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

Contents

Introduction

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.

Requirements

Cisco recommends that you have knowledge of these topics:

- Have basic knowledge of the WLC and Lightweight Access Points (LAPs).
- Have functional knowledge of the AAA server such as ISE.
- Have a thorough knowledge of wireless networks and wireless security issues.

- Have functional knowledge on dynamic 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 Identity Service Engine (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

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.

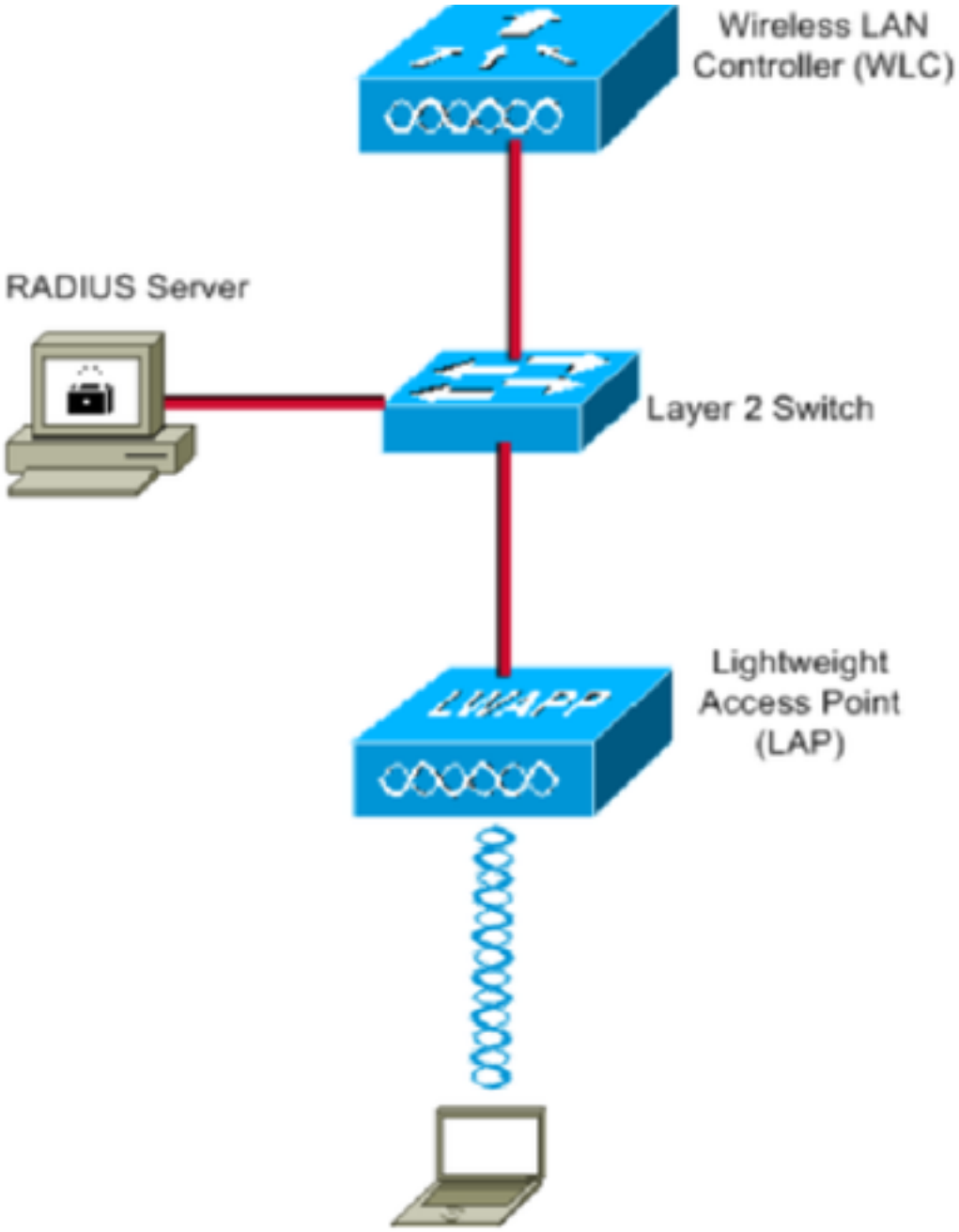
The VLAN ID is 12-bits and takes a value between 1 and 4094, inclusive. Because the Tunnel-Private-Group-ID is of type string, as defined in RFC2868 for use with IEEE 802.1X, the VLAN ID integer value is encoded as a string. When these tunnel attributes are sent, it is necessary to enter them in the 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 jonathga-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:

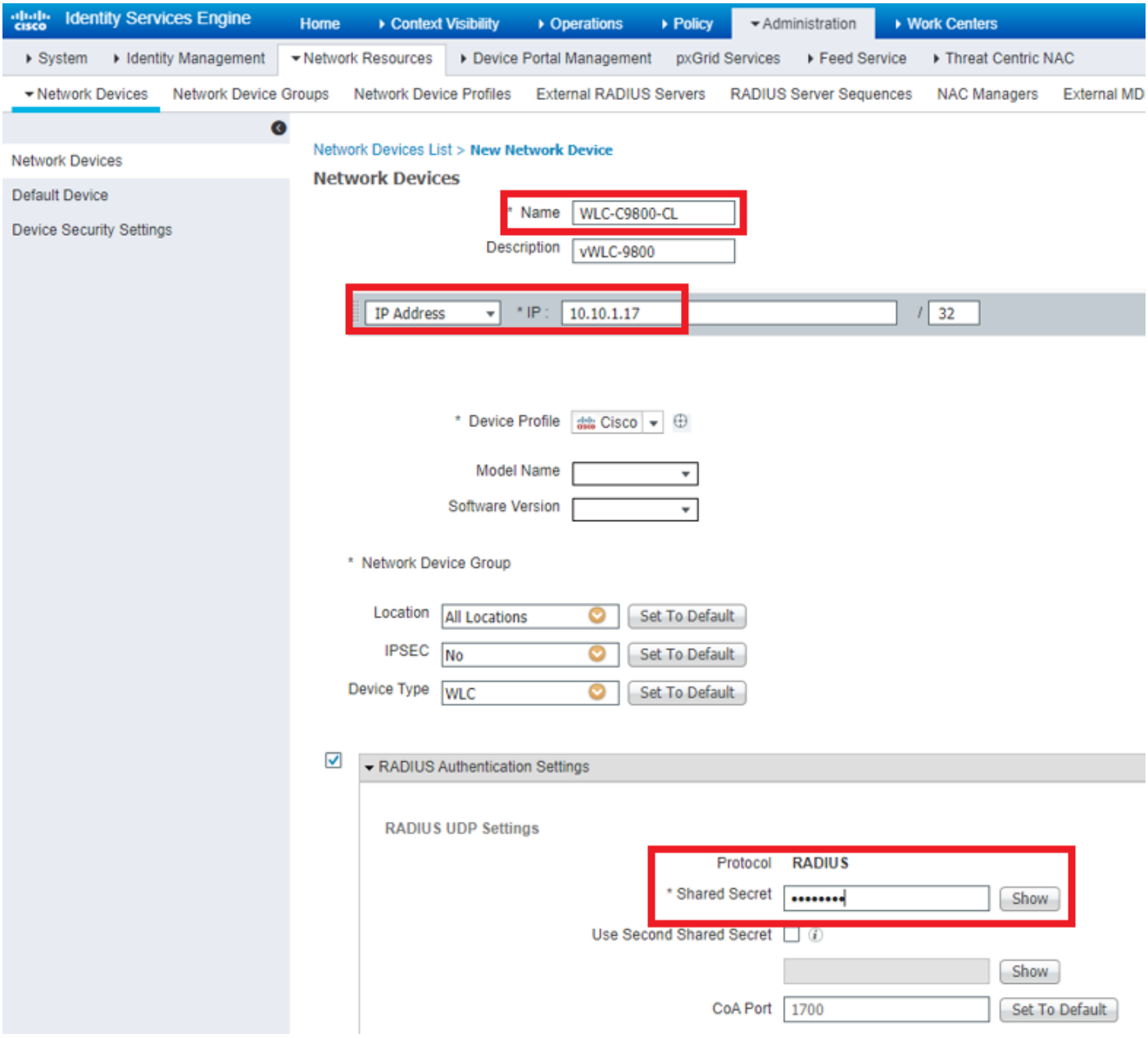
- Configure the Catalyst WLC as an AAA Client on the Cisco ISE Server.
- Configure Internal users on Cisco ISE.
- Configure the RADIUS (IETF) attributes used for dynamic VLAN Assignment on Cisco ISE.

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:

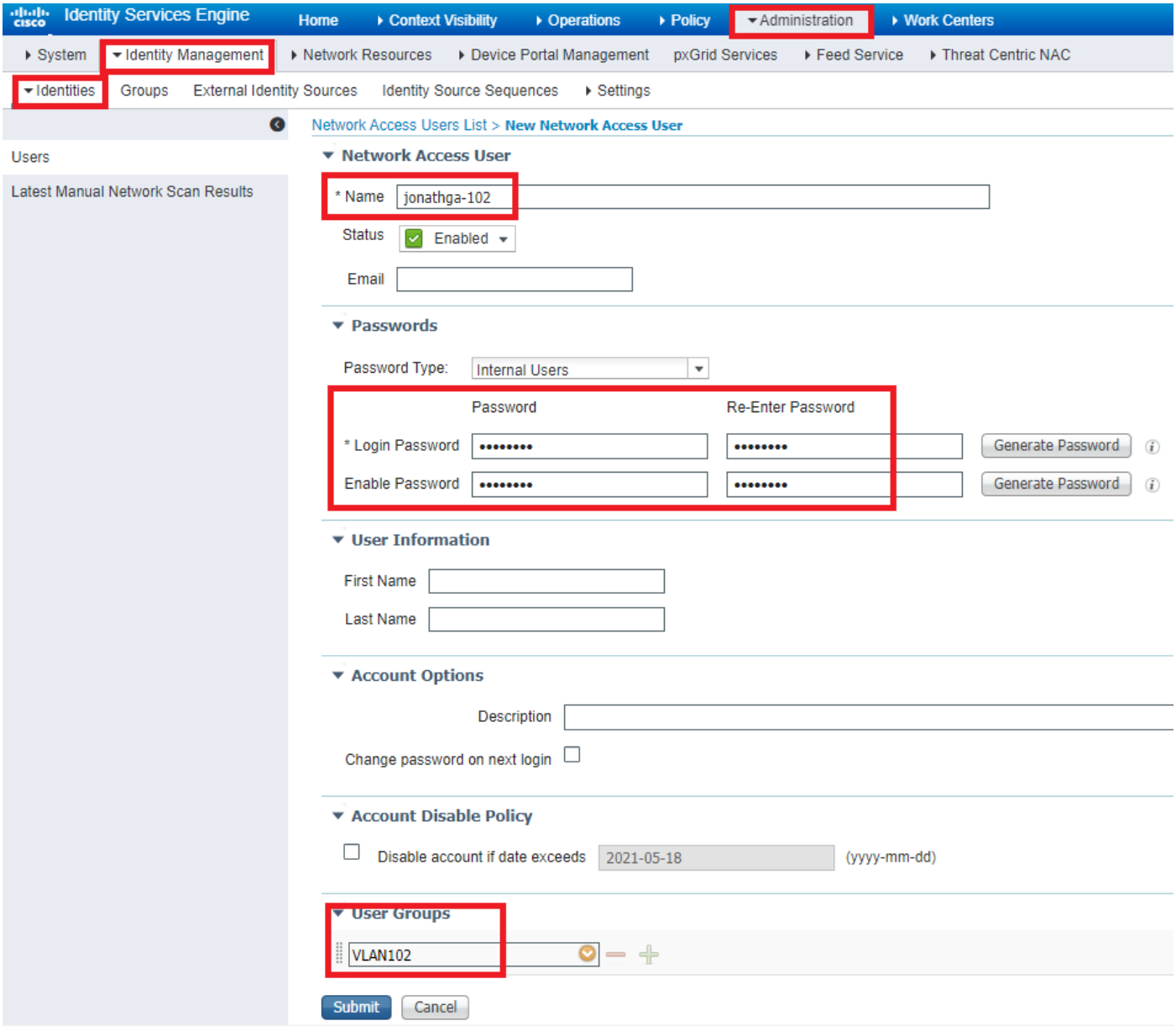


Step 2. Configure internal users on Cisco ISE

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:

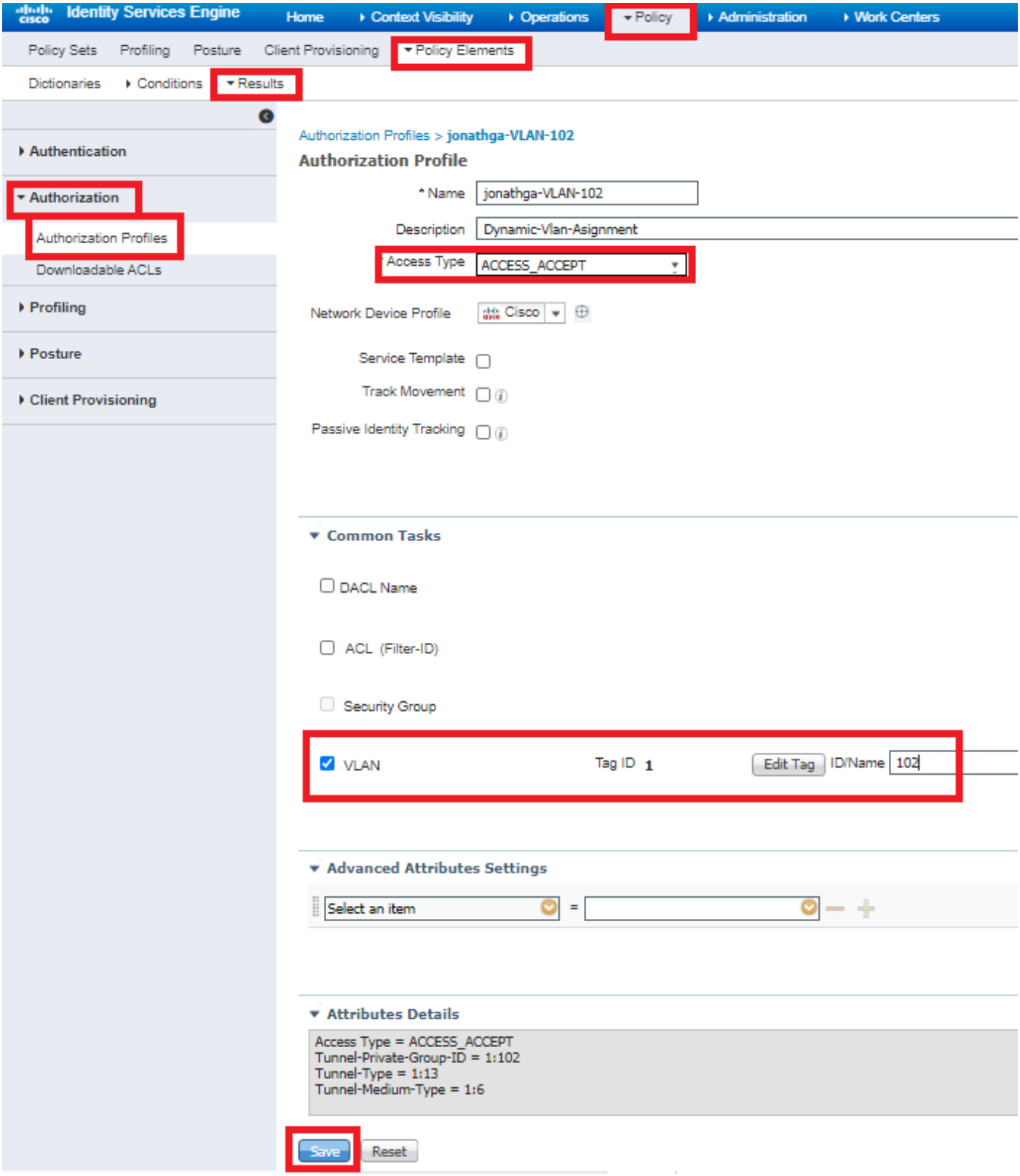


Step 3. Configure the RADIUS (IETF) attributes used for dynamic VLAN Assignment

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

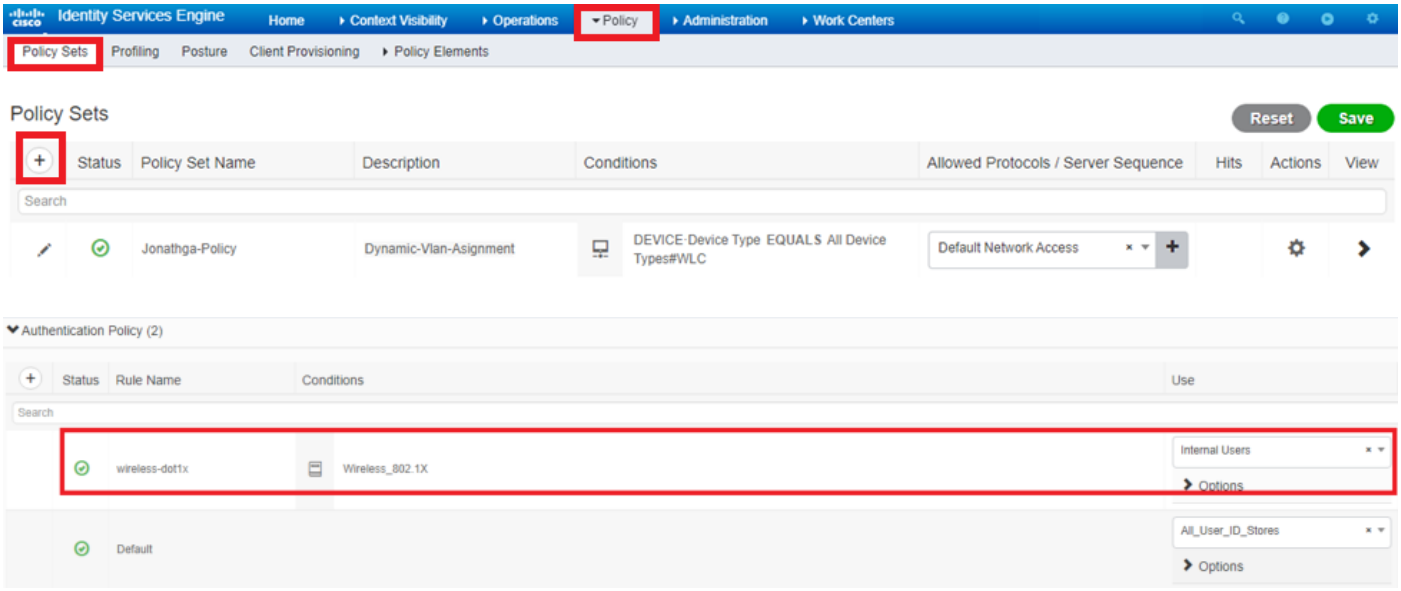
Complete these steps:

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.



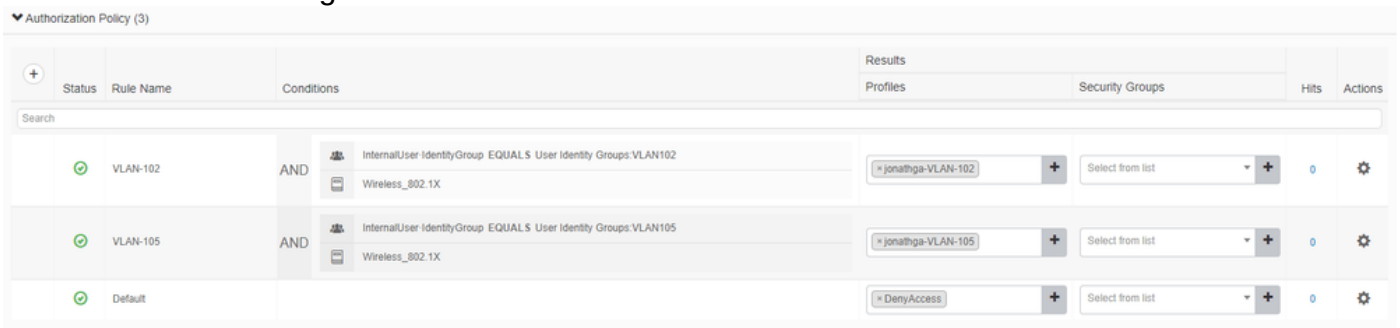
After the authorization profiles are configured, an authentication policy for wireless users needs to be created. You can use a new **Custom** policy or modify the **Default** Policy set. In this example, a custom profile is created.

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:

```
Switch(config-if)#switchport mode trunk

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:

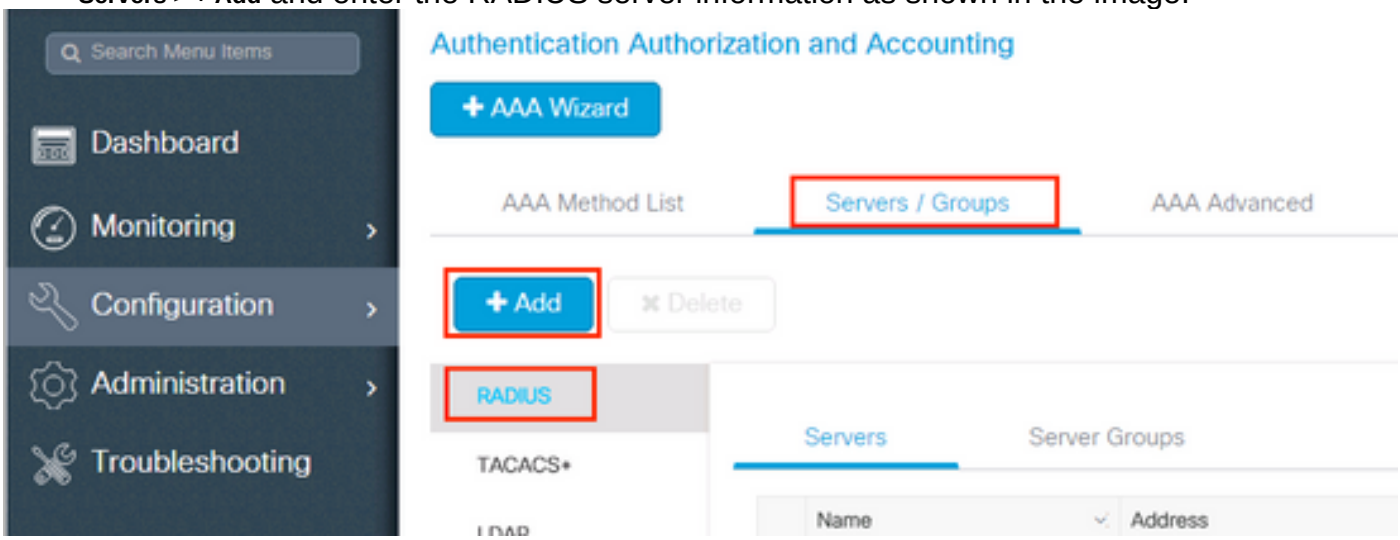
- Configure the WLC with the Details of the Authentication Server.
- Configure the VLANs.
- Configure the WLANs (SSID).
- Configure the Policy Profile.
- Configure the Policy tag.
- Assign the Policy tag to an AP.

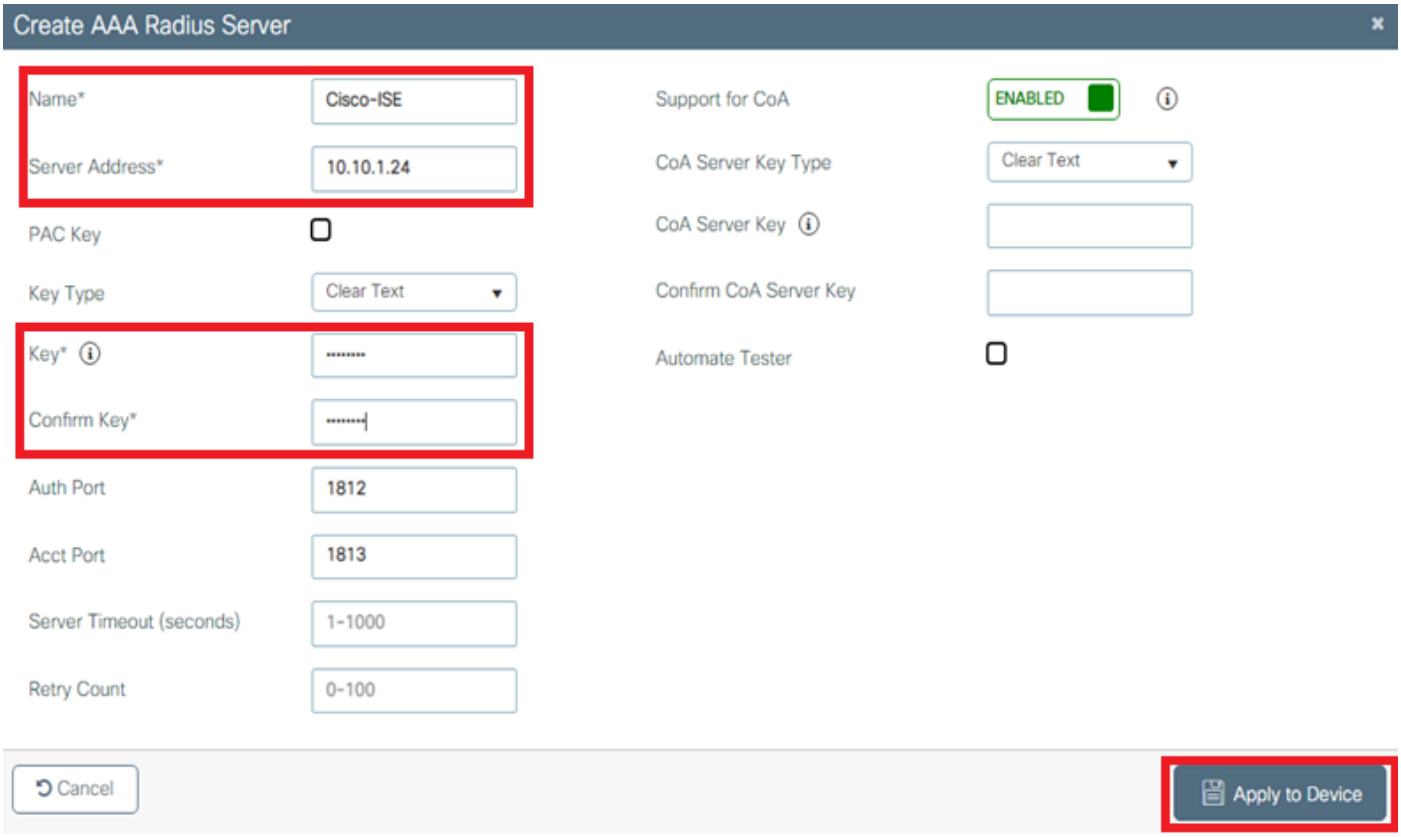
Step 1. Configure the WLC with the Details of the Authentication Server

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

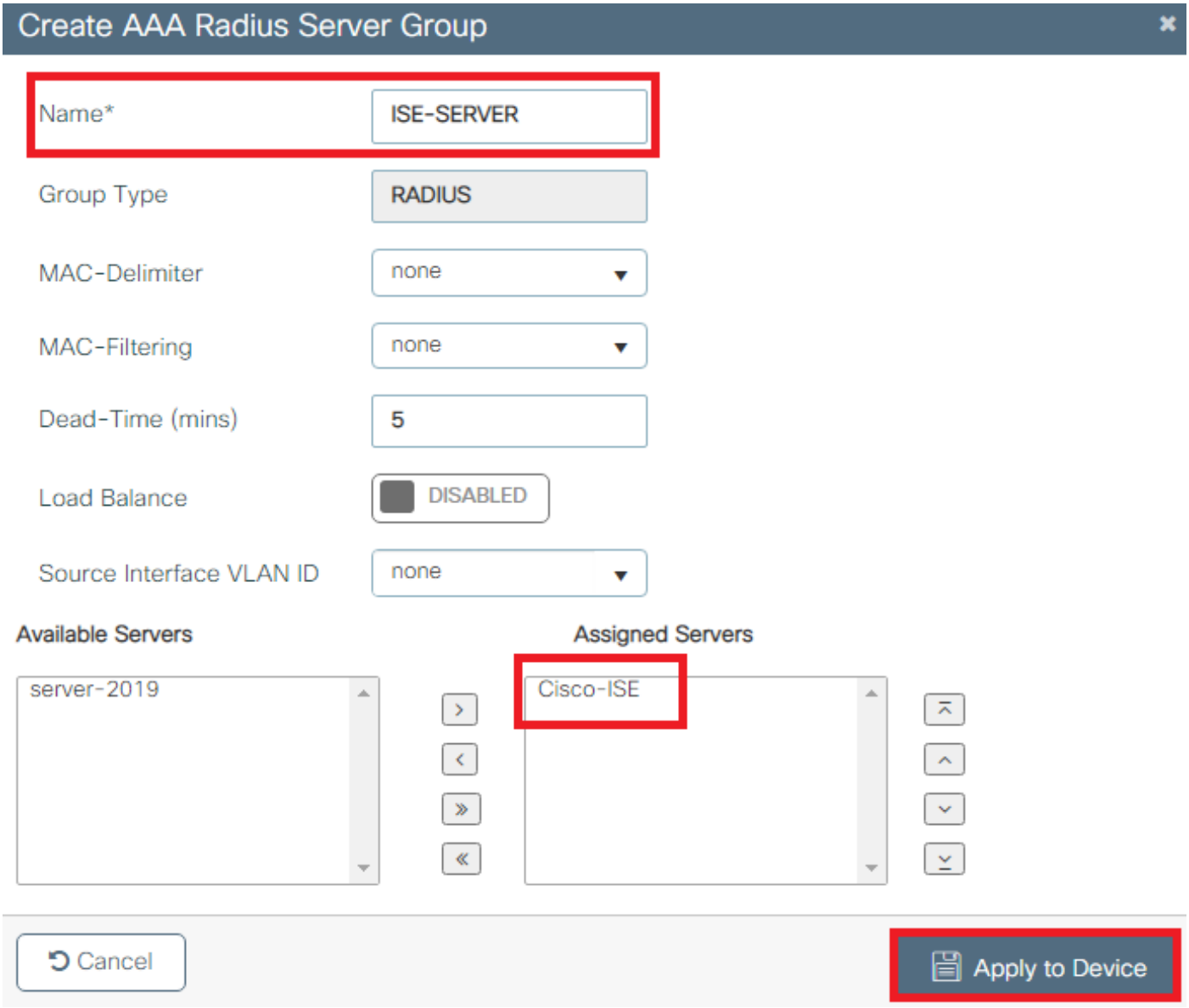
Complete these steps:

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:

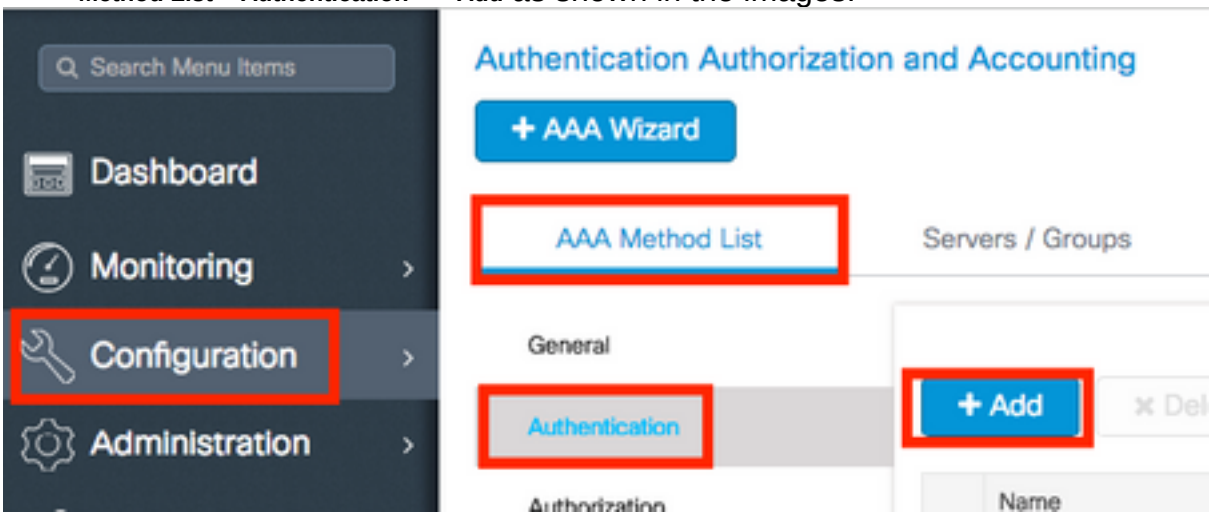


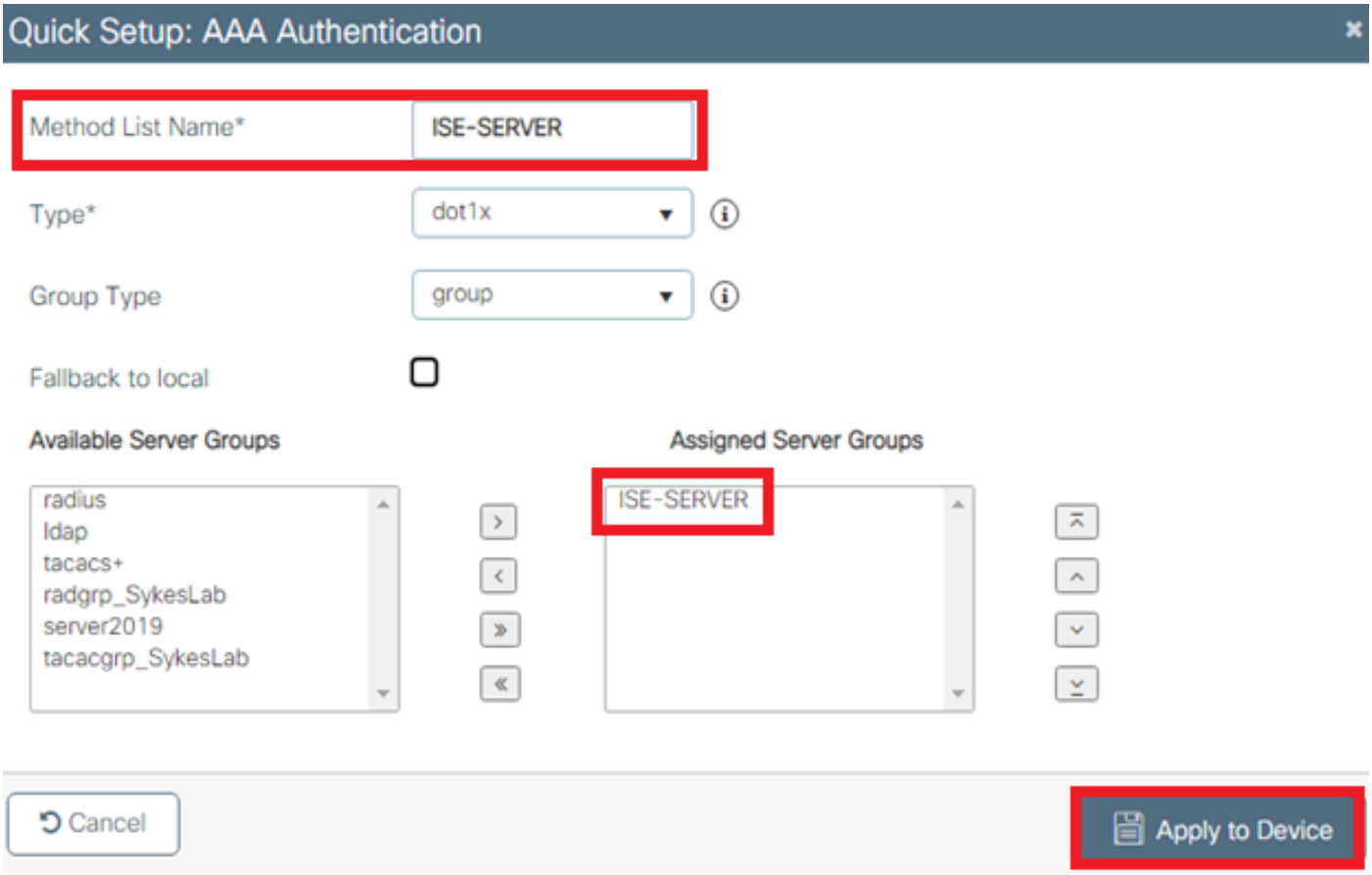


2. In order to add the RADIUS server to a RADIUS group, navigate to **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add** as shown in the image:



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



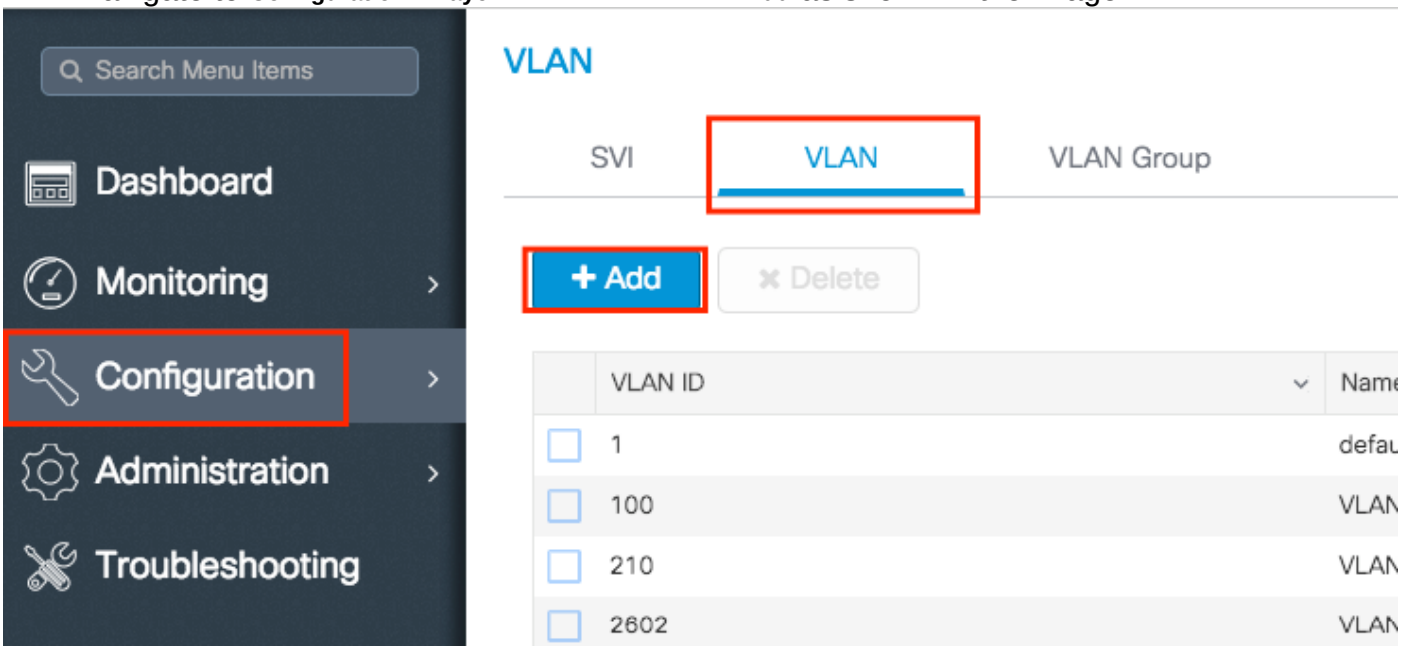


Step 2. Configure the VLANs

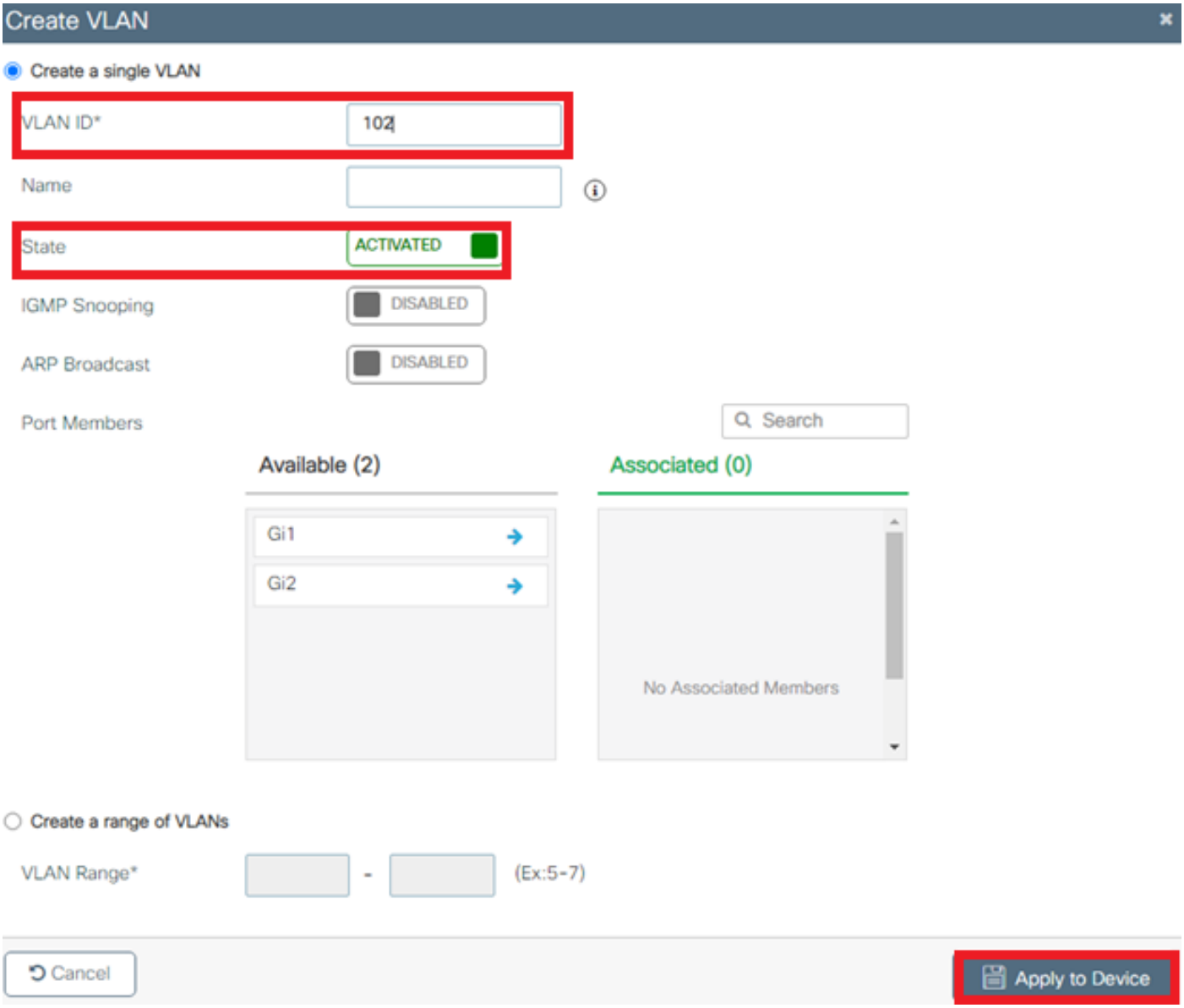
This procedure explains how to configure VLANs on the Catalyst 9800 WLC. As explained earlier in this document, the VLAN ID specified under the Tunnel-Private-Group ID attribute of the RADIUS server must also exist in the WLC.

In the example, the user jonathga-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:



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



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

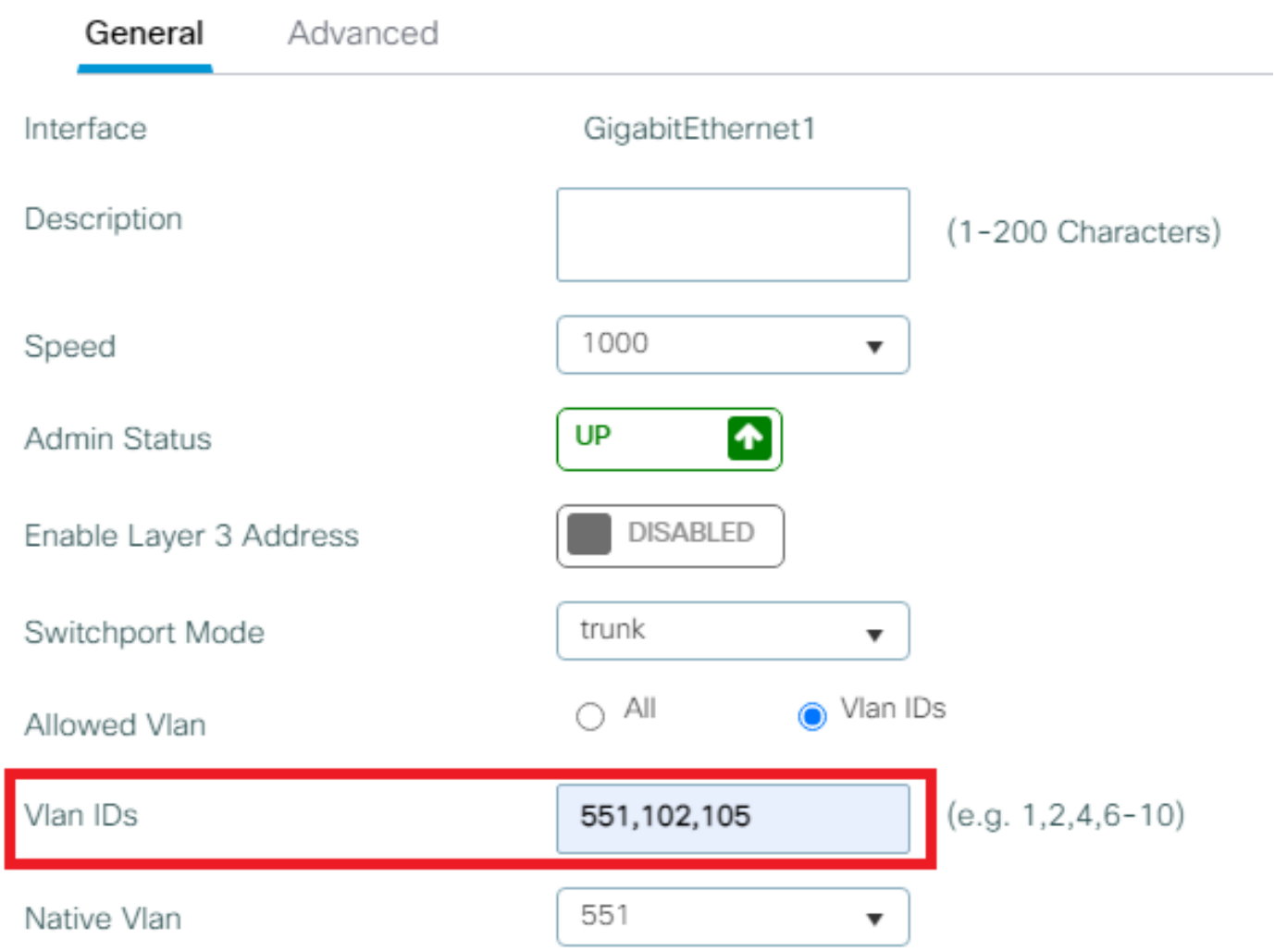
Repeat steps 1 and 2 for all the needed VLANs, once done you can continue to step 3.

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	

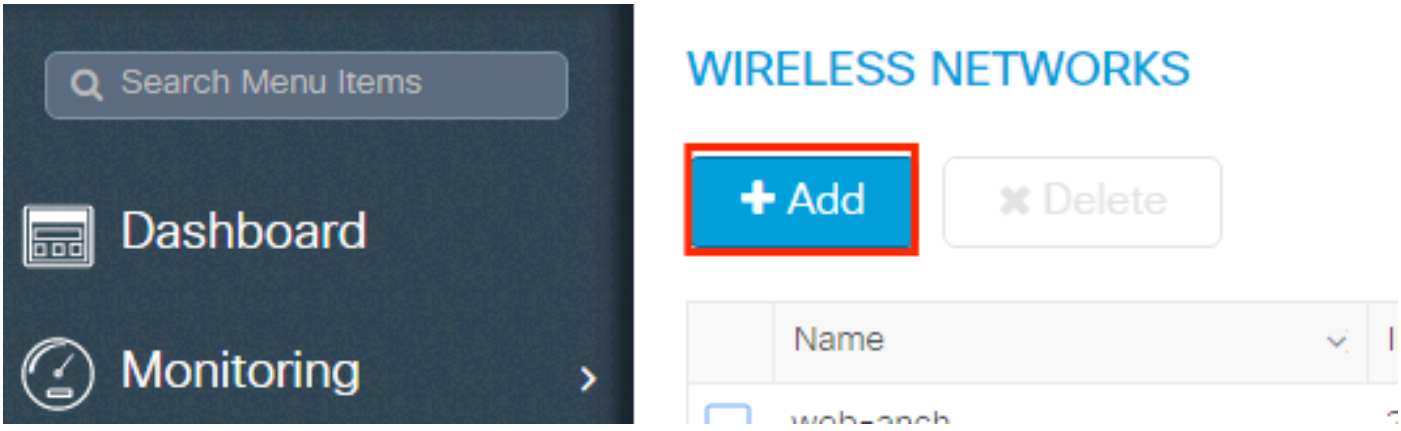


Step 3. Configure the WLANs (SSID)

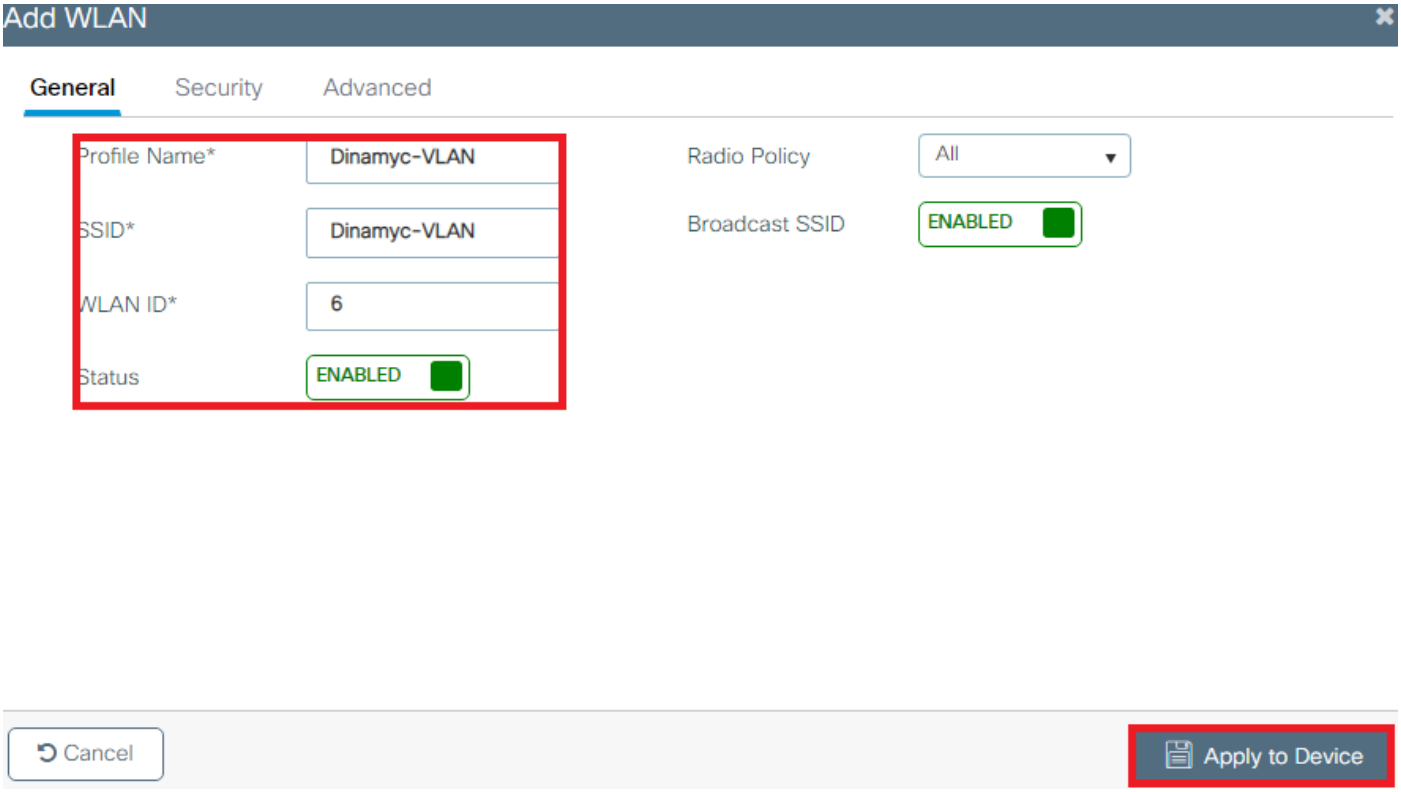
This procedure explains how to configure the WLANs in the WLC.

Complete these steps:

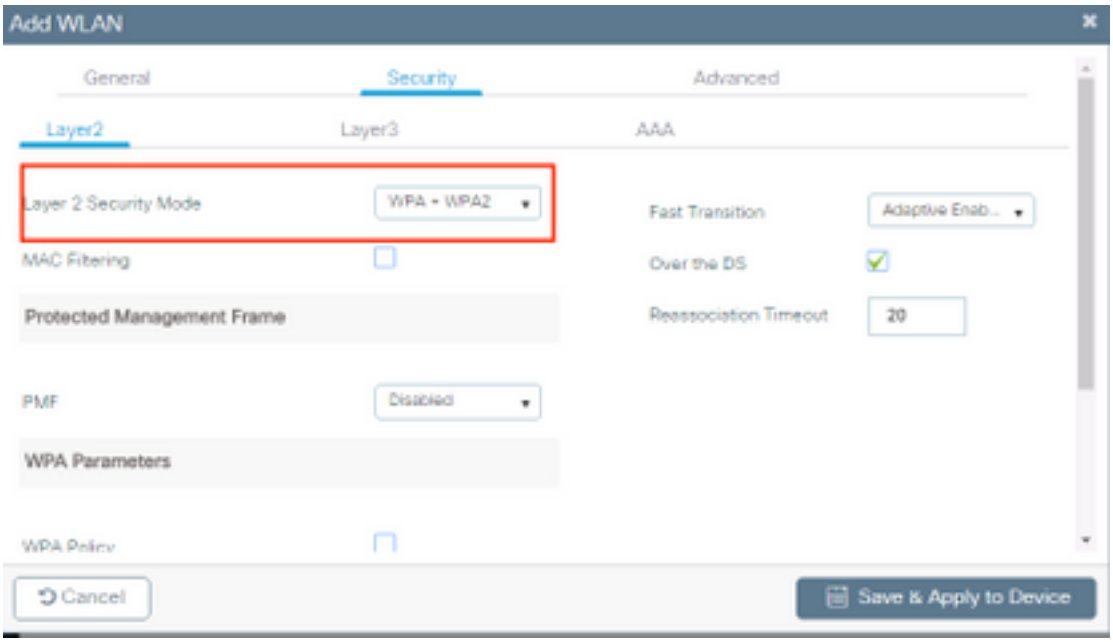
1. In order to create the WLAN. Navigate to **Configuration > Wireless > WLANs > + Add** and configure the network as needed, as shown in the image:

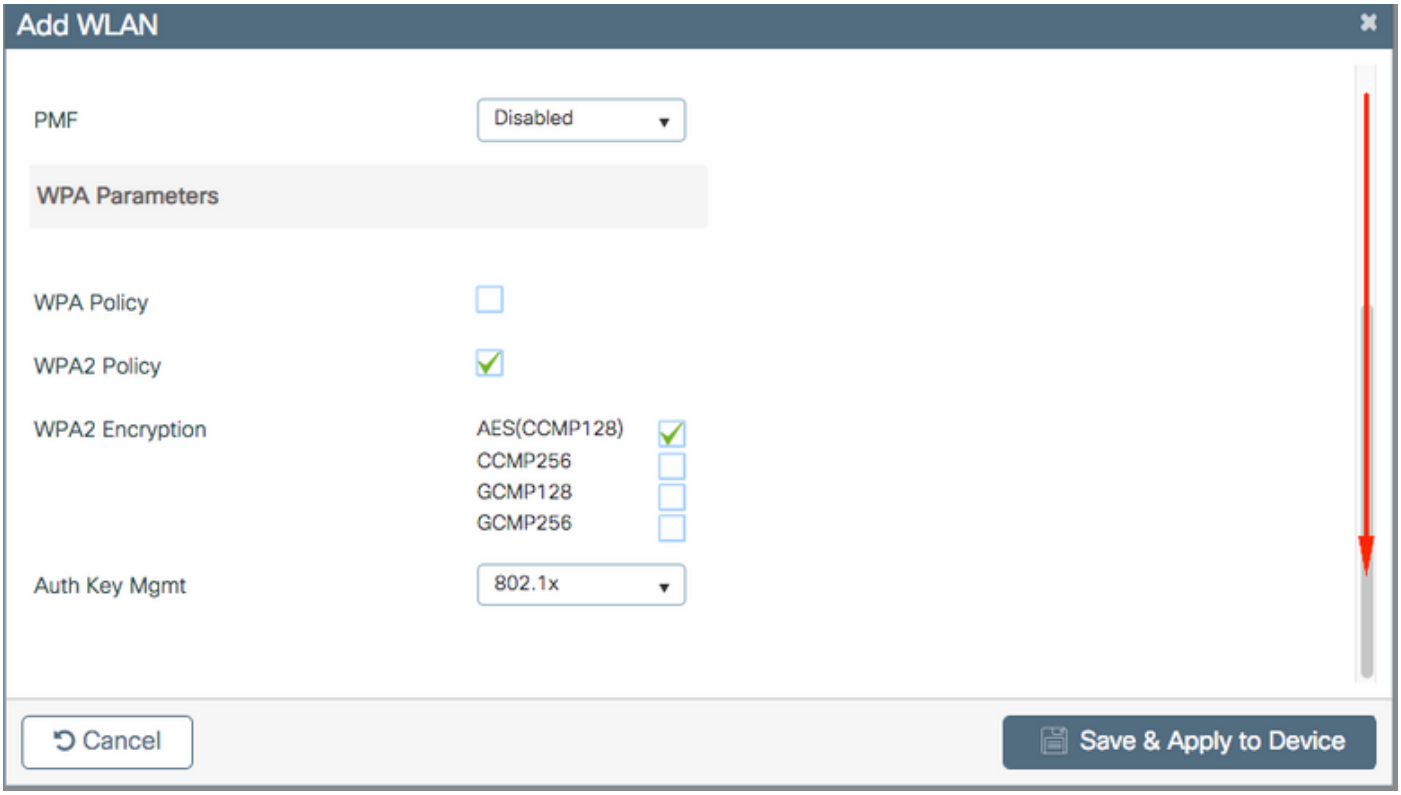


2. Enter the WLAN information as shown in the image:

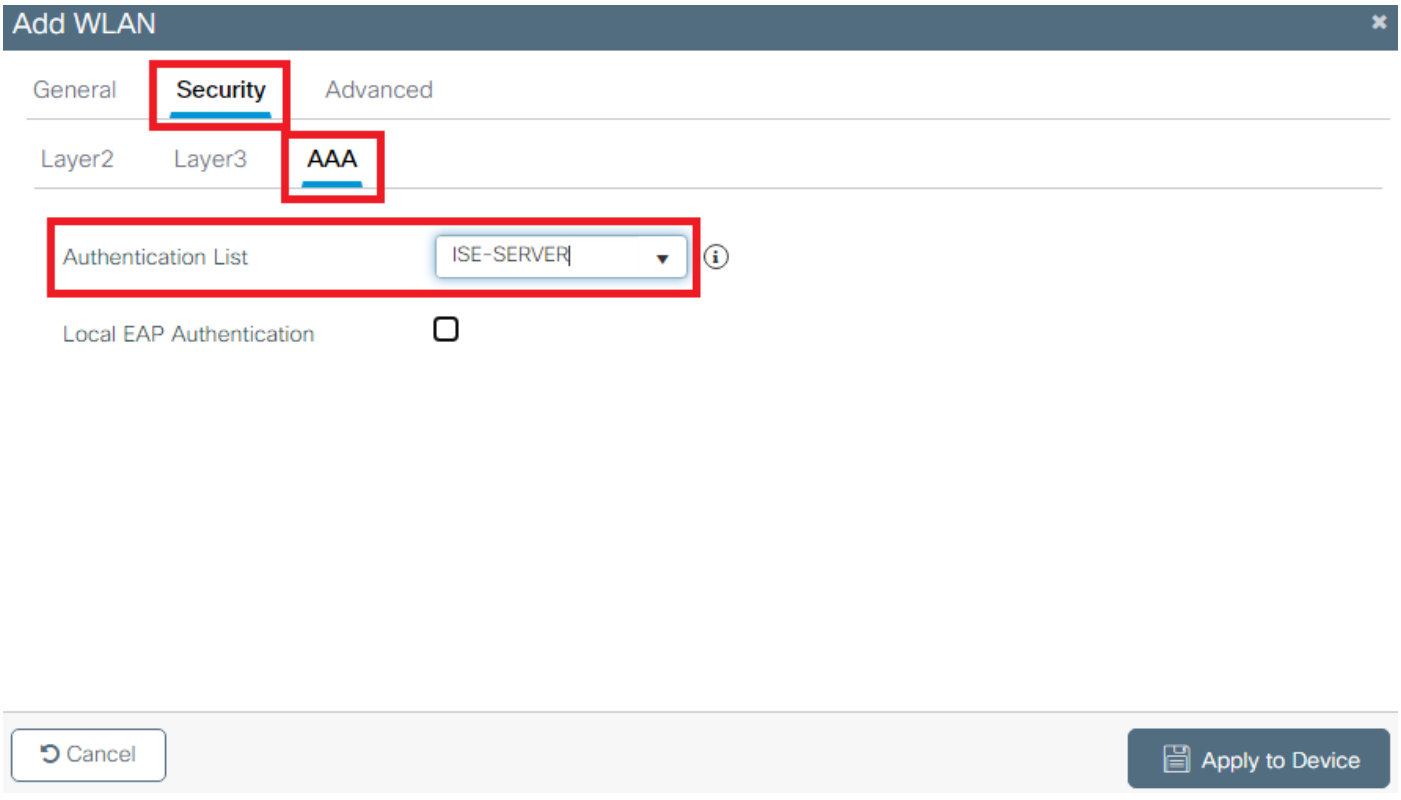


3. Navigate to **Security** tab and select the needed security method. In this case WPA2 + 802.1x as shown in the images:





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:



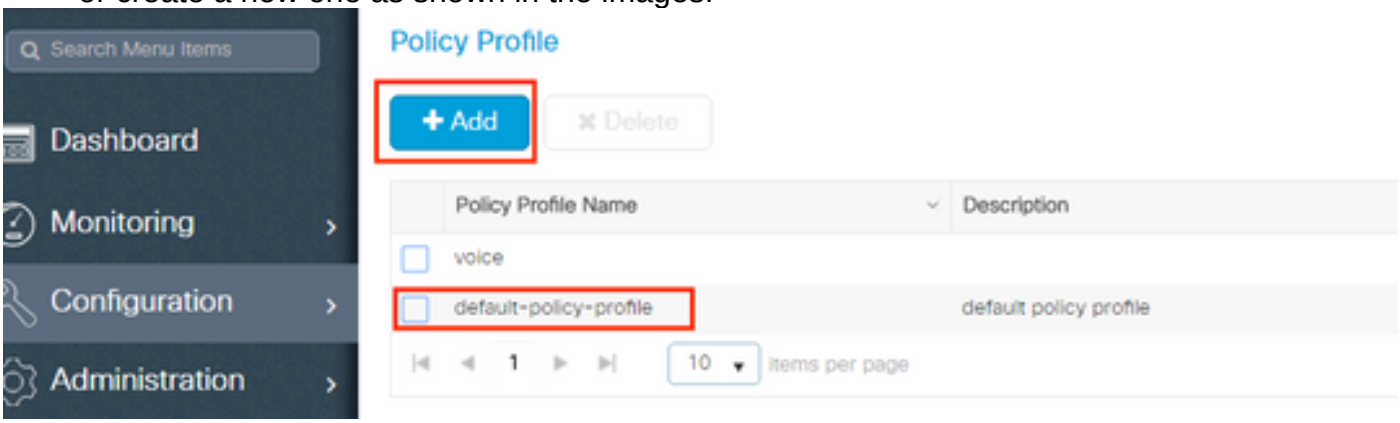
Step 4. Configure the Policy Profile

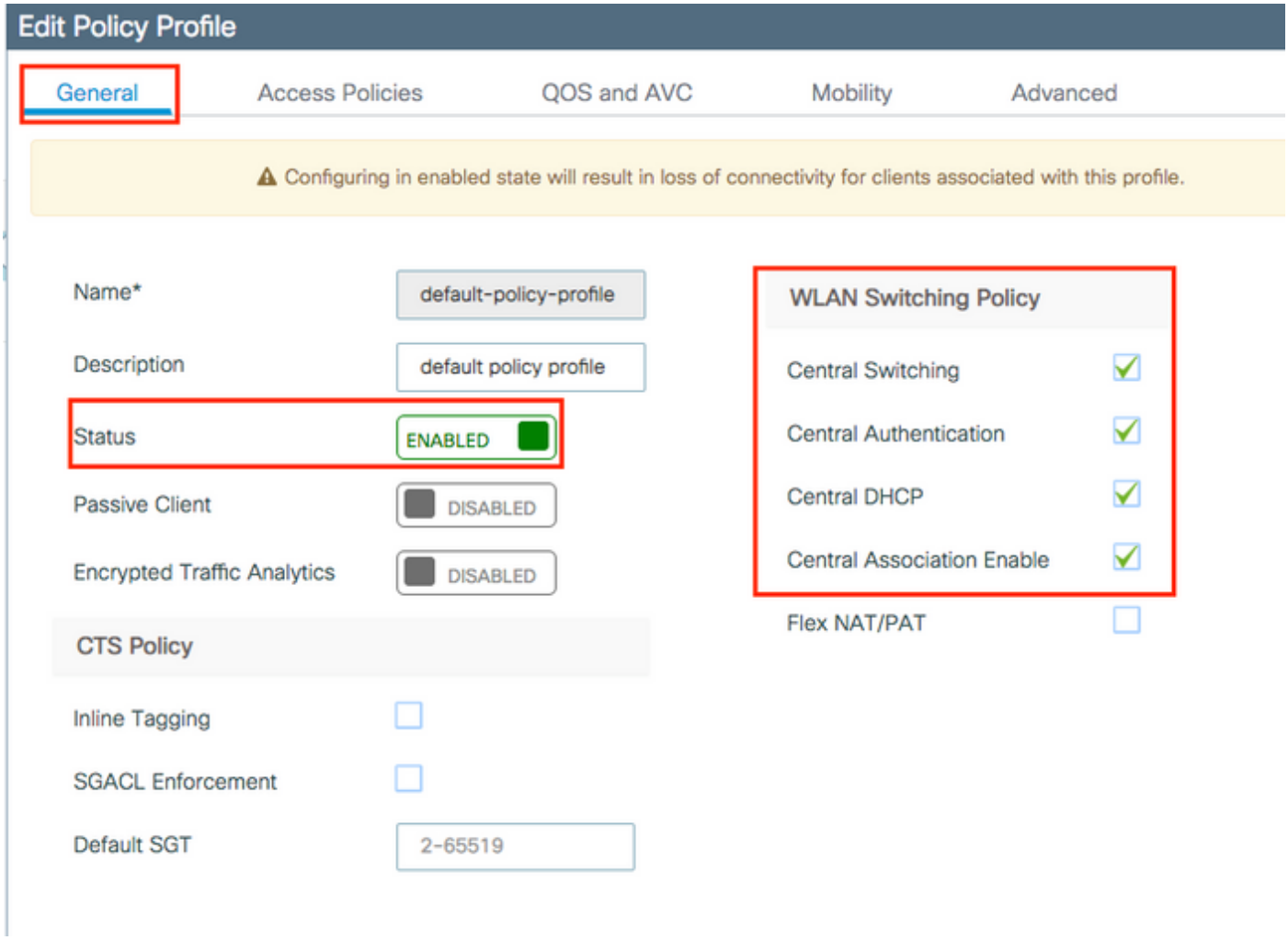
This procedure explains how to configure the Policy Profile in the WLC.

Complete these steps:

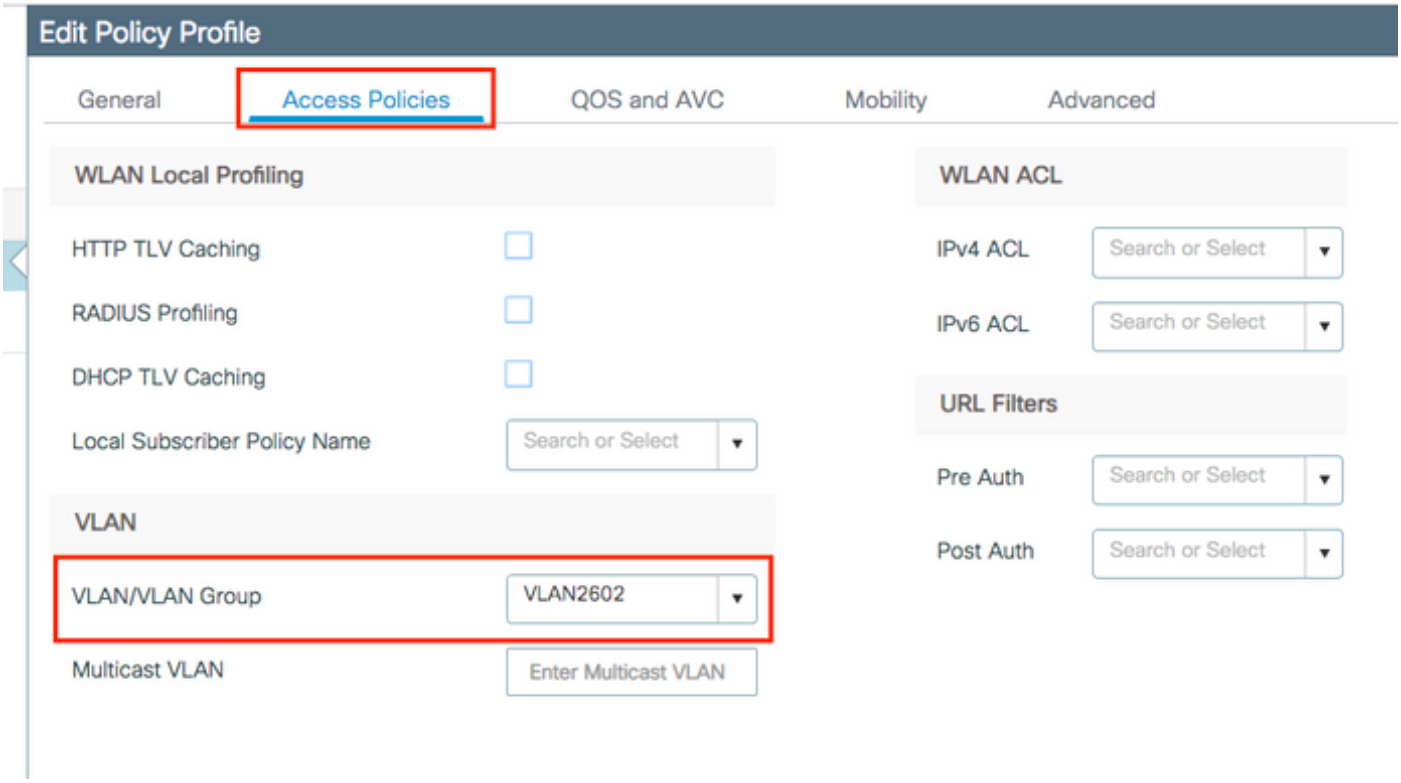
1. Navigate to **Configuration > Tags & Profiles > Policy Profile** and either configure your **default-policy-profile**

or create a new one as shown in the images:



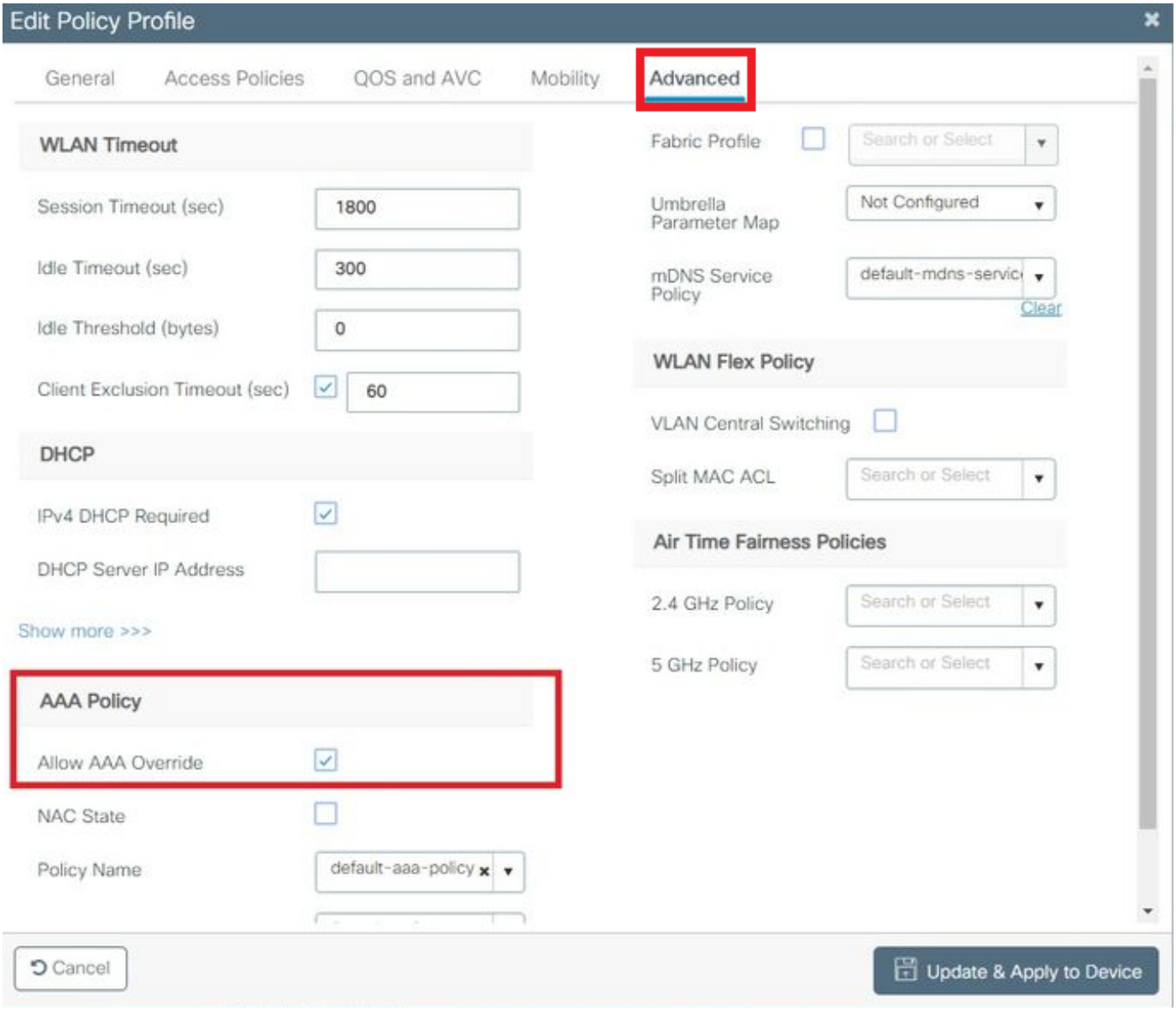


2. From the **Access Policies** tab assign the VLAN to which the wireless clients are assigned when they connect to this WLAN by default as shown in the image:



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.

3. 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:

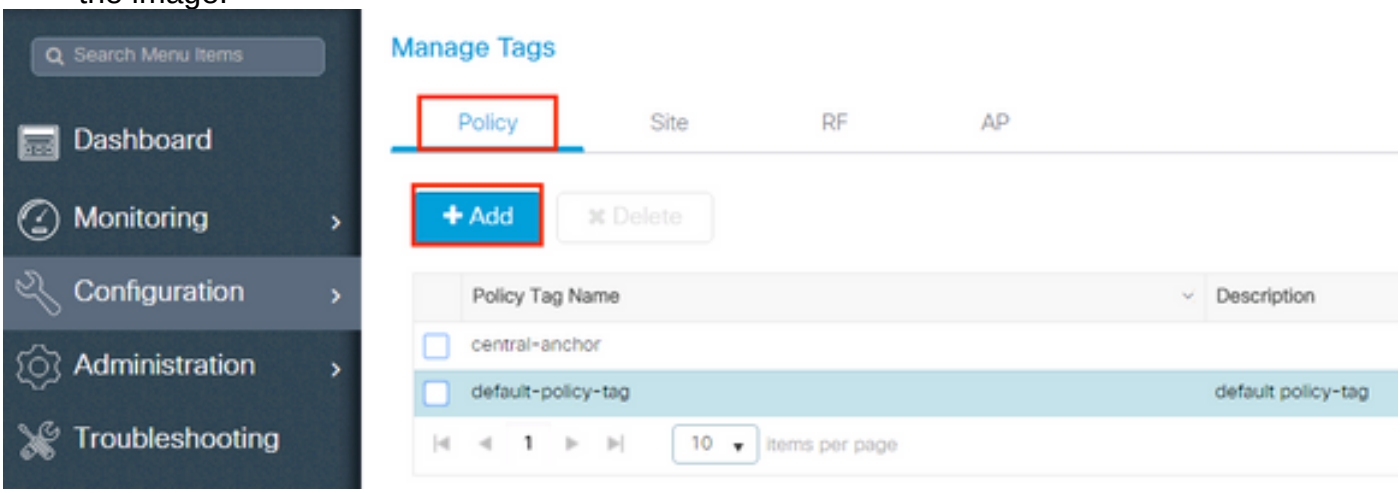


Step 5. Configure the Policy Tag

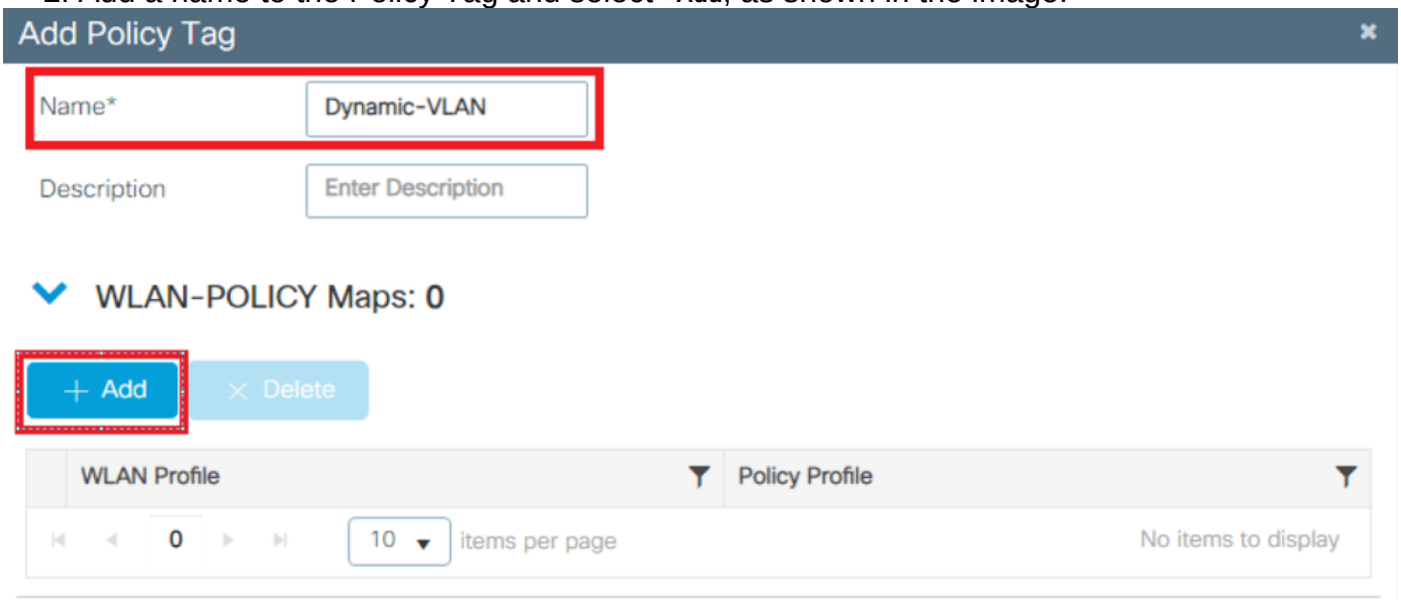
This procedure explains how to configure the Policy tag in the WLC.

Complete these steps:

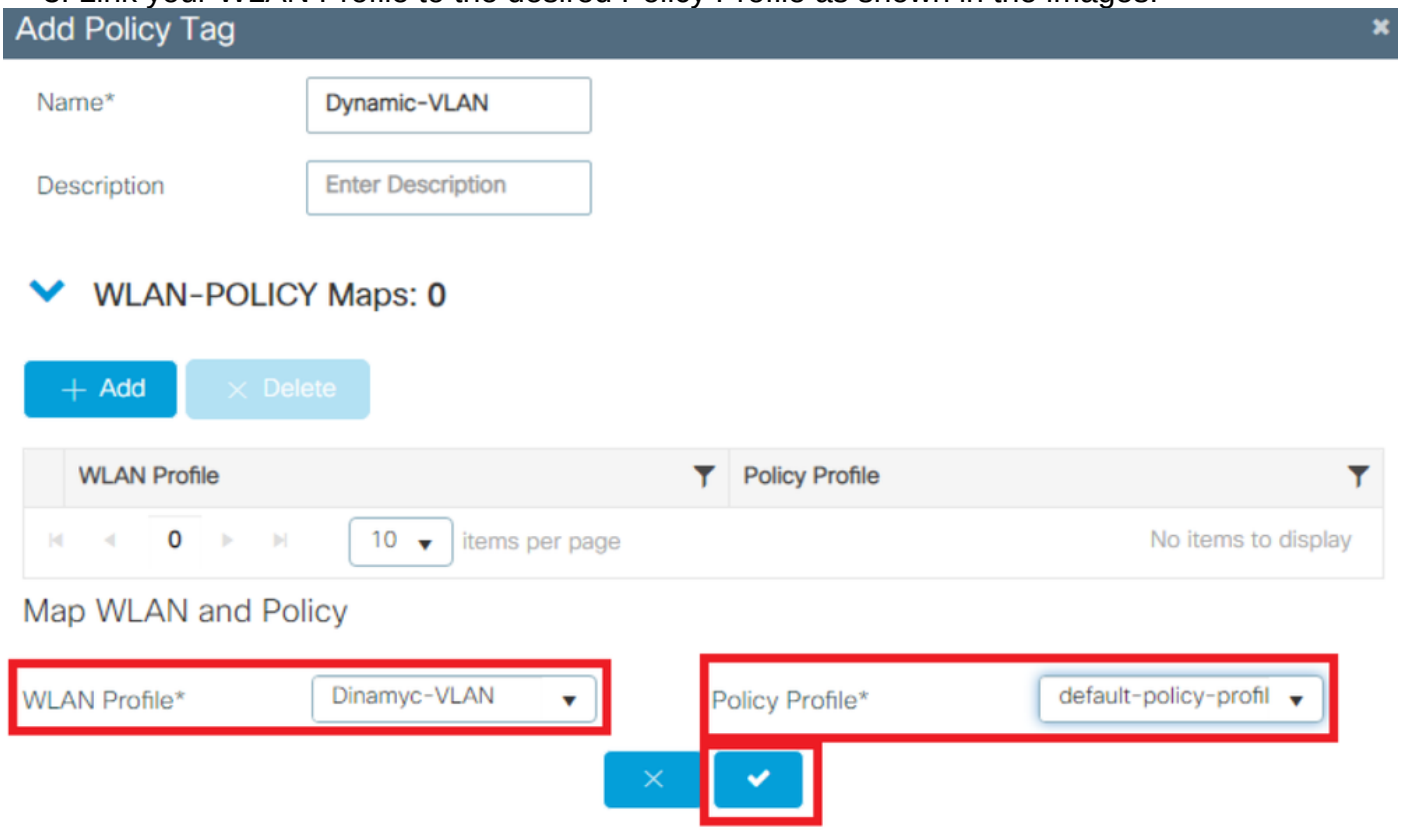
1. Navigate to **Configuration > Tags & Profiles > Tags > Policy** and add a new one if needed as shown in the image:

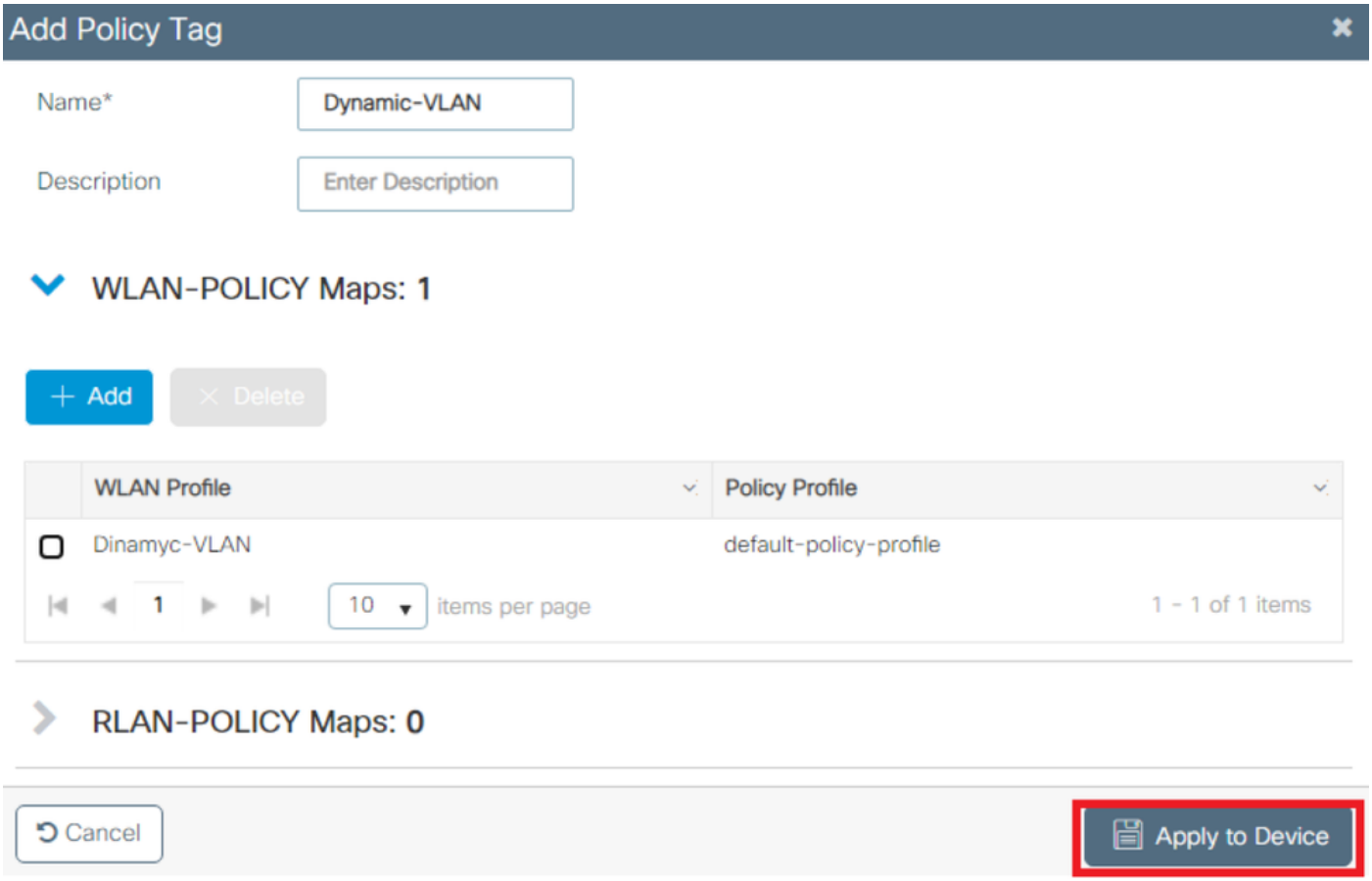


2. Add a name to the Policy Tag and select **+Add**, as shown in the image:



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



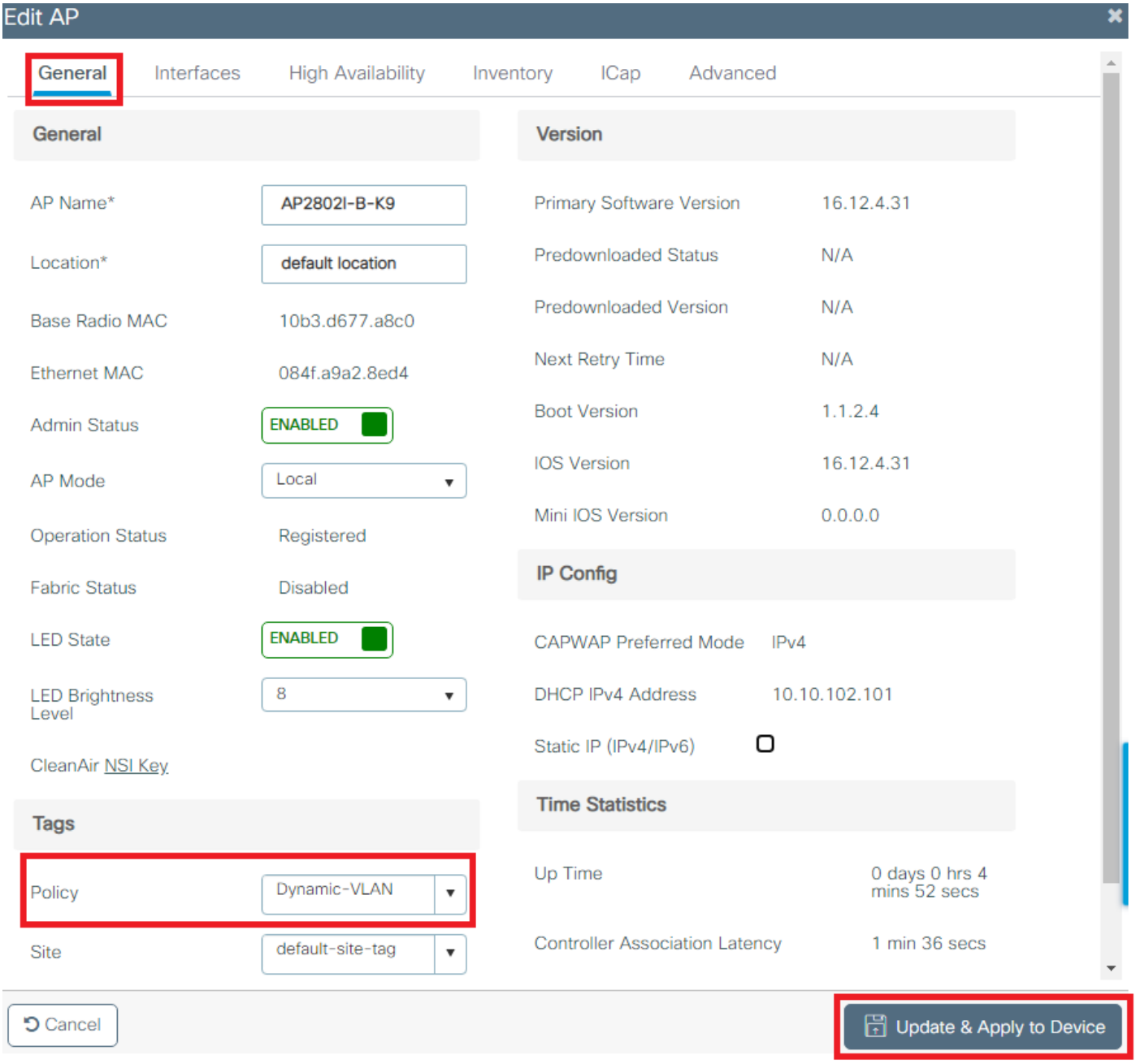


Step 6. Assign the Policy Tag to an AP

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:



Caution: Be aware that when the policy tag on an AP is changed, it drops its association to the WLC and joins back.

Verify

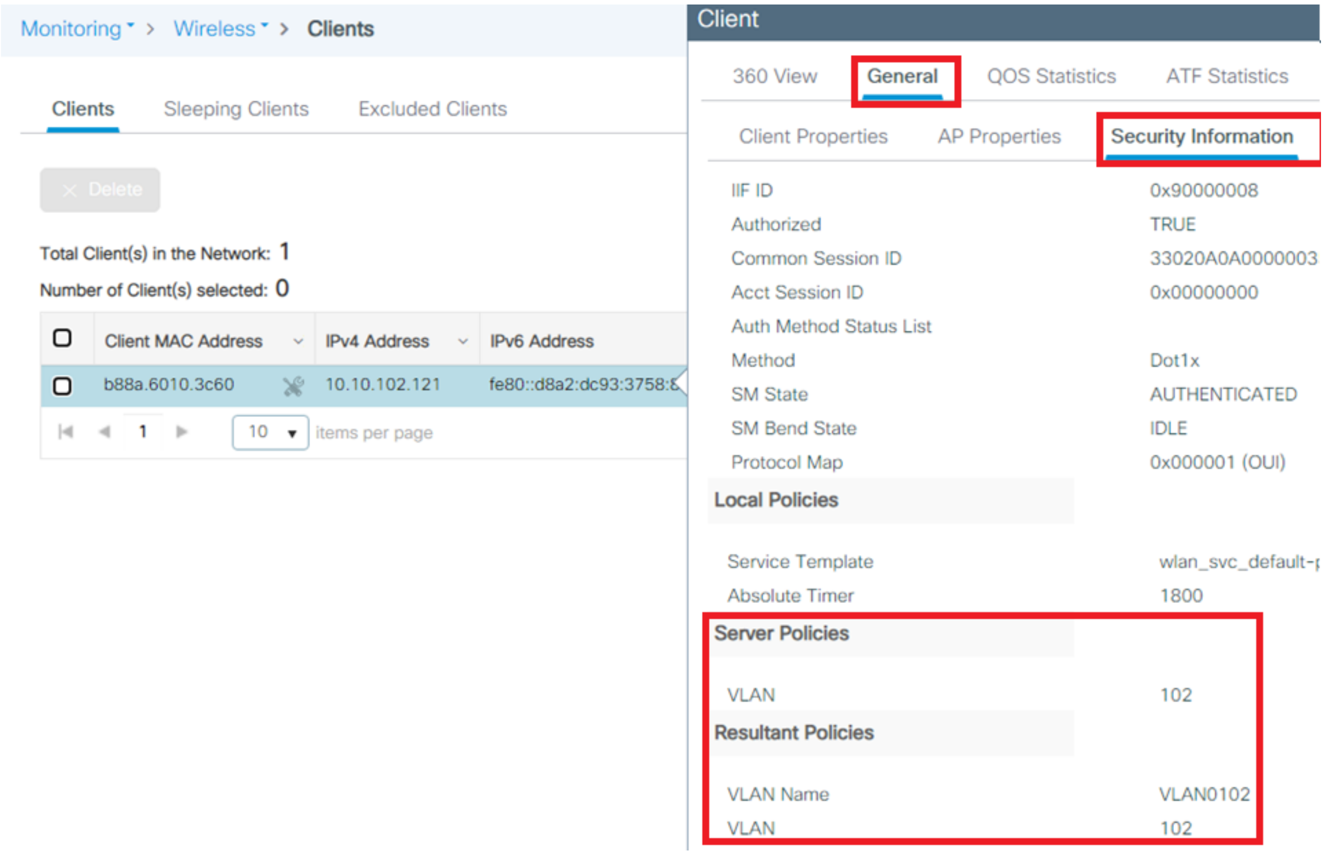
Use this section to confirm that your configuration works properly.

Test connection with Windows 10 and native supplicant, once you are prompted for a username and password, enter the information of the user mapped to a VLAN on ISE.

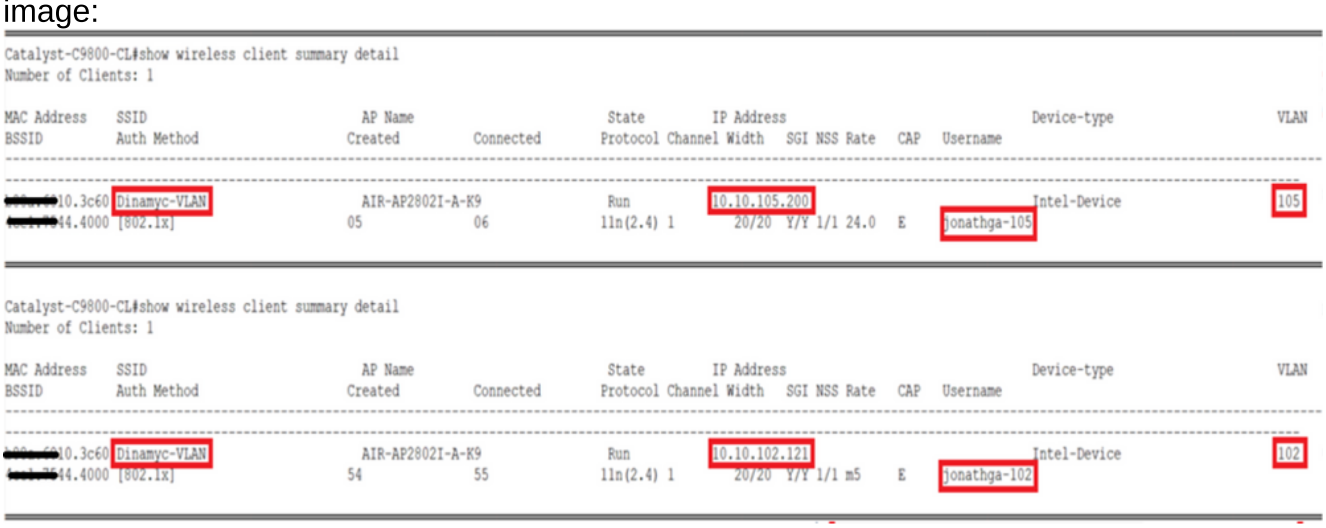
In the previous example, notice that jonathga-102 is assigned to the VLAN102 as specified in the RADIUS server. This example uses this username to receive authentication and to be assigned to a VLAN by the RADIUS server:

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:



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]44.4000 [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]44.4000 [802.1x]      54          55     11n(2.4) 1   20/20  Y/Y 1/1 m5    E  jonathga-102
```

2. It is possible to enable the **Radioactive traces** to ensure successful transfer of the RADIUS attributes to the WLC. In order to do so, follow 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.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:

```
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Received from id
1812/60 10.10.1.24:0, 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 da 0a c7 55 - 53 55 7d 43 97 5a 8b 17
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  User-Name
[1]     13  "jonathga-102"
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  State
[24]    40  ...
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  Class
[25]    54  ...
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]     6  ...
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  Message-
Authenticator[80]    18  ...
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]   67  *
2021/03/21 22:22:45.237 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:   MS-MPPE-Send-Key
[16]    52  *
2021/03/21 22:22:45.237 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:   MS-MPPE-Recv-Key
[17]    52  *
2021/03/21 22:22:45.238 {wncd_x_R0-0}{1}: [eap-auth] [25253]: (info): SUCCESS for EAP method
name: PEAP on handle 0x0C000008

2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
:            username   0 "jonathga-102" ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
:               class   0 43 41 43 53 3a 33 33 30 32 30 41 30 41 30 30 30 30 30 30 33 35 35 36
45 32 32 31 36 42 3a 49 53 45 2d 32 2f 33 39 33 33 36 36 38 37 32 2f 31 31 32 36 34 30  ]
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
:             timeout   0 1800 (0x708) ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [25253]: (info):
[0000.0000.0000:unknown] AAA override is enabled under policy profile
```

Troubleshoot

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

Related Information

- End User Guide