to initiate SSH sessions: click on the ">_" icon in the upper right corner of the page.



Determining Offline Status

FortiNAC versions 8.8.2 and Below

During L2 poll, FortiNAC uses the FortiGates **last_seen** attribute to determine online/offline status. When poll is performed, if the last_seen value is greater than 5 minutes (300000 milli secs) FortiNAC will "logoff" the FSSO session on the FortiGate, removing the FSSO tag.

To verify, enable SSOManager debug and review output.master output:

```
PollThread-poll0 com.bsc.forwarding.Fortigate endpoint json =
{"os":{"src":"http","name":"Windows"},"hardware_vendor_signature_id":0
,"last_seen":922,"master_mac":"xx:xx:xx:xx:xx:xx"...
```

FortiNAC versions 8.8.3 and Above

During L2 poll, FortiNAC now only filters for online entries. The FortiGate determines online/offline status based on the how long the device has been idle in seconds. The default idle time is 5 minutes (300 seconds) and can be modified via the FortiGate CLI (see below). Once a host is determined to be offline by the FortiGate, the host will also be marked offline in FortiNAC after the next L2 poll.

Online/Offline record status on the FortiGate can been seen on the **User & Device > Device Inventory View**.

Modify timeout in FortiGate CLI:

```
config system global
set device-idle-timeout 300
end
```

Manually remove a client from the table via the FortiGate CLI:

```
diagnose user device del xx:xx:xx:xx:xx:xx
```

API Calls Made to FortiGate During Poll

Layer 2 Poll

```
yams.Fortigate.FortigateCommon INFO :: 2020-11-30 12:37:44:723 ::
PollThread-trap2 request WebTarget =
https://10.12.240.13:443/api/v2/monitor/user/detected-
device?filter=is_online%3D%3Dtrue&global=1
yams.Fortigate.FortigateCommon INFO :: 2020-11-30 12:37:44:830 ::
PollThread-trap2 request WebTarget =
https://10.12.240.13:443/api/v2/monitor/wifi/client/select?global=1
yams.Fortigate.FortigateCommon INFO :: 2020-11-30 12:37:44:926 ::
PollThread-trap2 request WebTarget =
https://10.12.240.13:443/api/v2/monitor/vpn/ssl/select?vdom=%2A
yams.Fortigate.FortigateCommon INFO :: 2020-11-30 12:37:46:995 ::
PollThread-trap2 request WebTarget =
https://10.12.240.13:443/api/v2/monitor/vpn/ipsec/select?vdom=%2A
```

FSWs linked to the FortiGate

```
https://10.180.2.6:443/api/v2/monitor/switch-controller/managed-switch
```

Layer 3 Poll

```
yams.Fortigate.FortigateCommon INFO :: 2020-11-30 13:37:23:288 ::
pool-5-thread-1 request WebTarget =
https://10.12.240.13:443/api/v2/cmdb/system/vdom
SSH to the device
modify each vdom returned by the previous command
issue a "get system arp" in each vdom and exit
yams.Fortigate.FortigateCommon INFO :: 2020-11-30 13:37:23:677 ::
pool-5-thread-1 request WebTarget =
https://10.12.240.13:443/api/v2/monitor/user/detected-
device?filter=is_online%3D%3Dtrue&global=1
yams.Fortigate.FortigateCommon INFO :: 2020-11-30 13:37:23:787 ::
pool-5-thread-1 request WebTarget =
https://10.12.240.13:443/api/v2/monitor/vpn/ipsec/select?vdom=%2A
yams.Fortigate.FortigateCommon INFO :: 2020-11-30 13:37:23:884 ::
pool-5-thread-1 request WebTarget =
https://10.12.240.13:443/api/v2/monitor/vpn/ssl/select?vdom=%2A
```

Syslog

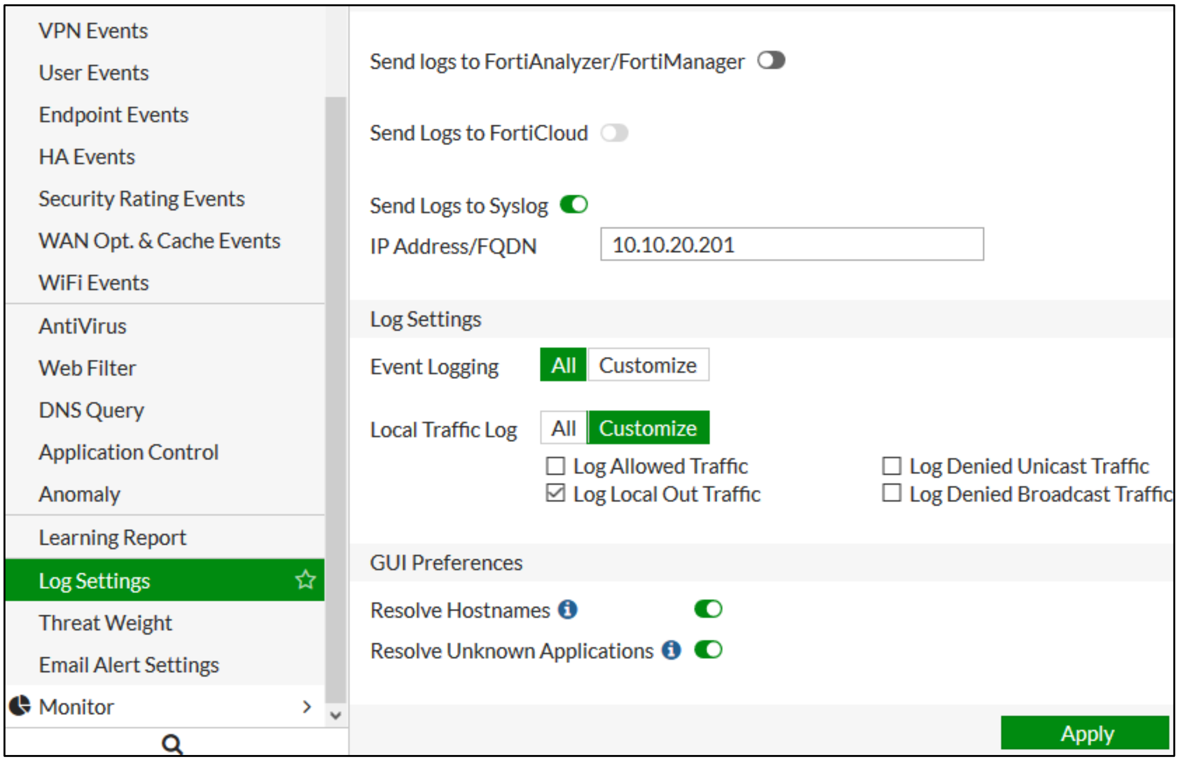
This section is for informational purposes only for existing syslog configurations. As of versions 8.7.6 and 8.8.2, the use of Syslog is no longer recommended due to performance and scalability issues.

When host connects to the port, the FortiGate sends a Syslog message to FortiNAC. Each Syslog message triggers extensive messaging between FortiNAC and FortiGate.

Note: FortiGate does not send a message when hosts disconnect. Host continues to show online in FortiNAC until the next L2 poll of the FortiGate. See Determining Offline Status in Appendix for details.

FortiGate

1. Navigate to **Log & Report > Log Settings**
2. Enable **Send Logs to Syslog**
3. **IP Address/FQDN:** FortiNAC Server/Control server eth0 interface IP Address
4. Under **Local Traffic Log**, select **Customize** and select **Log Local Out Traffic**
5. Click **Apply**



Send logs to FortiAnalyzer/FortiManager

Send Logs to FortiCloud

Send Logs to Syslog

IP Address/FQDN 10.10.20.201

Log Settings

Event Logging [✓ All] Customize

Local Traffic Log All [✓ Customize]

☐ Log Allowed Traffic
☑ Log Local Out Traffic
☐ Log Denied Unicast Traffic
☐ Log Denied Broadcast Traffic

GUI Preferences

Resolve Hostnames

Resolve Unknown Applications

Apply

FortiNAC

Configure **L2 Polling** frequency for 15 minutes

ARP Data Collection Prioritization

ARP collection can be done via CLI, API and SNMP. If FortiNAC receives ARP data using more than one method, FortiNAC will update tables based upon following precedence:

1. CLI
2. API
3. SNMP