

# Configure Dynamic VLAN Assignment with ISE and Catalyst 9800 Wireless LAN Controller

## Contents

---

### [Introduction](#)

[Requirements](#)

[Components Used](#)

### [Background Information](#)

[Dynamic VLAN Assignment with RADIUS Server](#)

### [Configure](#)

[Network Diagram](#)

[Configuration Steps](#)

[Cisco ISE Configuration](#)

[Step 1. Configure the Catalyst WLC as an AAA Client on the Cisco ISE server](#)

[Step 2. Configure internal users on Cisco ISE](#)

[Step 3. Configure the RADIUS \(IETF\) attributes used for dynamic VLAN Assignment](#)

[Configure the Switch for Multiple VLANs](#)

[Catalyst 9800 WLC Configuration](#)

[Step 1. Configure the WLC with the Details of the Authentication Server](#)

[Step 2. Configure the VLANs](#)

[Step 3. Configure the WLANs \(SSID\)](#)

[Step 4. Configure the Policy Profile](#)

[Step 5. Configure the Policy Tag](#)

[Step 6. Assign the Policy Tag to an AP](#)

### [Flexconnect](#)

[Configure the Switch for Multiple VLANs](#)

[Flexconnect Policy Profile configuration](#)

[Assign the Flexconnect policy profile to a WLAN and Policy tag](#)

[Configure the Flex Profile](#)

[Flex Site tag configuration](#)

[Assign the Policy and Site Tag to an AP.](#)

### [Verify](#)

### [Troubleshoot](#)

### [Related Information](#)

---

## Introduction

This document describes how to configure the Catalyst 9800 WLC and Cisco ISE to assign Wireless LAN (WLAN).

## Requirements

Cisco recommends that you have knowledge of these topics:

- Have basic knowledge of the Wireless LAN Controller (WLC and Lightweight Access Points (LAPs).
- Have functional knowledge of the AAA server such as Identity Services Engine (ISE).
- Have a thorough knowledge of wireless networks and wireless security issues.
- Have functional knowledge on dynamic Virtual LAN (VLAN) assignment.
- Have basic knowledge of Control and Provisioning for Wireless Access Point (CAPWAP).

## Components Used

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

- Cisco Catalyst 9800 WLC (Catalyst 9800-CL) that runs firmware release 16.12.4a.
- Cisco 2800 Series LAP in local mode.
- Native Windows 10 supplicant.
- Cisco ISE that runs version 2.7.
- Cisco 3850 series switch that runs firmware release 16.9.6.

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.

## Background Information

### Dynamic VLAN Assignment with RADIUS Server

This document describes the concept of dynamic VLAN assignment and how to configure the Catalyst 9800 wireless LAN controller (WLC) and Cisco Identity Service Engine (ISE) to assign wireless LAN (WLAN) in order to accomplish this for the wireless clients.

In most Wireless Local Area Network (WLAN) systems, each WLAN has a static policy that applies to all clients associated with a Service Set Identifier (SSID). Although powerful, this method has limitations because it requires clients to associate with different SSIDs to inherit different QoS and security policies.

However, the Cisco WLAN solution supports identity networking. This allows the network to advertise a single SSID and allows specific users to inherit different QoS or security policies based on the user credential.

Dynamic VLAN assignment is one such feature that places a wireless user into a specific VLAN based on the credentials supplied by the user. The task to assign users to a specific VLAN is handled by a RADIUS authentication server, such as Cisco ISE. This can be used, for example, to allow the wireless host to remain on the same VLAN as it moves within a campus network.

Therefore, when a client attempts to associate to a LAP registered with a controller, the WLC passes the credentials of the user to the RADIUS server for validation. Once the authentication is successful, the RADIUS server passes certain Internet Engineering Task Force (IETF) attributes to the user. These RADIUS attributes decide the VLAN ID that must be assigned to the wireless client. The SSID of the client does not matter because the user is always assigned to this predetermined VLAN ID.

The RADIUS user attributes used for the VLAN ID assignment are:

- IETF 64 (Tunnel Type)—Set this to VLAN.
- IETF 65 (Tunnel Medium Type)—Set this to 802.
- IETF 81 (Tunnel Private Group ID)—Set this to VLAN ID.

The VLAN ID is 12-bits and takes a value between 1 and 4094, inclusive. Because the Tunnel-Private-

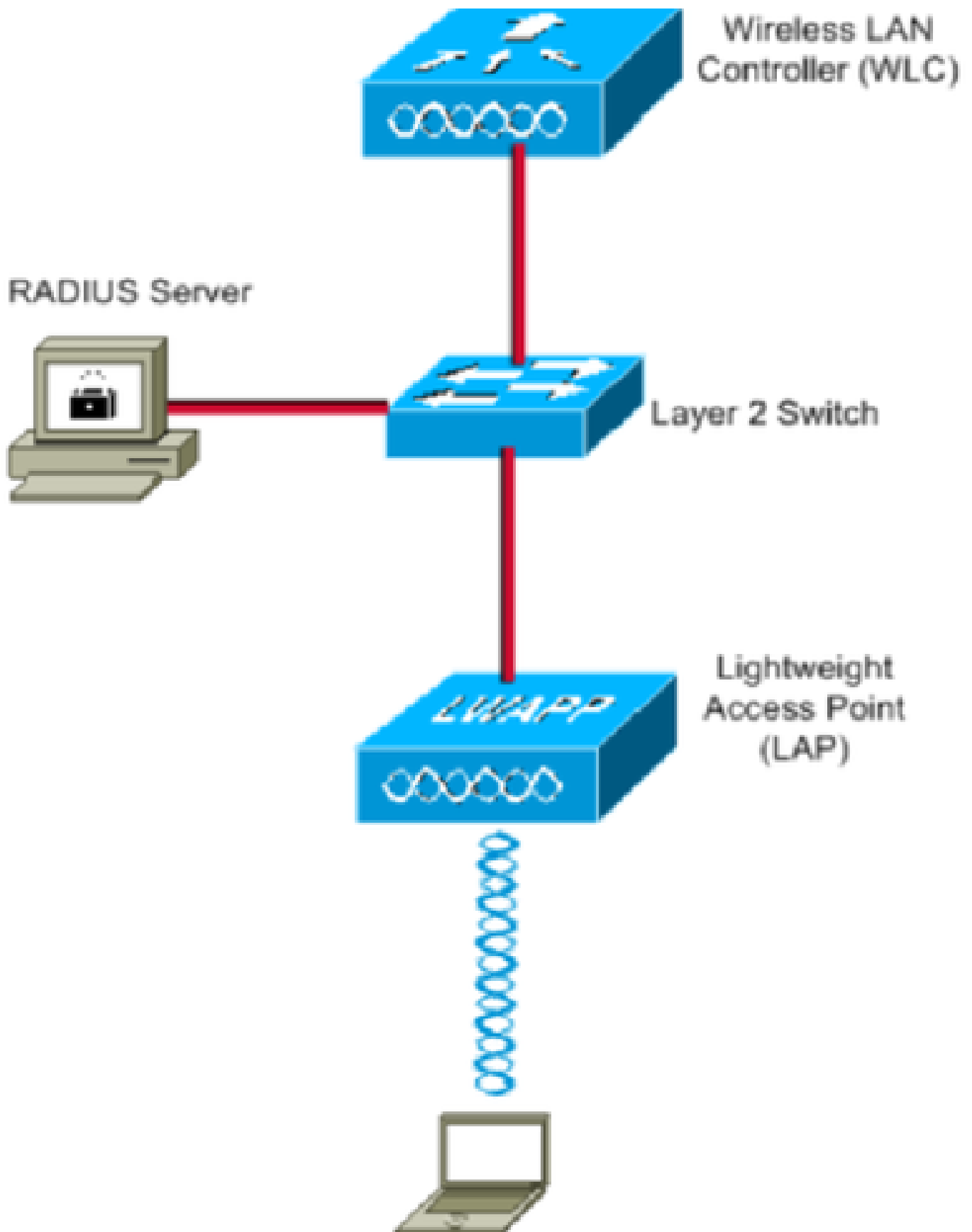
Group-ID is of type string, as defined in [RFC2868](#) for use with IEEE 802.1X, the VLAN ID integer value is encoded as a string. When these tunnel attributes are sent, it is necessary to enter them in the Tag field.

## **Configure**

In this section, you are presented with the information to configure the features described in this document.

## **Network Diagram**

This document uses this network setup:



These are the configuration details of the components used in this diagram:

- The IP address of Cisco ISE (RADIUS) server is 10.10.1.24.
- The Management Interface address of the WLC is 10.10.1.17.
- The internal DHCP server on the controller is used to assign the IP address to wireless clients.

- This document uses 802.1x with PEAP as the security mechanism.
- VLAN102 is used throughout this configuration. The username smith -102 is configured to be placed into the VLAN102 by the RADIUS server.

## **Configuration Steps**

This configuration is separated into three categories:

- Cisco ISE Configuration.
- Configure the Switch for Multiple VLANs.
- Catalyst 9800 WLC Configuration.

## **Cisco ISE Configuration**

This configuration requires these steps:

- Configure the Catalyst WLC as an AAA Client on the Cisco ISE Server.
- Configure Internal users on Cisco ISE.
- Configure the RADIUS (IETF) attributes used for dynamic VLAN Assignment on Cisco ISE.

### **Step 1. Configure the Catalyst WLC as an AAA Client on the Cisco ISE server**

This procedure explains how to add the WLC as a AAA client on the ISE server so that the WLC can pass the user credentials to ISE.

Complete these steps:

1. From the ISE GUI, navigate to **Administration > Network Resources > Network Devices** and select **Add**.
2. Complete the configuration with the WLC management IP address and RADIUS shared secret between WLC and ISE as shown in the image:

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

System > Identity Management > Network Resources > Device Portal Management pxGrid Services > Feed Service > Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MD

Network Devices List > **New Network Device**

**Network Devices**

\* Name  (highlighted)

Description

IP Address  /  (highlighted)

\* Device Profile

Model Name

Software Version

\* Network Device Group

Location

IPSEC

Device Type

**RADIUS Authentication Settings**

RADIUS UDP Settings

Protocol  (highlighted)

\* Shared Secret   (highlighted)

Use Second Shared Secret

CoA Port

## Step 2. Configure internal users on Cisco ISE

This procedure explains how to add the users on the internal user database of Cisco ISE.

Complete these steps:

1. From the ISE GUI, navigate to **Administration > Identity Management > Identities** and select **Add**.
2. Complete the configuration with the username, password, and user group as shown in the image:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Network Access Users List > New Network Access User

Users

Latest Manual Network Scan Results

**Network Access User**

\* Name: jonathga-102

Status:  Enabled

Email:

**Passwords**

Password Type: Internal Users

	Password	Re-Enter Password	
* Login Password	.....	.....	Generate Password ⓘ
Enable Password	.....	.....	Generate Password ⓘ

**User Information**

First Name:

Last Name:

**Account Options**

Description:

Change password on next login:

**Account Disable Policy**

Disable account if date exceeds: 2021-05-18 (yyyy-mm-dd)

**User Groups**

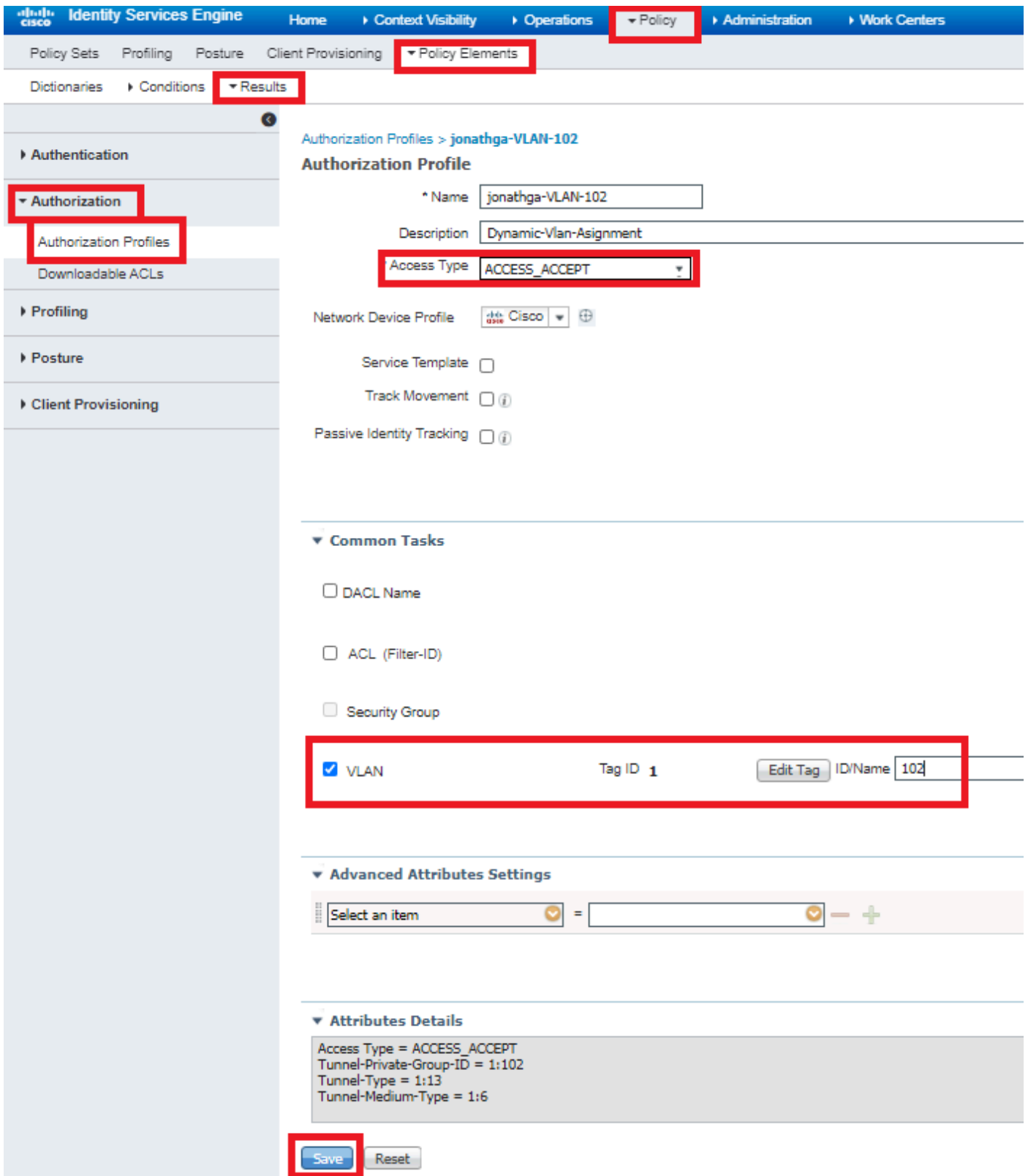
VLAN102

### Step 3. Configure the RADIUS (IETF) attributes used for dynamic VLAN Assignment

This procedure explains how to create an authorization profile and an authentication policy for wireless users.

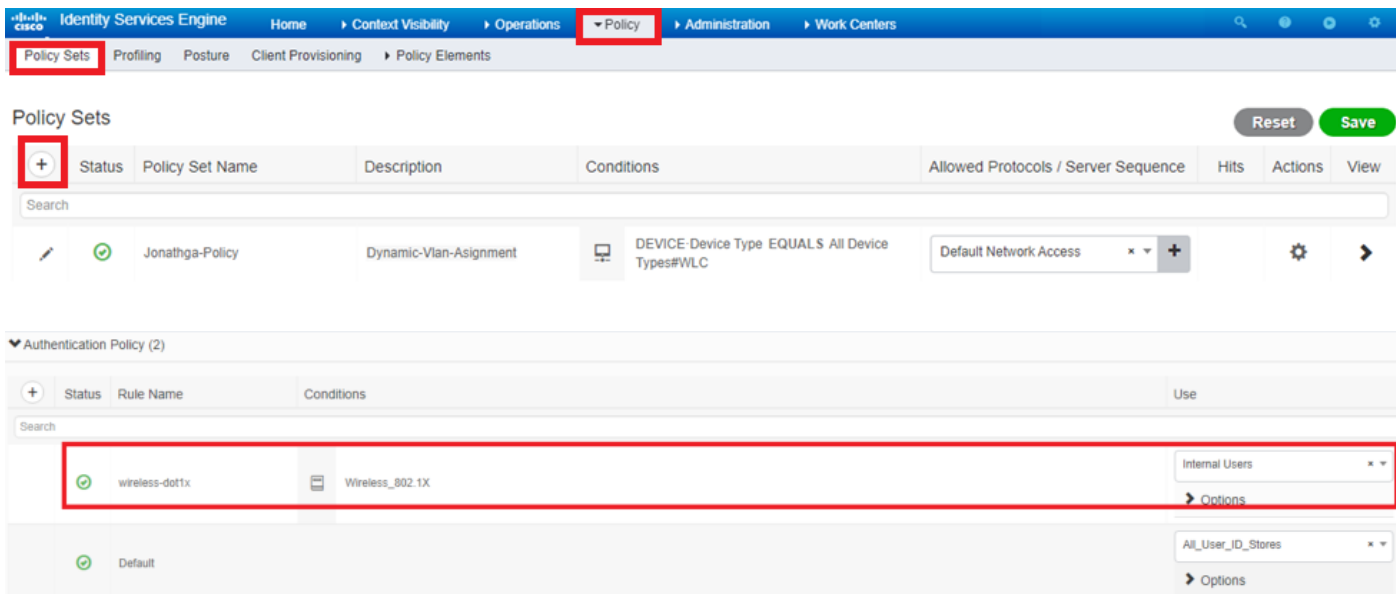
Complete these steps:

1. From the ISE GUI, navigate to **Policy > Policy Elements > Results > Authorization > Authorization profiles** and select **Add** to create a new profile.
2. Complete the authorization profile configuration with VLAN information for the respective group. This image shows **jonathga-VLAN-102** group configuration settings.



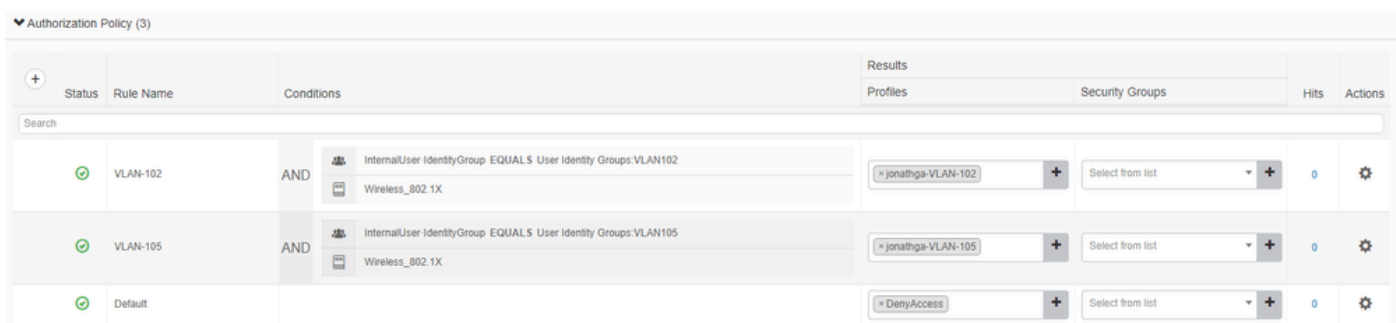
After the authorization profiles are configured, an authentication policy for wireless users needs to be created. You can use a new **Custom** policy or modify the **Default** Policy set. In this example, a custom profile is created.

3. Navigate to **Policy > Policy Sets** and select **Add** to create a new policy as shown in the image:



Now you need to create authorization policies for users in order to assign a respective authorization profile based on group membership.

5. Open the **Authorization** policy section and create policies to accomplish that requirement as shown in the image:



## Configure the Switch for Multiple VLANs

To allow multiple VLANs through the switch, you need to issue these commands to configure the switch port connected to the controller:

```
<#root>
```


```
Switch(config-if)#
```

```
switchport mode trunk
```

```
<#root>
```

```
Switch(config-if)#
```

```
switchport trunk encapsulation dot1q
```

 **Note:** By default, most of the switches allow all VLANs created on that switch via the trunk port. If a wired network is connected to the switch, then this same configuration can be applied to the switch port that connects to the wired network. This enables the communication between the same VLANs in the wired and wireless network.

## Catalyst 9800 WLC Configuration

This configuration requires these steps:

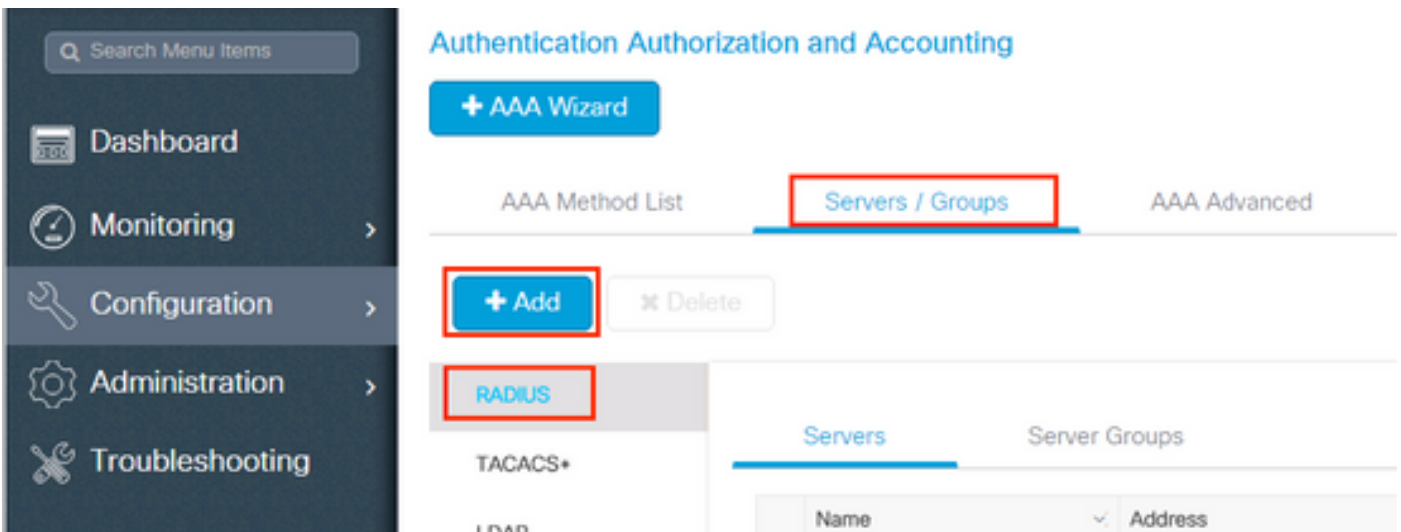
- Configure the WLC with the Details of the Authentication Server.
- Configure the VLANs.
- Configure the WLANs (SSID).
- Configure the Policy Profile.
- Configure the Policy tag.
- Assign the Policy tag to an AP.

### Step 1. Configure the WLC with the Details of the Authentication Server

It is necessary to configure the WLC so it can communicate with the RADIUS server to authenticate the clients.

Complete these steps:

1. From the controller GUI, navigate to **Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add** and enter the RADIUS server information as shown in the image:



The screenshot displays the Catalyst 9800 WLC GUI. On the left is a dark sidebar menu with a search bar and navigation options: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main content area is titled "Authentication Authorization and Accounting" and features a "+ AAA Wizard" button. Below this are three tabs: "AAA Method List", "Servers / Groups" (highlighted with a red box), and "AAA Advanced". Under the "Servers / Groups" tab, there are two buttons: "+ Add" (highlighted with a red box) and "Delete". Below the buttons is a list of AAA methods, with "RADIUS" (highlighted with a red box) selected. The "RADIUS" section has two sub-tabs: "Servers" (highlighted with a blue bar) and "Server Groups". Under the "Servers" sub-tab, there is a table with columns for "Name" and "Address".

## Create AAA Radius Server

Name*	Cisco-ISE	Support for CoA	ENABLED <input checked="" type="checkbox"/> ⓘ
Server Address*	10.10.1.24	CoA Server Key Type	Clear Text ▼
PAC Key	<input type="checkbox"/>	CoA Server Key ⓘ	<input type="text"/>
Key Type	Clear Text ▼	Confirm CoA Server Key	<input type="text"/>
Key* ⓘ	.....	Automate Tester	<input type="checkbox"/>
Confirm Key*	.....		
Auth Port	1812		
Acct Port	1813		
Server Timeout (seconds)	1-1000		
Retry Count	0-100		

2. In order to add the RADIUS server to a RADIUS group, navigate to **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add** as shown in the image:

## Create AAA Radius Server Group



Name\*

ISE-SERVER

Group Type

RADIUS

MAC-Delimiter

none

MAC-Filtering

none

Dead-Time (mins)

5

Load Balance

DISABLED

Source Interface VLAN ID

none

Available Servers

Assigned Servers

server-2019

Cisco-ISE

Cancel

Apply to Device

3. In order to create an Authentication Method List, navigate to **Configuration > Security > AAA > AAA Method List > Authentication > + Add** as shown in the images:

The screenshot shows the network configuration interface. On the left is a dark sidebar with menu items: Dashboard, Monitoring, Configuration (highlighted with a red box), and Administration. The main content area is titled "Authentication Authorization and Accounting". It contains a blue "+ AAA Wizard" button, a blue "AAA Method List" button (highlighted with a red box), and a "Servers / Groups" section. Under "Servers / Groups", there is a "General" tab (highlighted with a red box) and an "Authentication" tab. In the "Authentication" tab, there is a blue "+ Add" button (highlighted with a red box) and a grey "x Del" button. Below the tabs, there is a table with a header "Name".

## Quick Setup: AAA Authentication ✕

**Method List Name\***

Type\*  ⓘ

Group Type  ⓘ

Fallback to local

Available Server Groups

- radius
- ldap
- tacacs+
- radgrp\_SykesLab
- server2019
- tacacgrp\_SykesLab

Assigned Server Groups

- ISE-SERVER

### Step 2. Configure the VLANs

This procedure explains how to configure VLANs on the Catalyst 9800 WLC. As explained earlier in this document, the VLAN ID specified under the Tunnel-Private-Group ID attribute of the RADIUS server must also exist in the WLC.

In the example, the user smith-102 is specified with the **Tunnel-Private-Group ID of 102 (VLAN =102)** on the RADIUS server.

1. Navigate to **Configuration > Layer2 > VLAN > VLAN > + Add** as shown in the image:

**Configuration**

Search Menu Items

- Dashboard
- Monitoring
- Configuration**
- Administration
- Troubleshooting

### VLAN

SVI **VLAN** VLAN Group

VLAN ID	Name
<input type="checkbox"/> 1	default
<input type="checkbox"/> 100	VLAN
<input type="checkbox"/> 210	VLAN
<input type="checkbox"/> 2602	VLAN

2. Enter the needed information as shown in the image:

Create VLAN

Create a single VLAN

VLAN ID\*

Name

State **ACTIVATED**

IGMP Snooping  DISABLED

ARP Broadcast  DISABLED

Port Members

Available (2)

- Gi1 →
- Gi2 →

Associated (0)

No Associated Members

Create a range of VLANs

VLAN Range\*  -  (Ex:5-7)

 **Note:** If you do not specify a name, the VLAN automatically gets assigned the name of VLANXXXX, where XXXX is the VLAN ID.

Repeat steps 1 and 2 for all the needed VLANs, once done you can continue to step 3.

3. Verify the VLANs are allowed in your data interfaces.

- If you have a port channel in use, navigate to **Configuration > Interface > Logical > PortChannel name > General**. If you see it configured as **Allowed VLAN = All** you are done with the configuration. If you see **Allowed VLAN = VLANs IDs**, add the needed VLANs and after that select **Update & Apply to Device**.
- If you do not have port channel in use, navigate to **Configuration > Interface > Ethernet > Interface Name > General**. If you see it configured as **Allowed VLAN = All** you are done with the configuration. If you see **Allowed VLAN = VLANs IDs**, add the needed VLANs and after that select **Update & Apply to Device**.

This images show the configuration related to the interface setup if you use All or specific VLAN IDs.

General

Advanced

Interface

GigabitEthernet3

Description

(1-200 Characters)

Admin Status

UP 

Port Fast

disable ▼

Enable Layer 3 Address

DISABLED

Switchport Mode

trunk ▼

Allowed Vlan

All  Vlan IDs

Native Vlan

▼

**General**    Advanced

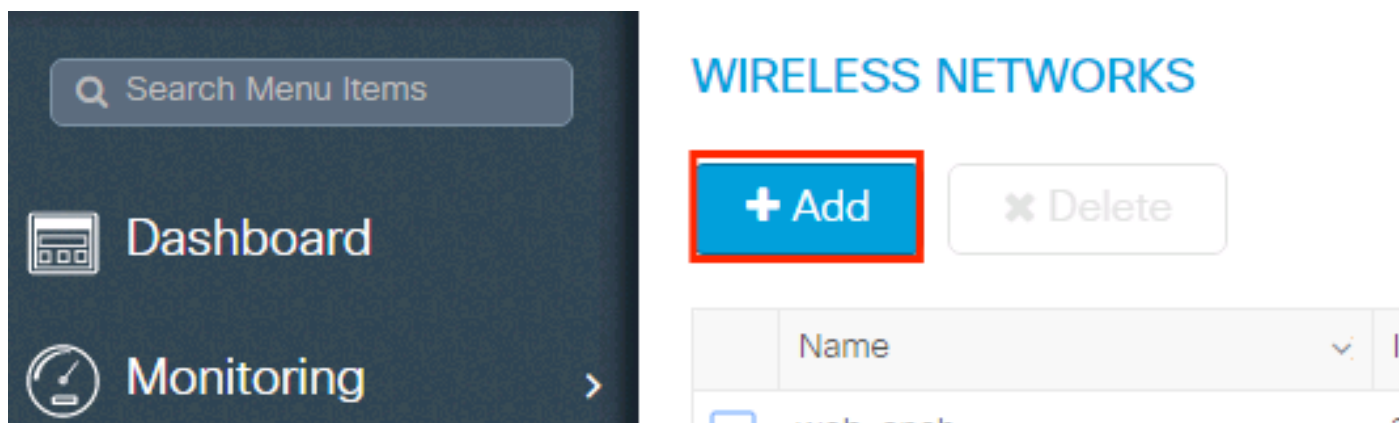
Interface	GigabitEthernet1	
Description	<input type="text"/>	(1-200 Characters)
Speed	1000 ▼	
Admin Status	UP	
Enable Layer 3 Address	<input type="checkbox"/> DISABLED	
Switchport Mode	trunk ▼	
Allowed Vlan	<input type="radio"/> All <input checked="" type="radio"/> Vlan IDs	
Vlan IDs	<input type="text" value="551,102,105"/>	(e.g. 1,2,4,6-10)
Native Vlan	551 ▼	

**Step 3. Configure the WLANs (SSID)**

This procedure explains how to configure the WLANs in the WLC.

Complete these steps:

1. In order to create the WLAN. Navigate to **Configuration > Wireless > WLANs > + Add** and configure the network as needed, as shown in the image:



2. Enter the WLAN information as shown in the image:

The screenshot shows the 'Add WLAN' configuration window with the 'General' tab selected. The following fields are visible:

Profile Name*	Dinamyc-VLAN	Radio Policy	All
SSID*	Dinamyc-VLAN	Broadcast SSID	ENABLED
WLAN ID*	6		
Status	ENABLED		

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

3. Navigate to **Security** tab and select the needed security method. In this case WPA2 + 802.1x as shown in the images:

The screenshot shows the 'Add WLAN' configuration window with the 'Security' tab selected. The 'Layer2' sub-tab is active. The following fields are visible:

Layer 2 Security Mode	WPA + WPA2	Fast Transition	Adaptive Enabl...
MAC Filtering	<input type="checkbox"/>	Over the DS	<input checked="" type="checkbox"/>
Protected Management Frame		Reassociation Timeout	30
PMF	Disabled		
WPA Parameters			
WPA Reliev	<input type="checkbox"/>		

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

**Add WLAN**

PMF Disabled

**WPA Parameters**

WPA Policy

WPA2 Policy

WPA2 Encryption

AES(CCMP128)

CCMP256

GCMP128

GCMP256

Auth Key Mgmt 802.1x

Cancel Save & Apply to Device

From **Security > AAA** tab, select the authentication method created on step 3 from **Configure the WLC with the Details of the Authentication Server** section as shown in the image:

**Add WLAN**

General **Security** Advanced

Layer2 Layer3 **AAA**

Authentication List ISE-SERVER ⓘ

Local EAP Authentication

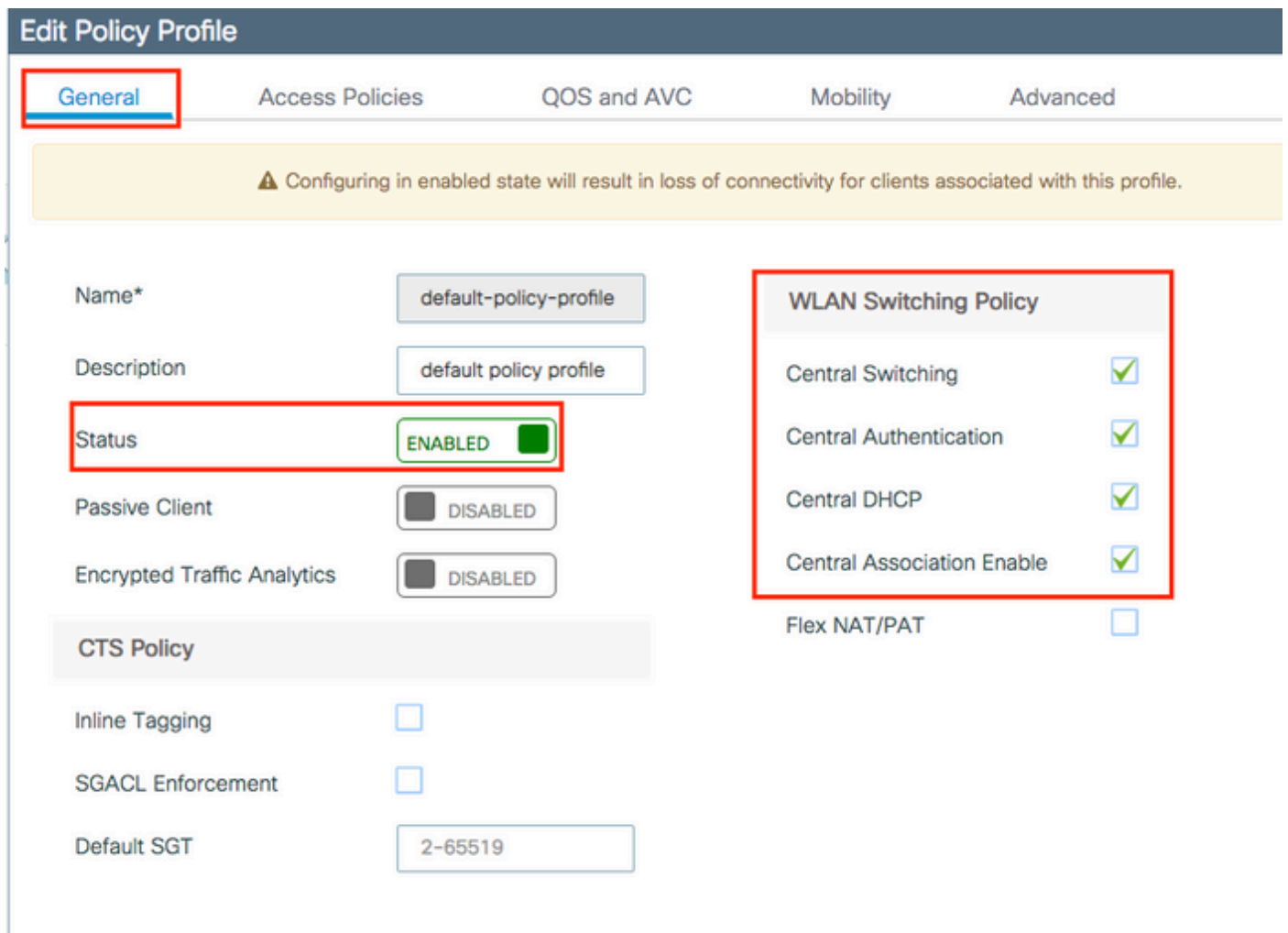
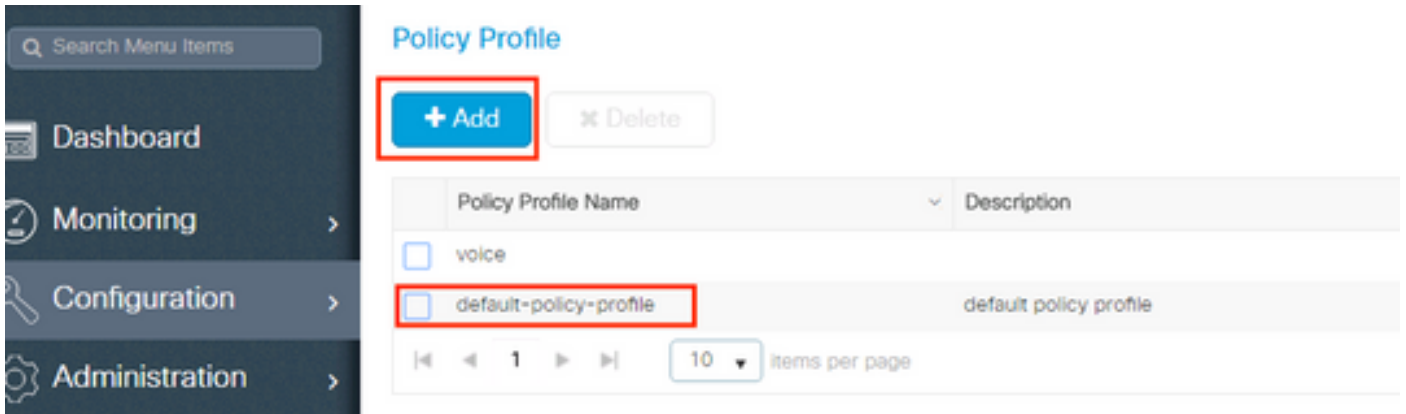
Cancel Apply to Device

#### Step 4. Configure the Policy Profile

This procedure explains how to configure the Policy Profile in the WLC.

Complete these steps:

1. Navigate to Configuration > Tags & Profiles > Policy Profile and either configure your default-policy-profile or create a new one as shown in the images:



2. From the Access Policies tab assign the VLAN to which the wireless clients are assigned when they connect to this WLAN by default as shown in the image:

**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

**VLAN**

VLAN/VLAN Group

Multicast VLAN

**WLAN ACL**


IPv4 ACL

IPv6 ACL

**URL Filters**

Pre Auth

Post Auth

 **Note:** In the example provided, it is the job of the RADIUS server to assign a wireless client to a specific VLAN upon successful authentication, therefore the VLAN configured on the policy profile can be a black hole VLAN, the RADIUS server overrides this mapping and assigns the user that comes through that WLAN to the VLAN specified under the user Tunnel-Group-Private-ID field in the RADIUS server.

- From the **Advance** tab, enable the **Allow AAA Override** check box to override the WLC configuration when the RADIUS server returns the attributes needed to place the client on the proper VLAN as shown in the image:

**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)

**DHCP**

IPv4 DHCP Required

DHCP Server IP Address

Show more >>>

**AAA Policy**

Allow AAA Override

NAC State

Policy Name

Fabric Profile  Search or Select

Umbrella Parameter Map Not Configured

mDNS Service Policy default-mdns-service [Clear](#)

**WLAN Flex Policy**

VLAN Central Switching

Split MAC ACL Search or Select

**Air Time Fairness Policies**

2.4 GHz Policy Search or Select

5 GHz Policy Search or Select

Cancel   Update & Apply to Device

### Step 5. Configure the Policy Tag

This procedure explains how to configure the Policy tag in the WLC.

Complete these steps:

1. Navigate to **Configuration > Tags & Profiles > Tags > Policy** and add a new one if needed as shown in the image:

Search Menu Items

Dashboard

Monitoring >

Configuration >

Administration >

Troubleshooting

### Manage Tags

Policy Site RF AP

+ Add x Delete

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

10 items per page

2. Add a name to the Policy Tag and select +Add, as shown in the image:

### Add Policy Tag

Name\* Dynamic-VLAN

Description Enter Description

WLAN-POLICY Maps: 0

+ Add x Delete

WLAN Profile	Policy Profile
--------------	----------------

0 10 items per page No items to display

3. Link your WLAN Profile to the desired Policy Profile as shown in the images:

Add Policy Tag ✕

Name\*

Description

▼ WLAN-POLICY Maps: 0

+ Add ✕ Delete

WLAN Profile	Policy Profile
<span>◀ 0 ▶</span> <span style="border: 1px solid #ccc; padding: 2px;">10</span> items per page <span style="float: right;">No items to display</span>	

Map WLAN and Policy

WLAN Profile\*

Policy Profile\*

✕
✓

Add Policy Tag ✕

Name\*

Description

▼ WLAN-POLICY Maps: 1

+ Add ✕ Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> Dinamyc-VLAN	default-policy-profile
<span>◀ 1 ▶</span> <span style="border: 1px solid #ccc; padding: 2px;">10</span> items per page <span style="float: right;">1 - 1 of 1 items</span>	

➤ RLAN-POLICY Maps: 0

↶ Cancel
📄 Apply to Device

### Step 6. Assign the Policy Tag to an AP

This procedure explains how to configure the Policy tag in the WLC.

Complete these steps:

1. Navigate to **Configuration > Wireless > Access Points > AP Name > General Tags** and assign the relevant policy tag and then select **Update & Apply to Device** as shown in the image:

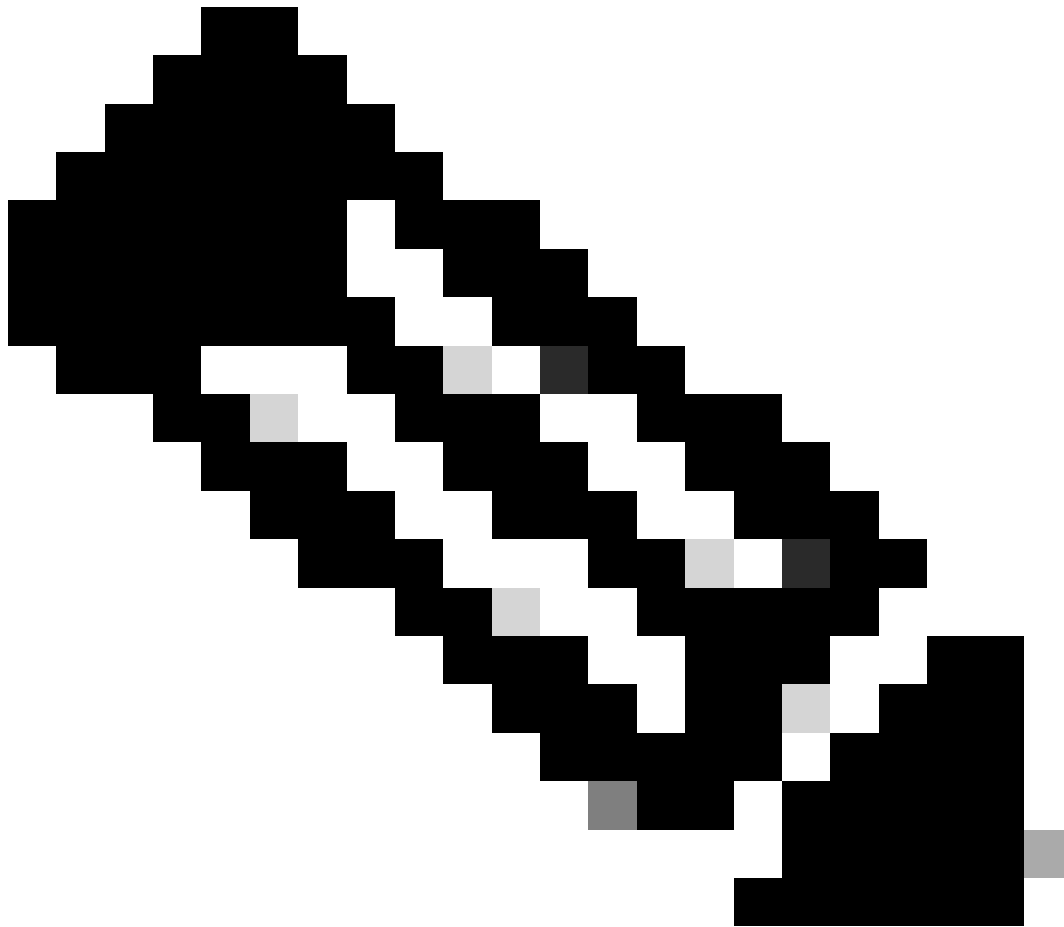
The screenshot shows the 'Edit AP' configuration page. The 'General' tab is selected and highlighted with a red box. The 'Tags' section is also highlighted with a red box, showing the 'Policy' dropdown set to 'Dynamic-VLAN'. The 'Update & Apply to Device' button is highlighted with a red box.

General		Version	
AP Name*	AP2802I-B-K9	Primary Software Version	16.12.4.31
Location*	default location	Predownloaded Status	N/A
Base Radio MAC	10b3.d677.a8c0	Predownloaded Version	N/A
Ethernet MAC	084f.a9a2.8ed4	Next Retry Time	N/A
Admin Status	ENABLED <input checked="" type="checkbox"/>	Boot Version	1.1.2.4
AP Mode	Local	IOS Version	16.12.4.31
Operation Status	Registered	Mini IOS Version	0.0.0.0
Fabric Status	Disabled	IP Config	
LED State	ENABLED <input checked="" type="checkbox"/>	CAPWAP Preferred Mode	IPv4
LED Brightness Level	8	DHCP IPv4 Address	10.10.102.101
CleanAir NSI Key		Static IP (IPv4/IPv6)	<input type="checkbox"/>
Tags		Time Statistics	
Policy	Dynamic-VLAN	Up Time	0 days 0 hrs 4 mins 52 secs
Site	default-site-tag	Controller Association Latency	1 min 36 secs

**Caution:** Be aware that changing the policy tag on an AP results in the AP disconnecting from the WLC and then reconnecting.

## Flexconnect

The Flexconnect feature allows APs to send wireless client data to egress through the AP LAN port when configured as a trunk. This mode, known as Flexconnect Local Switching, allows the AP to segregate client traffic by tagging it in separate VLANs from its management interface. This section provides instructions on how to configure Dynamic VLAN assignment for the local switching scenario.



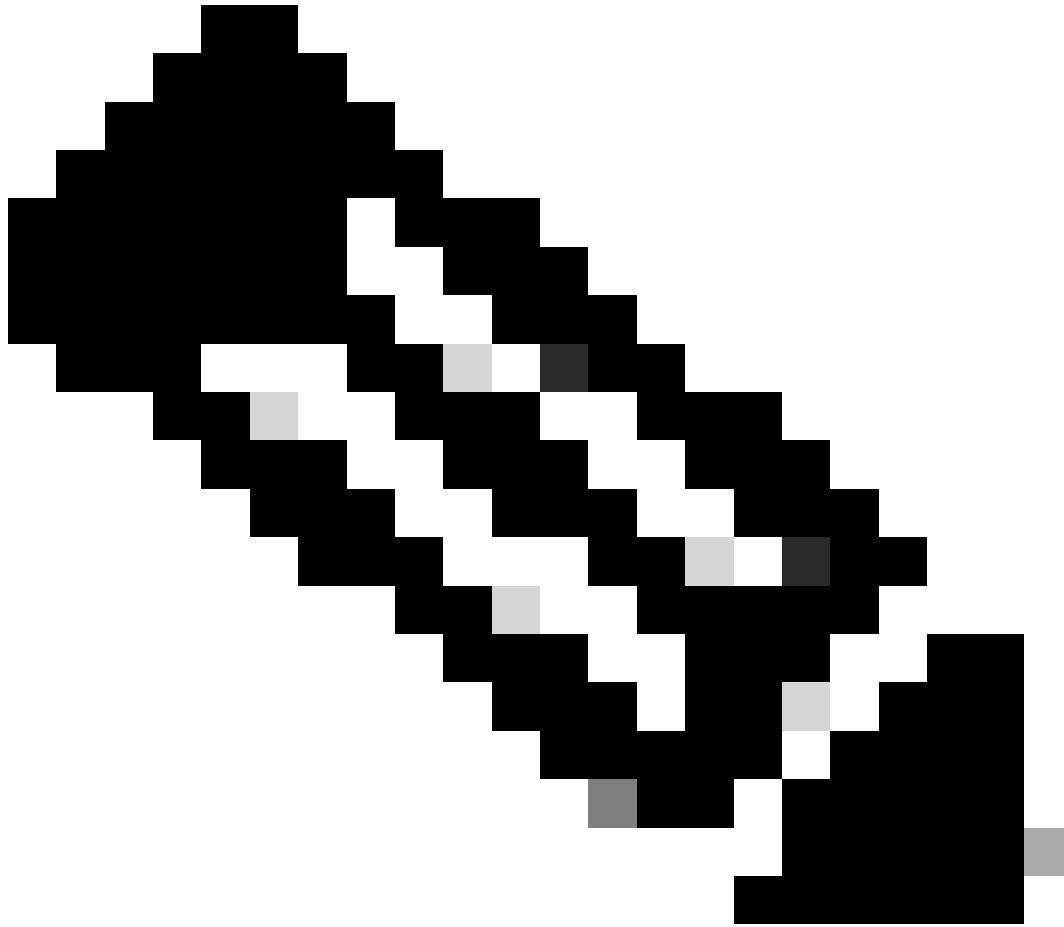
**Note:** The steps outlined in the previous section are applicable to the Flexconnect scenario as well. To complete the configuration for Flexconnect, please do the additional steps provided in this section.

---

## Configure the Switch for Multiple VLANs

To allow multiple VLANs through the switch, you need to issue the next commands to configure the switch port connected to the AP:

1. Switch(config-if)#**switchport mode trunk**
2. Switch(config-if)#**switchport trunk encapsulation dot1q**



**Note:** By default, most of the switches allow all VLANs created on the switch via the trunk port.

---

## Flexconnect Policy Profile configuration

1. Navigate to **Configuration > Tags & Profiles > Policy Profile > +Add** and create a new policy.
2. Add the name, unselect the Central Switching and Central DHCP check box. With this configuration, the controller handles client authentication, while the FlexConnect Access Point switches client data packets and DHCP locally.

**Edit Policy Profile** ✕

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

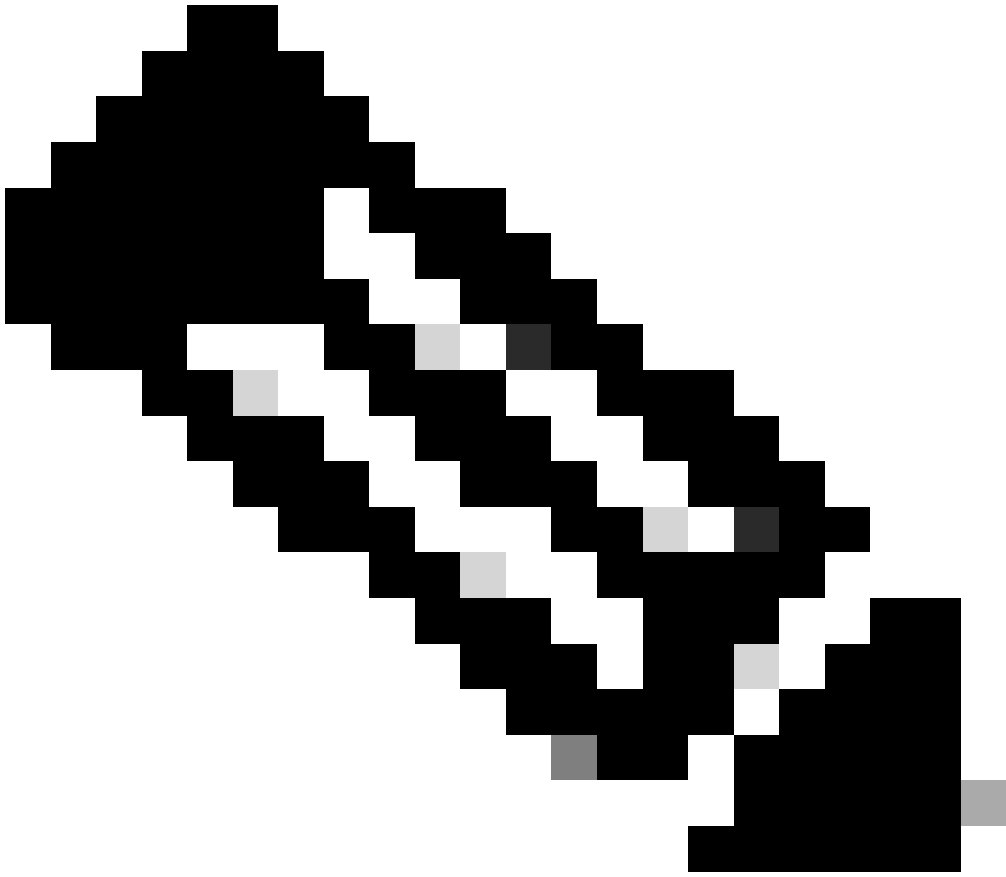
**⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.**

Name*	Flexconnect-Policy
Description	Enter Description
Status	ENABLED <input checked="" type="checkbox"/>
Passive Client	<input type="checkbox"/> DISABLED
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED

**WLAN Switching Policy**

Central Switching	<input type="checkbox"/> DISABLED
Central Authentication	ENABLED <input checked="" type="checkbox"/>
Central DHCP	<input type="checkbox"/> DISABLED
Central Association	<input type="checkbox"/> DISABLED
Flex NAT/PAT	<input type="checkbox"/> DISABLED

**CTS Policy**



**Note:** Starting with the 17.9.x code, the policy-profile appearance has been updated as depicted in the picture.

## WLAN Switching Policy

Central Switching

DISABLED

Central Authentication

ENABLED

Central DHCP

DISABLED

Flex NAT/PAT

DISABLED

- From the **Access Policies** tab assign the VLAN to which the wireless clients are assigned when they connect to this WLAN by default.

### Edit Policy Profile

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

RADIUS Profiling   
HTTP TLV Caching   
DHCP TLV Caching

#### WLAN Local Profiling

Global State of Device Classification **Enabled** ⓘ

Local Subscriber Policy Name

#### VLAN

VLAN/VLAN Group

#### WLAN ACL

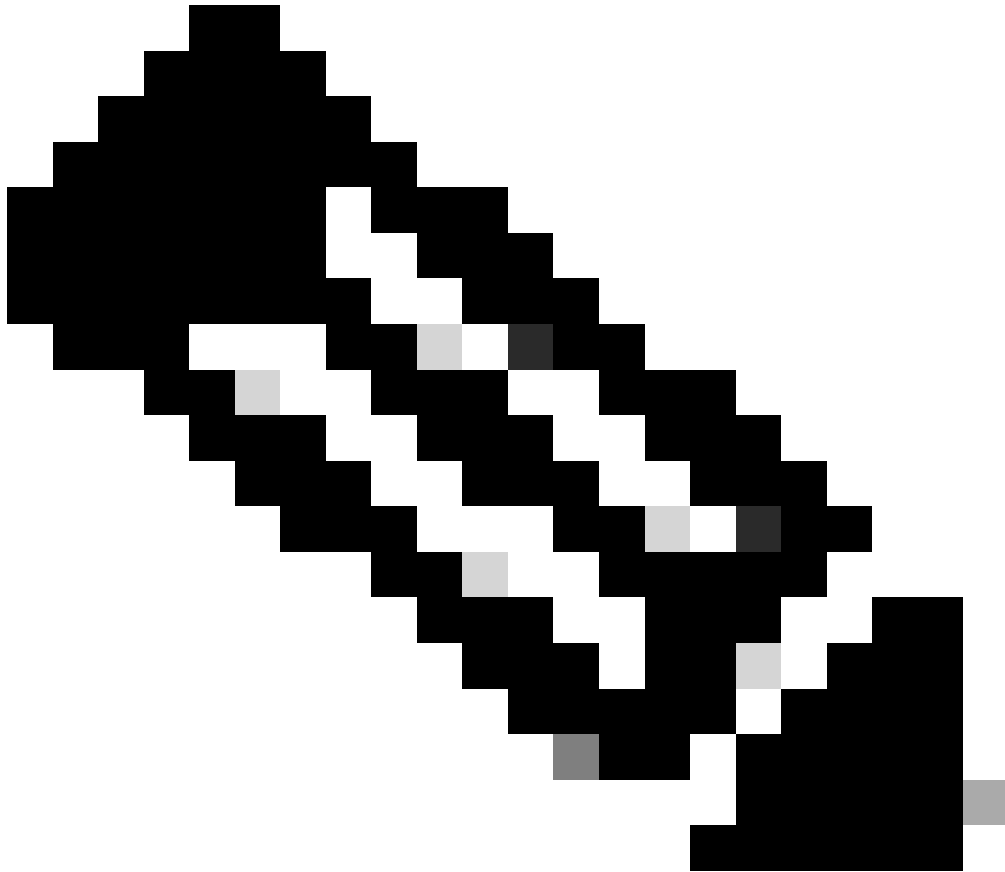
IPv4 ACL

IPv6 ACL

#### URL Filters

Pre Auth

Post Auth



**Note:** The VLAN configured on this step is not required to be present on the VLAN list of the WLC. Necessary VLANs are added on the Flex-Profile later, which creates the VLANs on the AP itself.

- 
4. From the **Advance** tab, enable the **Allow AAA Override** check box to override the WLC configurations by the RADIUS server.

## 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)

### DHCP

IPv4 DHCP Required

DHCP Server IP Address

[Show more >>>](#)

### AAA Policy

Allow AAA Override

Fabric Profile

Umbrella Parameter Map

mDNS Service Policy  [Clear](#)

### WLAN Flex Policy

VLAN Central Switching

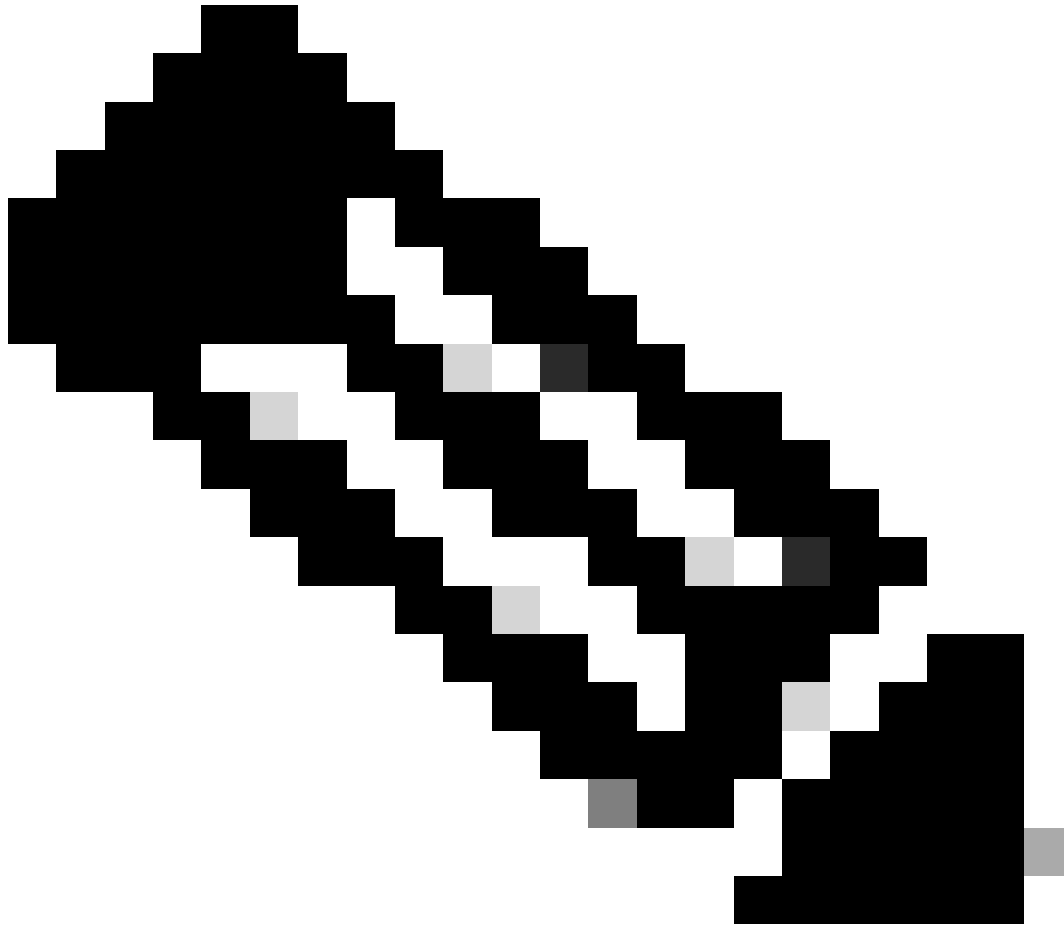
Split MAC ACL

### Air Time Fairness Policies

2.4 GHz Policy

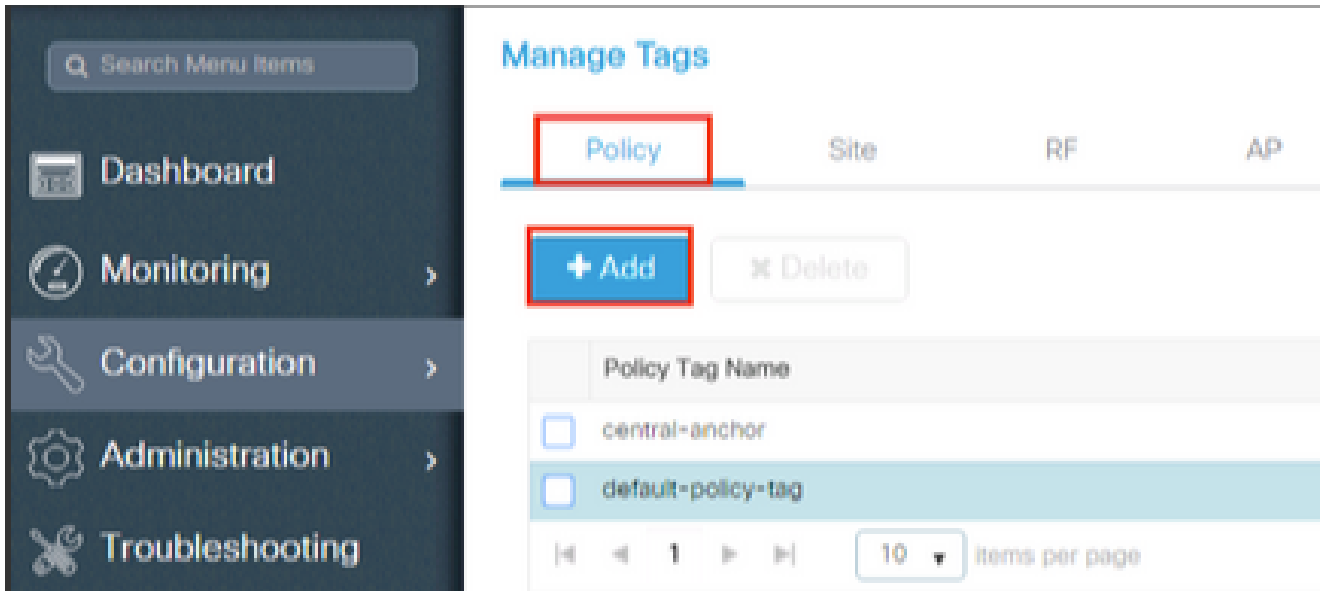
5 GHz Policy

**Assign the Flexconnect policy profile to a WLAN and Policy tag**

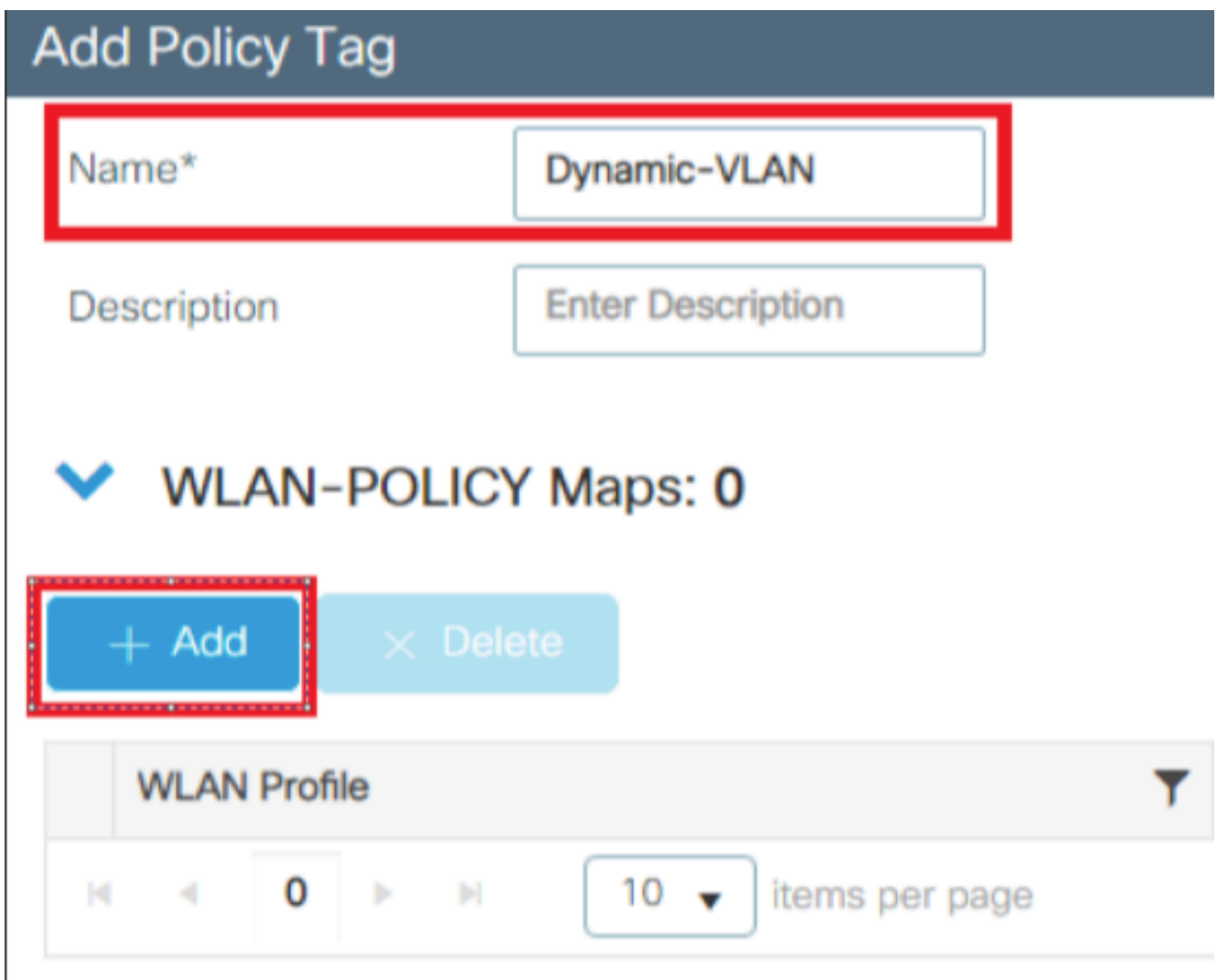


**Note:** A Policy Tag is used to link the WLAN with the Policy Profile. You can either create a new Policy Tag or use the default-policy tag.

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



2. Enter a name for the Policy Tag and click on the “add” button.



3. Link your WLAN Profile to the desired Policy Profile.

## Add Policy Tag

Name\*

Description

### WLAN-POLICY Maps: 0

[+ Add](#) [× Delete](#)

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

Map WLAN and Policy

WLAN Profile\*

Policy Profile\*

[×](#) [✓](#)

### RLAN-POLICY Maps: 0

[↶ Cancel](#)

[📄 Apply to Device](#)

4. Click on the **Apply to Device** button.

## Add Policy Tag

Name\*

Description

### WLAN-POLICY Maps: 1

[+ Add](#) [× Delete](#)

WLAN Profile	Policy Profile
<input checked="" type="checkbox"/> Dinamyc-VLAN	Flexconnect-Policy
◀ 1 ▶ 10 items per page 1 - 1 of 1 items	

### RLAN-POLICY Maps: 0

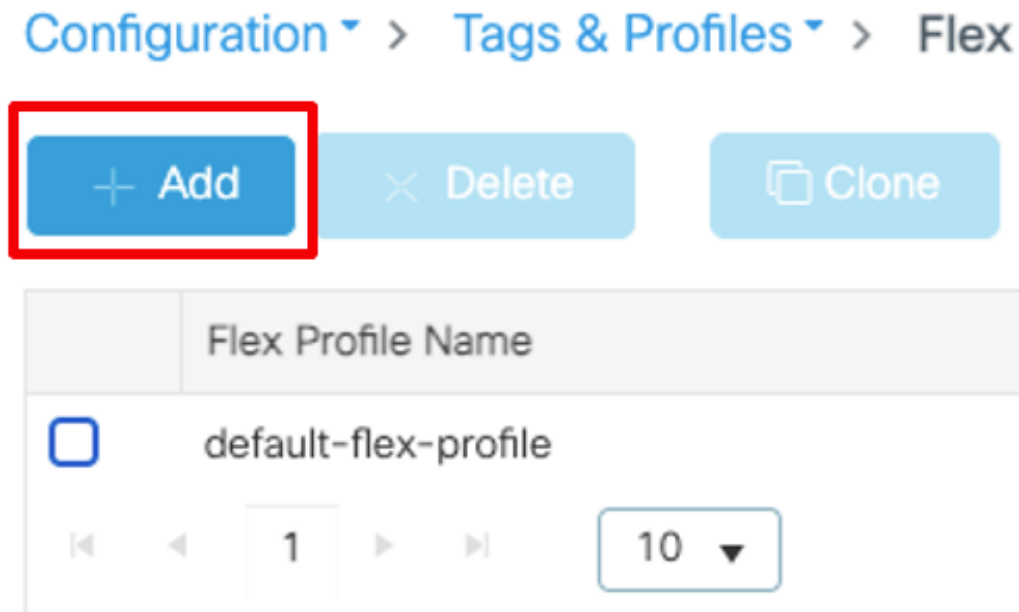
[↶ Cancel](#)

[📄 Apply to Device](#)

## Configure the Flex Profile

To dynamically assign a VLAN ID via RADIUS on a FlexConnect AP, it is necessary for the VLAN ID mentioned in the Tunnel-Private-Group ID attribute of the RADIUS response to be present on the access points. The VLANs are configured on the Flex profile.

1. Navigate to **Configuration > Tags & Profiles > Flex > + Add**.



2. Click on the General tab, assign a name for the Flex profile, and configure a native VLAN ID for the AP.

Add Flex Profile

**General**    Local Authentication    Policy ACL    VLAN    Umbrella

Name\*    Dynamic-VLAN-Flex    Fallback Radio Shut   

Description    Enter Description    Flex Resilient   

Native VLAN ID    103    ARP Caching   

HTTP Proxy Port    0    Efficient Image Upgrade   

HTTP-Proxy IP Address    0.0.0.0    Office Extend AP   

Join Minimum Latency   

IP Overlap   

mDNS Flex Profile    Search or Select    ▼

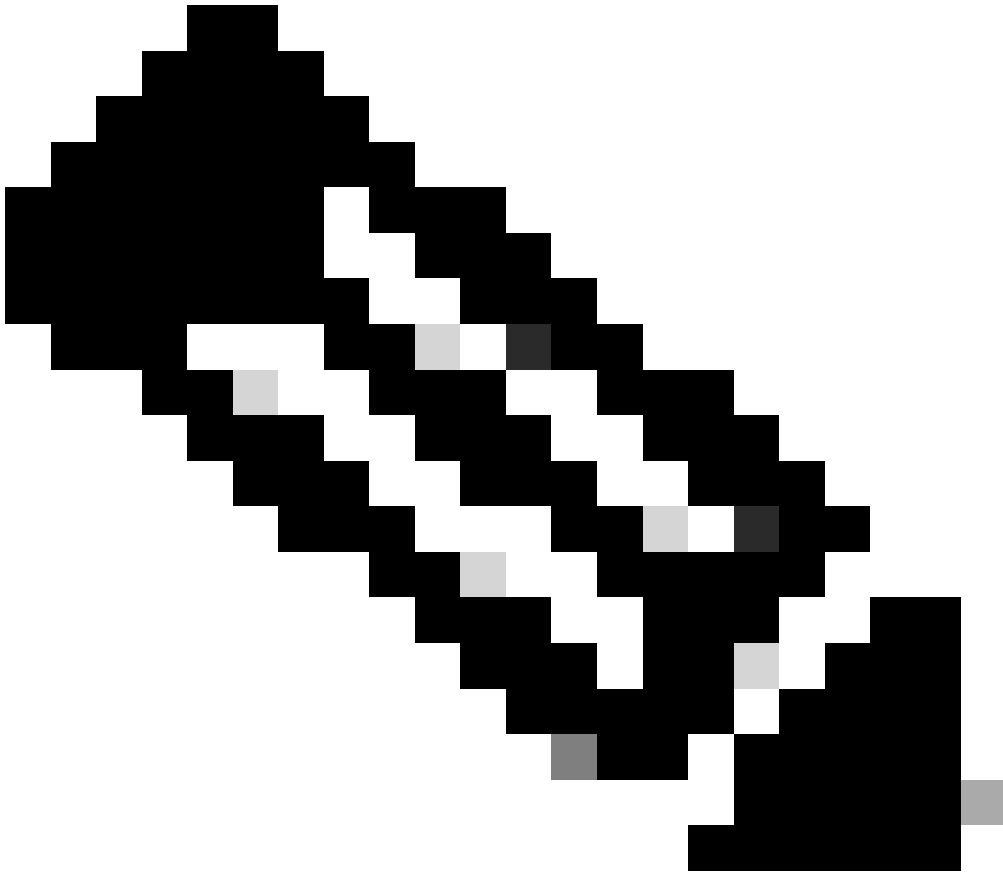
CTS Policy

Inline Tagging   

SGACL Enforcement   

CTS Profile Name    default-sxp-profile    ▼

Cancel    Apply to Device



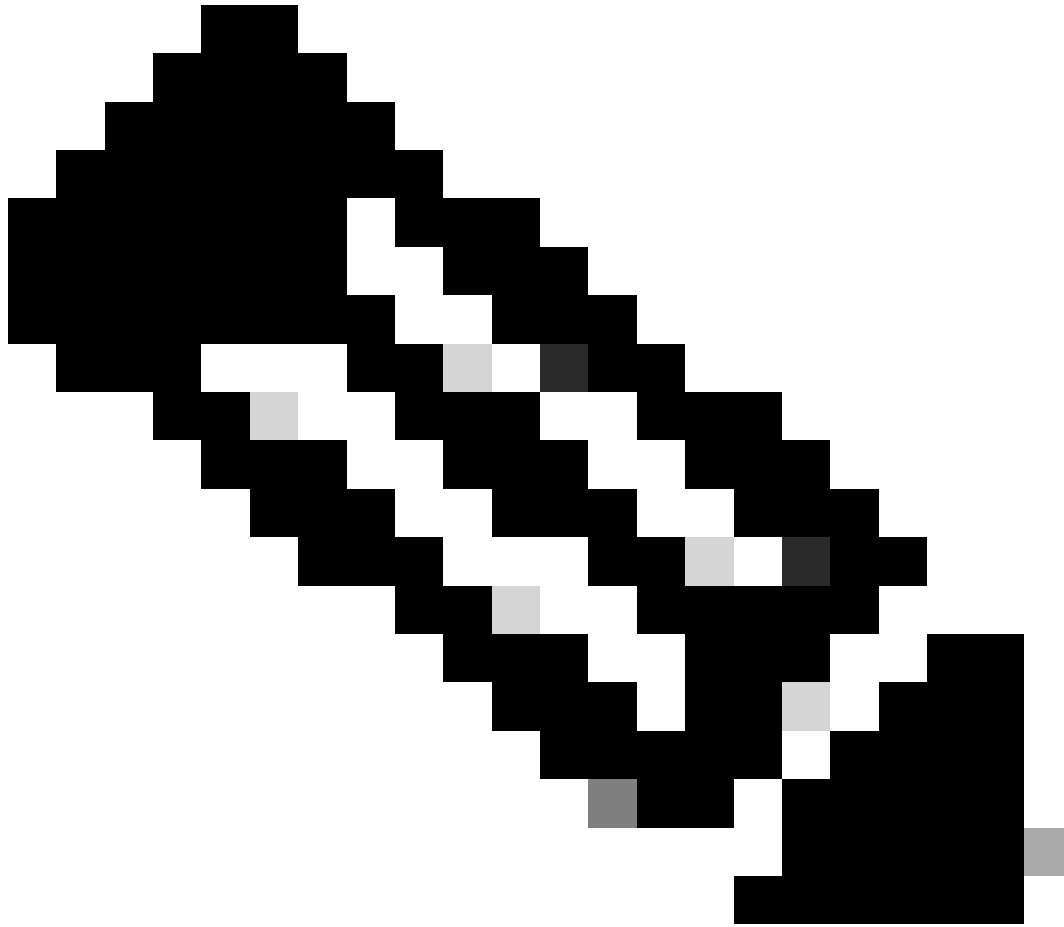
**Note:** The native VLAN ID refers management VLAN for the AP, so it must match the native VLAN configuration of the switch the AP is connected to

3. Navigate to the VLAN tab and click on the “Add” button to enter all the necessary VLANs.

The screenshot shows the 'Add Flex Profile' interface with the 'VLAN' tab selected. The 'Add' button is highlighted in red. A table lists existing VLANs, with 'VLAN102' shown. A modal form for adding a new VLAN is open, with 'VLAN Name\*' and 'VLAN Id\*' fields highlighted in red. The 'Save' button is also highlighted in red.

VLAN Name	ID	Ingress ACL	Egress ACL
VLAN102	102		

VLAN Name\* VLAN105  
VLAN Id\* 105  
ACL  Unidirectional  Bidirectional  
Ingress ACL Select ACL  
Egress ACL Select ACL  
Save Cancel



**Note:** In step 3 of the section Flexconnect Policy Profile Configuration, you configured the default VLAN assigned to the SSID. If you use a VLAN name on that step, ensure that you use the same VLAN name on the Flex Profile configuration, otherwise, clients are not able to connect to the WLAN.

---

## Flex Site tag configuration

1. Navigate to **Configuration > Tags & Profiles > Tags > Site > +Add**, to create a new site tag.
2. Unselect the Enable Local Site box to allow APs to switch the client data traffic locally and add the Flex Profile created on the Configure the Flex Profile section.

Add Site Tag
✕

Name\*

DynamicVLAN-FlexTag

Description

Enter Description

AP Join Profile

default-ap-profile ▼

Flex Profile

Dynamic-VLAN-Flex ▼

Fabric Control Plane Name

▼

Enable Local Site

↶ Cancel

📄 Apply to Device

## Assign the Policy and Site Tag to an AP.

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

Edit AP
✕

General

Interfaces

High Availability

Inventory

ICap

Advanced

Support Bundle

General

AP Name\*

AIR-AP3802I-A-K9

Location\*

default location

Base Radio MAC

4ce1.7544.4000

Ethernet MAC

4ce1.751c.91c8

Admin Status

ENABLED ■

AP Mode

Local ▼

Operation Status

Registered

Fabric Status

Disabled

LED

State

ENABLED ■

Brightness Level

8 ▼

Flash 💡

ENABLED ■

Flash Duration (sec) ⓘ \*

0

Tags

⚠ Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.

Policy

Dynamic-VLAN ▼

Site

DynamicVLAN-FlexT ▼

RF

default-rf-tag ▼

Write Tag Config to AP

Version

Primary Software Version

17.4.1.6

Predownloaded Status

N/A

Predownloaded Version

N/A

Next Retry Time

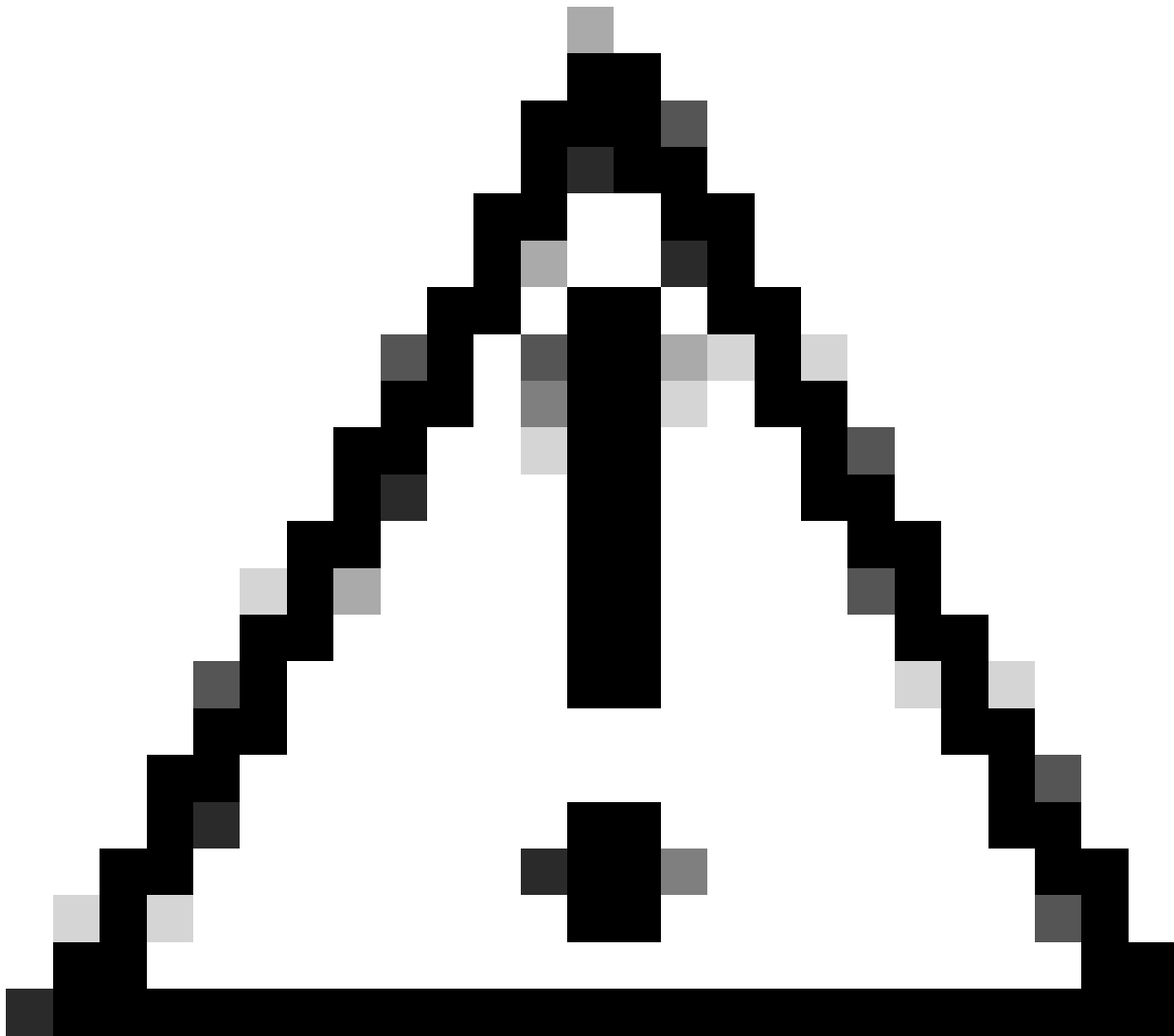
N/A

Boot Version

1.1.2.4

↶ Cancel

📄 Update & Apply to Device



**Caution:** Be aware that changing the policy and site tag on an AP results in the AP disconnecting from the WLC and then reconnecting.

---

---

**Note:** If the AP is configured in Local mode (or any other mode) and then it gets a Site Tag with the "Enable Local Site" setting disabled, the AP reboots and comes back in FlexConnect mode

---

## Verify

Use this section to confirm that your configuration works properly.

Configure the test client SSID profile using the proper EAP protocol and credentials defined in ISE that can return a Dynamic VLAN assignment. Once you are prompted for a username and password, enter the information of the user mapped to a VLAN on ISE.

In the previous example, notice that smith-102 is assigned to the VLAN102 as specified in the RADIUS server. This example uses this username to receive authentication and to be assigned to a VLAN by the RADIUS server:

Once the authentication is completed, you need to verify that your client is assigned to the proper VLAN as per the RADIUS attributes sent. Complete these steps to accomplish this task:

1. From the controller GUI, navigate to **Monitoring > Wireless > Clients > Select the client MAC address > General >**

Security Information and look for the VLAN field as shown in the image:

The screenshot shows the Cisco Catalyst GUI for monitoring wireless clients. On the left, a table lists client details:

Client MAC Address	IPv4 Address	IPv6 Address
b88a.6010.3c60	10.10.102.121	fe80::d8a2:dc93:3758:8...

On the right, the 'Client' details page is shown. The 'Security Information' tab is selected, and the 'Server Policies' section is highlighted with a red box:

Local Policies	Server Policies	Resultant Policies
Service Template		
Absolute Timer		
VLAN	102	
VLAN Name		VLAN0102
VLAN		102

From this window, you can observe that this client is assigned to VLAN102 as per the RADIUS attributes configured on the RADIUS server.

From the CLI you can use the `show wireless client summary detail` to view the same information as shown in the image:

```
Catalyst-C9800-CL#show wireless client summary detail
Number of Clients: 1
MAC Address      SSID      AP Name      State      IP Address      Device-type      VLAN
BSSID           Auth Method  Created      Connected  Protocol Channel Width  SGI NSS Rate  CAP  Username
-----
[REDACTED] 10.3c60 Dinamyc-VLAN AIR-AP2802I-A-K9 Run 10.10.105.200 Intel-Device 105
[REDACTED] 14.4000 [802.1x] 05 06 11n(2.4) 1 20/20 Y/Y 1/1 24.0 E jonathga-105

Catalyst-C9800-CL#show wireless client summary detail
Number of Clients: 1
MAC Address      SSID      AP Name      State      IP Address      Device-type      VLAN
BSSID           Auth Method  Created      Connected  Protocol Channel Width  SGI NSS Rate  CAP  Username
-----
[REDACTED] 10.3c60 Dinamyc-VLAN AIR-AP2802I-A-K9 Run 10.10.102.121 Intel-Device 102
[REDACTED] 14.4000 [802.1x] 54 55 11n(2.4) 1 20/20 Y/Y 1/1 m5 E jonathga-102
```

- It is possible to enable the **Radioactive traces** to ensure successful transfer of the RADIUS attributes to the WLC. In order to do so, do these steps:
  - From the controller GUI, navigate to **Troubleshooting > Radioactive Trace > +Add**.
  - Enter the Mac Address of the wireless client.
  - Select **Start**.
  - Connect the client with the WLAN.

5. Navigate to Stop > Generate > Choose 10 minutes > Apply to Device > Select the trace file to download the log.

This portion of the trace output ensures a successful transmission of RADIUS attributes:

<#root>

2021/03/21 22:22:45.236 {wncd\_x\_R0-0}{1}: [radius] [25253]: (info): RADIUS: Received from id 1812/60 10

Access-Accept

, len 352

2021/03/21 22:22:45.236 {wncd\_x\_R0-0}{1}: [radius] [25253]: (info): RADIUS: authenticator e5 5e 58 fa

2021/03/21 22:22:45.236 {wncd\_x\_R0-0}{1}:

[radius] [25253]: (info): RADIUS: User-Name [1] 13 "smith-102

"

2021/03/21 22:22:45.236 {wncd\_x\_R0-0}{1}: [radius] [25253]: (info): RADIUS: State [24]

2021/03/21 22:22:45.236 {wncd\_x\_R0-0}{1}: [radius] [25253]: (info): RADIUS: Class [25]

2021/03/21 22:22:45.236 {wncd\_x\_R0-0}{1}: [radius] [25253]: (info): 01:

2021/03/21 22:22:45.236

{wncd\_x\_R0-0}{1}: [radius] [25253]: (info): RADIUS: Tunnel-Type [64] 6 VLAN

[13]

2021/03/21 22:22:45.236 {wncd\_x\_R0-0}{1}: [radius] [25253]: (info): 01:

2021/03/21 22:22:45.236

{wncd\_x\_R0-0}{1}: [radius] [25253]: (info): RADIUS: Tunnel-Medium-Type [65] 6 ALL\_802

[6]

2021/03/21 22:22:45.236 {wncd\_x\_R0-0}{1}: [radius] [25253]: (info): RADIUS: EAP-Message [79]

2021/03/21 22:22:45.236 {wncd\_x\_R0-0}{1}: [radius] [25253]: (info): RADIUS: Message-Authenticator[80]

2021/03/21 22:22:45.236 {wncd\_x\_R0-0}{1}: [radius] [25253]: (info): 01:

2021/03/21 22:22:45.236

{wncd\_x\_R0-0}{1}: [radius] [25253]: (info): RADIUS: Tunnel-Private-Group-Id[81] 6 "102"

2021/03/21 22:22:45.236 {wncd\_x\_R0-0}{1}: [radius] [25253]: (info): RADIUS: EAP-Key-Name [102]

2021/03/21 22:22:45.237 {wncd\_x\_R0-0}{1}: [radius] [25253]: (info): RADIUS: MS-MPPE-Send-Key [16]

2021/03/21 22:22:45.237 {wncd\_x\_R0-0}{1}: [radius] [25253]: (info): RADIUS: MS-MPPE-Recv-Key [17]

2021/03/21 22:22:45.238 {wncd\_x\_R0-0}{1}: [eap-auth] [25253]: (info): SUCCESS for EAP method name: PEAP

2021/03/21 22:22:46.700 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [25253]: (info):

[ Applied attribute : username 0 "smith-102" ]

2021/03/21 22:22:46.700 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute :

2021/03/21 22:22:46.700 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [25253]: (info):

[ Applied attribute : tunnel-type 1 13 [vlan] ]

2021/03/21 22:22:46.700 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [25253]: (info):

[ Applied attribute : tunnel-medium-type 1 6 [ALL\_802] ]

2021/03/21 22:22:46.700 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [25253]: (info):

[ Applied attribute :tunnel-private-group-id 1 "102" ]

2021/03/21 22:22:46.700 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute :

2021/03/21 22:22:46.700 {wncd\_x\_R0-0}{1}: [auth-mgr-feat\_wireless] [25253]: (info): [0000.0000.0000:unk

## Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

## Related Information

- [End User Guide](#)
- [Cisco Technical Support & Downloads](#)