Configuración de la Asignación de VLAN Dinámica con ISE y Catalyst 9800 Wireless LAN Controller

Contenido

Introducción

Este documento describe el concepto de asignación de VLAN dinámica y cómo configurar el controlador de LAN inalámbrica (WLC) Catalyst 9800 y Cisco Identity Service Engine (ISE) para asignar LAN inalámbrica (WLAN) a fin de lograr esto para los clientes inalámbricos.

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Tener conocimiento básico del WLC y los Lightweight Access Points (LAP).
- Tener conocimiento funcional del servidor AAA como ISE.
- Conozca a fondo las redes inalámbricas y los problemas de seguridad inalámbrica.

- Tener conocimientos funcionales sobre asignación de VLAN dinámica.
- Contar con conocimientos básicos sobre control y aprovisionamiento para puntos de acceso inalámbricos (CAPWAP).

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- WLC de Cisco Catalyst 9800 (Catalyst 9800-CL) que ejecuta la versión de firmware 16.12.4a.
- Cisco 2800 Series LAP en modo local.
- Suplicante nativo de Windows 10.
- Cisco Identity Service Engine (ISE) que ejecuta la versión 2.7.
- Cisco 3850 Series Switch que ejecuta la versión de firmware 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Asignación de VLAN Dinámica con Servidor RADIUS

En la mayoría de los sistemas de red de área local inalámbrica (WLAN), cada WLAN tiene una política estática que se aplica a todos los clientes asociados a un identificador de conjunto de servicios (SSID). Aunque poderoso, este método tiene limitaciones porque requiere que los clientes se asocien con diferentes SSID para heredar diferentes QoS y políticas de seguridad.

Sin embargo, la solución de WLAN de Cisco admite redes de identidad. Esto permite a la red anunciar un único SSID y permite a usuarios específicos heredar diferentes QoS o políticas de seguridad basadas en las credenciales de usuario.

La asignación de VLAN dinámica es una de estas funciones que colocan a un usuario inalámbrico en una VLAN específica en función de las credenciales suministradas por el usuario. La tarea de asignar usuarios a una VLAN específica es manejada por un servidor de autenticación RADIUS, como Cisco ISE. Esto se puede utilizar, por ejemplo, para permitir que el host inalámbrico permanezca en la misma VLAN a medida que se desplaza dentro de una red de campus.

Por lo tanto, cuando un cliente intenta asociarse a un LAP registrado con un controlador, el WLC pasa las credenciales del usuario al servidor RADIUS para la validación. Cuando la autenticación es correcta, el servidor RADIUS transmite una serie de atributos del Grupo de trabajo en ingeniería de Internet (IETF) al usuario. Estos atributos RADIUS deciden el ID de VLAN que se debe asignar al cliente inalámbrico. El SSID del cliente no importa porque el usuario siempre está asignado a este ID de VLAN predeterminado.

Los atributos del usuario de RADIUS que se utilizan para la asignación del ID de VLAN son:

- IETF 64 (Tipo de túnel): Defina esto en VLAN.
- IETF 65 (Tipo de túnel medio): Defina este valor en 802.
- IETF 81 (ID de grupo privado de túnel): Defina esta opción en ID de VLAN.

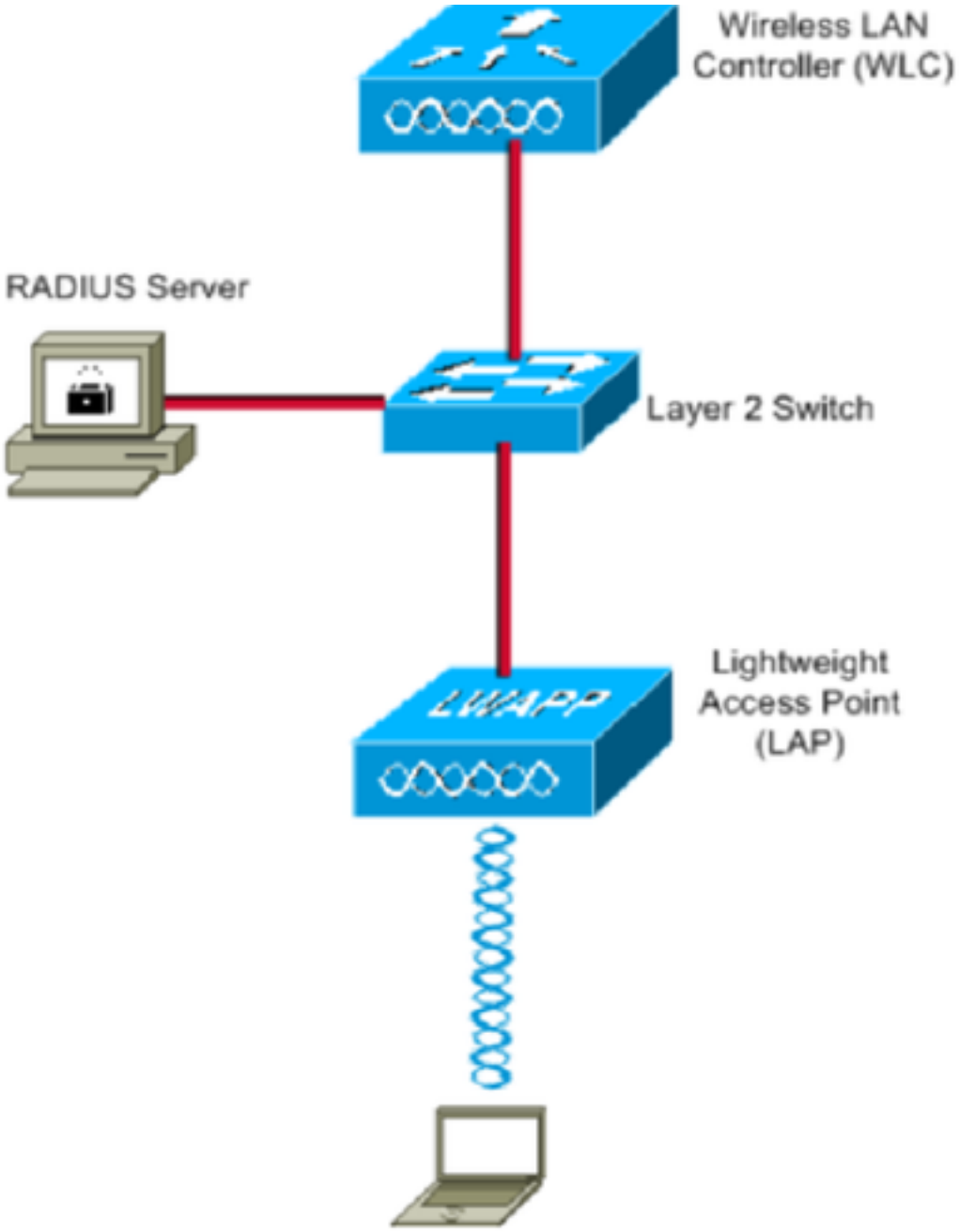
El ID de VLAN es de 12 bits y toma un valor entre 1 y 4094, ambos inclusive. Debido a que el ID de grupo privado de túnel es de tipo string, como se define en RFC2868 para su uso con IEEE 802.1X, el valor entero de ID de VLAN se codifica como una cadena. Cuando se envían estos atributos de túnel, es necesario introducirlos en el campo Etiqueta.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Estos son los detalles de configuración de los componentes utilizados en este diagrama:

- La dirección IP del servidor Cisco ISE (RADIUS) es 10.10.1.24.
- La dirección de la interfaz de administración del WLC es 10.10.1.17.
- El servidor DHCP interno del controlador se utiliza para asignar la dirección IP a los clientes inalámbricos.
- Este documento utiliza 802.1x con PEAP como mecanismo de seguridad.
- VLAN102 se utiliza a lo largo de esta configuración. El nombre de usuario jonathga-102 está configurado para que el servidor RADIUS lo coloque en la VLAN102.

Configuration Steps

Esta configuración se divide en tres categorías:

- Configuración de Cisco ISE.
- Configure el switch para varias VLAN.
- Configuración del WLC del Catalyst 9800.

Configuración de Cisco ISE

La configuración requiere estos pasos:

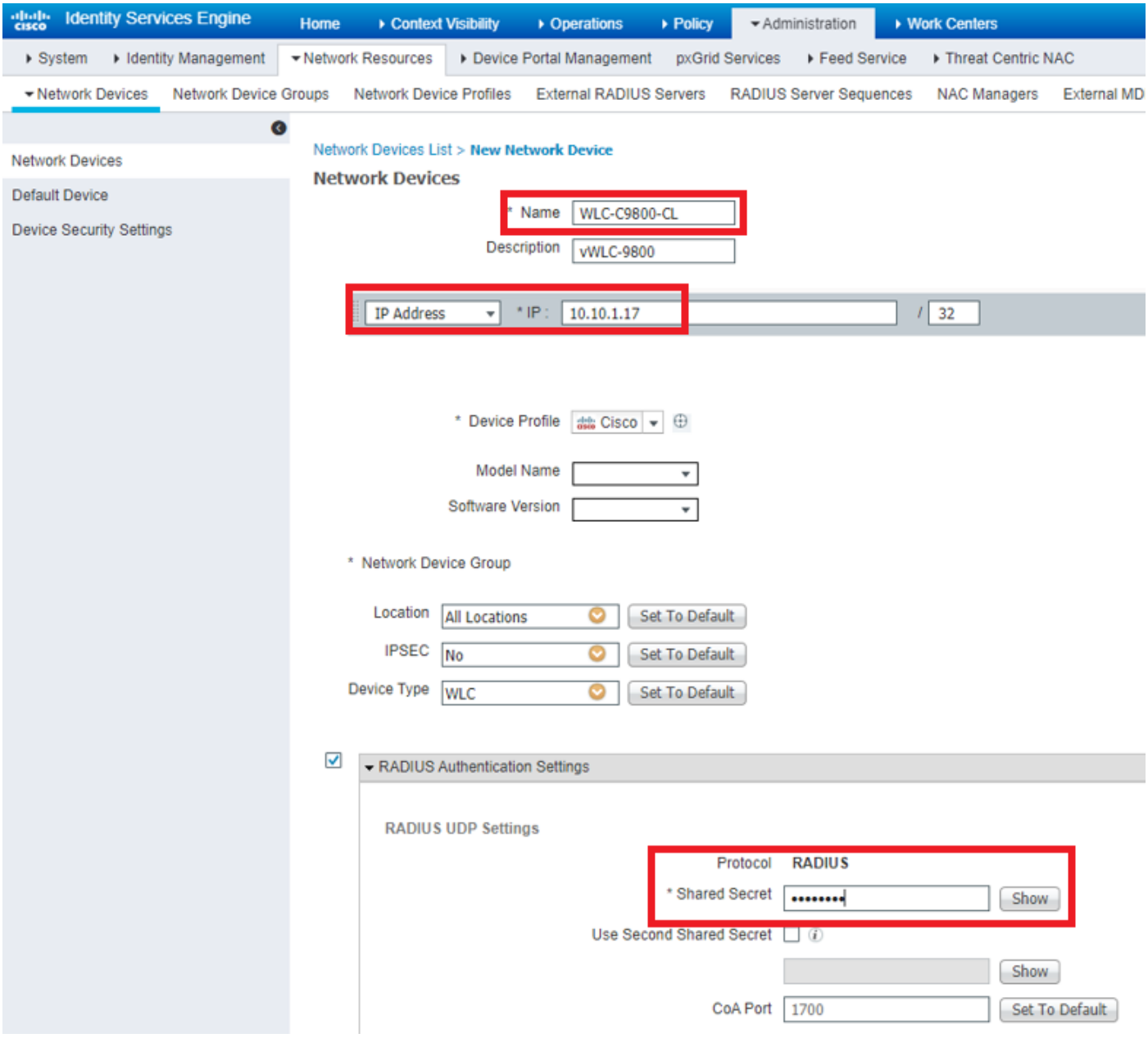
- Configure el WLC Catalyst como un Cliente AAA en el Servidor Cisco ISE.
- Configure los usuarios internos en Cisco ISE.
- Configure los atributos RADIUS (IETF) utilizados para la asignación de VLAN dinámica en Cisco ISE.

Paso 1. Configure el WLC Catalyst como un Cliente AAA en el servidor Cisco ISE

Este procedimiento explica cómo agregar el WLC como un cliente AAA en el servidor ISE para que el WLC pueda pasar las credenciales del usuario a ISE.

Complete estos pasos:

1. Desde la GUI de ISE, vaya a **Administration > Network Resources > Network Devices**y seleccione **Add**.
2. Complete la configuración con la dirección IP de administración del WLC y el secreto compartido RADIUS entre el WLC y el ISE como se muestra en la imagen:

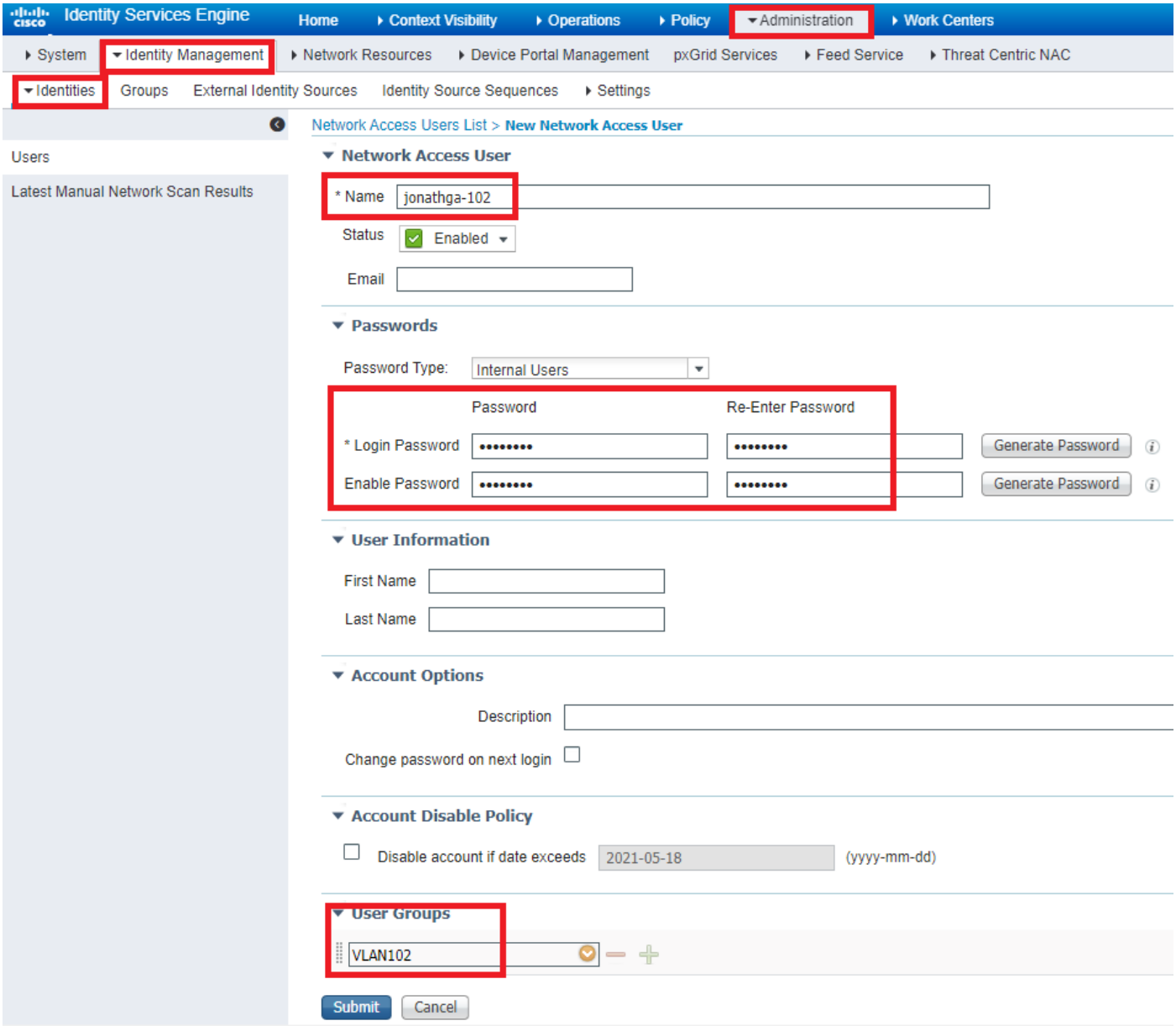


Paso 2. Configuración de usuarios internos en Cisco ISE

Este procedimiento explica cómo agregar los usuarios en la base de datos interna de usuarios de Cisco ISE.

Complete estos pasos:

1. Desde la GUI de ISE, vaya a **Administration > Identity Management > Identities** y seleccione **Add**.
2. Complete la configuración con el nombre de usuario, la contraseña y el grupo de usuarios como se muestra en la imagen:

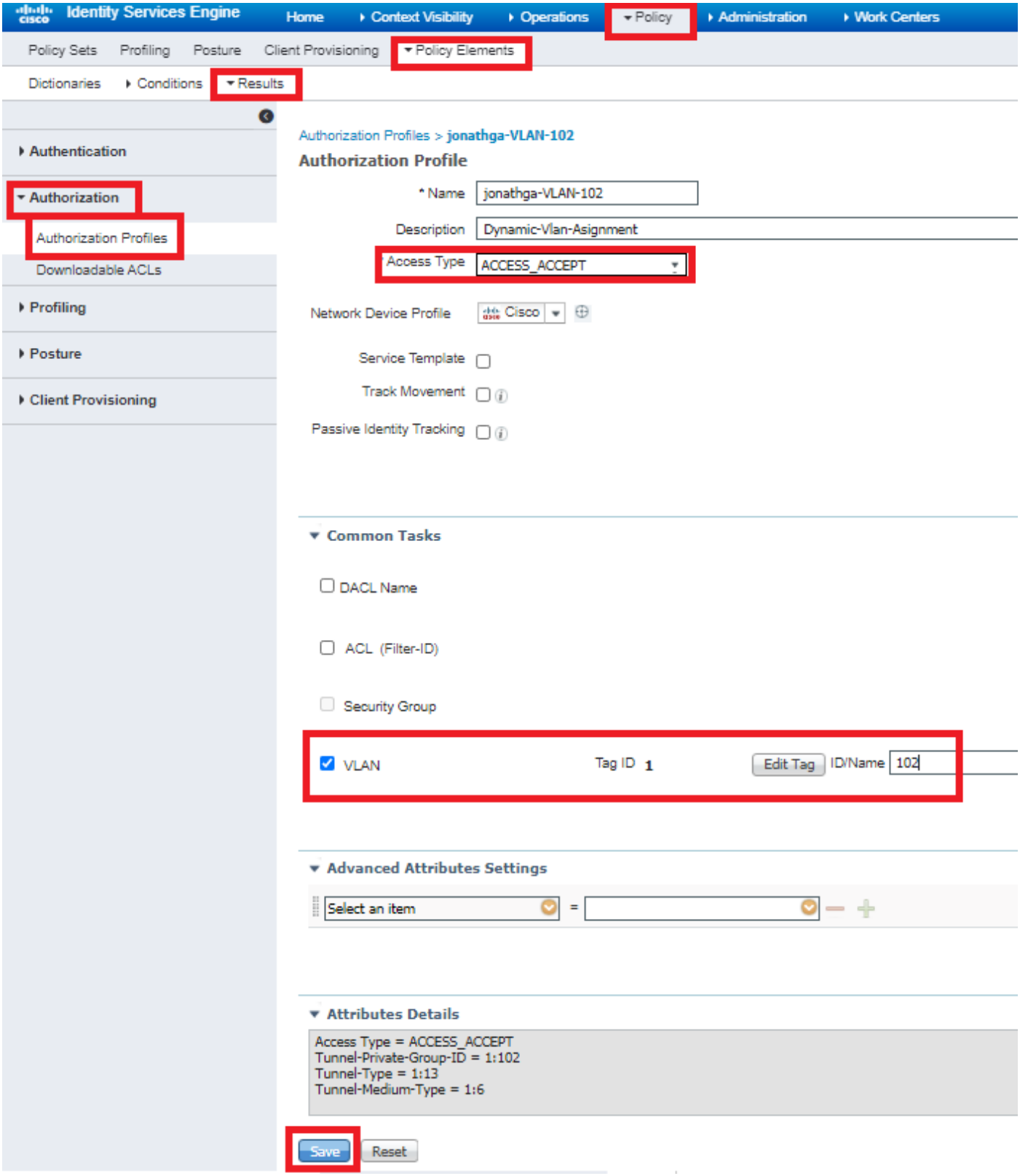


Paso 3. Configure los atributos RADIUS (IETF) utilizados para la asignación de VLAN dinámica

Este procedimiento explica cómo crear un perfil de autorización y una política de autenticación para usuarios inalámbricos.

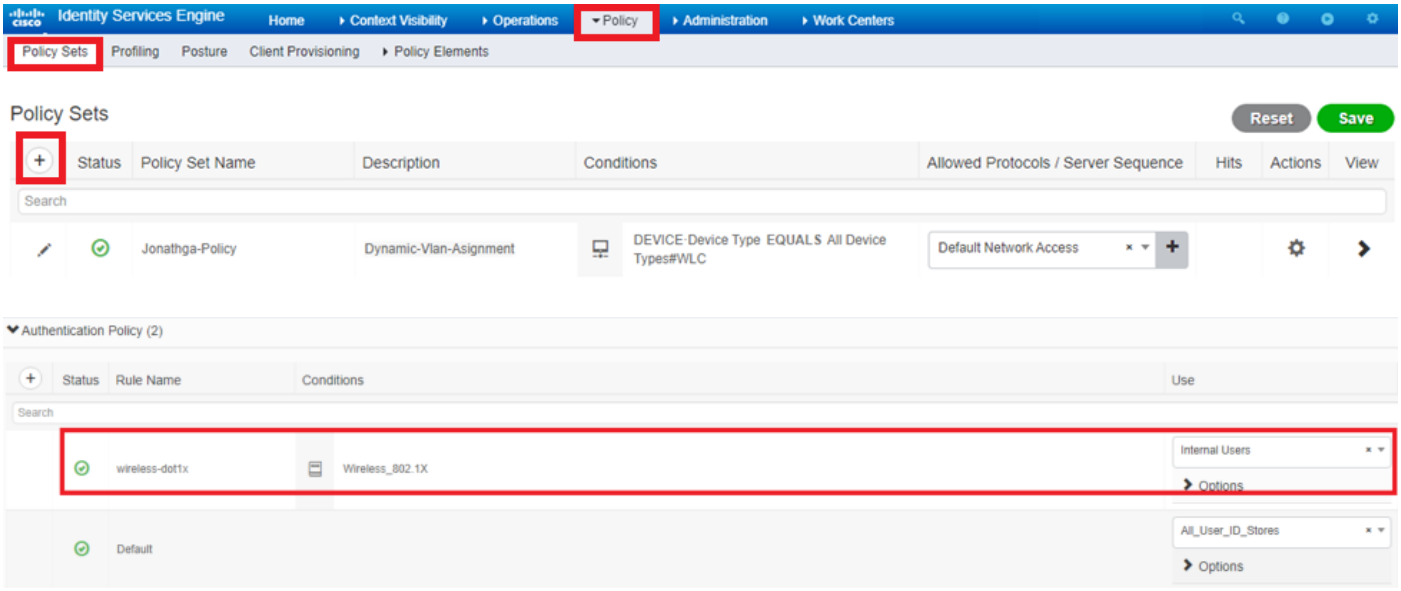
Complete estos pasos:

1. Desde la GUI de ISE, vaya a **Policy > Policy Elements > Results > Authorization > Authorization profiles** y seleccione **Add** para crear un nuevo perfil.
2. Complete la configuración del perfil de autorización con información de VLAN para el grupo respectivo. Esta imagen muestra **jonathga-VLAN-102** configuración de grupo.



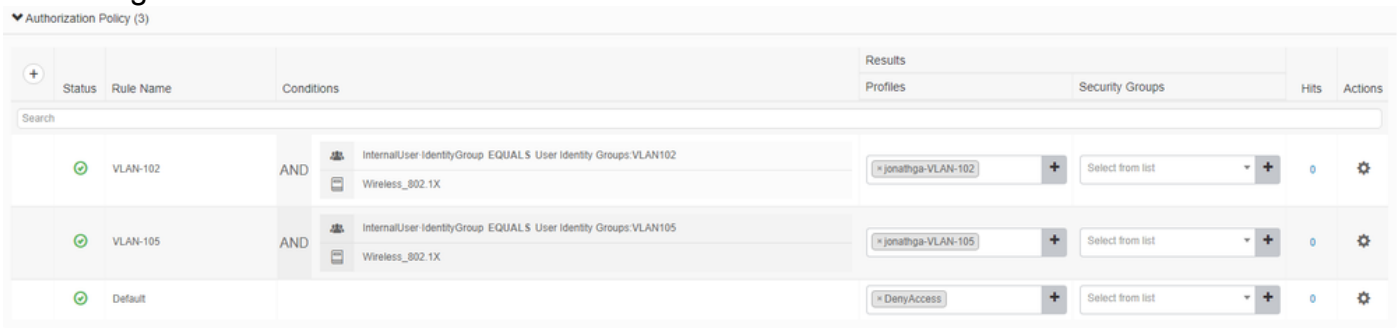
Una vez configurados los perfiles de autorización, se debe crear una política de autenticación para los usuarios inalámbricos. Puede utilizar un **Custom** o modificar el **Default** Conjunto de políticas. En este ejemplo, se crea un perfil personalizado.

3. Vaya a **Policy > Policy Sets** y seleccione **Add** para crear una nueva política como se muestra en la imagen:



Ahora necesita crear políticas de autorización para los usuarios para asignar un perfil de autorización respectivo basado en la pertenencia al grupo.

5. Abra el **Authorization policy** y crear políticas para cumplir ese requisito, como se muestra en la imagen:



Configuración del Switch para Varias VLAN

Para permitir varias VLAN a través del switch, debe ejecutar estos comandos para configurar el puerto del switch conectado al controlador:

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

Switch(config-if)#switchport trunk encapsulation dot1q
```

Nota: De forma predeterminada, la mayoría de los switches permiten todas las VLAN creadas en ese switch a través del puerto troncal. Si hay una red con cables conectada al switch, se puede aplicar la misma configuración al puerto del switch que se conecta a la red con cables. Esto habilita la comunicación entre las mismas VLAN en la red por cable e inalámbrica.

Configuración del WLC de Catalyst 9800

La configuración requiere estos pasos:

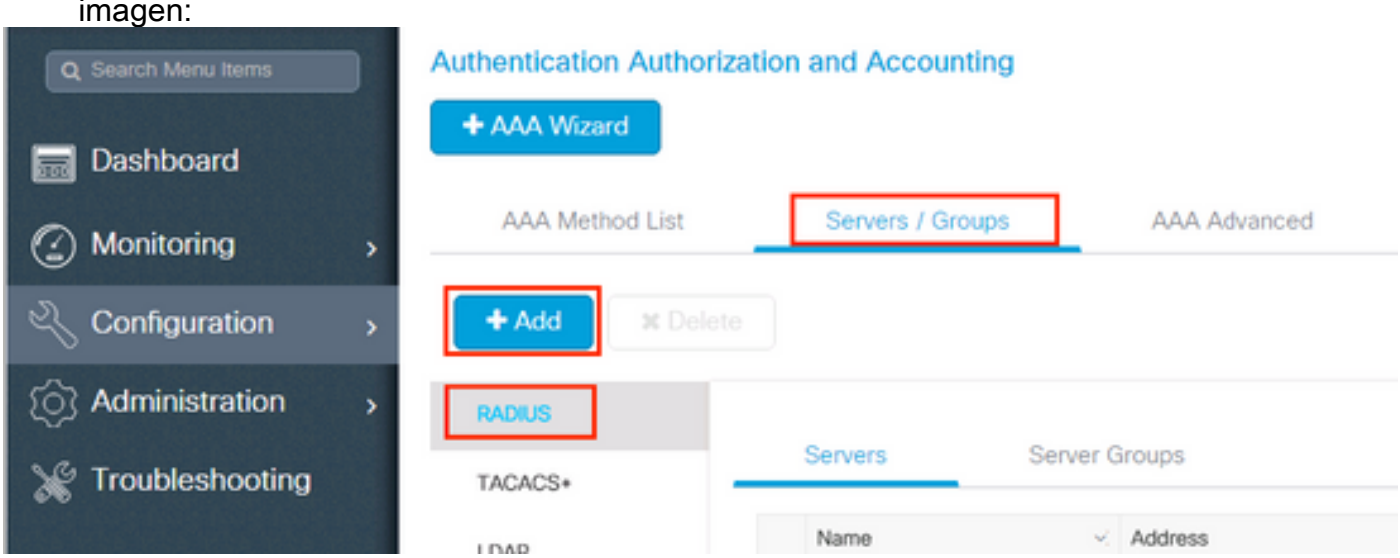
- Configure el WLC con los detalles del servidor de autenticación.
- Configure las VLAN.
- Configure las WLAN (SSID).
- Configure el perfil de política.
- Configure la etiqueta Policy (Política).
- Asigne la etiqueta Policy a un AP.

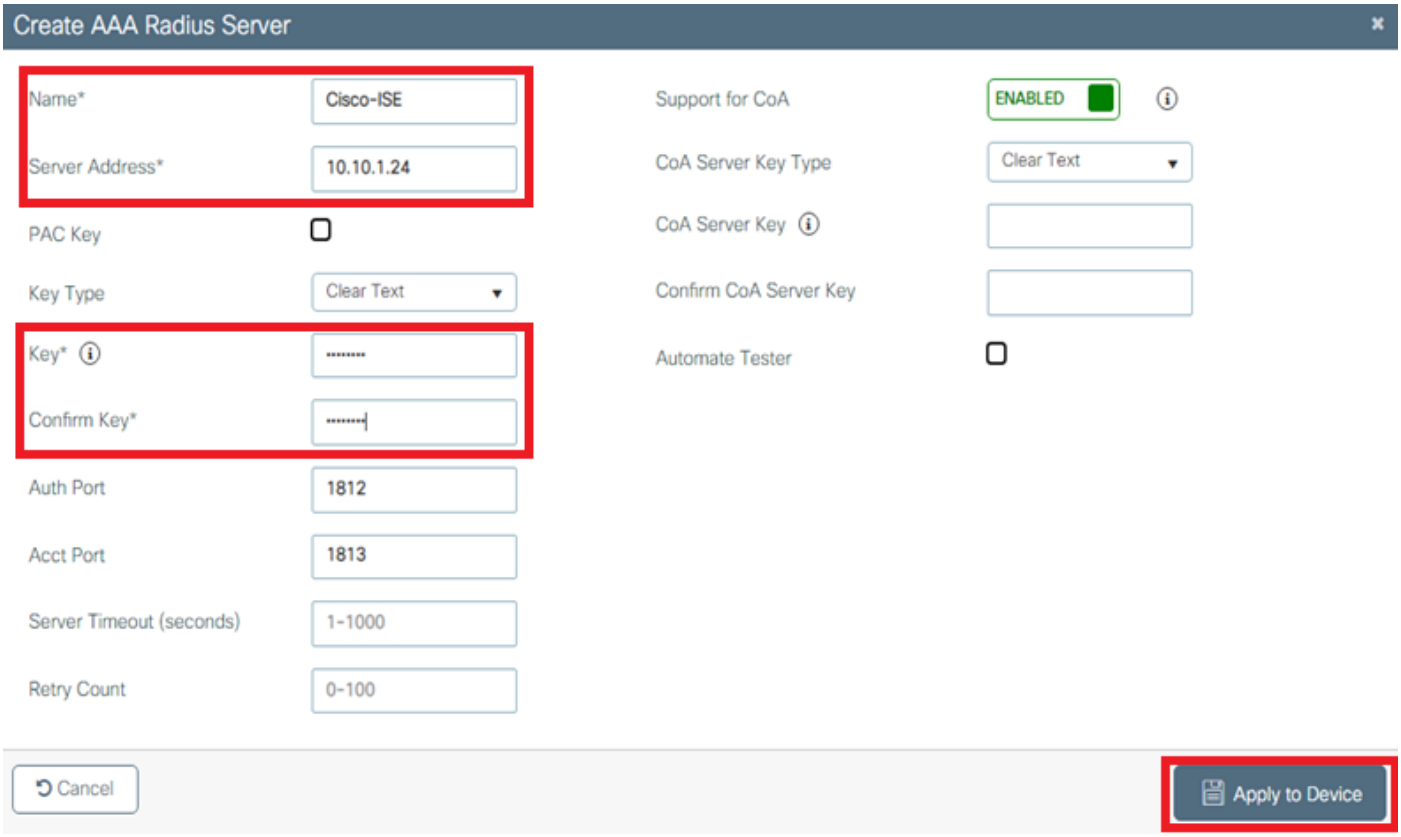
Paso 1. Configure el WLC con los detalles del servidor de autenticación

Es necesario configurar el WLC para que se pueda comunicar con el servidor RADIUS para autenticar los clientes.

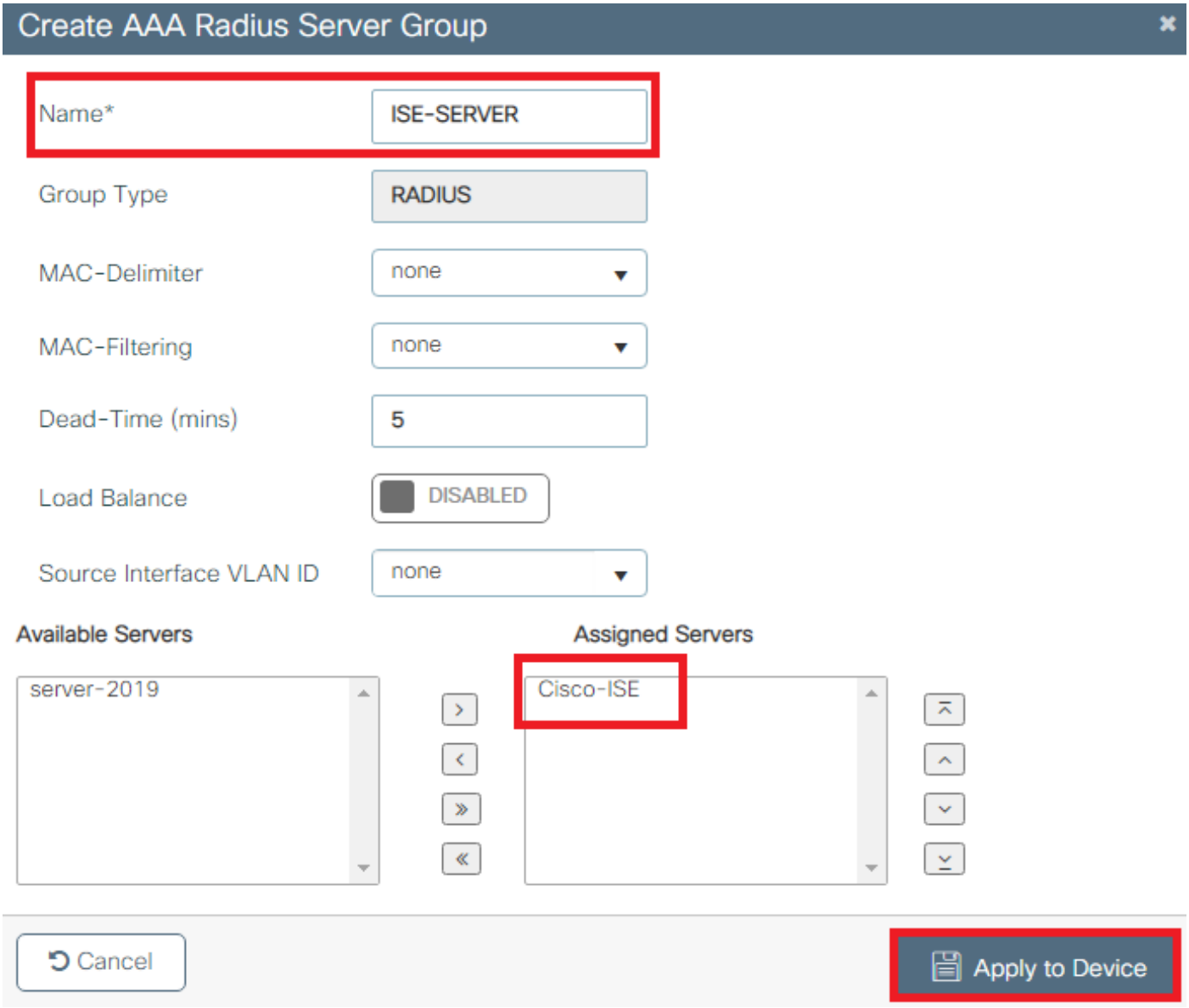
Complete estos pasos:

1. Desde la GUI del controlador, vaya a **Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add** e introduzca la información del servidor RADIUS como se muestra en la imagen:

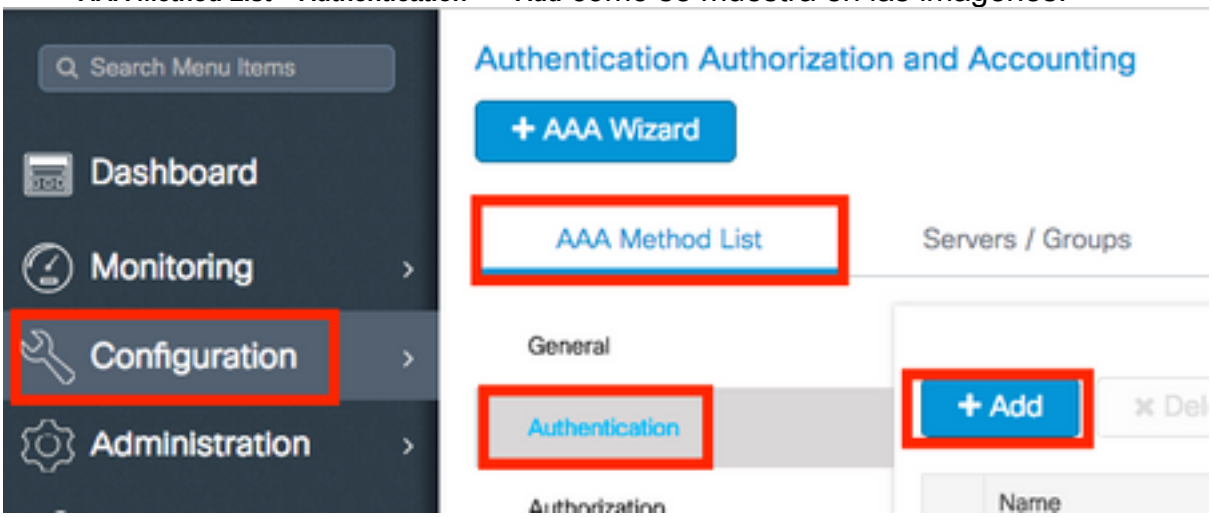


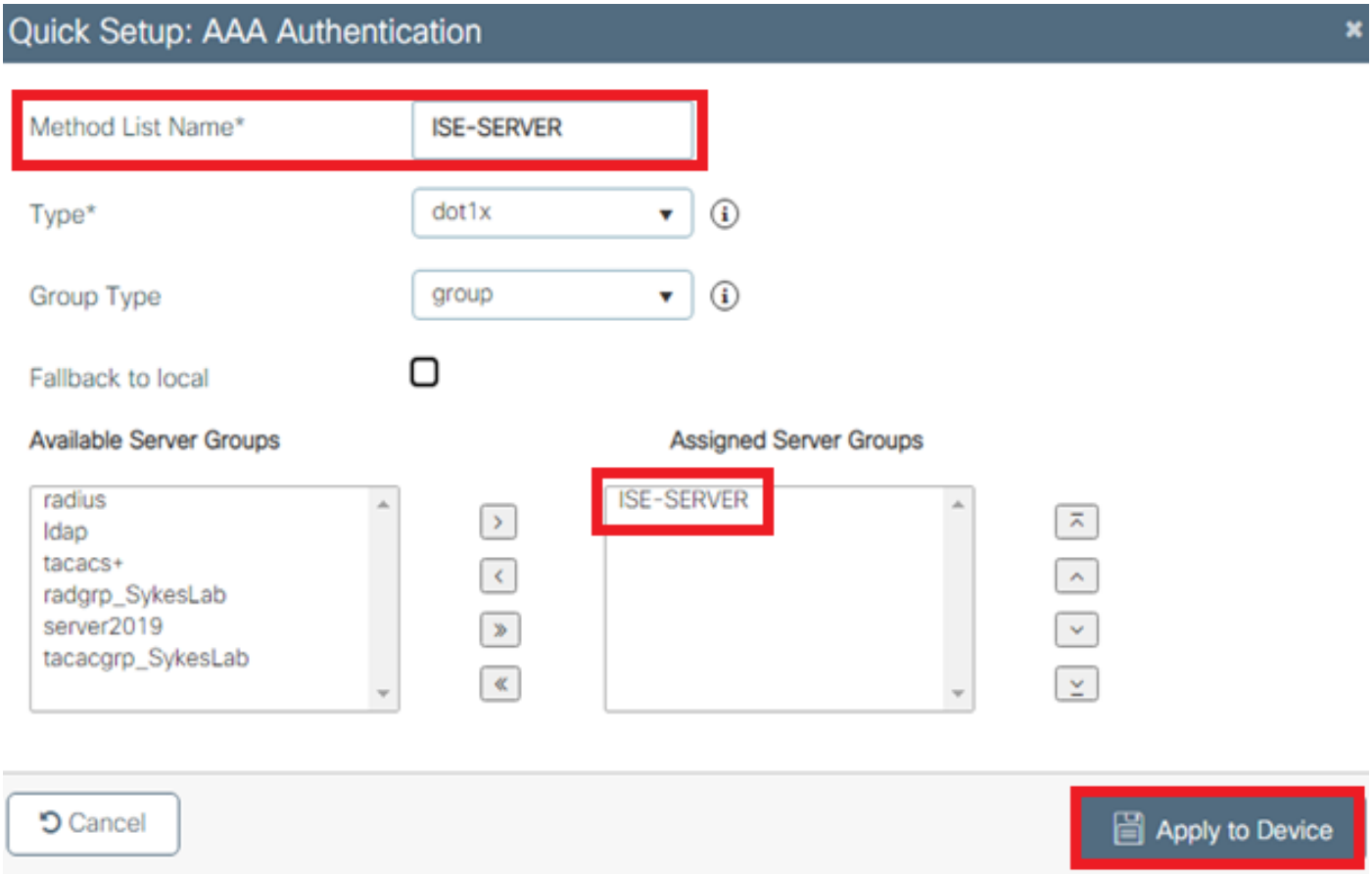


2. Para agregar el servidor RADIUS a un grupo RADIUS, navegue hasta **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add** como se muestra en la imagen:



3. Para crear una lista de métodos de autenticación, navegue hasta **Configuration > Security > AAA > AAA Method List > Authentication > + Add** como se muestra en las imágenes:



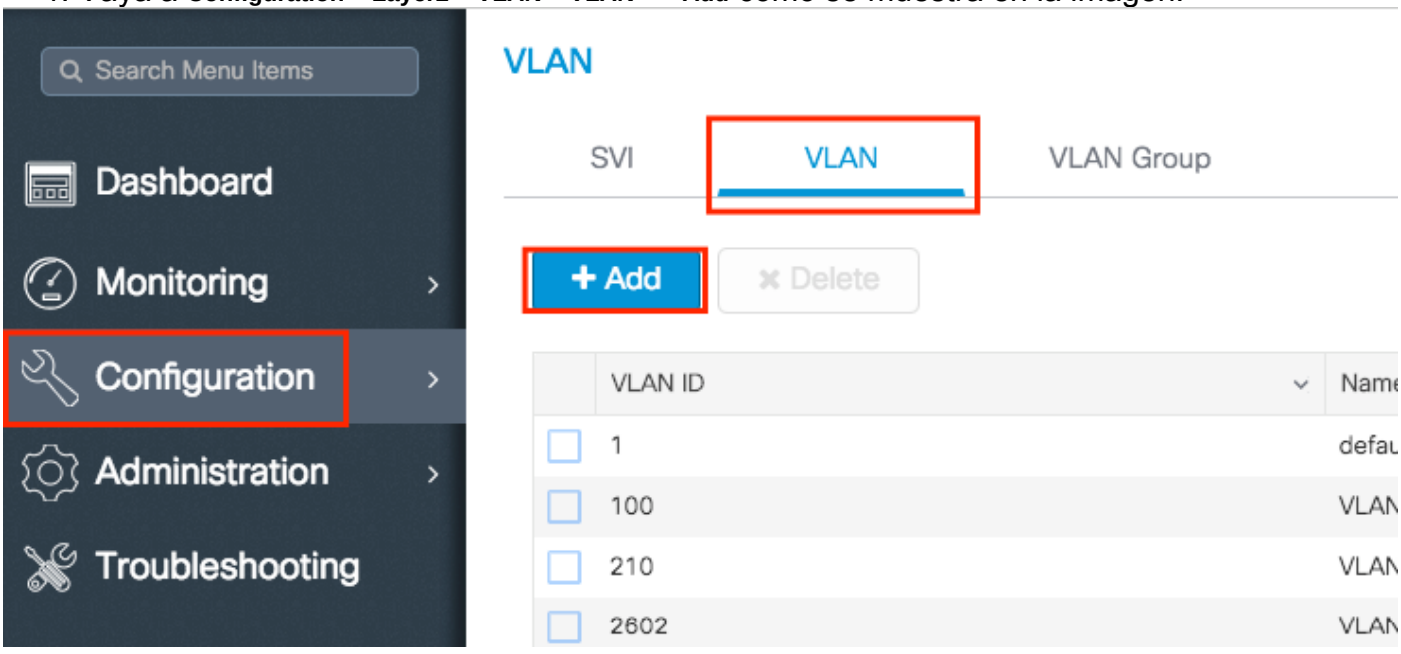


Paso 2. Configuración de las VLAN

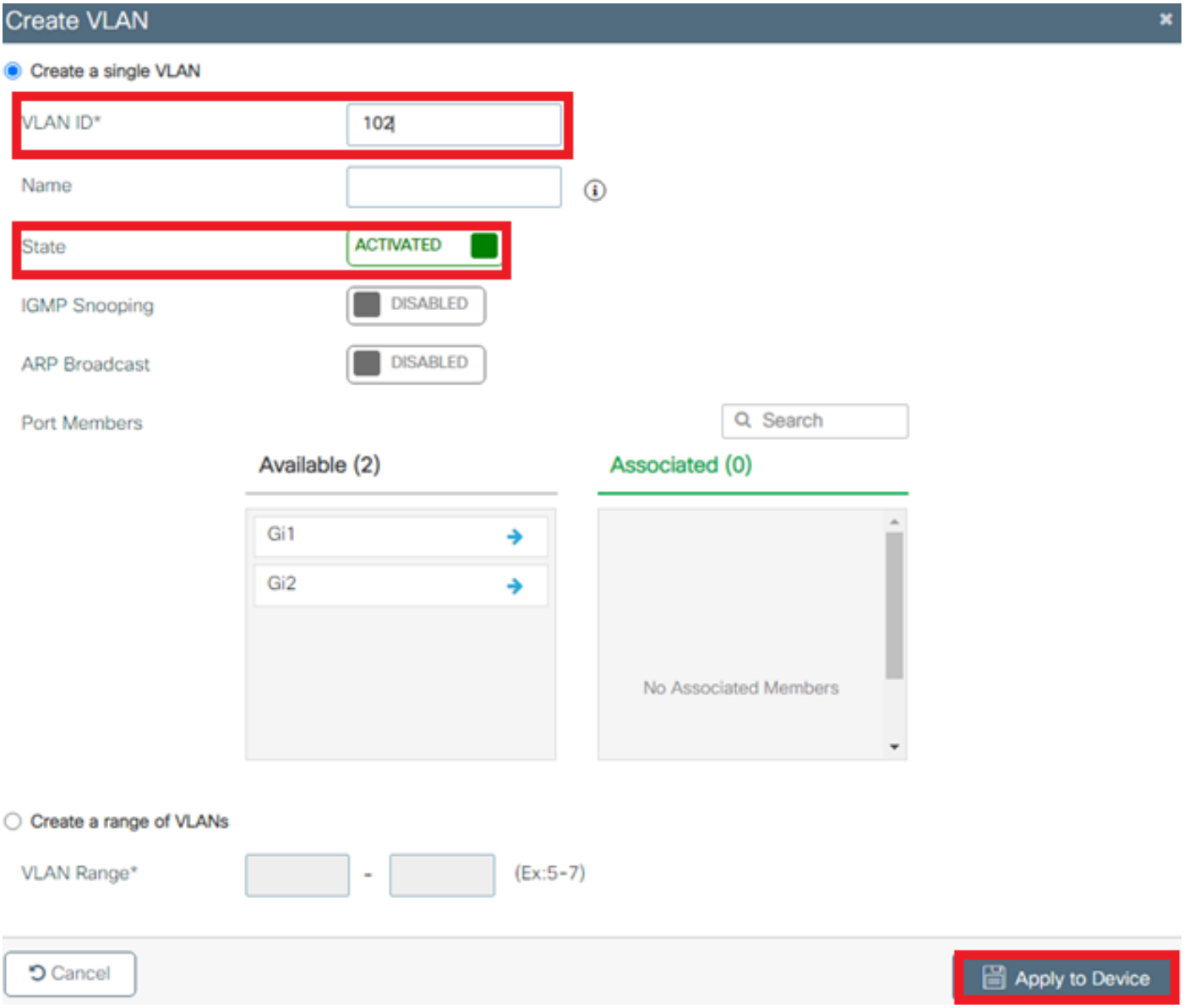
Este procedimiento explica cómo configurar las VLAN en el WLC Catalyst 9800. Como se explicó anteriormente en este documento, el ID de VLAN especificado en el atributo de ID de grupo privado de túnel del servidor RADIUS también debe existir en el WLC.

En el ejemplo, el usuario jonathga-102 se especifica con el **Tunnel-Private-Group ID of 102 (VLAN =102)** en el servidor RADIUS.

1. Vaya a **Configuration > Layer2 > VLAN > VLAN > + Add** como se muestra en la imagen:



2. Introduzca la información necesaria, tal y como se muestra en la imagen:



Nota: Si no especifica un nombre, a la VLAN se le asigna automáticamente el nombre de VLANXXXX, donde XXXX es el ID de VLAN.

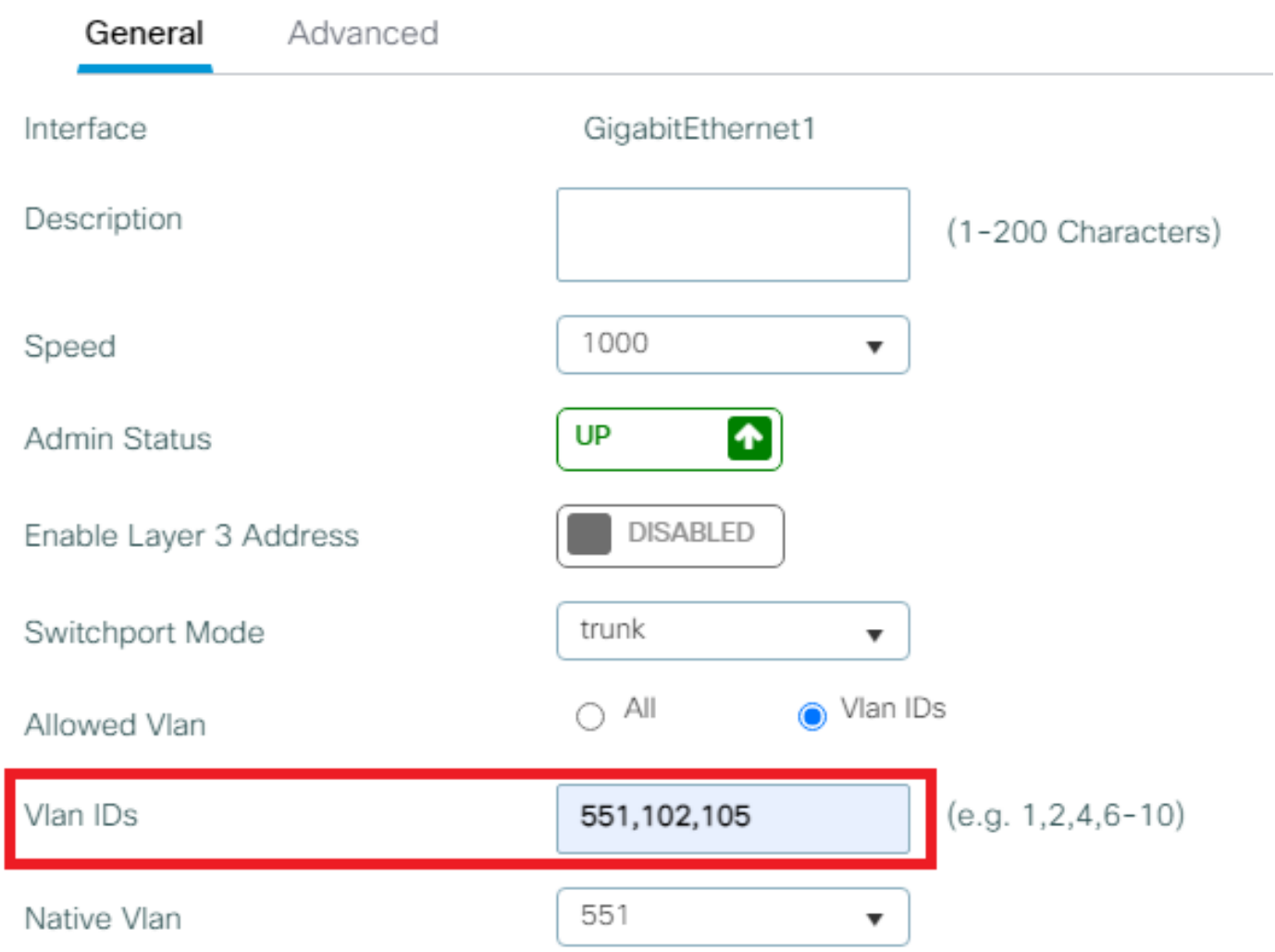
Repita los pasos 1 y 2 para todas las VLAN necesarias, una vez que lo haya hecho, podrá continuar con el paso 3.

3. Verifique que las VLAN estén permitidas en sus interfaces de datos. Si tiene un canal de puerto en uso, navegue hasta **Configuration > Interface > Logical > PortChannel name > General**. Si la ve configurada como **Allowed VLAN = All** ya ha terminado con la configuración. Si ve **Allowed VLAN = VLANs IDs**, agregue las VLAN necesarias y, después, seleccione **Update & Apply to Device**.Si no tiene el canal de puerto en uso, navegue hasta **Configuration > Interface > Ethernet > Interface Name > General**. Si la ve configurada como **Allowed VLAN = All** ya ha terminado con la configuración. Si ve **Allowed VLAN = VLANs IDs**, agregue las VLAN necesarias y, después, seleccione **Update & Apply to Device**.

Estas imágenes muestran la configuración relacionada con la configuración de la interfaz si utiliza Todos o ID de VLAN específicos.

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	

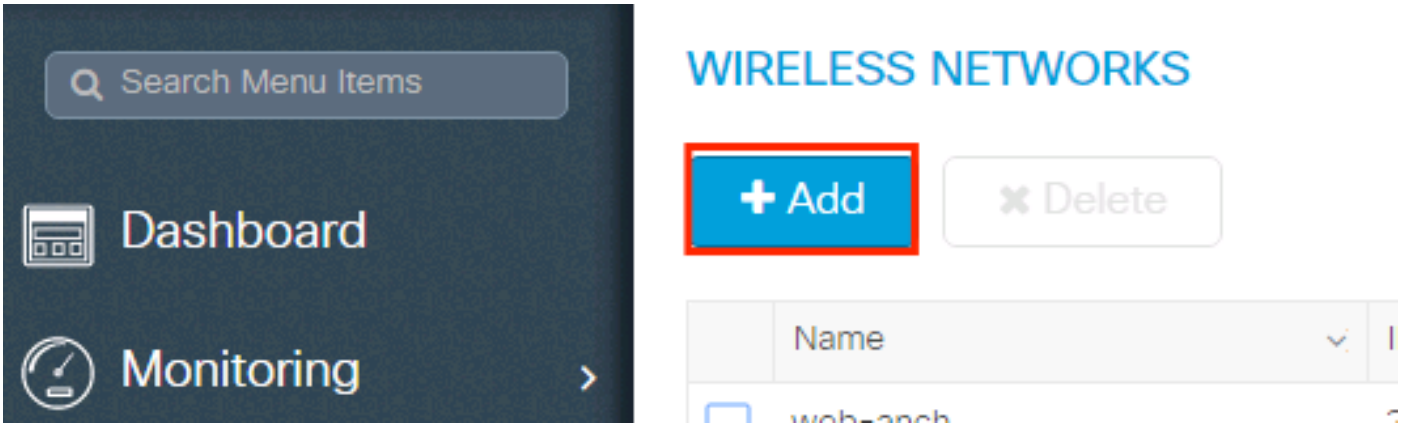


Paso 3. Configuración de WLAN (SSID)

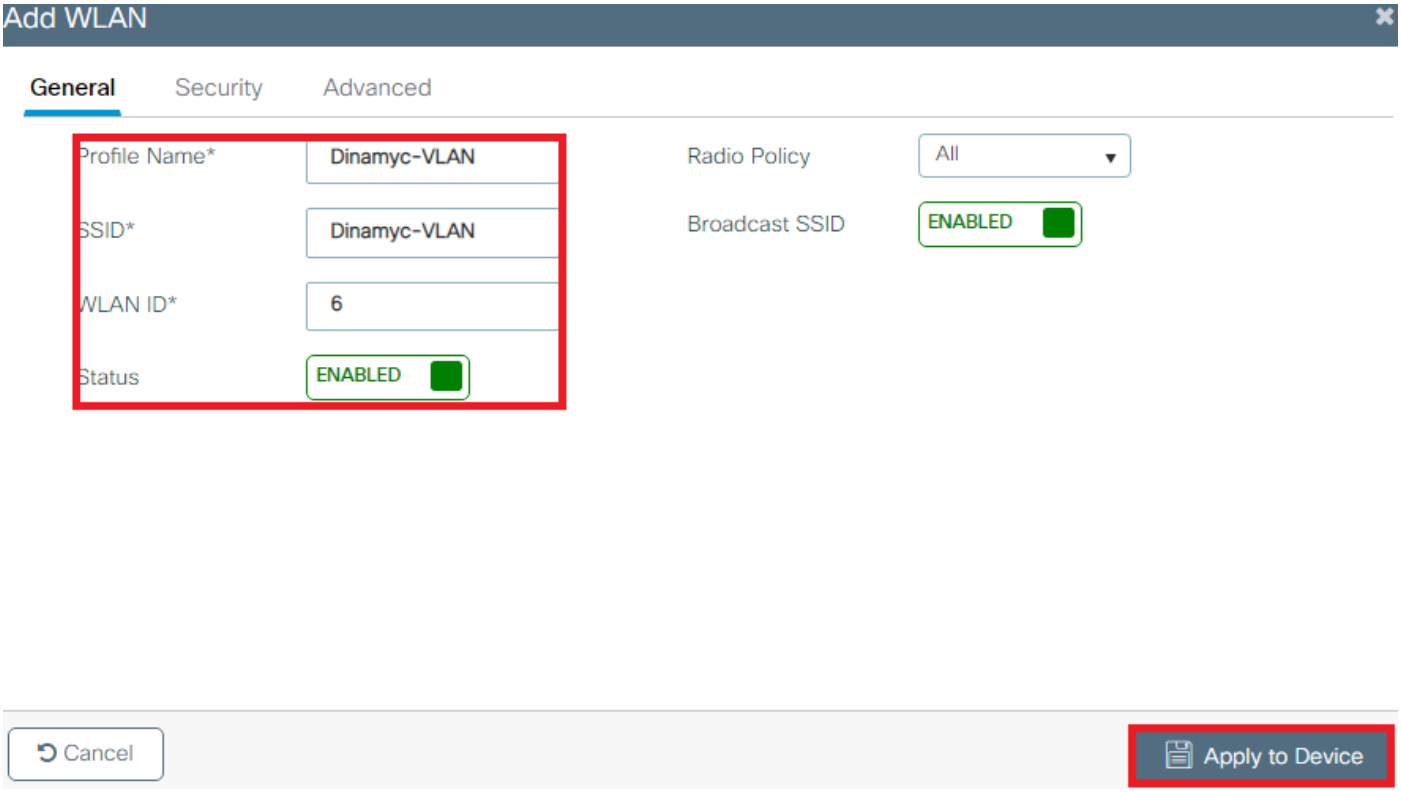
Este procedimiento explica cómo configurar las WLAN en el WLC.

Complete estos pasos:

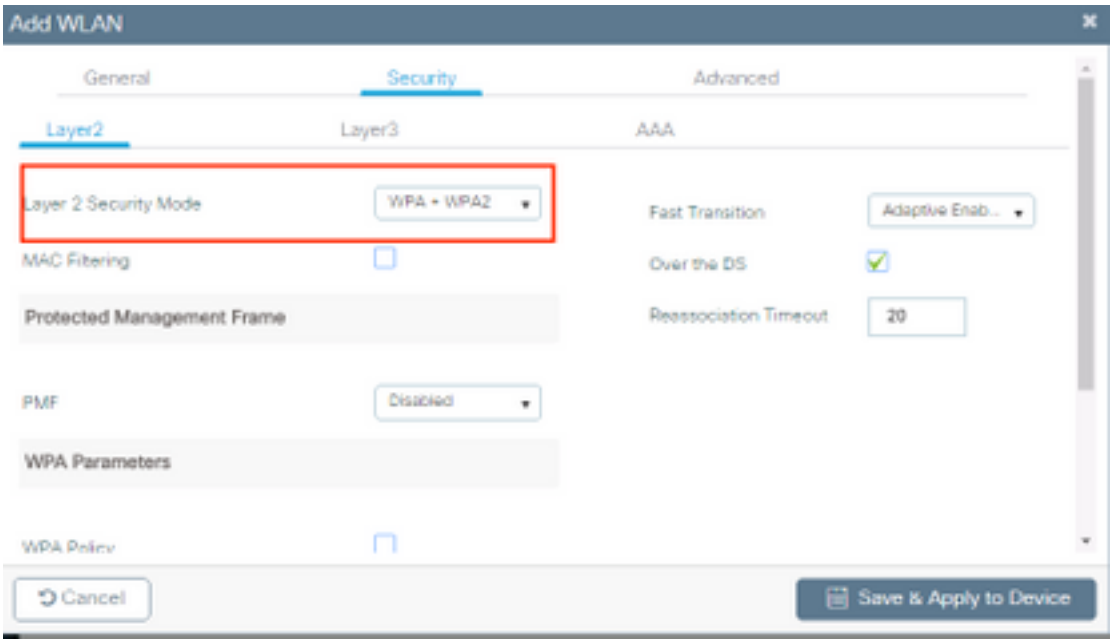
1. Para crear la WLAN. Vaya a **Configuration > Wireless > WLANs > + Add** y configurar la red según sea necesario, como se muestra en la imagen:

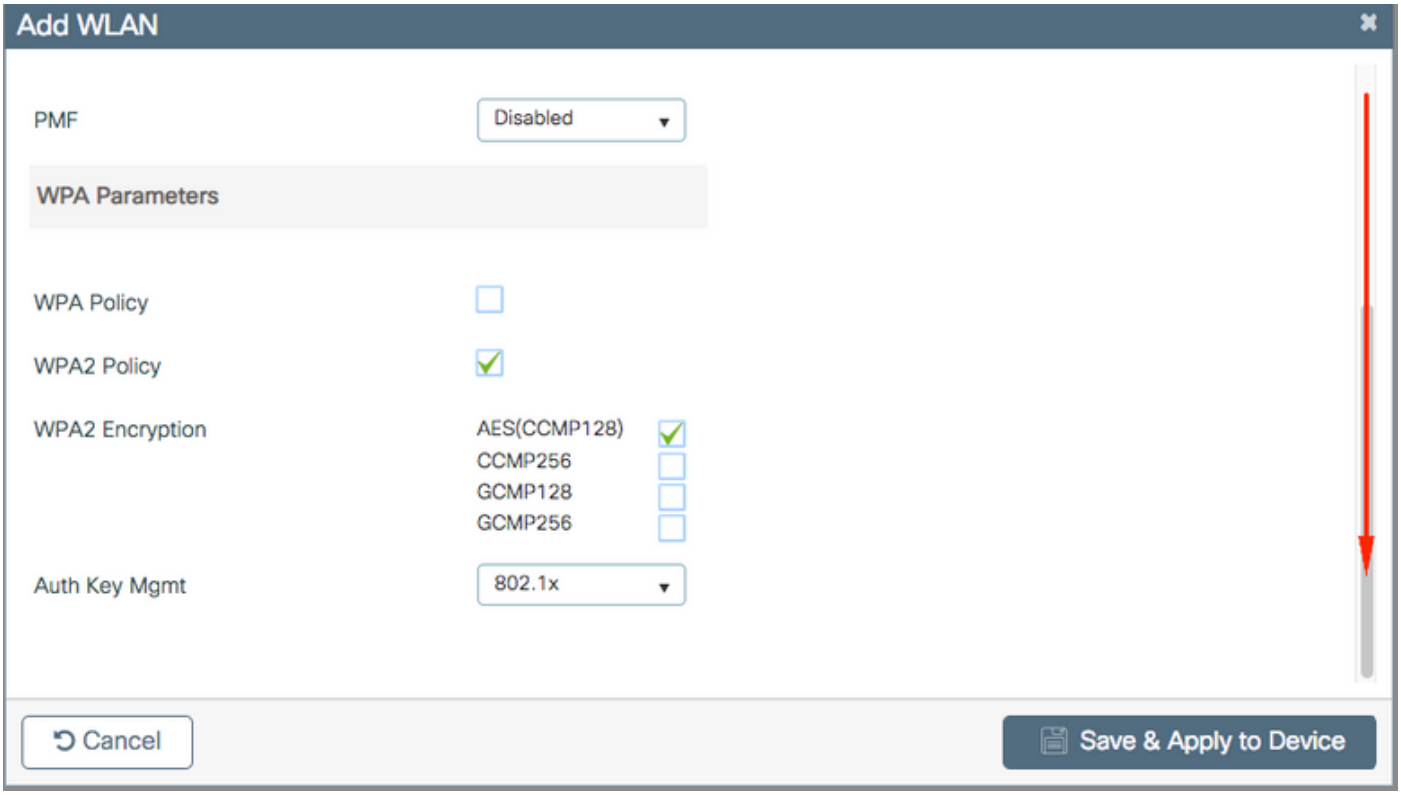


2. Introduzca la información de WLAN como se muestra en la imagen:

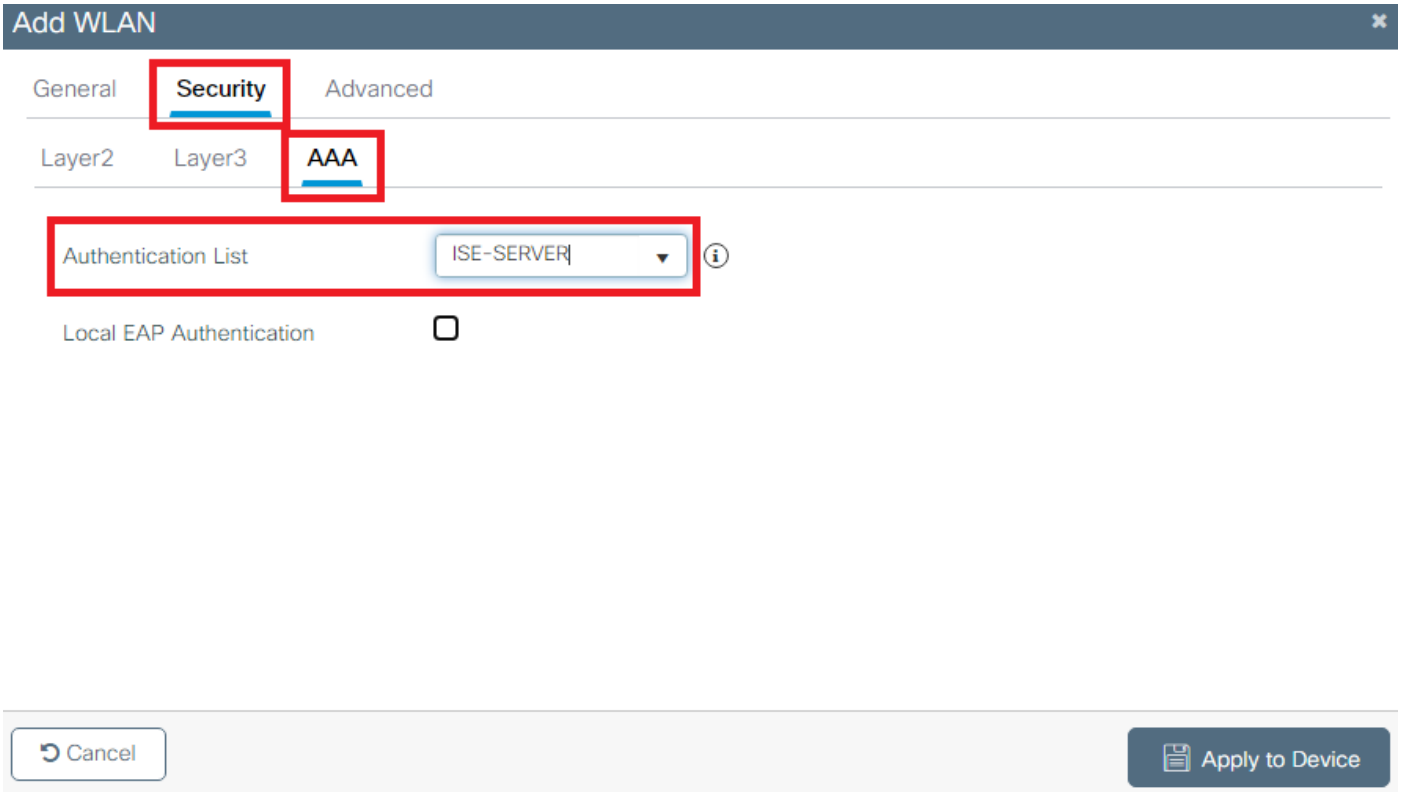


3. Vaya a **Security** y seleccione el método de seguridad necesario. En este caso, WPA2 + 802.1x como se muestra en las imágenes:





Desde**Security > AAA** , seleccione el método de autenticación creado en el paso 3 de **Configure the WLC with the Details of the Authentication Server** como se muestra en la imagen:



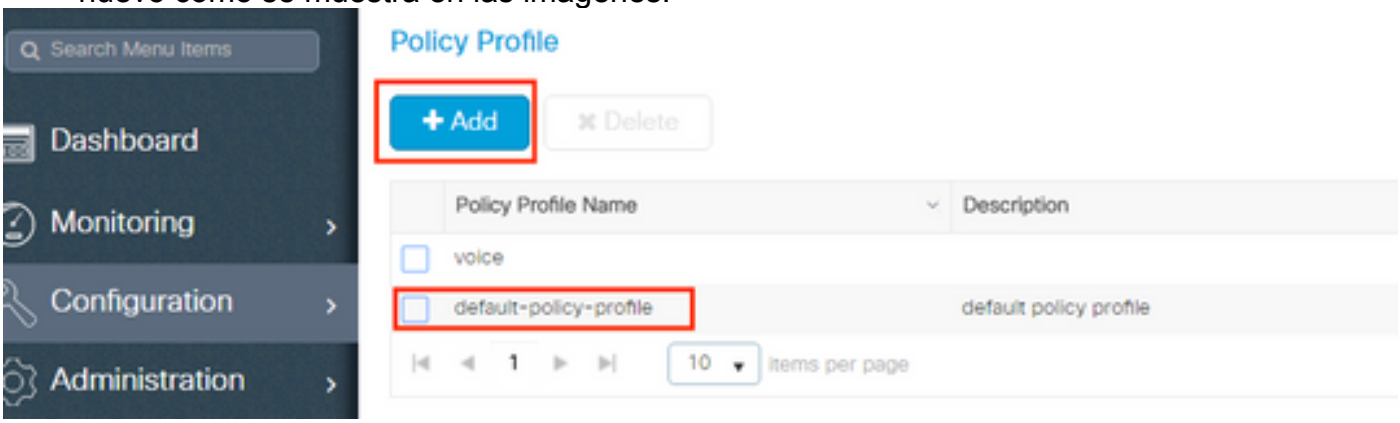
Paso 4. Configuración del perfil de política

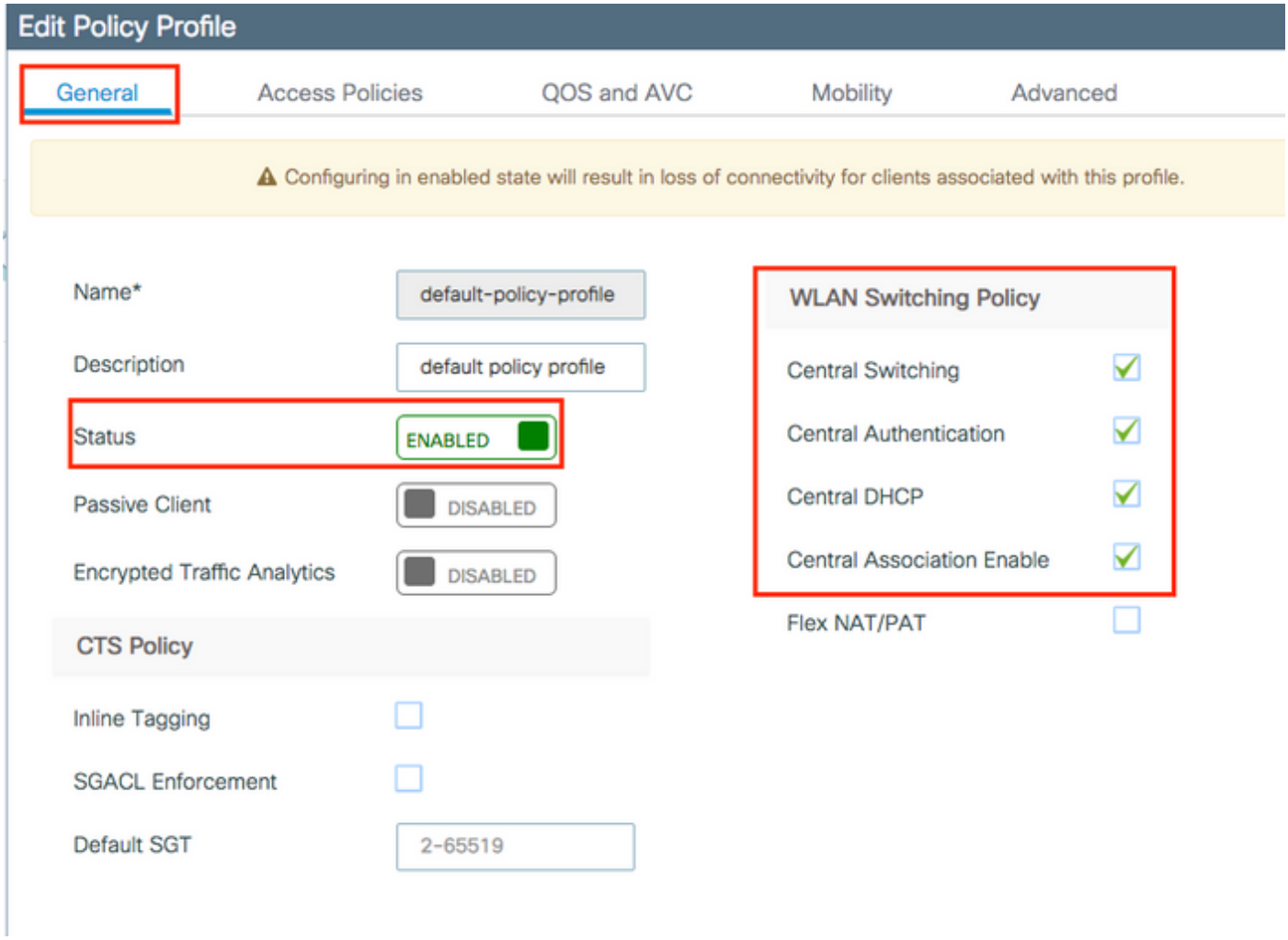
Este procedimiento explica cómo configurar el perfil de política en el WLC.

Complete estos pasos:

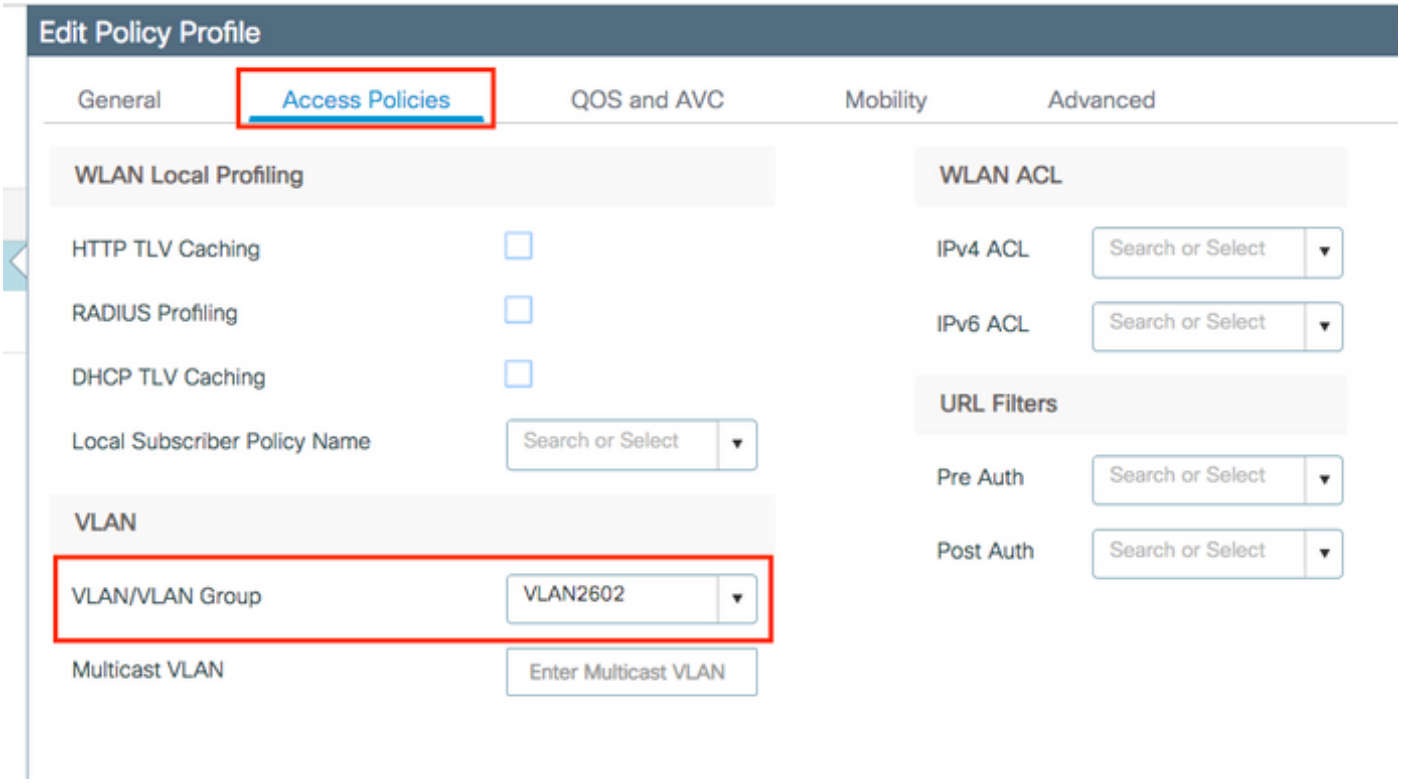
1. Vaya a **Configuration > Tags & Profiles > Policy Profile** y configure el **default-policy-profile** o crear uno

nuevo como se muestra en las imágenes:



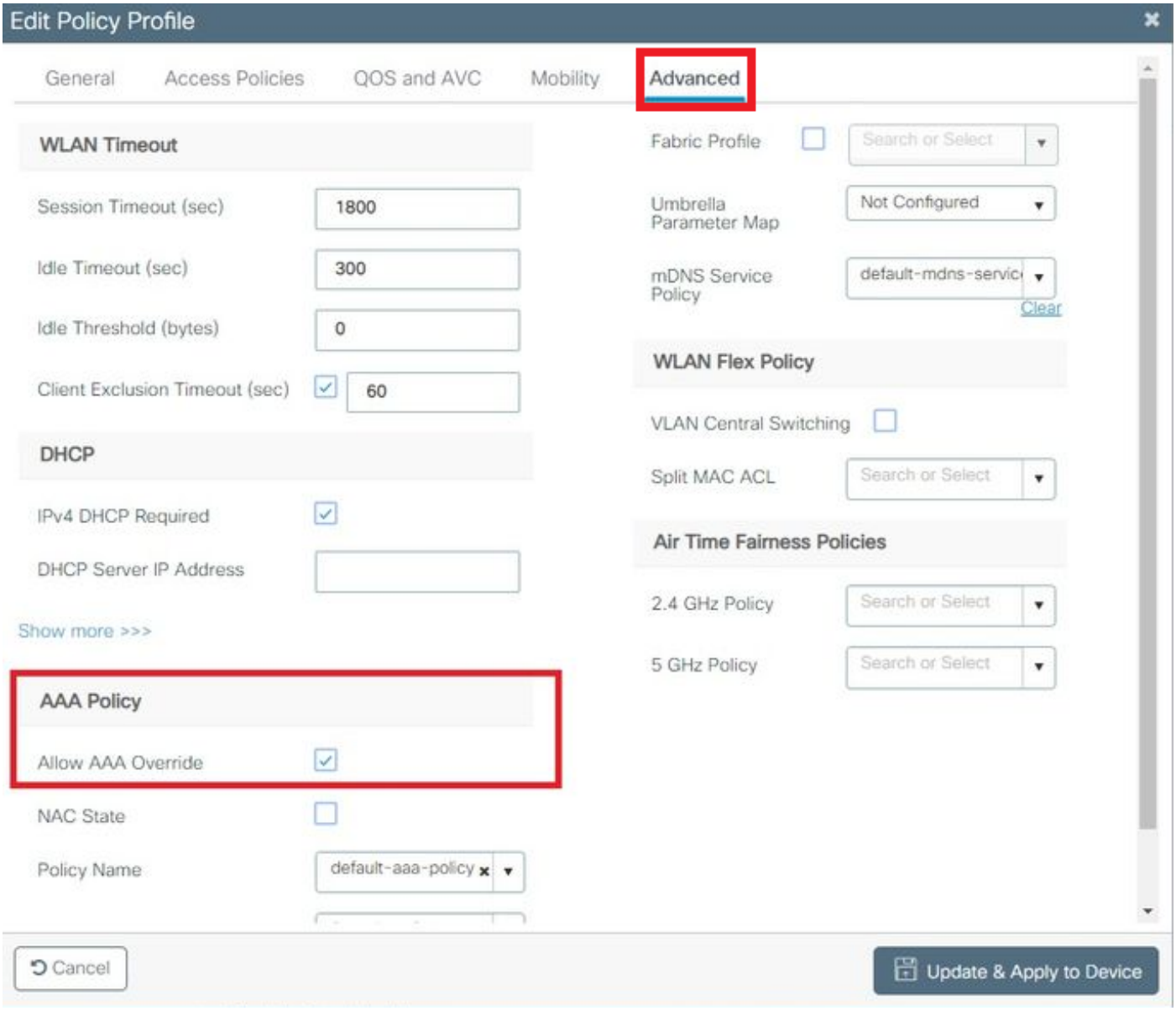


2. Desde **Access Policies** asigne la VLAN a la que se asignan los clientes inalámbricos cuando se conectan a esta WLAN de forma predeterminada, como se muestra en la imagen:



Nota: En el ejemplo proporcionado, es tarea del servidor RADIUS asignar un cliente inalámbrico a una VLAN específica tras una autenticación exitosa, por lo tanto la VLAN configurada en el perfil de política puede ser una VLAN de agujero negro, el servidor RADIUS invalida esta asignación y asigna el usuario que pasa a través de esa WLAN a la VLAN especificada bajo el campo Usuario Tunnel-Group-Private-ID en el servidor RADIUS.

3. Desde **Advance** , active la **Allow AAA Override** para anular la configuración del WLC cuando el servidor RADIUS devuelve los atributos necesarios para colocar el cliente en la VLAN adecuada como se muestra en la imagen:

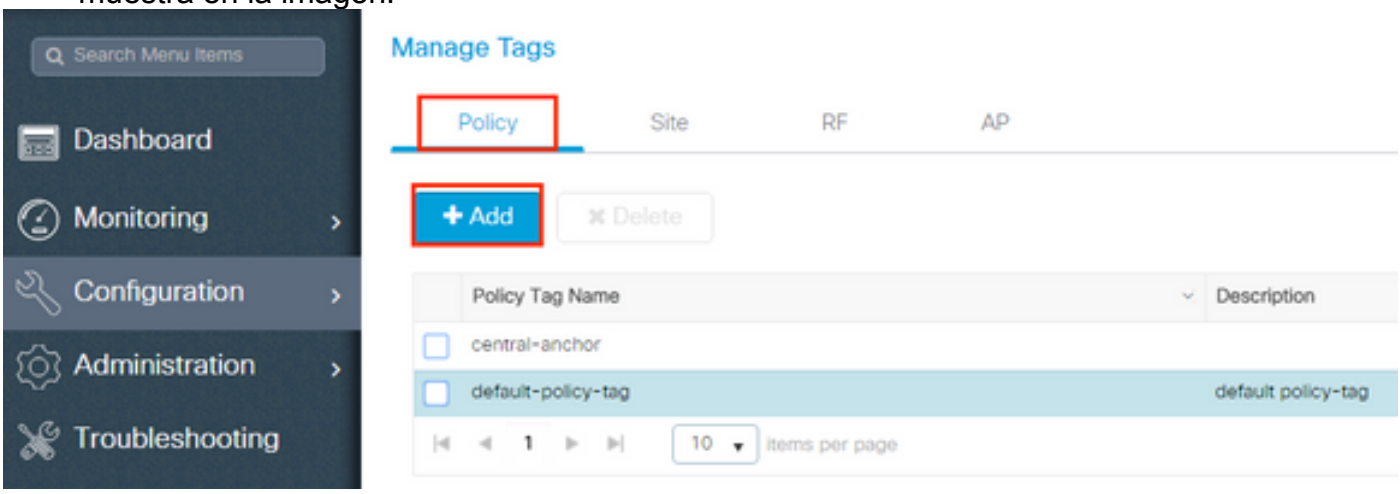


Paso 5. Configuración de la etiqueta de política

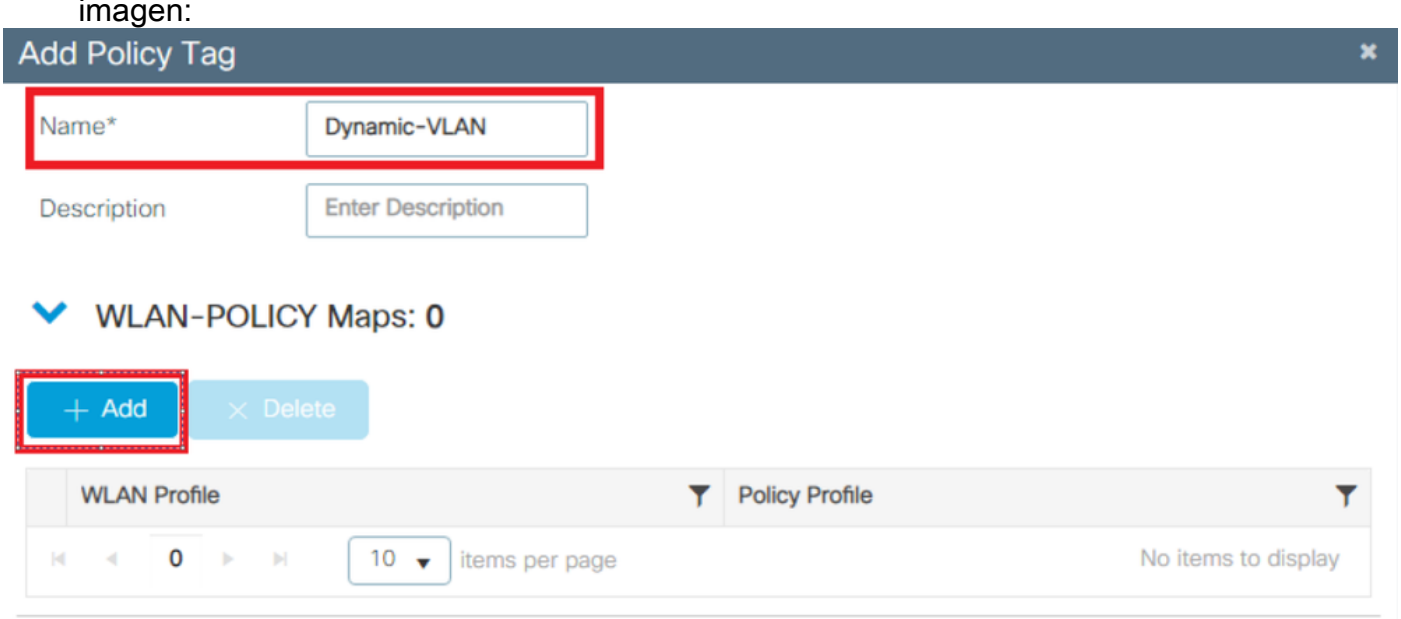
Este procedimiento explica cómo configurar la etiqueta Policy en el WLC.

Complete estos pasos:

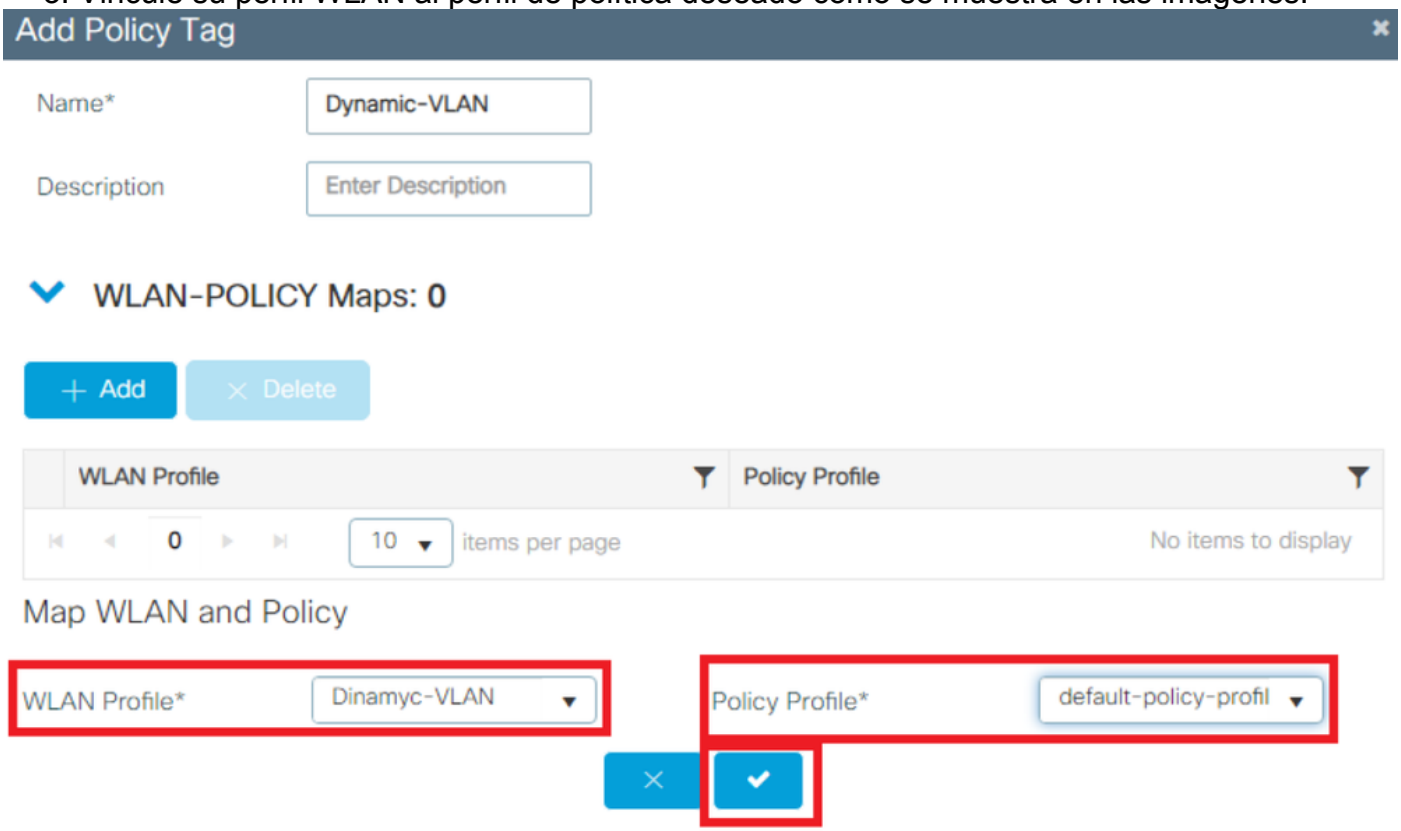
1. Vaya a **Configuration > Tags & Profiles > Tags > Policy** y añada uno nuevo si es necesario, como se muestra en la imagen:

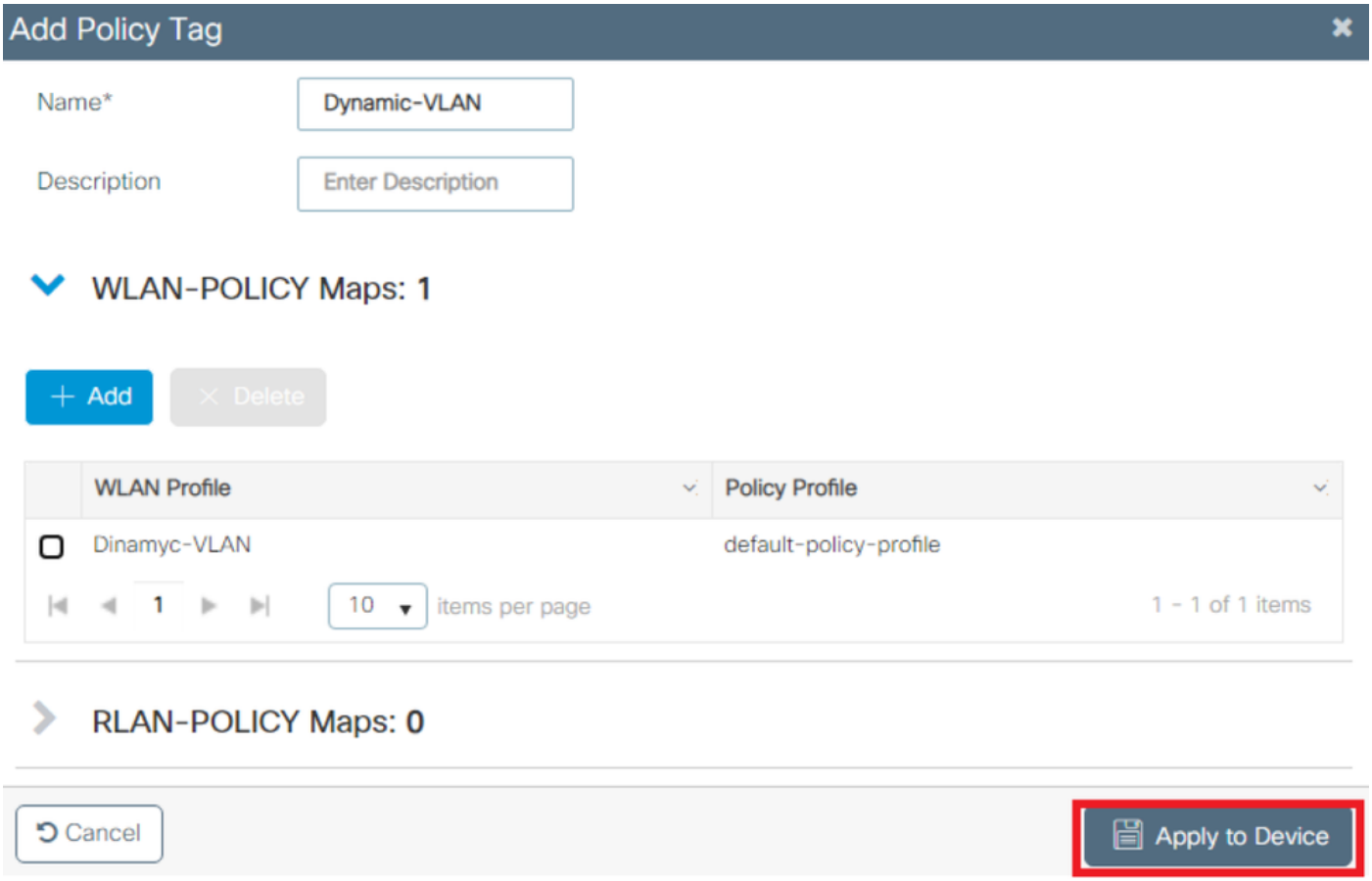


2. Agregue un nombre a la etiqueta de política y seleccione **+Add**, como se muestra en la imagen:



3. Vincule su perfil WLAN al perfil de política deseado como se muestra en las imágenes:



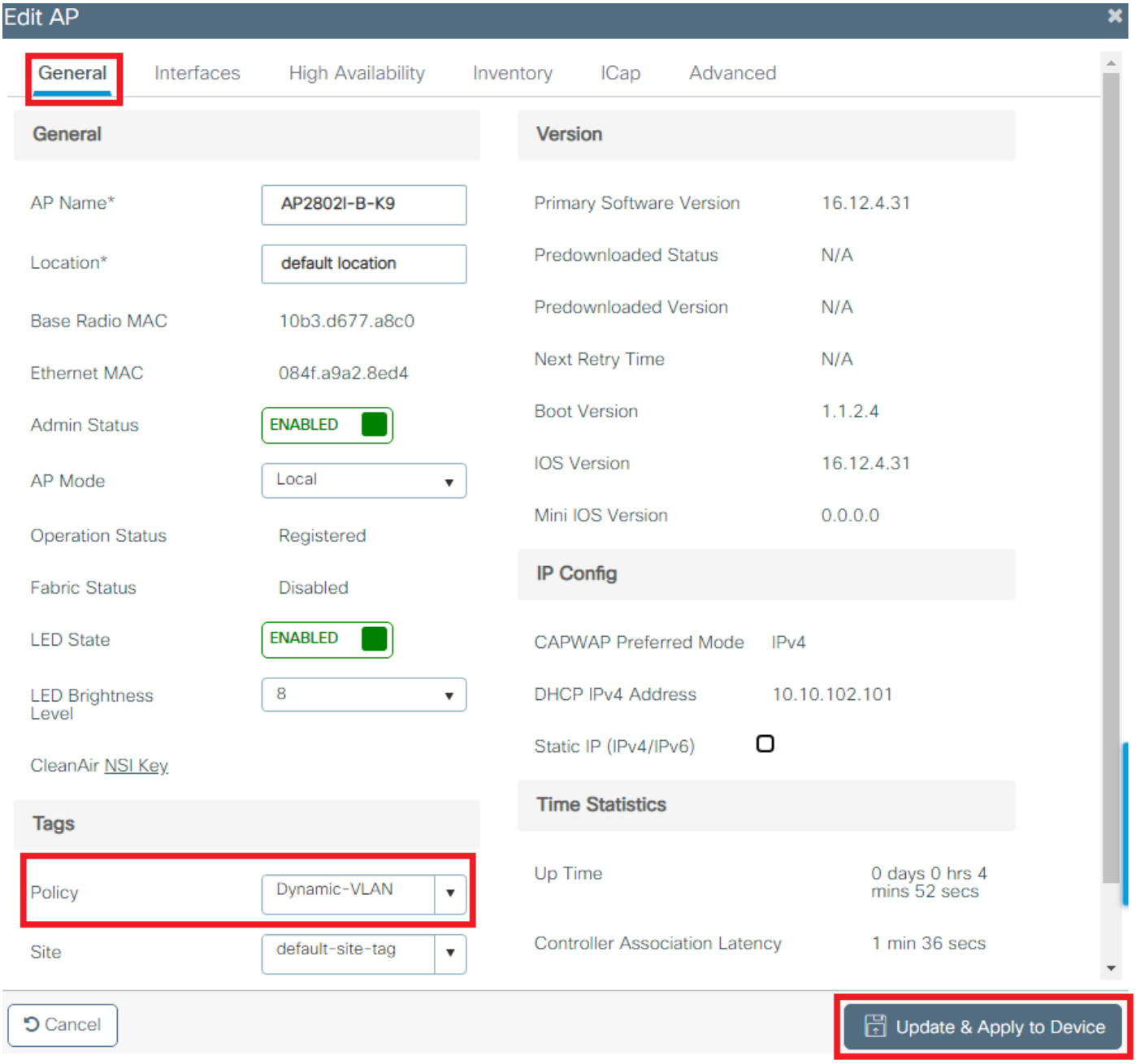


Paso 6. Asignar la etiqueta de política a un AP

Este procedimiento explica cómo configurar la etiqueta Policy en el WLC.

Complete estos pasos:

1. Vaya a **Configuration > Wireless > Access Points > AP Name > General Tags** y asignar la etiqueta de política pertinente y, a continuación, seleccionar **Update & Apply to Device** como se muestra en la imagen:



Precaución: Tenga en cuenta que cuando se cambia la etiqueta de política en un AP, deja su asociación al WLC y se une de nuevo.

Verificación

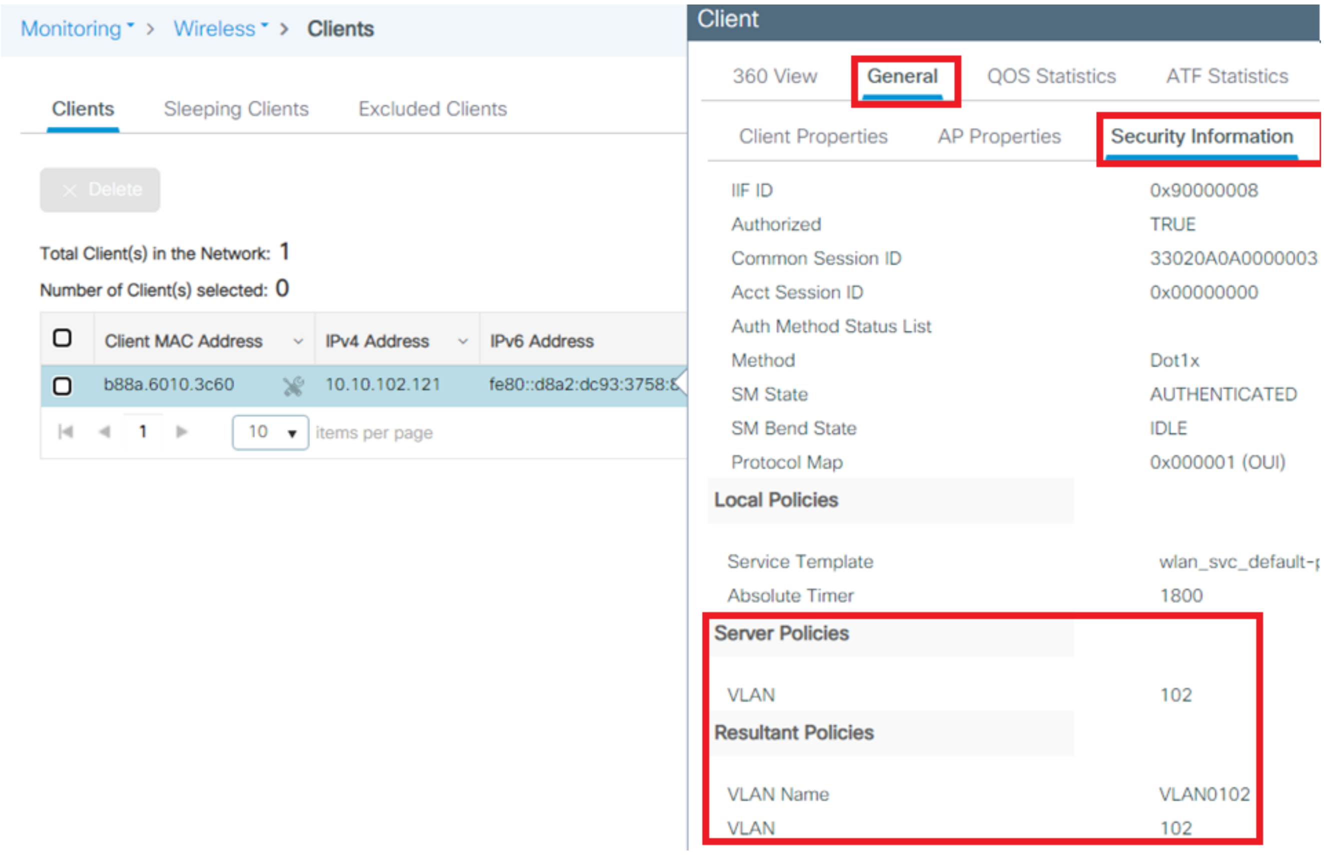
Use esta sección para confirmar que su configuración funciona correctamente.

Probar la conexión con Windows 10 y suplicante nativo, una vez que se le pida un nombre de usuario y una contraseña, introduzca la información del usuario asignada a una VLAN en ISE.

En el ejemplo anterior, observe que jonathga-102 está asignada a la VLAN102 como se especifica en el servidor RADIUS. Este ejemplo utiliza este nombre de usuario para recibir autenticación y ser asignado a una VLAN por el servidor RADIUS:

Una vez completada la autenticación, debe verificar que su cliente esté asignado a la VLAN adecuada según los atributos RADIUS enviados. Complete estos pasos para realizar esta tarea:

1. Desde la GUI del controlador, vaya a **Monitoring > Wireless > Clients > Select the client MAC address > General > Security Information** y busque el campo VLAN como se muestra en la imagen:



Desde esta ventana, puede observar que este cliente está asignado a VLAN102 según los atributos RADIUS configurados en el servidor RADIUS.Desde la CLI puede utilizar la **show wireless client summary detail** para ver la misma información que se muestra en la imagen:

```
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. Es posible habilitar **Radioactive traces** para asegurar la transferencia exitosa de los atributos RADIUS al WLC. Para hacerlo, siga estos pasos: Desde la GUI del controlador, vaya a **Troubleshooting > Radioactive Trace > +Add**.Introduzca la dirección MAC del cliente inalámbrico.Seleccionar **Start**.Conecte el cliente con la WLAN.Vaya a **Stop > Generate > Choose 10 minutes > Apply to Device > Select the trace file to download the log.**

Esta parte del resultado del seguimiento asegura una transmisión exitosa de los atributos RADIUS:

```
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

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Guía del usuario final