

Configure 802.1X Authentication on Catalyst 9800 Wireless Controller Series

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Network Diagram](#)

[WLC Configuration](#)

[AAA Configuration on 9800 WLCs](#)

[WLAN Profile Configuration](#)

[Policy Profile Configuration](#)

[Policy Tag Configuration](#)

[Policy Tag Assignment](#)

[ISE Configuration](#)

[Declare the WLC on ISE](#)

[Create New User on ISE](#)

[Create Authorization Profile](#)

[Create a Policy Set](#)

[Create Authentication Policy](#)

[Create Authorization Policy](#)

[Verify](#)

[Troubleshoot](#)

[Troubleshoot on the WLC](#)

[Troubleshoot on ISE](#)

Introduction

This document describes how to set up a WLAN with 802.1X security on a Cisco Catalyst 9800 Series Wireless Controller.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- 802.1X

Components Used

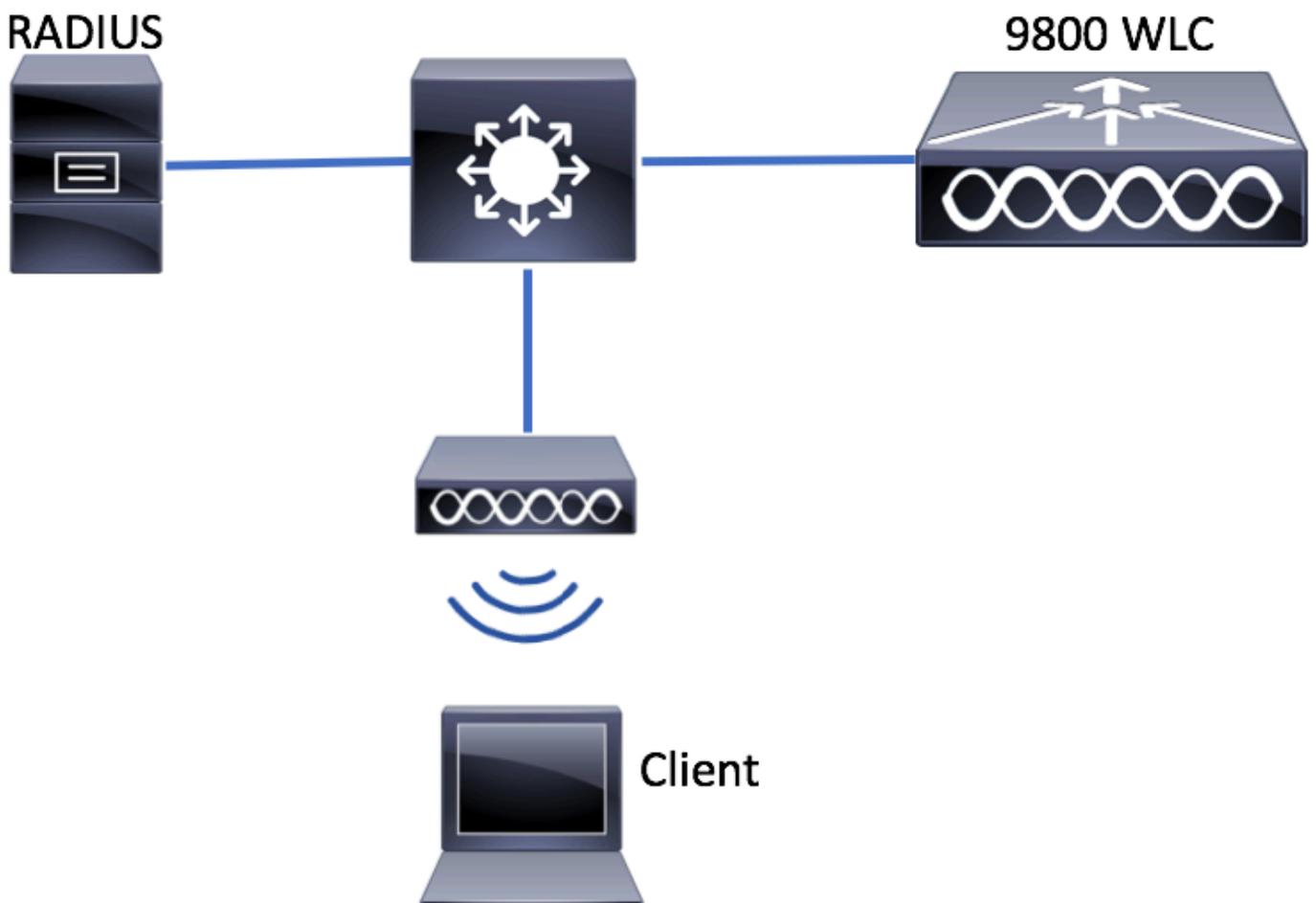
The information in this document is based on these software and hardware versions:

- Catalyst 9800 Wireless Controller Series (Catalyst 9800-CL)
- Cisco IOS® XE Gibraltar 17.3.x
- Cisco ISE 3.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram



WLC Configuration

AAA Configuration on 9800 WLCs

GUI:

Step 1. Declare RADIUS server. Navigate to **Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add** and enter the RADIUS server information.

Ensure **Support for CoA** is enabled if you plan to use Central Web Authentication (or any kind of security that requires Change of Authorization [CoA]) in the future.

Create AAA Radius Server ✕

Name*	<input type="text" value="ISE-kcg"/>	Clear PAC Key	<input type="checkbox"/>
IPv4/IPv6 Server Address*	<input type="text" value="172.16.0.11"/>	Set New PAC Key	<input type="checkbox"/>
Shared Secret*	<input type="password" value="....."/>		
Confirm Shared Secret*	<input type="password" value="....."/>		
Auth Port	<input type="text" value="1812"/>		
Acct Port	<input type="text" value="1813"/>		
Server Timeout (seconds)	<input type="text" value="1-1000"/>		
Retry Count	<input type="text" value="0-100"/>		
Support for CoA	<input checked="" type="checkbox"/> ENABLED		

Step 2. Add the RADIUS server to a RADIUS group. Navigate to **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add**. Give a name to your group and move the server you created earlier in the list of **Assigned Servers**.

Create AAA Radius Server Group

Name*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Available Servers

Assigned Servers

Step 3. Create an Authentication Method List. Navigate to **Configuration > Security > AAA > AAA Method List > Authentication > + Add**.

Authentication Authorization and Accounting

Servers / Groups

General

Authorization

Name

Enter the information:

Quick Setup: AAA Authentication

Method List Name*

Type*

Group Type

Fallback to local

Available Server Groups

- radius
- ldap
- tacacs+
- ISE-kcg-grp

Assigned Server Groups

- ISE-grp-name

CLI:

```
# config t
# aaa new-model

# radius server <radius-server-name>
# address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813
# timeout 300
# retransmit 3
# key <shared-key>
# exit

# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>
# aaa authentication dot1x <dot1x-list-name> group <radius-grp-name>
```

Note on the AAA Dead-Server Detection

After you have configured your RADIUS server, you can check if it is considered as "ALIVE":

```
#show aaa servers | s WNCN Platform State from WNCN (1) : current UP Platform State from WNCN
(2) : current UP Platform State from WNCN (3) : current UP Platform State from WNCN (4) :
current UP ...
```

You can configure the **dead criteria**, as well as the **deadtime** on your WLC, especially if you use multiple RADIUS servers.

```
#radius-server dead-criteria time 5 tries 3 #radius-server deadtime 5
```

Note: The **dead criteria** is the criteria used to mark a RADIUS server as dead. It consists of: 1. A timeout (in seconds) which represents the amount of time that must elapse from the time the controller last received a valid packet from the RADIUS server to the time the server is

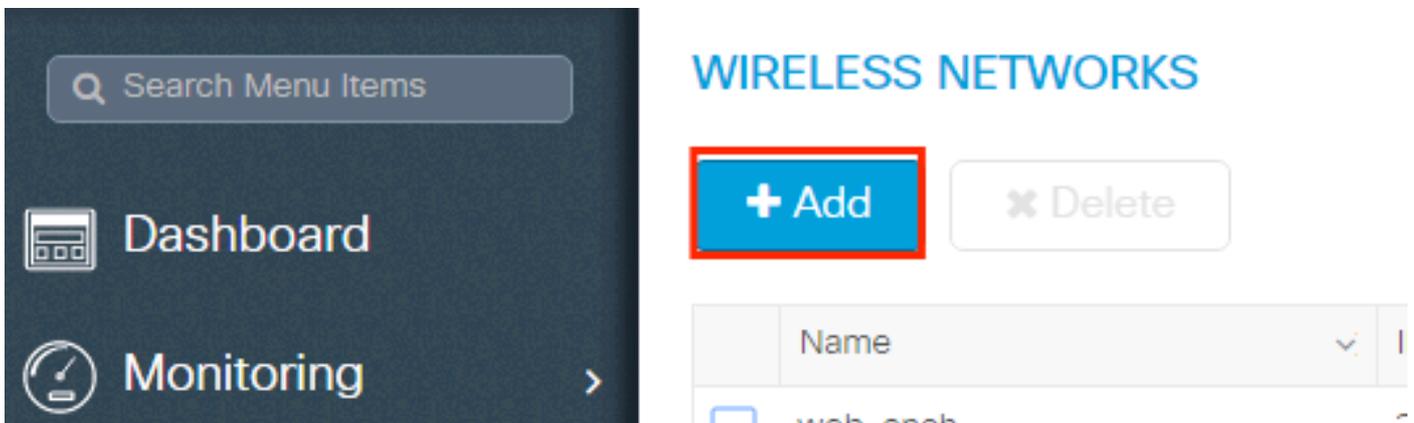
marked as dead. 2. A counter, which represents the number of consecutive timeouts that must occur on the controller before the RADIUS server is marked as dead.

Note: The `deadtime` specifies the amount of time (in minutes) the server remains in dead status after dead-criteria marks it as dead. Once the deadtime expires, the controller marks the server as UP (ALIVE) and notifies the registered clients about the state change. If the server is still unreachable after the state is marked as UP and if the dead criteria is met, then server is marked as dead again for the deadtime interval.

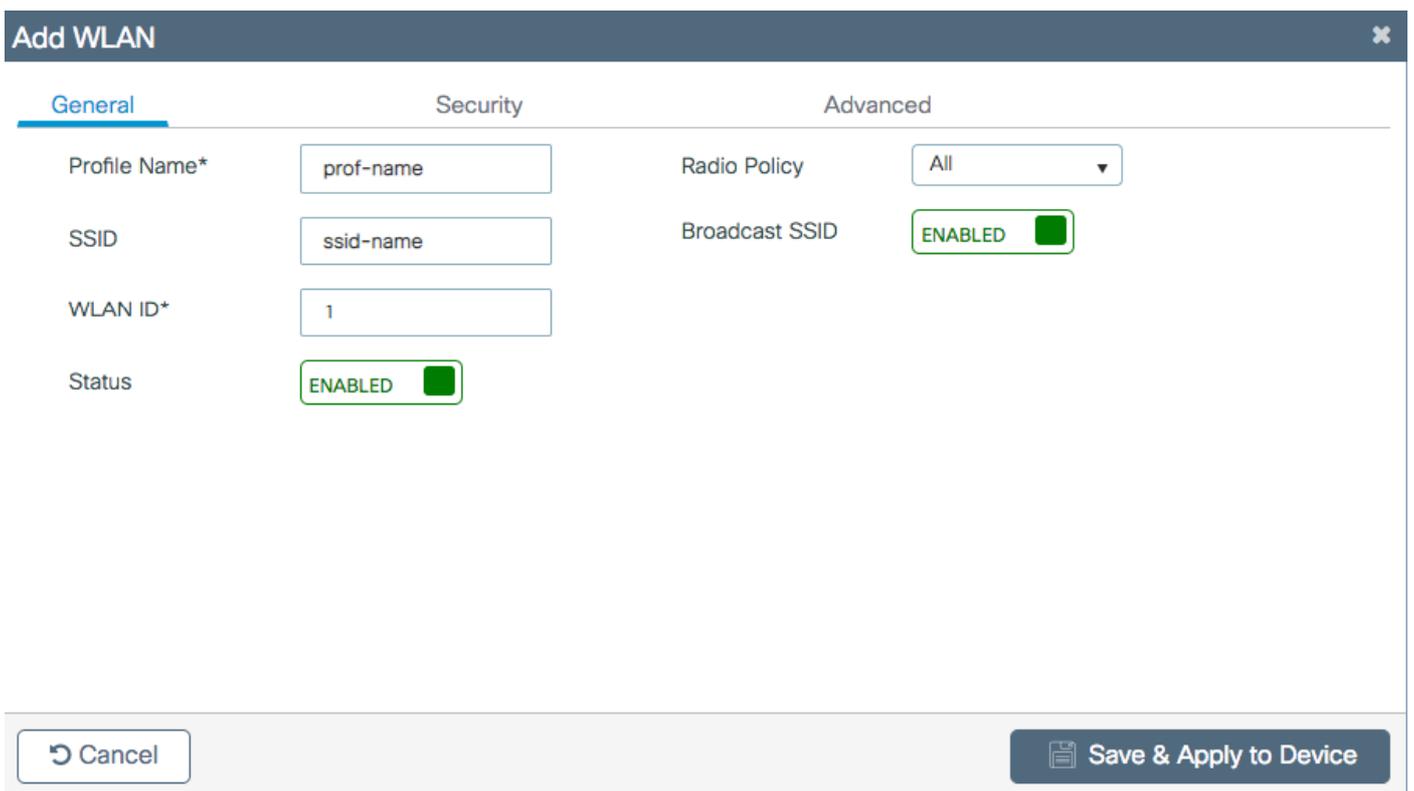
WLAN Profile Configuration

GUI:

Step 1. Create the WLAN. Navigate to **Configuration > Wireless > WLANs > + Add** and configure the network as needed.



Step 2. Enter the WLAN information

The image shows a 'Add WLAN' configuration window with three tabs: 'General', 'Security', and 'Advanced'. The 'General' tab is active and contains the following fields:

- Profile Name*: prof-name
- SSID: ssid-name
- WLAN ID*: 1
- Status: ENABLED (with a green toggle switch)

The 'Advanced' tab contains:

- Radio Policy: All (with a dropdown arrow)
- Broadcast SSID: ENABLED (with a green toggle switch)

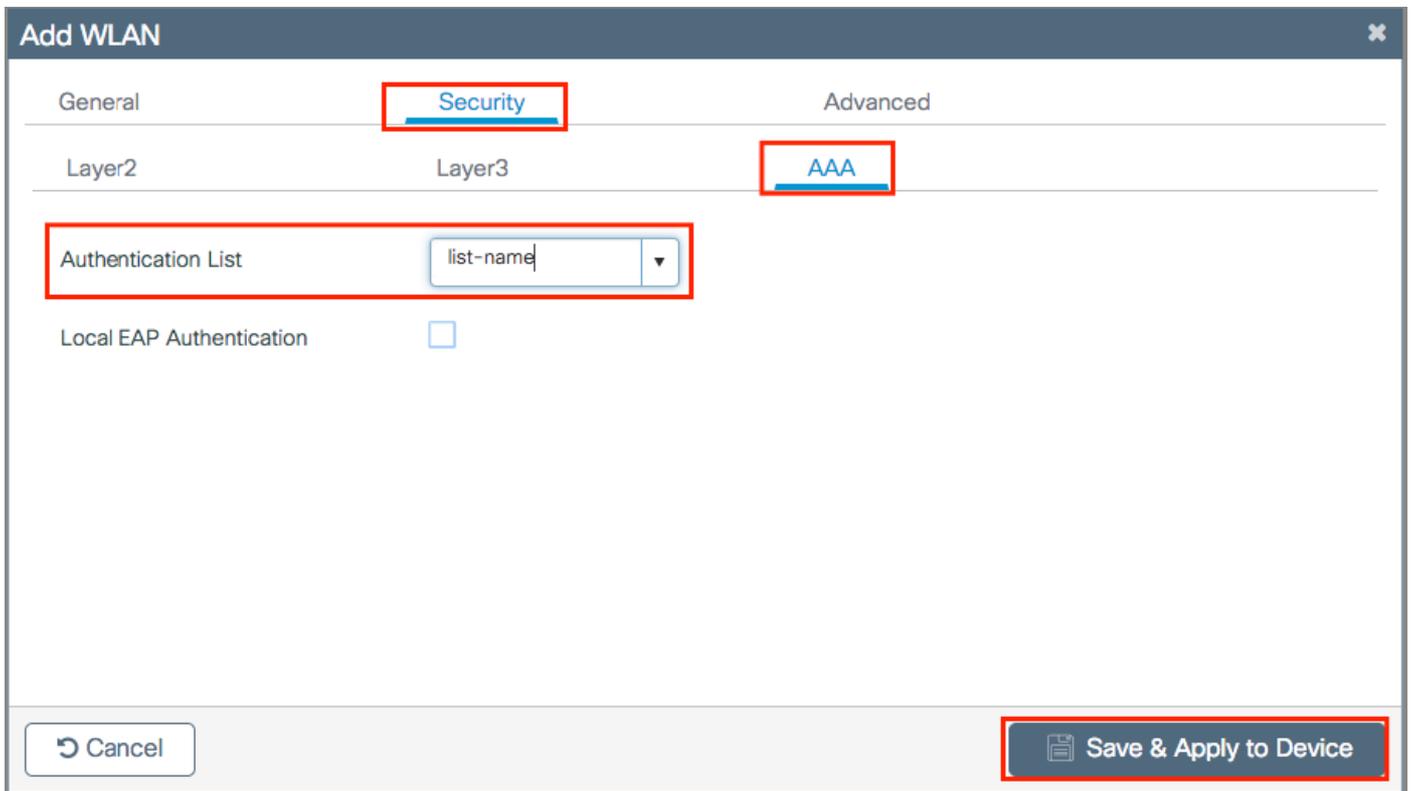
At the bottom of the window are two buttons: 'Cancel' and 'Save & Apply to Device'.

Step 3. Navigate to the **Security** tab and select the needed security method. In this case **WPA2 + 802.1x**.

The screenshot shows the 'Add WLAN' configuration window with the 'Security' tab selected. Under the 'Layer2' sub-tab, the 'Layer 2 Security Mode' dropdown menu is highlighted with a red box and set to 'WPA + WPA2'. Other settings include 'Fast Transition' set to 'Adaptive Enab...', 'Over the DS' checked, and 'Reassociation Timeout' set to '20'. The 'Protected Management Frame' and 'WPA Parameters' sections are currently collapsed. At the bottom, there are 'Cancel' and 'Save & Apply to Device' buttons.

The screenshot shows the 'Add WLAN' configuration window with the 'Security > AAA' tab selected. The 'WPA2 Policy' checkbox is checked. Under 'WPA2 Encryption', 'AES(CCMP128)' is selected with a checkmark, while 'CCMP256', 'GCMP128', and 'GCMP256' are unchecked. The 'Auth Key Mgmt' dropdown is set to '802.1x'. The 'WPA Policy' checkbox is unchecked. At the bottom, there are 'Cancel' and 'Save & Apply to Device' buttons. A red arrow on the right side of the window points downwards.

Step 4. From the **Security > AAA** tab, select the authentication method created on Step 3 from AAA Configuration on 9800 WLC section.



CLI:

```
# config t
# wlan <profile-name> <wlan-id> <ssid-name>
# security dot1x authentication-list <dot1x-list-name>
# no shutdown
```

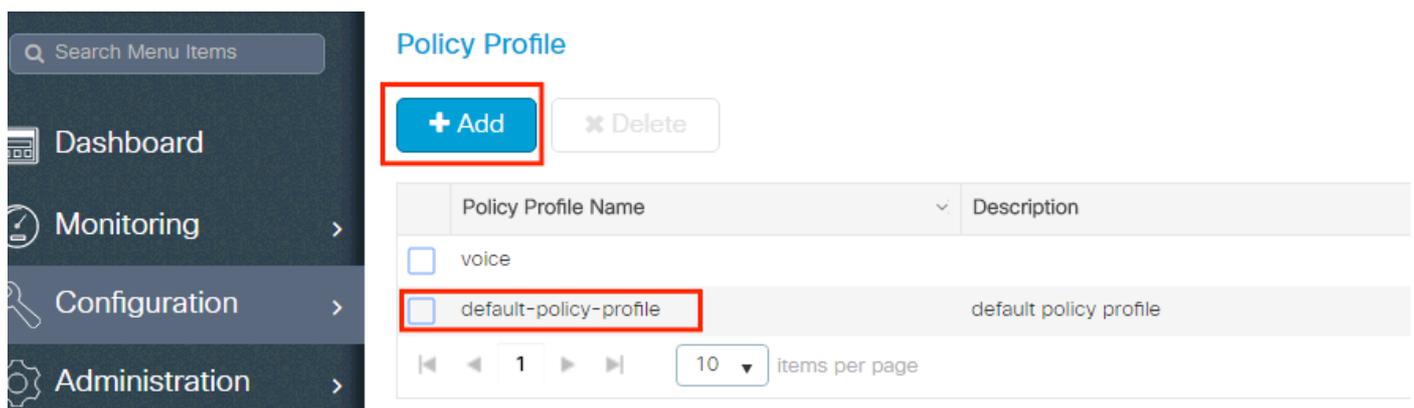
Policy Profile Configuration

Inside a Policy Profile you can decide to which VLAN to assign the clients, among other settings (like Access Controls List [ACLs], Quality of Service [QoS], Mobility Anchor, Timers, and so on).

You can either use your default policy profile or you can create a new profile.

GUI:

Navigate to **Configuration > Tags & Profiles > Policy Profile** and either configure your **default-policy-profile** or create a new one.



Ensure the profile is enabled.

Also, if your Access Point (AP) is in local mode, ensure the policy profile have **Central Switching** and **Central Authentication** enabled.

Edit Policy Profile

General | Access Policies | QOS and AVC | Mobility | Advanced

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name*	default-policy-profile	WLAN Switching Policy Central Switching <input checked="" type="checkbox"/> Central Authentication <input checked="" type="checkbox"/> Central DHCP <input checked="" type="checkbox"/> Central Association Enable <input checked="" type="checkbox"/> Flex NAT/PAT <input type="checkbox"/>
Description	default policy profile	
Status	ENABLED <input checked="" type="checkbox"/>	
Passive Client	<input type="checkbox"/> DISABLED	
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED	
CTS Policy		
Inline Tagging	<input type="checkbox"/>	
SGACL Enforcement	<input type="checkbox"/>	
Default SGT	2-65519	

Select the VLAN where the clients need to be assigned in the **Access Policies** tab.

Edit Policy Profile

General

Access Policies

QOS and AVC

Mobility

Advanced

WLAN Local Profiling

HTTP TLV Caching

RADIUS Profiling

DHCP TLV Caching

Local Subscriber Policy Name

Search or Select



VLAN

VLAN/VLAN Group

VLAN2602



Multicast VLAN

Enter Multicast VLAN

WLAN ACL

IPv4 ACL

Search or Select



IPv6 ACL

Search or Select



URL Filters

Pre Auth

Search or Select



Post Auth

Search or Select



If you plan to have ISE return attributes in the Access-Accept like VLAN Assignment, please enable AAA override in the **Advanced** tab:

Edit Policy Profile ✕

General
Access Policies
QOS and AVC
Mobility
Advanced

WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Fabric Profile

Umbrella Parameter Map

mDNS Service Policy

[Clear](#)

DHCP

IPv4 DHCP Required

DHCP Server IP Address

[Show more >>>](#)

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Air Time Fairness Policies

2.4 GHz Policy

5 GHz Policy

AAA Policy

Allow AAA Override

NAC State

Policy Name

↶ Cancel

📄 Update & Apply to Device

CLI:

```
# config
# wireless profile policy <policy-profile-name>
# aaa-override # central switching # description "<description>" # vlan <vlanID-or-VLAN_name> #
no shutdown
```

Policy Tag Configuration

Policy Tag is used to link the SSID with the Policy Profile. You can either create a new Policy Tag or use the default-policy tag.

Note: The default-policy-tag automatically maps any SSID with a WLAN ID between 1 and 16 to the default-policy-profile. It cannot be modified nor deleted. If you have a WLAN with ID 17 or higher, the default-policy-tag cannot be used.

GUI:

Navigate to **Configuation > Tags & Profiles > Tags > Policy** and add a new one if needed.

Search Menu Items

- Dashboard
- Monitoring >
- Configuration >
- Administration >
- Troubleshooting

Manage Tags

Policy Site RF AP

+ Add

Policy Tag Name	Description
<input type="checkbox"/> central-anchor	
<input type="checkbox"/> default-policy-tag	default policy-tag

1 10 items per page

Link your WLAN Profile to the desired Policy Profile.

Add Policy Tag

Name*

Description

+ Add

WLAN Profile	Policy Profile
No items to display	

0 10 items per page

Add Policy Tag ✕

Name*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
◀ ◁ 0 ▷ ▶	10 items per page
No items to display	

Map WLAN and Policy

WLAN Profile* Policy Profile*

✕ ✓

↶ Cancel Save & Apply to Device

Add Policy Tag ✕

Name*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> prof-name	default-policy-profile
◀ ◁ 1 ▷ ▶	10 items per page
1 - 1 of 1 items	

↶ Cancel Save & Apply to Device

CLI:

```
# config t
# wireless tag policy <policy-tag-name>
# wlan <profile-name> policy <policy-profile-name>
```

Policy Tag Assignment

Assign the Policy Tag to the needed APs.

GUI:

To assign the tag to one AP, navigate to **Configuration > Wireless > Access Points > AP Name > General Tags**, assign the relevant policy tag and then click **Update & Apply to Device**.

The screenshot shows the 'Edit AP' configuration interface. The 'General' tab is active. The 'Tags' section contains three dropdown menus: 'Policy' (set to 'default-policy-tag'), 'Site' (set to 'default-site-tag'), and 'RF' (set to 'default-rf-tag'). The 'Update & Apply to Device' button is located at the bottom right.

General		Version	
AP Name*	AP3802-02-WS	Primary Software Version	10.0.200.50
Location*	default location	Predownloaded Status	N/A
Base Radio MAC	00:42:68:c6:41:20	Predownloaded Version	N/A
Ethernet MAC	00:42:68:a0:d0:22	Next Retry Time	N/A
Admin Status	Enabled	Boot Version	1.0.0
AP Mode	Local	IOS Version	10.0.200.52
Operation Status	Registered	Mini IOS Version	0.0.0.0
Fabric Status	Disabled	IP Config	
Tags		IP Address	172.16.0.207
Policy	default-policy-tag	Static IP	<input type="checkbox"/>
Site	default-site-tag	Time Statistics	
RF	default-rf-tag	Up Time	9 days 1 hrs 17 mins 24 secs
		Controller Associated Time	0 days 3 hrs 26 mins 41 secs
		Controller Association Latency	8 days 21 hrs 50 mins 33 secs

Note: Be aware that when the policy tag on an AP is changed, it drops its association to the 9800 WLC and joins back a few moments later.

To assign the same Policy Tag to several APs, navigate to **Configuration > Wireless Setup > Advanced > Start Now > Apply**.

