FortiNAC

Aruba Instant AP
Wireless Integration

Version: 8.x

Date: July 26, 2022

Rev: H

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

FORTINET TRAINING AND CERTIFICATION PROGRAM

http://www.fortinet.com/support-and-trainingt/training.html

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 for configuring the Aruba IAP to be managed by FortiNAC. This document details the items that must be configured.

Note: As much information as possible about the integration of this device with FortiNAC is provided. However, the hardware vendor may have made modifications to the device's firmware that invalidate portions of this document. If having problems configuring the device, contact the vendor for additional support.

What it Does

Aruba Instant APs (IAP) can be configured to operate either autonomously (in a cluster) or with a traditional controller. This document discusses only those operating autonomously. In such a deployment, all IAPs in the same subnet communicate with one another to negotiate a master, based on which one has the most uptime. The master assumes ownership of a virtual IP address and runs a virtual controller instance that manages all other IAPs in the cluster. If the AP hosting the master fails, the AP on the same subnet with the next longest uptime will take over, assuming the virtual IP.

FortiNAC controls all IAPs in the cluster (same subnet) by interacting with the master using the virtual IP. All authentication and control of the IAPs in a cluster is accomplished through the master using the virtual IP.

How it Works

Visibility

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

- RADIUS communication
- L2 Polling (MAC address table read)
- L3 Polling (ARP cache read)

Control

FortiNAC provisions an endpoint's network access by managing VLAN assignments based on the Aruba IAP's model configuration or an applicable network access policy and the host state of the device. The VLAN configuration is modified using the appropriate method based upon the vendor and model (see chart below).

Device Support Methods

Endpoint Connectivity Notification	Reading MAC Address Tables (L2 Poll)	Reading IP Tables (L3 Poll)	Reading VLANs	VLAN Assignment	Reading SSIDs	De-auth
RADIUS (802.1x or MAC-auth)	CLI	SNMP + CLI	CLI	RADIUS	CLI	RADIUS Disconnect (UDP 3799)

For more information regarding wireless integrations with FortiNAC, refer to the **Wireless Integration Overview** reference manual in the Fortinet Document Library.

Requirements

- **Aruba**
  - Minimum: ArubaOS 6.1 or higher
  - SNMP community or account
  - Account for SSH or API access
  - RADIUS requests sent from the Virtual IP (VIP)
    - VIP must belong to one of the IAPs
    - Dynamic RADIUS Proxy feature is an option which ensures the VIP is used for RADIUS communication. Refer to the following link for details and configuration:

      https://www.arubanetworks.com/techdocs/Instant_40_Mobile/Advanced/Content/UG_files/Authentication/Dynamic%20Proxy%20RADIUS.htm
  - ESSID names must not include spaces. Otherwise, they will not be parsed correctly.
    - Incorrect: Guest SSID
    - Correct: Guest_SSID

- **FortiNAC**
  - Minimum: Version 6.2 or higher
  - FortiNAC version 8.6.1 required for ArubaOS 8.5
  - Preferred: Version 8.6.2 or higher – see Limitations

Considerations

- FortiNAC versions 8.6.1 and 8.6.2 include several Aruba integration fixes. For details, see 8.6.2 Release Notes in the Fortinet Document Library.
- FortiNAC versions 8.7.5, 8.8.1 and higher include a setting to prevent SSID removal from IAP models.
- Management of wired ports on Aruba IAP is not currently supported.
- In larger deployments, it may be necessary to configure the IAP to send accounting directly to the RADIUS server. This can avoid potential accounting alarms. For details see related KB article 189784.
- A port where the master Aruba Instant AP (IAP) with VIP is connected becomes a “learned uplink”. This type of uplink is not dynamically undone / removed when the IAP (with the VIP) is disconnected from that port. (ID 609046)

Aruba IAP Integration

Configure Access Point

Note: It is recommended that Aruba IAPs are configured with a static IP address. 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.

Before integrating a device with FortiNAC, set up the device on the network and ensure that it is working correctly:

- FortiNAC manages sessions on Instant APs by assigning their roles during authentication. Roles on the IAP may encapsulate either/both VLANs or/and firewall rules. Regardless of which is used, FortiNAC always disconnects sessions in order to transition them between different roles.
- For roles you create to support production and isolation states, confirm that hosts can connect to the device and access the network when assigned to them. When the device is running on your network, begin the integration process with FortiNAC.

WLANs

Use a browser to log into the IAP virtual address and configure the following items:

WLAN Settings

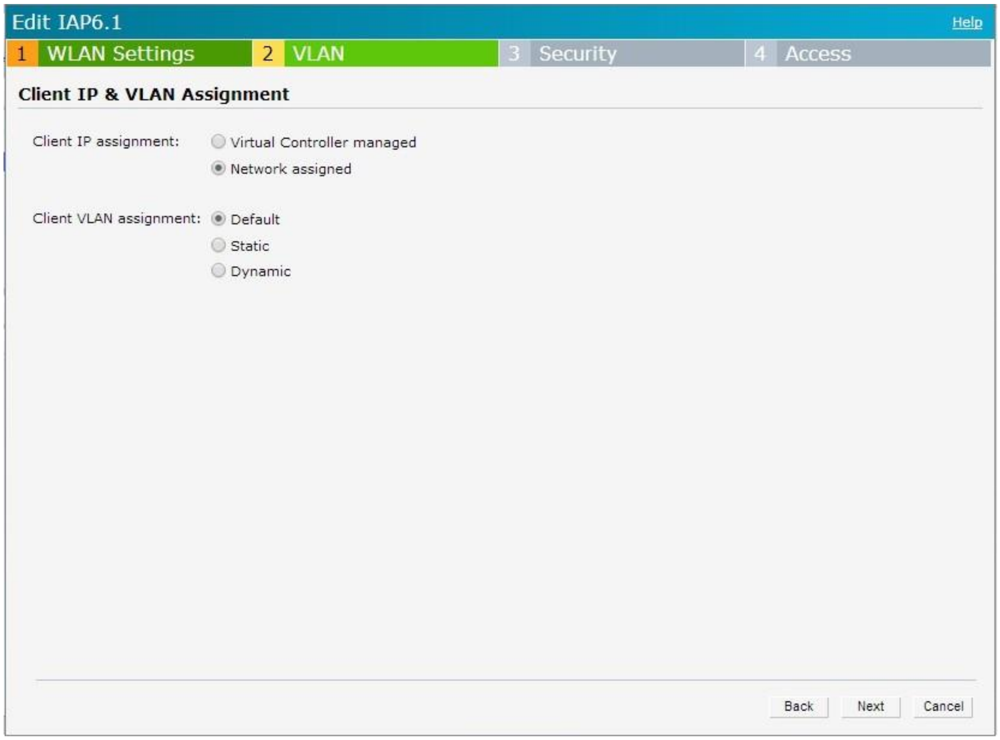
These correspond to the wireless network you want to create. FortiNAC places no constraints on the items configured in this section.

VLAN

FortiNAC has been tested with the following settings:

Client IP Assignment	Network Assigned
Client VLAN Assignment	Default

Note: Other settings have not been validated with FortiNAC.



Client IP & VLAN Assignment

Client IP assignment: ○ Virtual Controller managed ● Network assigned

Client VLAN assignment: ● Default ○ Static ○ Dynamic

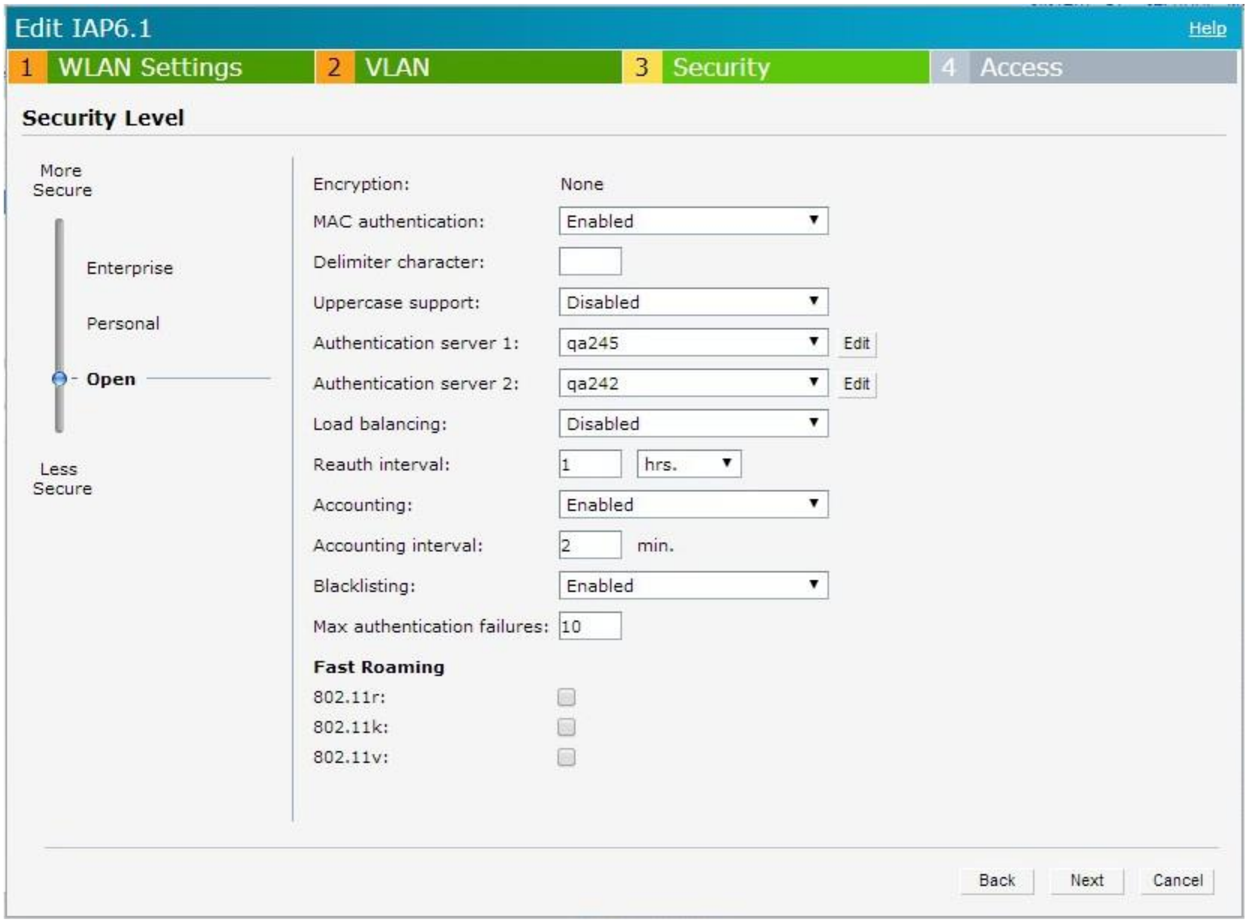
Security

The important settings for this section include:

Security Level	**Enterprise** or **Open** **Note:** The Personal setting has not been validated with FortiNAC.

Required Settings When Security Level = Open

MAC authentication	**Enabled** (Enables RADIUS authentication for the WLAN)
Authentication server 1	Server definition created for FortiNAC Control Server. See Authentication Server.
Accounting	**Enabled**
Accounting interval	Set to as large a value as possible since it is not used by FortiNAC, but does cause some amount of processing to occur.



Security Level

Open

Encryption: None

MAC authentication: Enabled

Delimiter character:

Uppercase support: Disabled

Authentication server 1: qa245

Authentication server 2: qa242

Load balancing: Disabled

Reauth interval: 1 hrs.

Accounting: Enabled

Accounting interval: 2 min.

Blacklisting: Enabled

Max authentication failures: 10

Fast Roaming

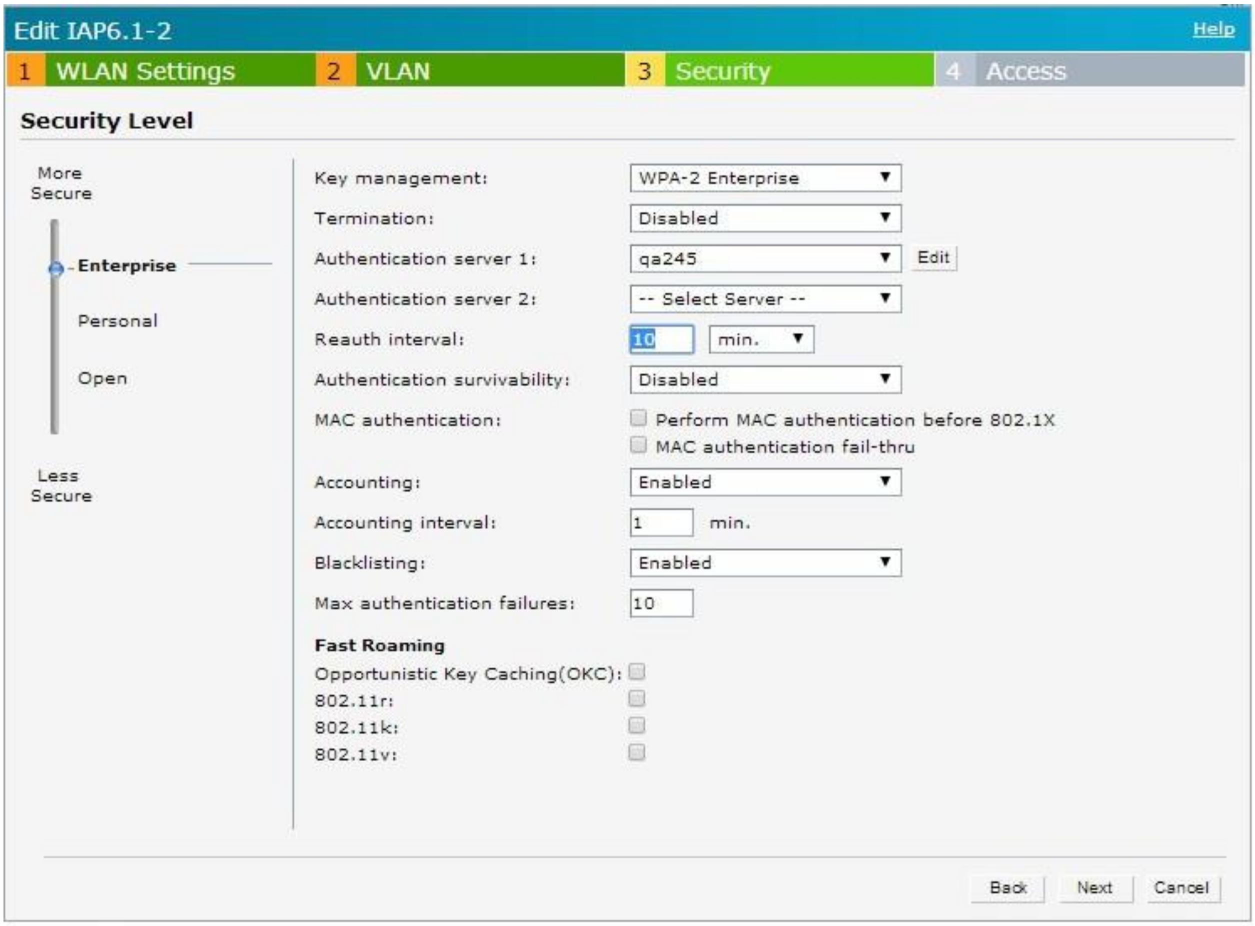
802.11r: □

802.11k: □

802.11v: □

Required Settings When Security Level = Enterprise

MAC authentication	**Perform MAC authentication before 802.1x** (unselected) Selecting this option may cause problems with FortiNAC if policies are configured in FortiNAC to provide different network roles for the device and user. Using both forms of authentication could cause FortiNAC to assign multiple roles to the same session, causing possible problems on the connecting machine. **MAC authentication fail-thru** (unselected)
Authentication server 1	Server definition created for FortiNAC Control Server. See Authentication Server.
Accounting	**Enabled**
Accounting interval	Set to as large a value as possible since it is not used by FortiNAC, but does cause some amount of processing to occur.



Security Level

Key management: WPA-2 Enterprise

Termination: Disabled

Authentication server 1: qa245

Authentication server 2: -- Select Server --

Reauth interval: 10 min.

Authentication survivability: Disabled

MAC authentication: □ Perform MAC authentication before 802.1X
□ MAC authentication fail-thru

Accounting: Enabled

Accounting interval: 1 min.

Blacklisting: Enabled

Max authentication failures: 10

Fast Roaming

Opportunistic Key Caching(OKC): □

802.11r: □

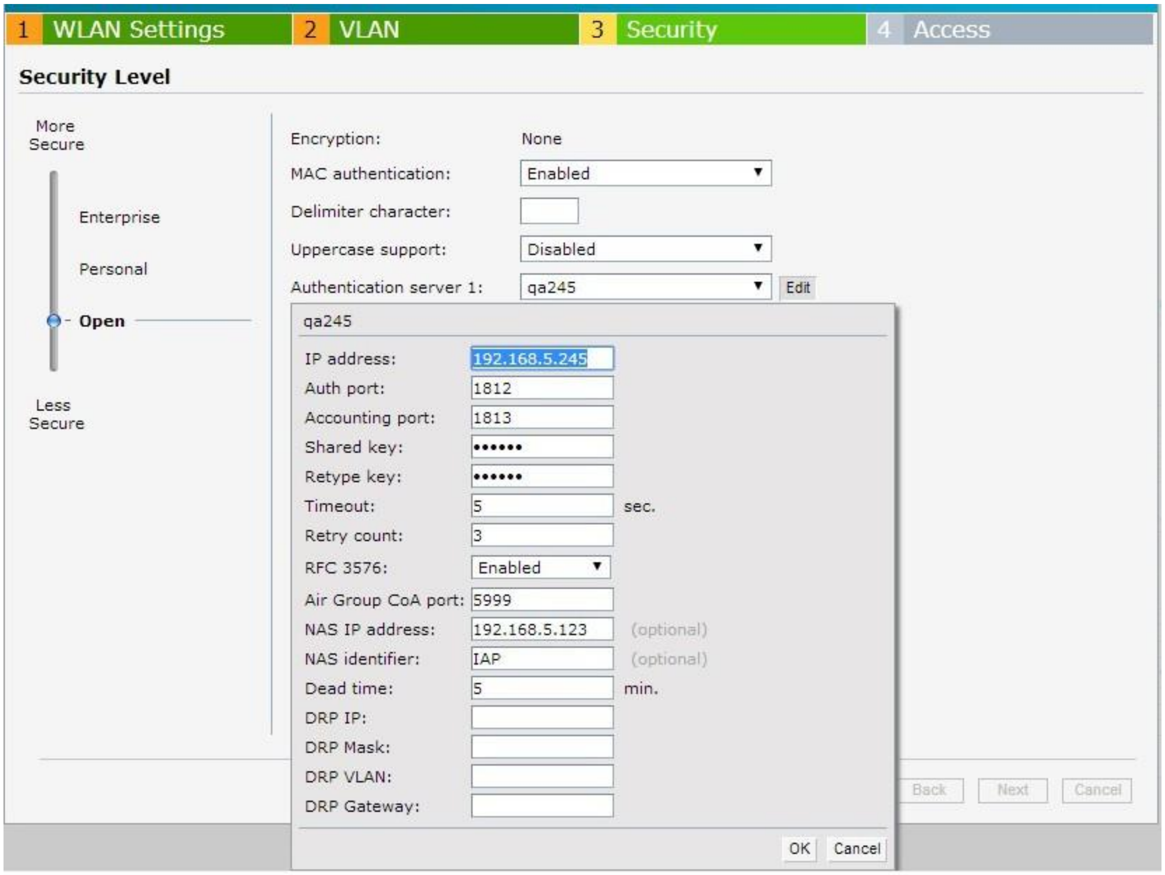
802.11k: □

802.11v: □

Authentication Server

Other settings may be set as desired.

IP Address	Must be the IP address of FortiNAC's physical ethernet interface on the Control Server (not a virtual IP address).
Auth port	Must be **1812**. This is the default port used by FortiNAC to receive RADIUS authentication requests (this can be changed by changing the RADIUS port values in the NS property files.)
Accounting port	must be **1813**. This is the default port used by FortiNAC to receive RADIUS accounting requests (you can change this by changing the RADIUS port values in the property files.)
Shared key	Can be any value but must match the value set in FortiNAC for the Instant AP model.
RFC 3576 **or** **Dynamic Authorization** **(InstantOS 8.5)**	Must be set to **Enabled**. This method is used for client disconnection.
AirGroup CoA port **(InstantOS 8.5)**	3799
NAS IP address	Must be the virtual IP address used for this Instant AP cluster.



Encryption: None
MAC authentication: Enabled
Delimiter character:
Uppercase support: Disabled
Authentication server 1: qa245

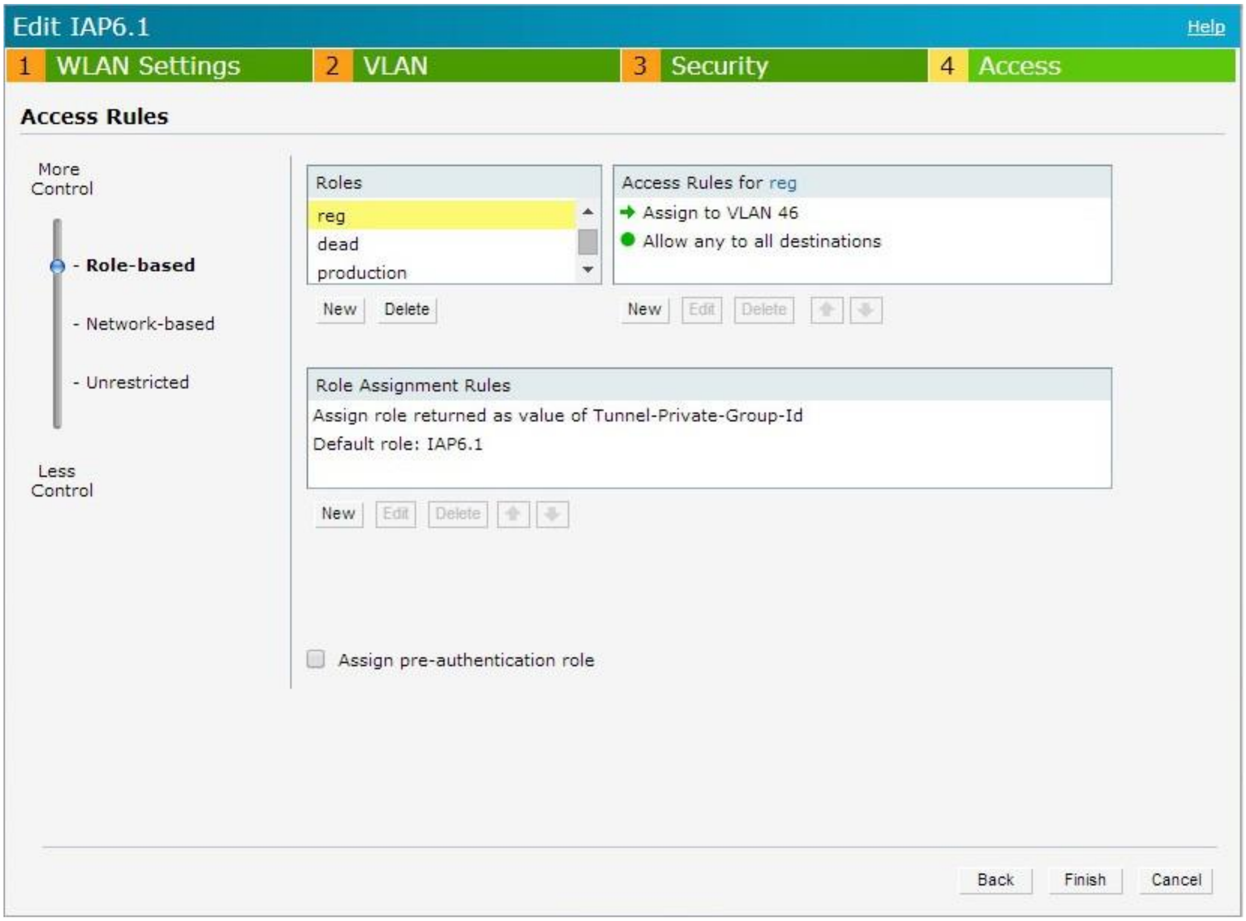
qa245

IP address: 192.168.5.245
Auth port: 1812
Accounting port: 1813
Shared key: ••••••
Retype key: ••••••
Timeout: 5 sec.
Retry count: 3
RFC 3576: Enabled
Air Group CoA port: 5999
NAS IP address: 192.168.5.123 (optional)
NAS identifier: IAP (optional)
Dead time: 5 min.
DRP IP:
DRP Mask:
DRP VLAN:
DRP Gateway:

Access

Access pertains to the roles that can be assigned to client sessions when connecting. FortiNAC requires that the control setting be set to **Role-based**, to allow for dynamic role assignment.

- FortiNAC manages clients on IAPs by assigning them roles appropriate to their state. Roles can encapsulate either VLANs, firewall rules, or both. Roles must be defined for the various networks that you want FortiNAC to assign. In the example below, there are several shown (reg, dead, production). These must have access rules as shown in the Access Rules panel. They should provide the necessary rules and/or VLAN mappings as required for the network.
- A **Role Assignment Rule** must be defined to "**Assign role returned as value of Tunnel-Private-Group-Id**."
- Other settings may be set as desired.



Edit IAP6.1

Access Rules

- Role-based
- Network-based
- Unrestricted

Roles

reg
dead
production

Access Rules for reg

→ Assign to VLAN 46

● Allow any to all destinations

Role Assignment Rules

Assign role returned as value of Tunnel-Private-Group-Id

Default role: IAP6.1

□ Assign pre-authentication role

SNMP

SNMP must be enabled on the IAP to allow FortiNAC to discover and manage the device. FortiNAC can use either the RO or RW community values. Use either SNMPv1 or SNMPv3.

Default CLI Prompt Requirements

FortiNAC must be able to communicate effectively with the device in order to read the session table to determine which hosts are connected and to disassociate or disconnect a host when necessary. FortiNAC communicates with this device via both SNMP and CLI, so the default prompt values should not be altered.

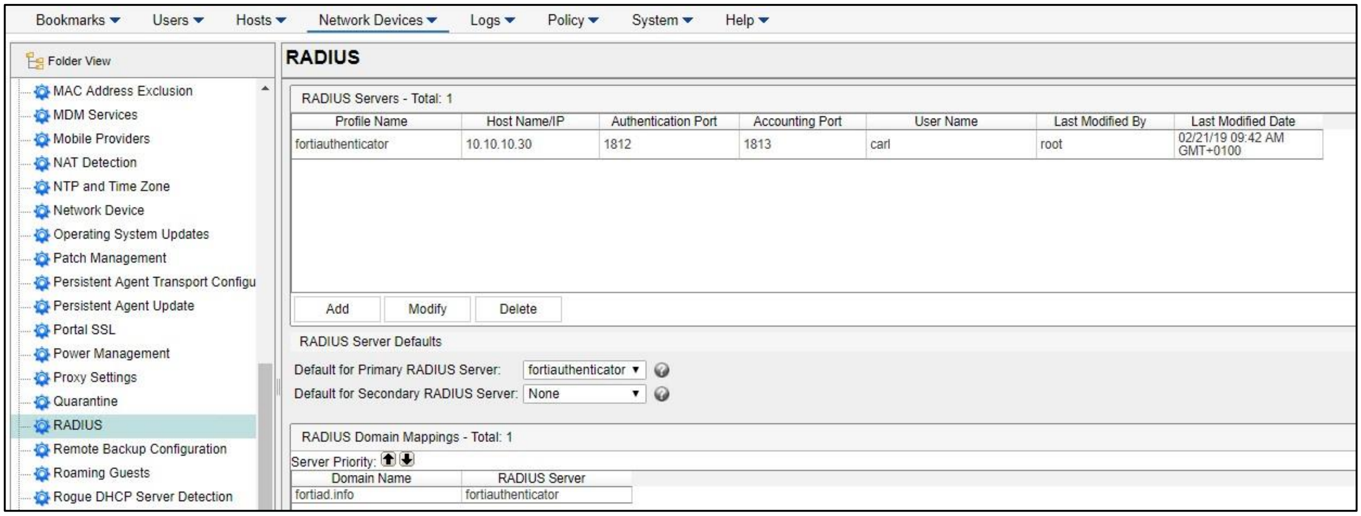
Prompt Type	User Login
Characters Required	# Prompt must end with this character or FortiNAC will not be able to communicate with the device.

Configure FortiNAC

RADIUS

Required for 802.1X authentication: 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.

Model the Device

1. Navigate to **Network Device > Topology**
2. Model the master AP using the VIP. See section **Add or modify a device** or **Discovery** of the Administration Guide in the Fortinet Documentation Library for instructions.

   SNMP Settings: SNMP v1 or v3 credentials

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.

Model Configuration

1. After modeling the device in the Topology View, right-click on the model and click **Model Configuration**.
2. Fill in the fields as appropriate:
   - **User Name** used for CLI access
   - **Password** used for CLI access

- **Protocol** used for CLI access
- **Primary RADIUS Server (802.1x authentication)**: Either the default RADIUS server or a pre-configured RADIUS server must be selected. RADIUS servers are configured on the RADIUS Settings window.
- **Secondary RADIUS Server (802.1x authentication):** Either the default RADIUS server or a pre-configured RADIUS server must be selected. RADIUS servers are configured on the RADIUS Settings window.
- **RADIUS Secret**: Required for both MAC and 802.1x authentication. Must match the value entered on the device itself and the value entered on the RADIUS settings window.

3. In the **Network Access** section, click the **Read VLANs** or **Read Roles** button. This populates the drop-down lists for the different connection states, such as Registration. Data in the drop-down lists represents the roles or VLANs created on the device.
4. Select a setting in **Access Enforcement** for each host state.
5. In the **Access Value** column select a Role or VLAN for each host state desired to enforce.
6. In the **Preferred Container** field, select the Container in Topology which the Wireless Access Points should be placed as they are discovered.
7. Click **Apply**.

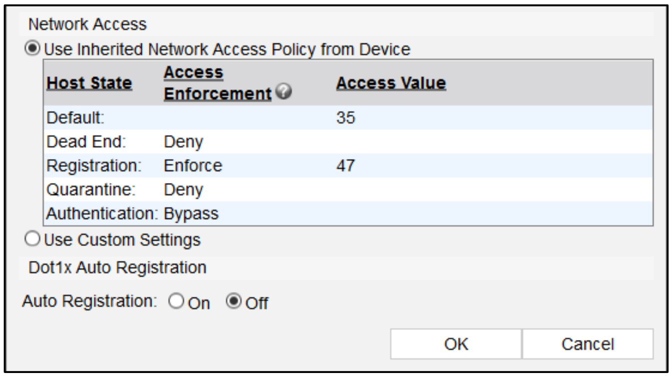
For individual SSID management, see SSID Configuration.

SSID Configuration

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, create an SSID configuration for each SSID to be managed 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 there is a corporate SSID and a guest SSID, it may be desired 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.

Dot1X Auto Registration (Version 8.5.2 and higher)

Automatic registration of a host based upon the user's 802.1x authentication with the RADIUS server. The feature is enabled/disabled in the **SSID Configuration** view of the Controller/Access Point model under **Network Devices** > **Topology**.



Network Access

● Use Inherited Network Access Policy from Device

Host State	Access Enforcement	Access Value
Default:		35
Dead End:	Deny	
Registration:	Enforce	47
Quarantine:	Deny	
Authentication:	Bypass	

○ Use Custom Settings

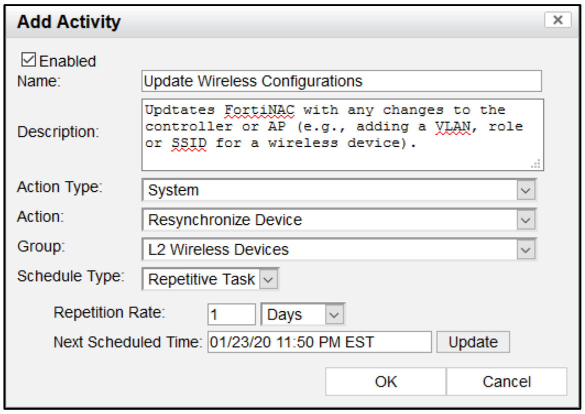
Dot1x Auto Registration

Auto Registration: ○ On ● Off

Updating SSID and VLAN Information

FortiNAC does not automatically discover SSIDs and Roles/VLANs as they are added to an Access Point. To update FortiNAC with this new information, right-click on the wireless model and click **Update Interfaces.** If the information is not updated, the new items will not appear in the Model.

The Scheduler can be configured to run this function regularly. The task **Resynchronize Device** can be associated to a group of APs and performs the same function. See section **Scheduler/Add a Task** of the Administration UI in the Fortinet Documentation Library for details.



Add Activity

☑ Enabled

Name: Update Wireless Configurations

Description: Updtates FortiNAC with any changes to the controller or AP (e.g., adding a VLAN, role or SSID for a wireless device).

Action Type: System

Action: Resynchronize Device

Group: L2 Wireless Devices

Schedule Type: Repetitive Task

Repetition Rate: 1 Days

Next Scheduled Time: 01/23/20 11:50 PM EST

Prevent SSID Removal After Failed Read

(Available with versions 8.7.5, 8.8.1 and higher)

If FortiNAC fails to read the SSIDs of an AP or controller, the existing SSIDs already associated with the device model are deleted (consequently removing SSID configuration and group membership).
To prevent this from occurring, run the following command in the CLI (**Note**: This attribute is not set by default). Contact Support for assistance.

device -ip <devip> -setAttr -name PreserveSSIDs -value true

Import All Access Points

Add all AP's (including the master) as pingable devices.

Individual

1. In the Topology Tree, right click on the applicable container and select **Add Pingable Device**.
2. Populate the following information then click **OK**:
    - Name
    - IP Address (for the master, use the actual IP and not the VIP)
    - Physical Address
    - Select Device Type **Wireless Access Point**

In Bulk

This is done by creating a .csv file containing information about the APs and importing the information using the CLI device import tool.

1. 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:

<Container name>,<IP address of AP>,<Name of AP>,<MAC address of AP>,,,,

Note:

- There must be a Unix style carriage return at the end of each line in the file, including the final line in the CSV file. Any lines without carriage returns at the end will not be imported.
- If a field is null, the field delimiter (comma) must still be included.
- The container specified will be the container in Topology where the AP models will be placed. This can be in a separate container if desired. If the container is not yet created, it will be created upon import.

Example:

```
East Campus,192.168.10.82,IAP_1,04:03:04:05:03:02,,,,

East Campus,192.168.10.83,IAP_2,04:03:04:05:03:03,,,,

East Campus,192.168.10.84,IAP_4,04:03:04:05:03:04,,,,
```

2. Use a secure copy tool to copy the CSV file from your local PC to the FortiNAC appliance (e.g., use Winscp).
3. Back up the current FortiNAC database before proceeding. See section Backup or restore a database of the Administration Guide in the Fortinet Documentation Library for instructions.
4. From the FortiNAC appliance CLI, navigate to the following directory:

   cd /bsc/campusMgr/bin

5. Run the DeviceImport tool to import the AP data and create the APs as WAP devices:
   DeviceImport <absolutePathToImportFile> -type WAP

   Example:

   ```
   > DeviceImport /root/IAPexport.csv -type WAP
   Unable to parse line:

   Unable to parse line:

   Unable to parse line:

    addDevice - start - ip = 192.168.10.82 contact = false
   Adding Pingable to domain - East Campus
    DeviceImport::setDeviceType - importType - 4
    addDevice - start - ip = 192.168.10.83 contact = false
   Adding Pingable to domain - East Campus
    DeviceImport::setDeviceType - importType - 4
    addDevice - start - ip = 192.168.10.84 contact = false
   Adding Pingable to domain - East Campus
    DeviceImport::setDeviceType - importType - 4
   ```

6. In the FortiNAC Administration UI, navigate to **Network Devices > Topology** and verify that the devices have been imported. If necessary, modify the device properties.
7. Right click on the VIP (master) model and click **Resync Interfaces**. This will associate the newly added APs with the master.

Once the WAPs are added, the switch ports connecting to the WAPs will display as WAP uplinks under the **Ports** tab of the switch model. See section **Port uplink types** of the Administration Guide in the Fortinet Documentation Library for details.

Validate

1. Configure test SSID to send RADIUS requests to FortiNAC.
2. Connect a rogue host to the newly enforced SSID.
3. 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.

Troubleshooting

Related KB Articles

Troubleshooting SNMP Communication Issues
Troubleshooting Poll Failures
Online wireless hosts displaying offline status
Rogue Wireless Clients Cannot Connect to SSID
Troubleshooting RADIUS clients not connecting
Troubleshooting Wireless Clients Moved to the Wrong VLAN
FortiNAC Local Radius Debug & Troubleshooting via GUI
Troubleshooting Tip: Local Radius server logs

Debugging

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
Aruba IAP specific	`nacdebug -name ArubaIAPlugin true`	/bsc/logs/output.master
SSH/Telnet CLI activity	`nacdebug -name TelnetServer true`	/bsc/logs/output.master
SNMP activity	`nacdebug -name SnmpV1 true`	/bsc/logs/output.master
Disable debug	`nacdebug -name <debug name> false`	

* Logging for a given MAC Address:

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

Disable:

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

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
```