Configurar atribuição dinâmica de VLAN com ISE e Catalyst 9800 Wireless LAN Controller

Contents

Introduction

Este documento descreve o conceito de atribuição de VLAN dinâmica e como configurar o controlador de LAN sem fio (WLC - Wireless LAN Controller) do Catalyst 9800 e o Cisco Identity Service Engine (ISE - Cisco Identity Service Engine) para atribuir a LAN sem fio (WLAN - Wireless LAN) para realizar isso para os clientes sem fio.

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Ter conhecimento básico da WLC e dos LAPs (Lightweight Access Points, pontos de acesso leves).
- Ter conhecimento funcional do servidor AAA, como o ISE.
- Tenha um conhecimento profundo de redes sem fio e problemas de segurança sem fio.

- Ter conhecimento funcional sobre a atribuição dinâmica de VLANs.
- Tenha conhecimento básico do Control and Provisioning for Wireless Access Point (CAPWAP).

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Catalyst 9800 WLC (Catalyst 9800-CL) que executa o firmware versão 16.12.4a.
- LAP Cisco 2800 Series no modo local.
- Suplicante nativo do Windows 10.
- Cisco Identity Service Engine (ISE) que executa a versão 2.7.
- Switch Cisco série 3850 que executa o firmware versão 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Atribuição da VLAN (Rede local virtual) dinâmica com servidor Radius

Na maioria dos sistemas de rede local sem fio (WLAN), cada WLAN tem uma política estática que se aplica a todos os clientes associados a um SSID (Service Set Identifier). Embora poderoso, esse método tem limitações porque exige que os clientes se associem a diferentes SSIDs para herdar diferentes políticas de QoS e segurança.

Mas a solução de Cisco WLAN suporta identidades na rede. Isso permite que a rede anuncie um único SSID e permite que usuários específicos herdem diferentes QoS ou políticas de segurança com base na credencial do usuário.

A atribuição da VLAN dinâmica é um recurso que coloca um usuário wireless em uma VLAN específica baseado nas credenciais fornecidas pelo usuário. A tarefa de atribuir usuários a uma VLAN específica é tratada por um servidor de autenticação RADIUS, como o Cisco ISE. Isto pode ser usado, por exemplo, para permitir que o host wireless permaneça na mesma VLAN enquanto ele se desloca em uma rede no campus.

Portanto, quando um cliente tenta se associar a um LAP registrado em um controlador, a WLC passa as credenciais do usuário ao servidor RADIUS para validação. Quando a autenticação é bem sucedida, o servidor Radius passa determinados atributos da Internet Engineering Task Force (IETF) ao usuário. Esses atributos RADIUS decidem a ID da VLAN que deve ser atribuída ao cliente sem fio. O SSID do cliente não importa porque o usuário é sempre atribuído a esse ID de VLAN predeterminado.

Os atributos do usuário do RADIUS usados para a atribuição de ID da VLAN são:

- IETF 64 (tipo de túnel) — Defina como VLAN.
- IETF 65 (Tunnel Medium Type - Tipo de Meio de Túnel)—Defina isso como 802.
- IETF 81 (ID do grupo privado do túnel) — Defina como a identificação da VLAN.

O ID da VLAN é de 12 bits e tem um valor entre 1 e 4094, inclusive. Como a ID de Grupo Privado

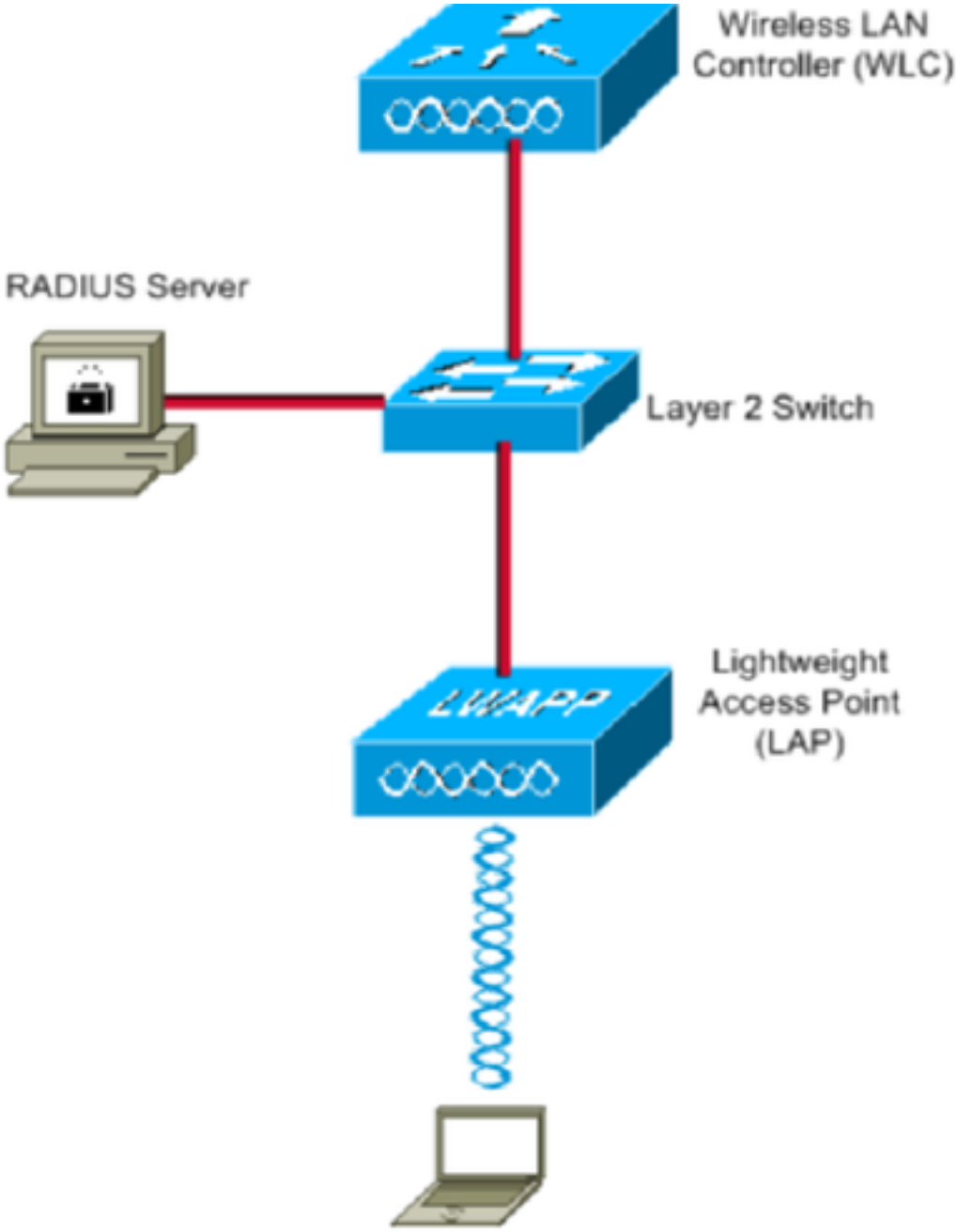
do Túnel é do tipo string, como definido na RFC2868 para uso com a IEEE 802.1X, o valor de número inteiro da ID de VLAN é codificado como uma string. Quando esses atributos de túnel são enviados, é necessário inseri-los no campo Tag (Etiqueta).

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Estes são os detalhes de configuração dos componentes usados neste diagrama:

- O endereço IP do servidor Cisco ISE (RADIUS) é 10.10.1.24.

- O endereço da interface de gerenciamento do WLC é 10.10.1.17.
- O servidor DHCP interno no controlador é usado para atribuir o endereço IP aos clientes wireless.
- Este documento usa 802.1x com PEAP como mecanismo de segurança.
- A VLAN102 é usada em toda esta configuração. O nome de usuário jonathga-102 é configurado para ser colocado na VLAN102 pelo servidor RADIUS.

Configuration Steps

Esta configuração é dividida em três categorias:

- Configuração do Cisco ISE.
- Configurar o Switch para várias VLANs.
- Configuração do Catalyst 9800 WLC.

Configuração do Cisco ISE

Essa configuração requer estes passos:

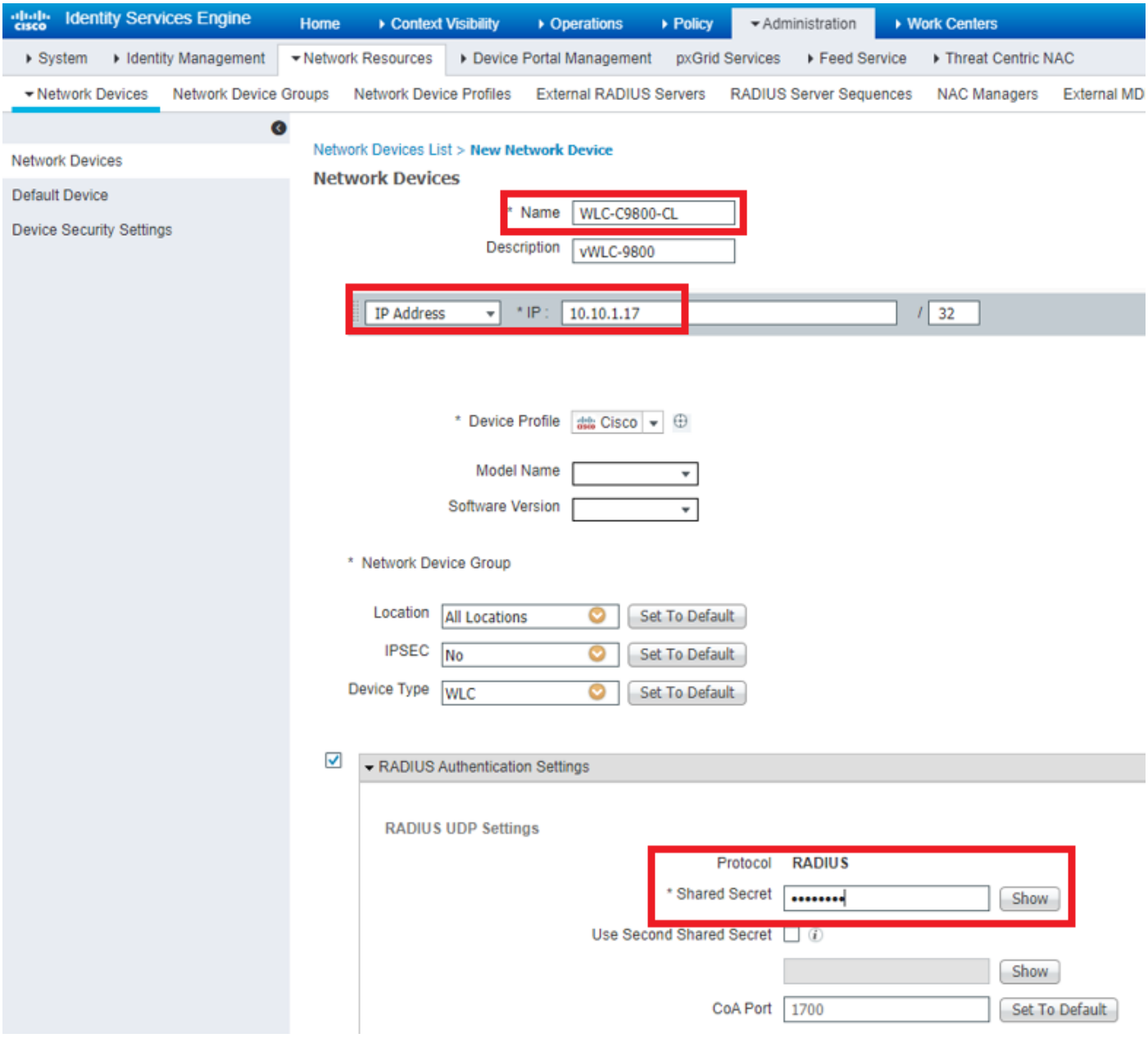
- Configure o Catalyst WLC como um cliente AAA no servidor Cisco ISE.
- Configurar usuários internos no Cisco ISE.
- Configure os atributos RADIUS (IETF) usados para atribuição dinâmica de VLAN no Cisco ISE.

Etapa 1. Configurar o Catalyst WLC como um cliente AAA no servidor Cisco ISE

Este procedimento explica como adicionar a WLC como um cliente AAA no servidor ISE para que a WLC possa passar as credenciais do usuário para o ISE.

Conclua estes passos:

1. Na GUI do ISE, navegue até **Administration > Network Resources > Network Devices**e selecionar **Add**.
2. Conclua a configuração com o endereço IP de gerenciamento WLC e o segredo compartilhado RADIUS entre WLC e ISE, como mostrado na imagem:

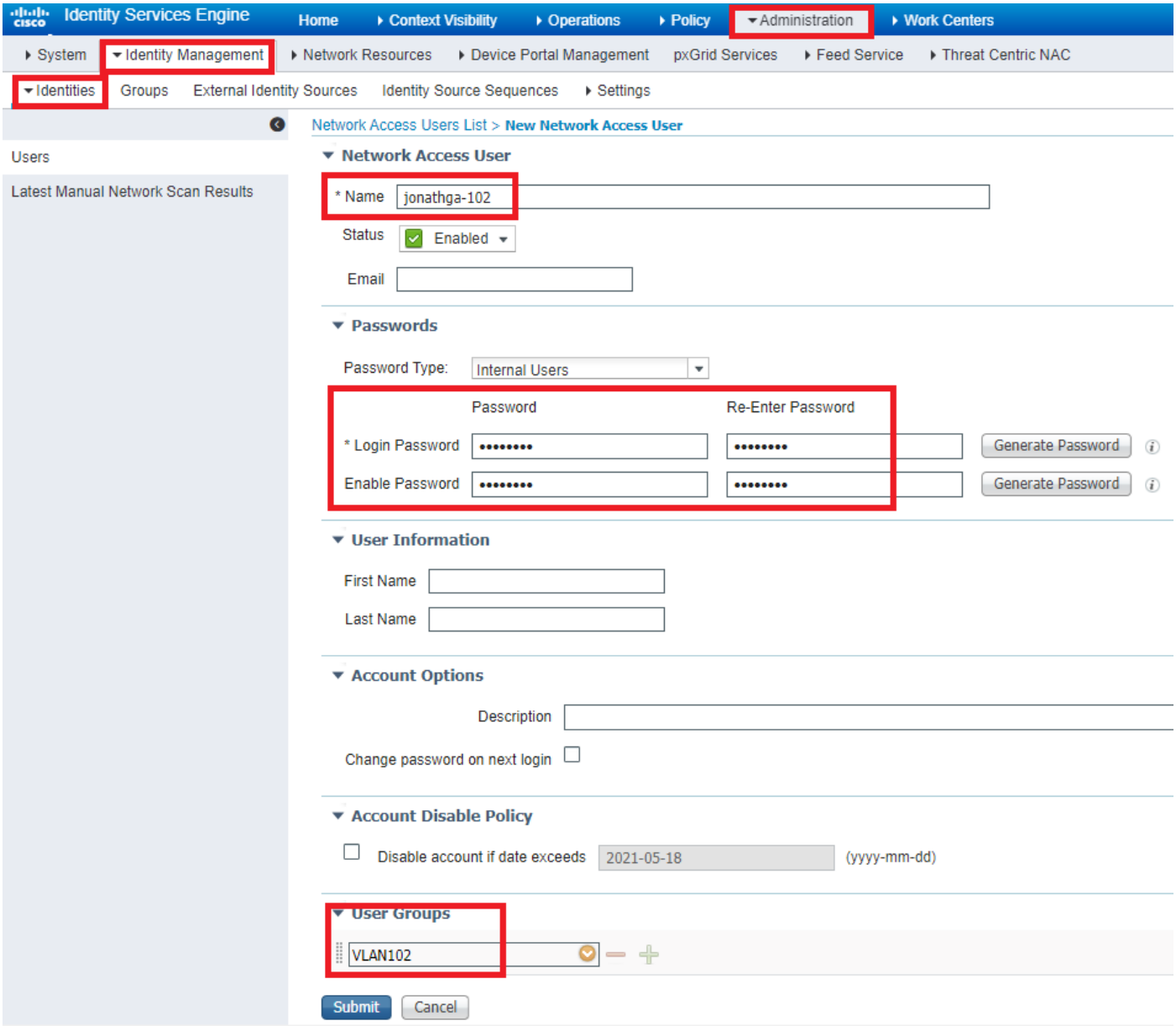


Etapa 2. Configurar usuários internos no Cisco ISE

Este procedimento explica como adicionar os usuários ao banco de dados interno do Cisco ISE.

Conclua estes passos:

1. Na GUI do ISE, navegue até **Administration > Identity Management > Identities** e selecionar **Add**.
2. Conclua a configuração com o nome de usuário, senha e grupo de usuários, conforme mostrado na imagem:

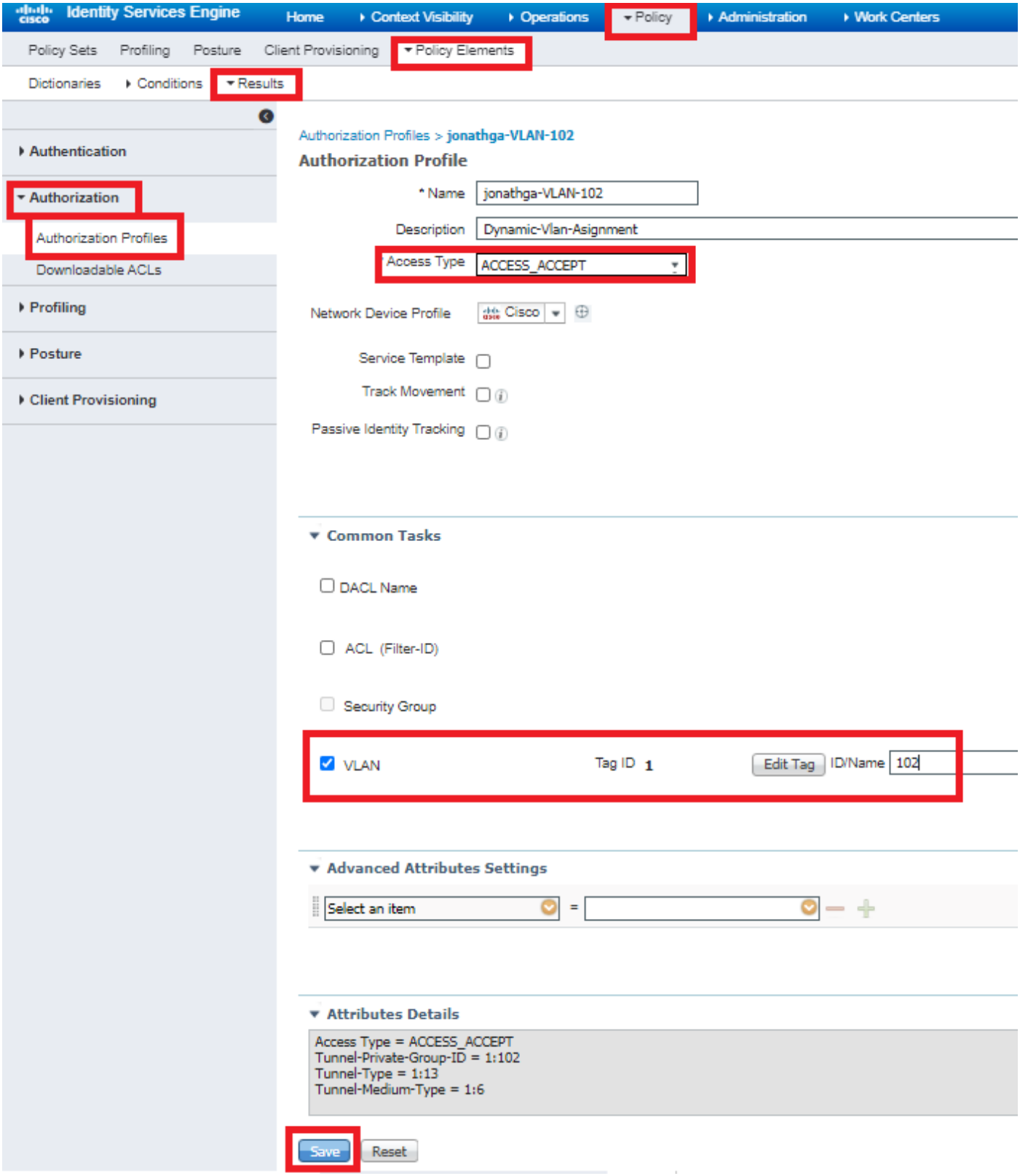


Etapa 3. Configurar os atributos RADIUS (IETF) usados para atribuição dinâmica de VLAN

Este procedimento explica como criar um perfil de autorização e uma política de autenticação para usuários sem fio.

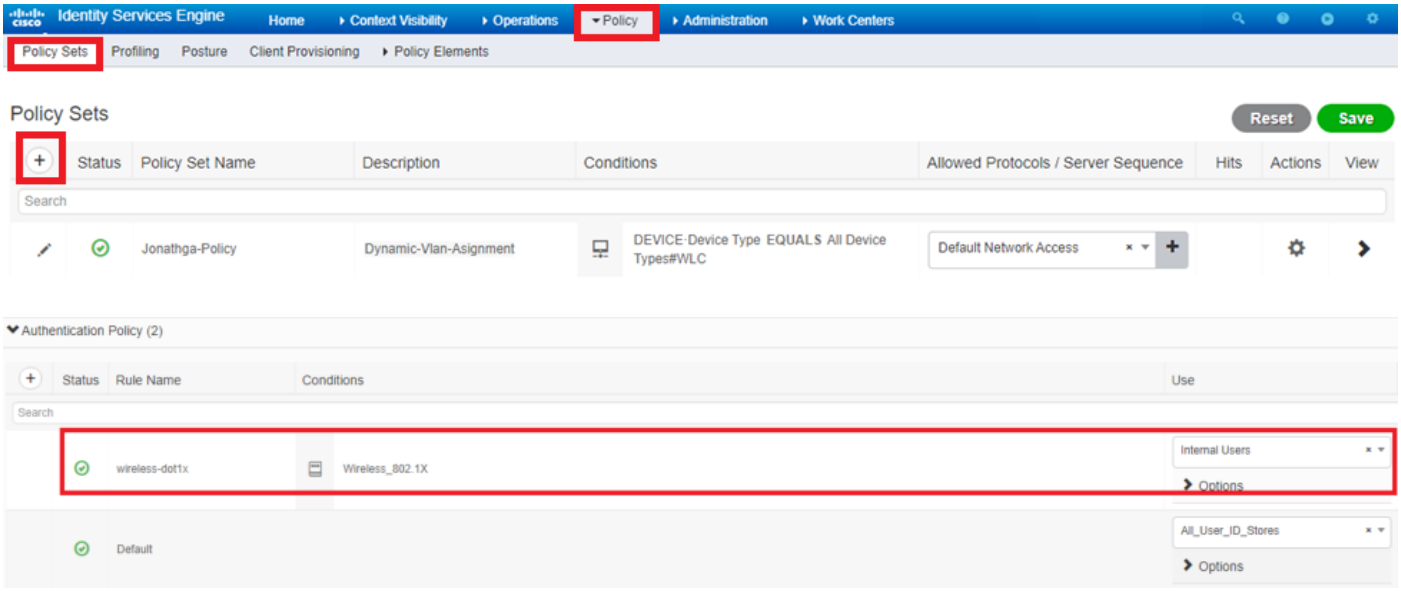
Conclua estes passos:

1. Na GUI do ISE, navegue até **Policy > Policy Elements > Results > Authorization > Authorization profiles** e selecionar **Add** para criar um novo perfil.
2. Conclua a configuração do perfil de autorização com informações de VLAN para o respectivo grupo. Esta imagem mostra **jonathga-VLAN-102** definições de configuração de grupo.



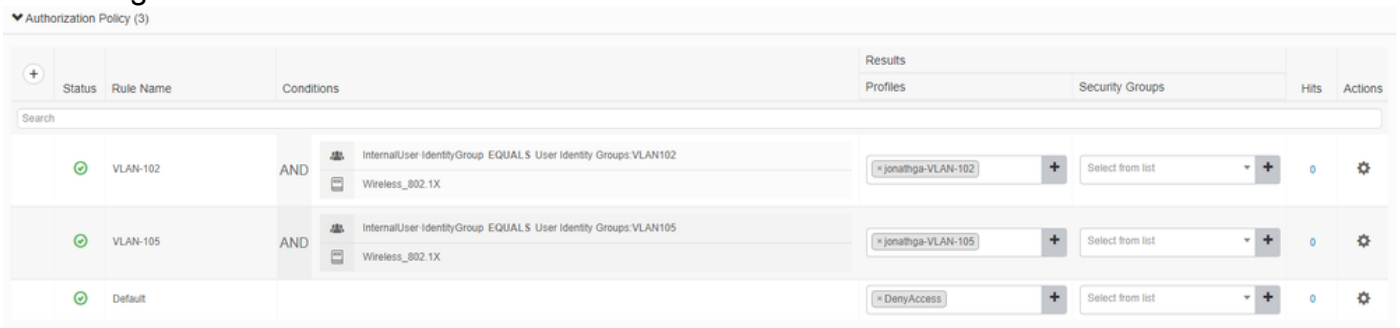
Após a configuração dos perfis de autorização, é necessário criar uma política de autenticação para usuários sem fio. Você pode usar um novo **Custom** ou modificar a **Default** Conjunto de políticas. Neste exemplo, um perfil personalizado é criado.

3. Navegar para **Policy > Policy Sets** e selecionar **Add** para criar uma nova política conforme mostrado na imagem:



Agora você precisa criar políticas de autorização para usuários para atribuir um perfil de autorização respectivo com base na associação ao grupo.

5. Abra o **Authorization policy** e criar políticas para realizar esse requisito conforme mostrado na imagem:



Configurar o Switch para várias VLANs

Para permitir várias VLANs através do switch, você precisa emitir estes comandos para configurar a porta do switch conectada ao controlador:

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

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

> **Note**: Por padrão, a maioria dos switches permitem todas as VLAN criadas nesse switch através da porta de tronco. Se uma rede com fio é conectada ao switch, então esta mesma configuração pode ser aplicada à porta do switch conectada à rede com fio. Isto permite a comunicação entre as mesmas VLANs nas redes com e sem fio.

Configuração do Catalyst 9800 WLC

Essa configuração requer estes passos:

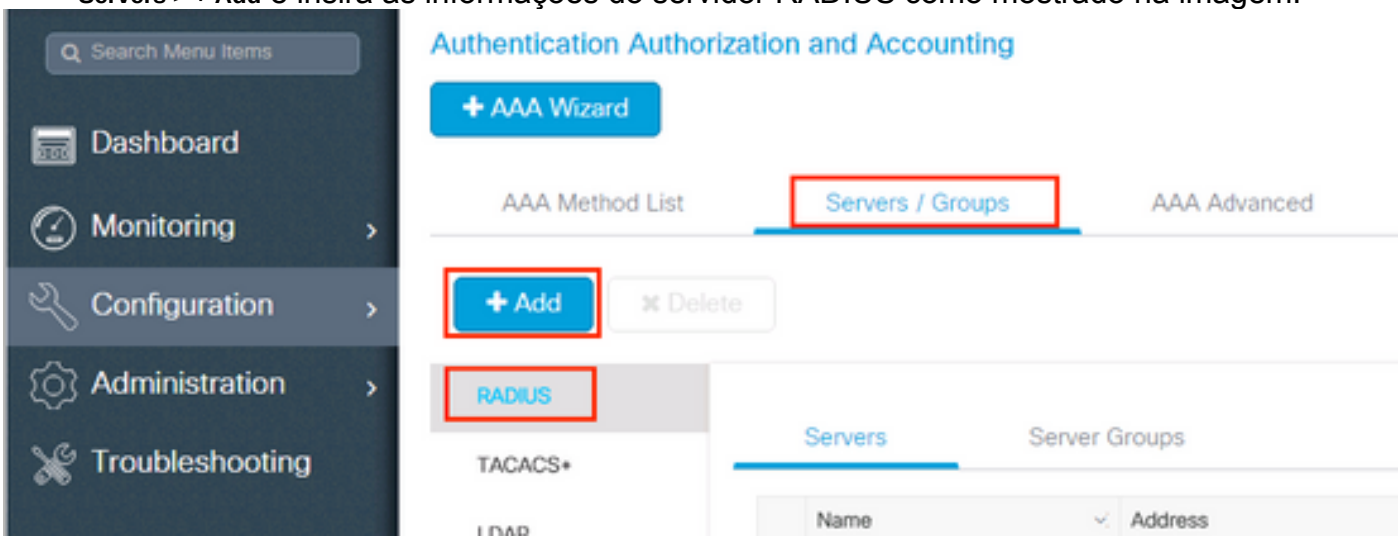
- Configurar o WLC com os detalhes do Servidor de Autenticação.
- Configure as VLANs.
- Configure as WLANs (SSID).
- Configure o perfil de política.
- Configure a tag Policy.
- Atribua a tag Policy a um AP.

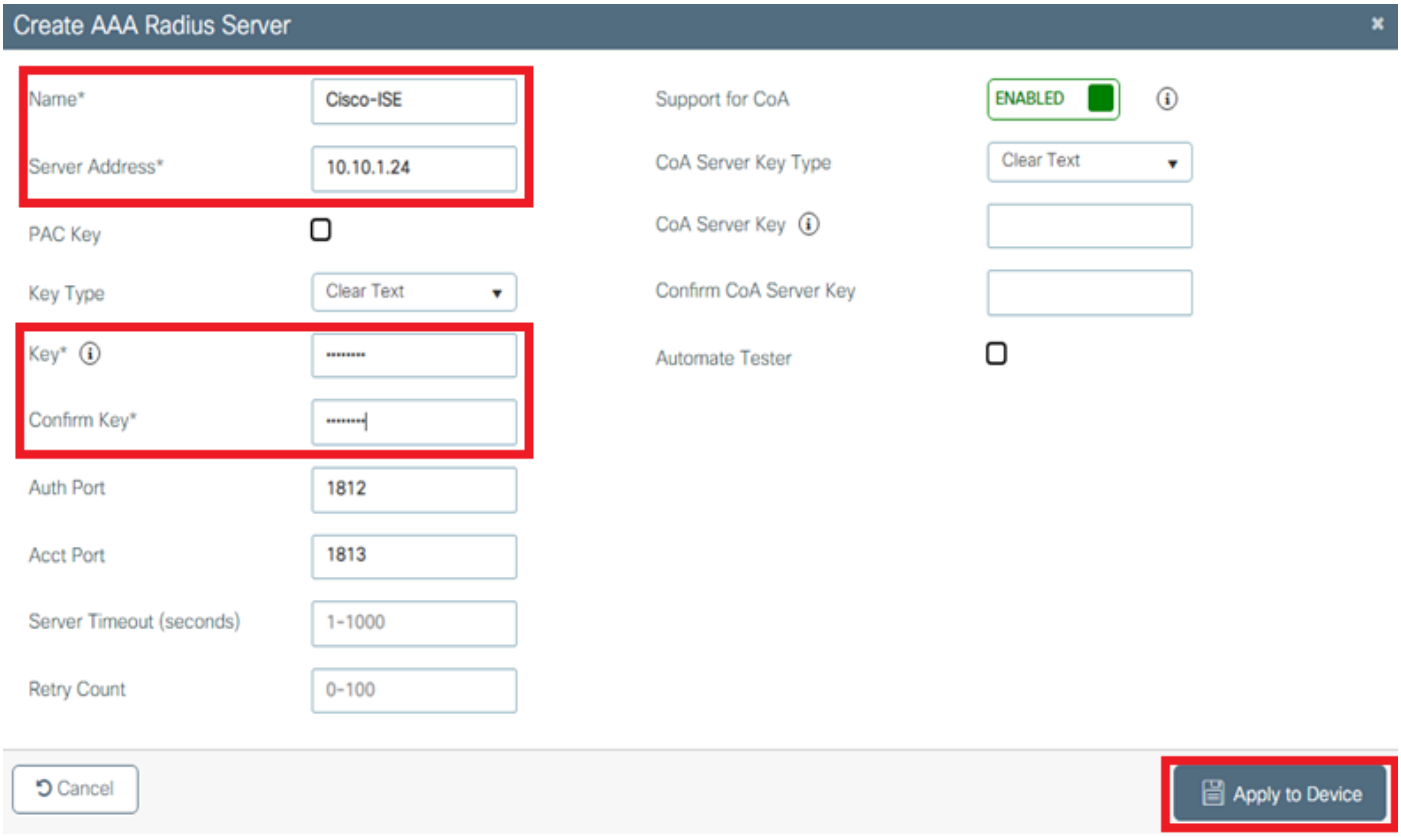
Etapa 1. Configurar o WLC com os detalhes do Servidor de Autenticação

Énecessário configurar a WLC para que ela possa se comunicar com o servidor RADIUS para autenticar os clientes.

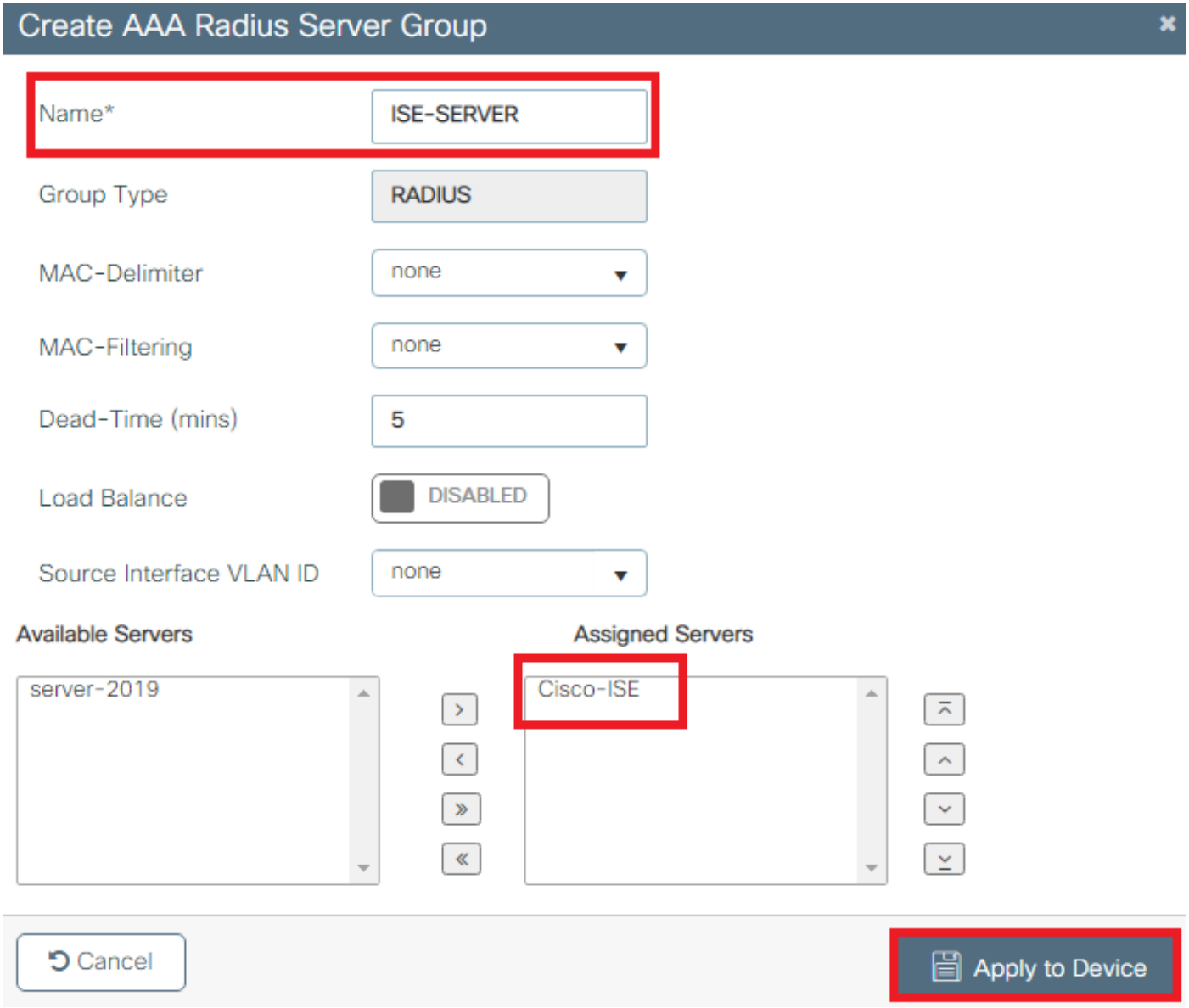
Conclua estes passos:

1. Na GUI do controlador, navegue para **Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add** e insira as informações do servidor RADIUS como mostrado na imagem:

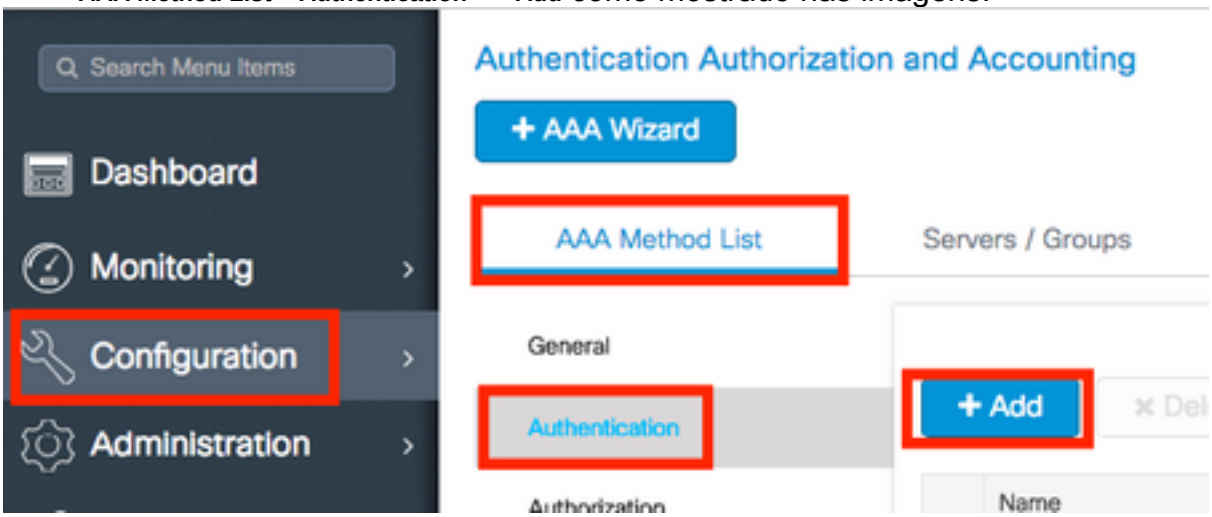


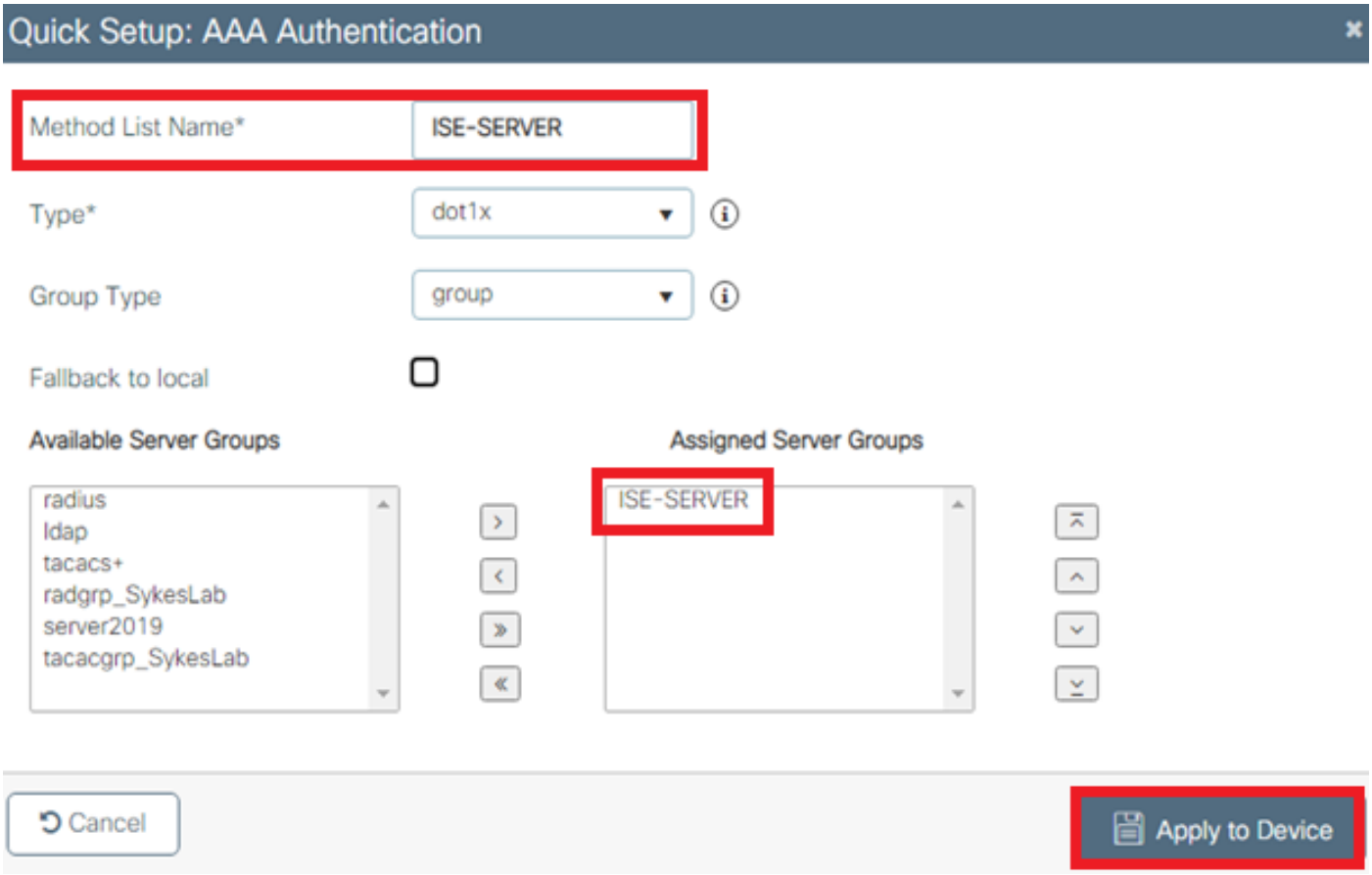


2. Para adicionar o servidor RADIUS a um grupo RADIUS, navegue para **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add** conforme mostrado na imagem:



3. Para criar uma lista de métodos de autenticação, navegue para **Configuration > Security > AAA > AAA Method List > Authentication > + Add** como mostrado nas imagens:



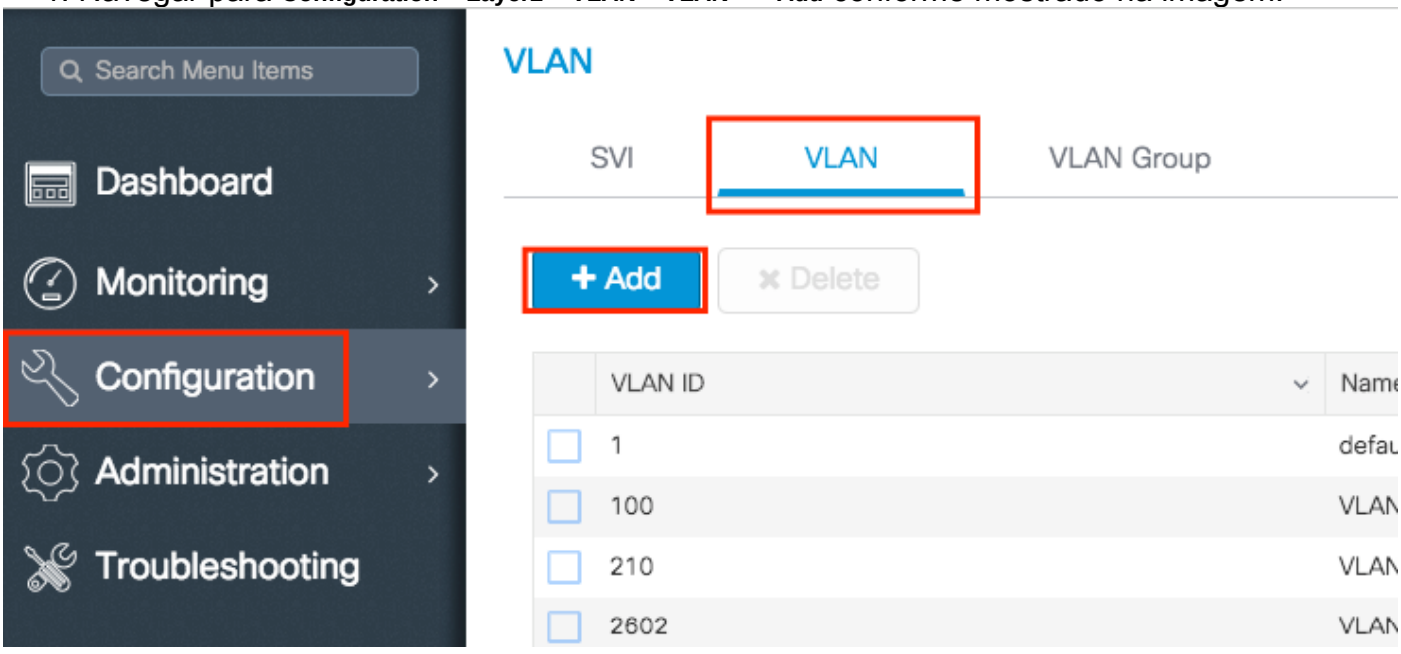


Etapa 2. Configurar as VLANs

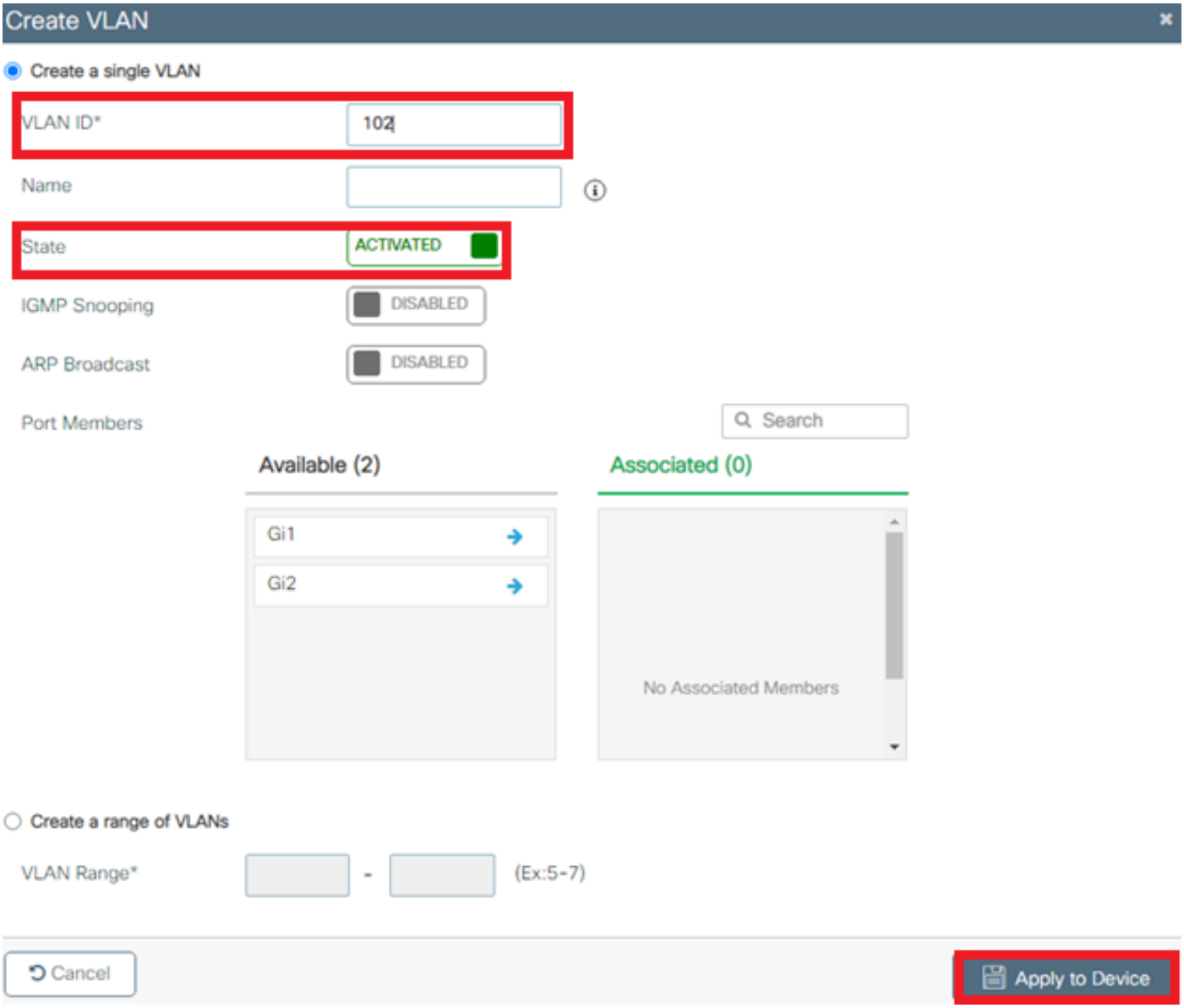
Este procedimento explica como configurar VLANs no Catalyst 9800 WLC. Como explicado antes neste documento, a ID de VLAN especificada sob o atributo Tunnel-Private-Group ID do servidor RADIUS deve igualmente existir no WLC.

No exemplo, o usuário jonathga-102 é especificado com o comando **Tunnel-Private-Group ID of 102 (VLAN =102)** no servidor RADIUS.

1. Navegar para **Configuration > Layer2 > VLAN > VLAN > + Add** conforme mostrado na imagem:



2. Insira as informações necessárias conforme mostrado na imagem:



Note: Se você não especificar um nome, a VLAN receberá automaticamente o nome de VLANXXXX, onde XXXX é a ID da VLAN.

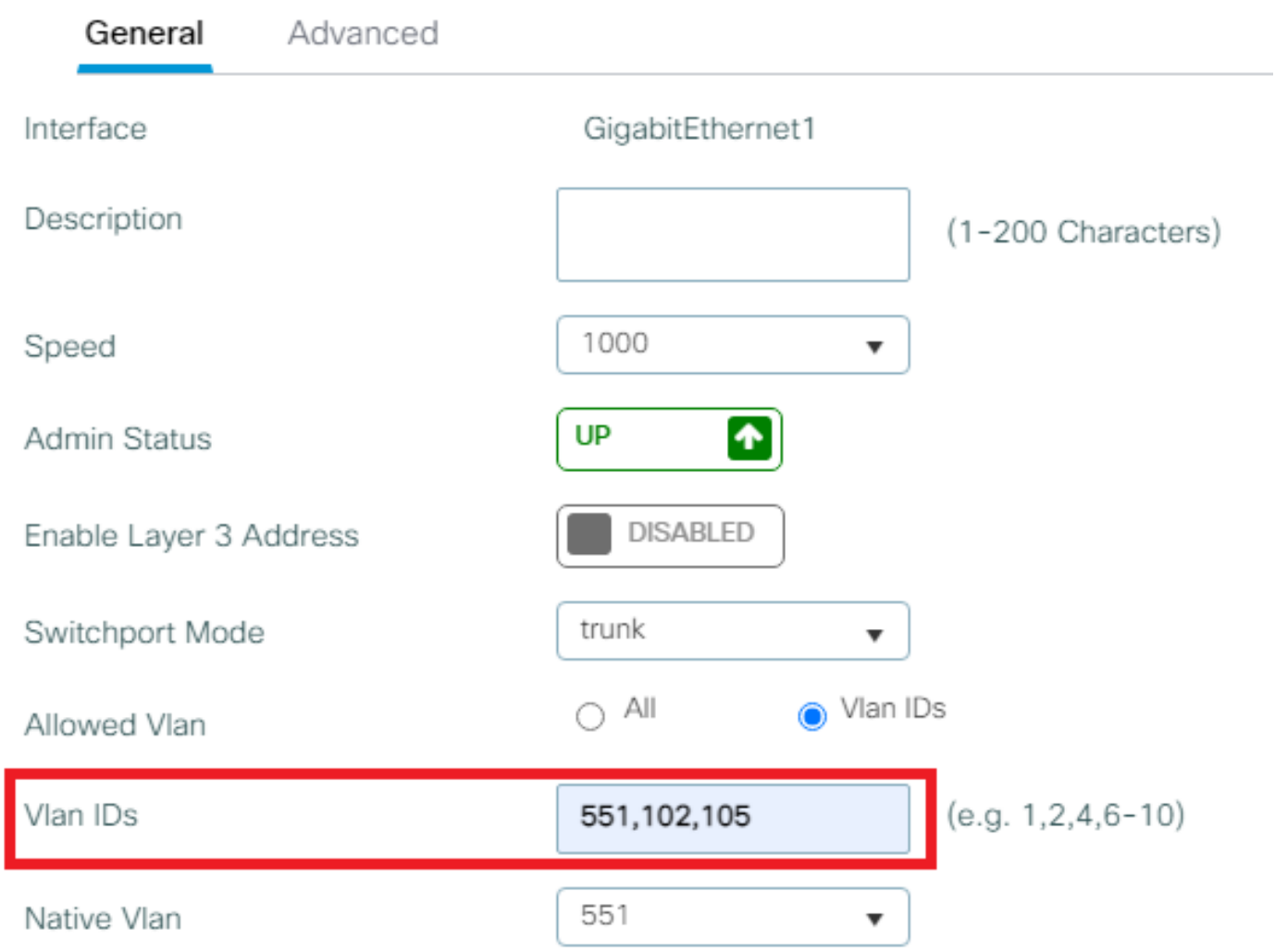
Repita as etapas 1 e 2 para todas as VLANs necessárias. Depois de concluir, você poderá continuar com a etapa 3.

3. Verifique se as VLANs são permitidas em suas interfaces de dados. Se você tiver um canal de porta em uso, navegue para **Configuration > Interface > Logical > PortChannel name > General**. Se você vir configurado como **Allowed VLAN = All** você terminou a configuração. Se você vir **Allowed VLAN = VLANs IDs**, adicione as VLANs necessárias e depois disso selecione **Update & Apply to Device**.Se você não tiver um canal de porta em uso, navegue para **Configuration > Interface > Ethernet > Interface Name > General**. Se você vir configurado como **Allowed VLAN = All** você terminou a configuração. Se você vir **Allowed VLAN = VLANs IDs**, adicione as VLANs necessárias e depois disso selecione **Update & Apply to Device**.

Essas imagens mostram a configuração relacionada à configuração da interface se você usar todas as IDs de VLAN ou IDs específicas.

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	

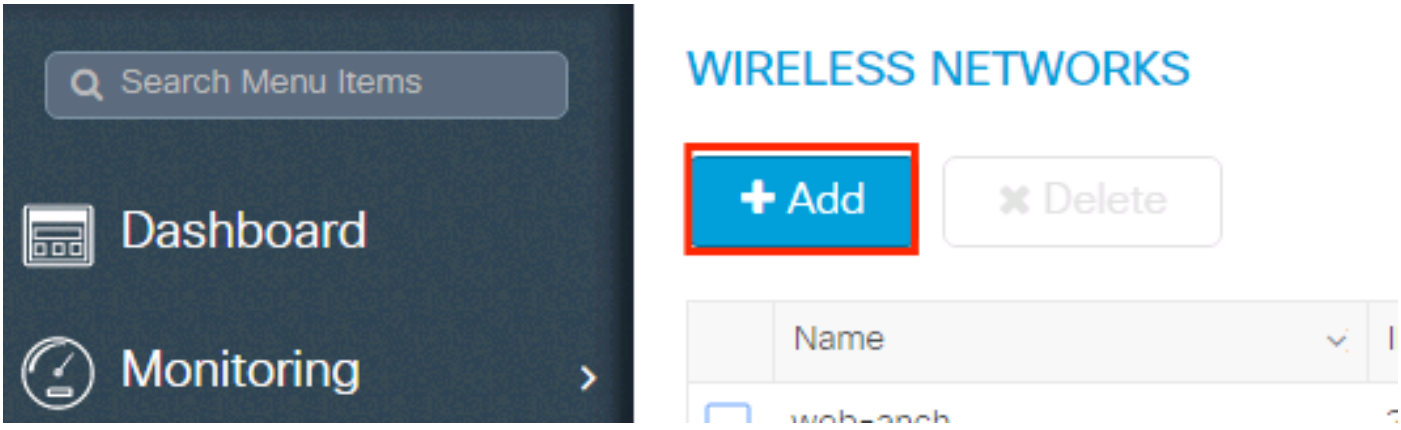


Etapa 3. Configurar as WLANs (SSID)

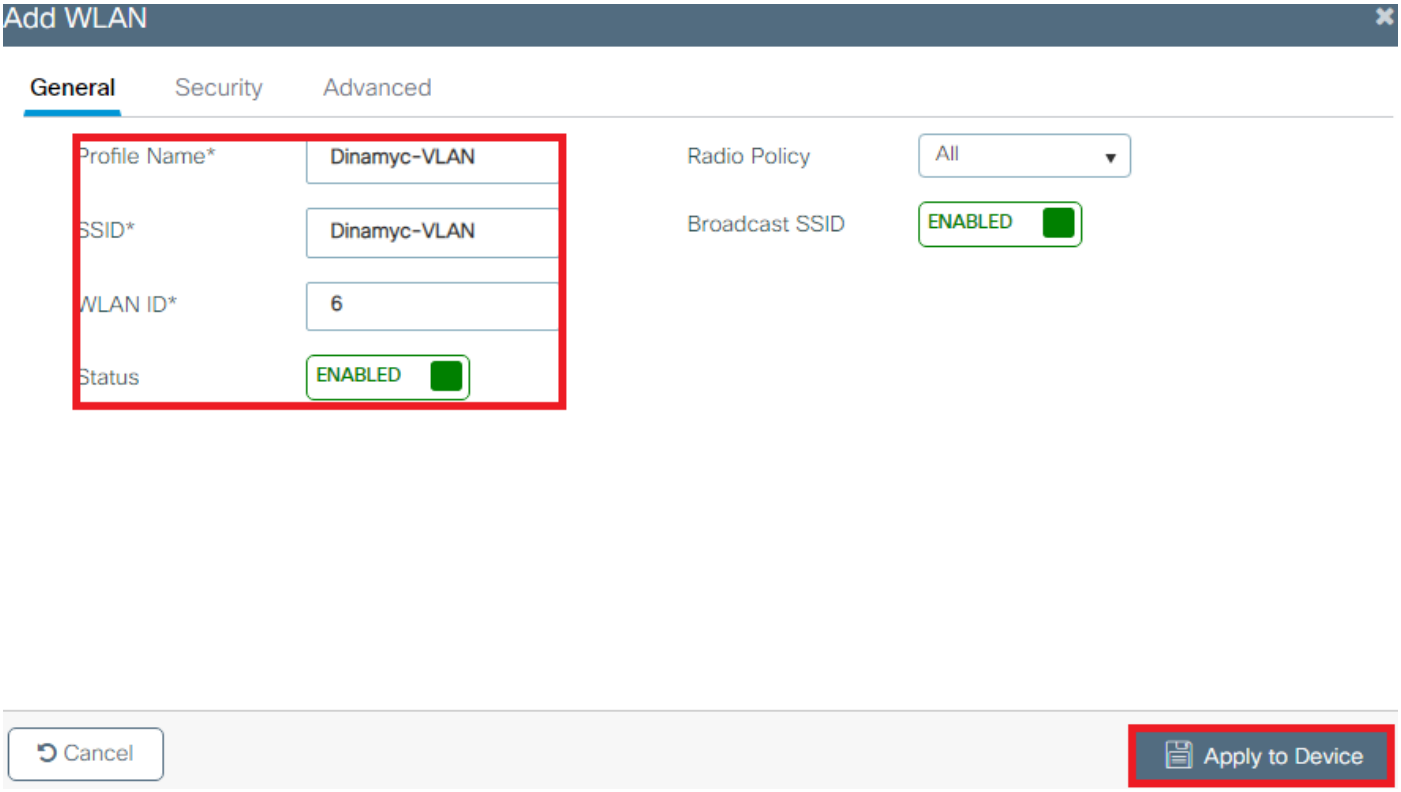
Este procedimento explica como configurar as WLANs no WLC.

Conclua estes passos:

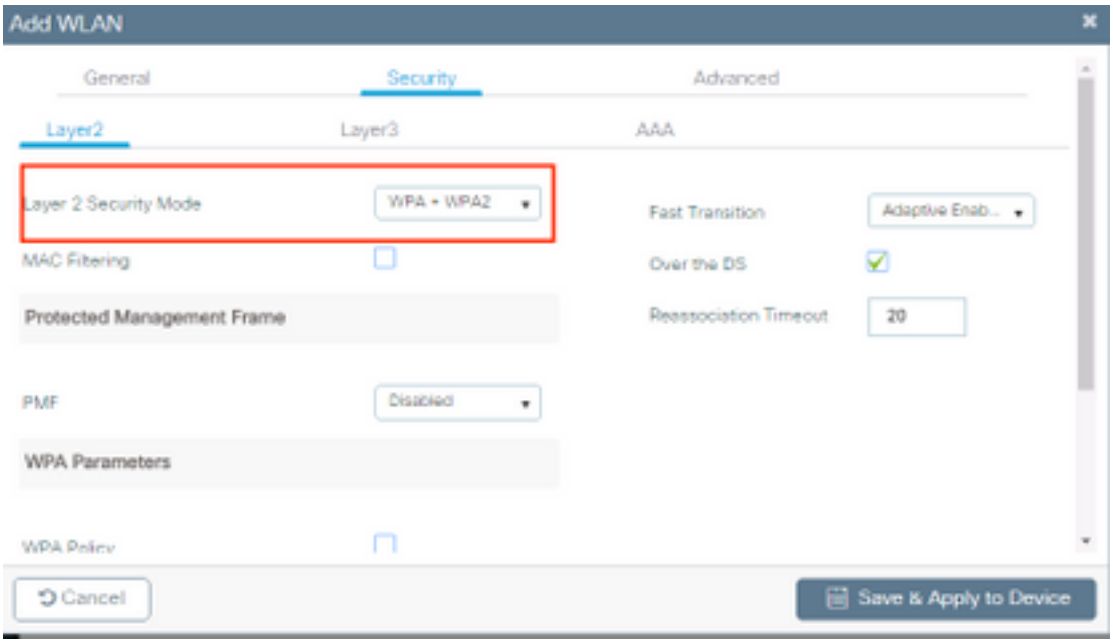
1. Para criar a WLAN. Navegar para **Configuration > Wireless > WLANs > + Add** e configurar a rede conforme necessário, como mostrado na imagem:

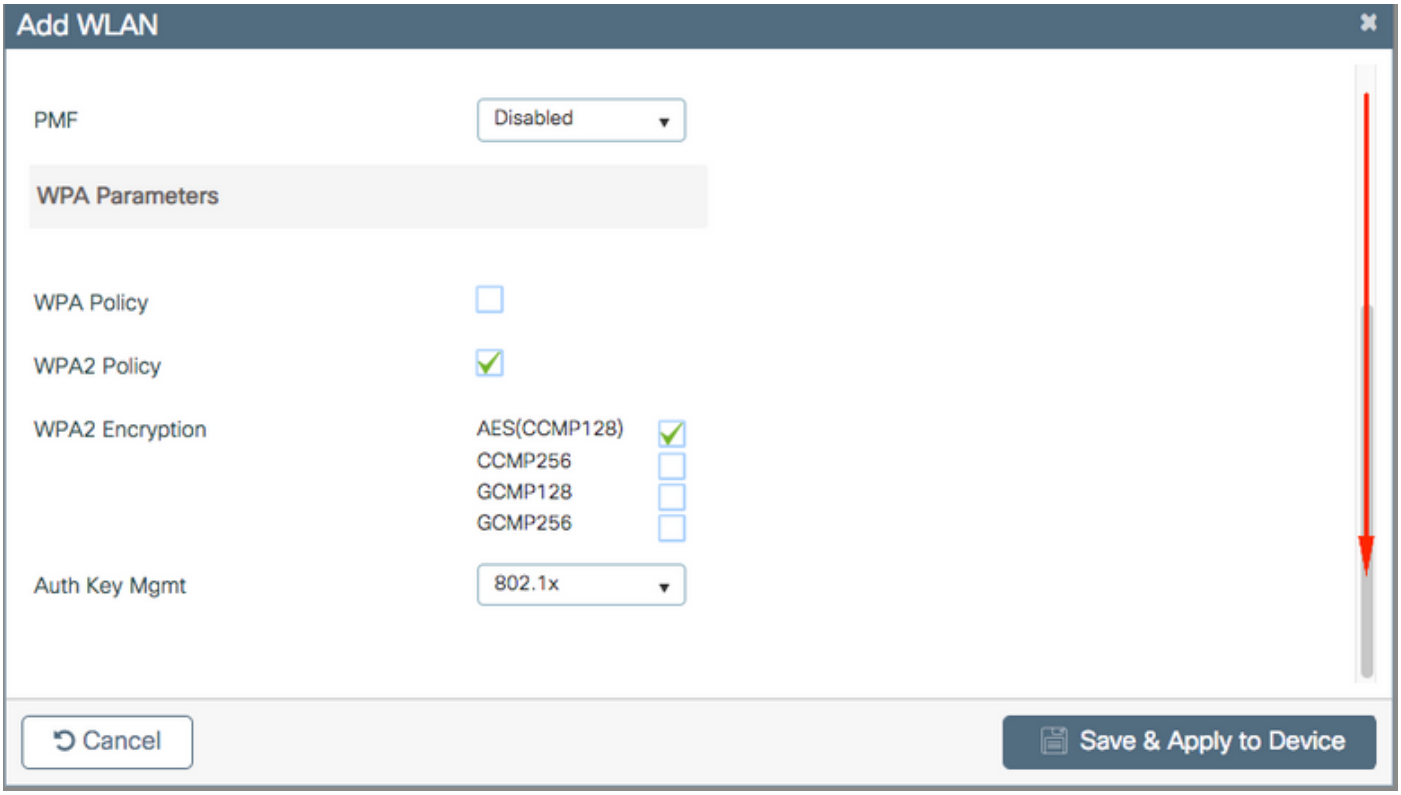


2. Insira as informações da WLAN conforme mostrado na imagem:

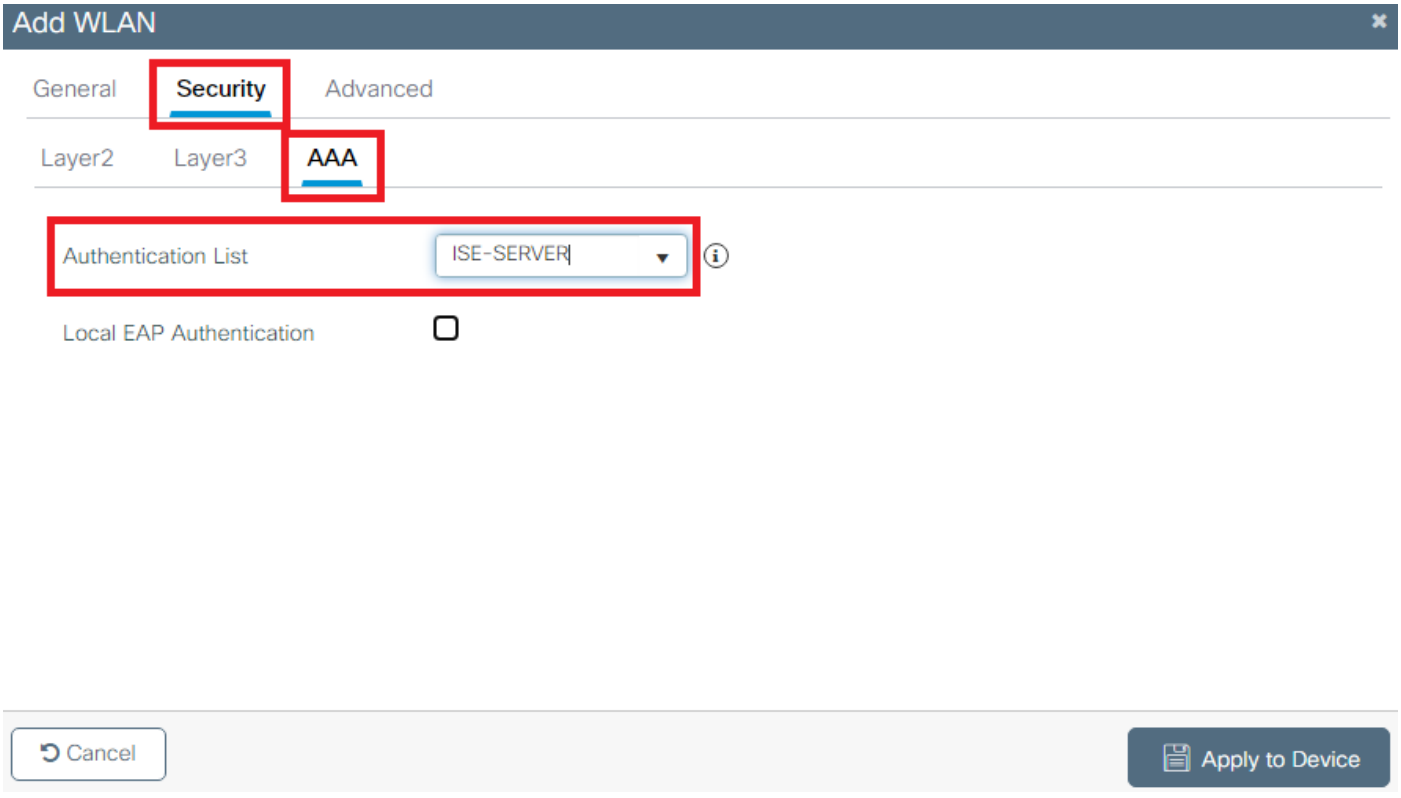


3. Navegar para **Security** e selecione o método de segurança necessário. Nesse caso, WPA2 + 802.1x como mostrado nas imagens:





Des**Security > AAA** selecione o método de autenticação criado na etapa 3 em **Configure the WLC with the Details of the Authentication Server** conforme mostrado na imagem:



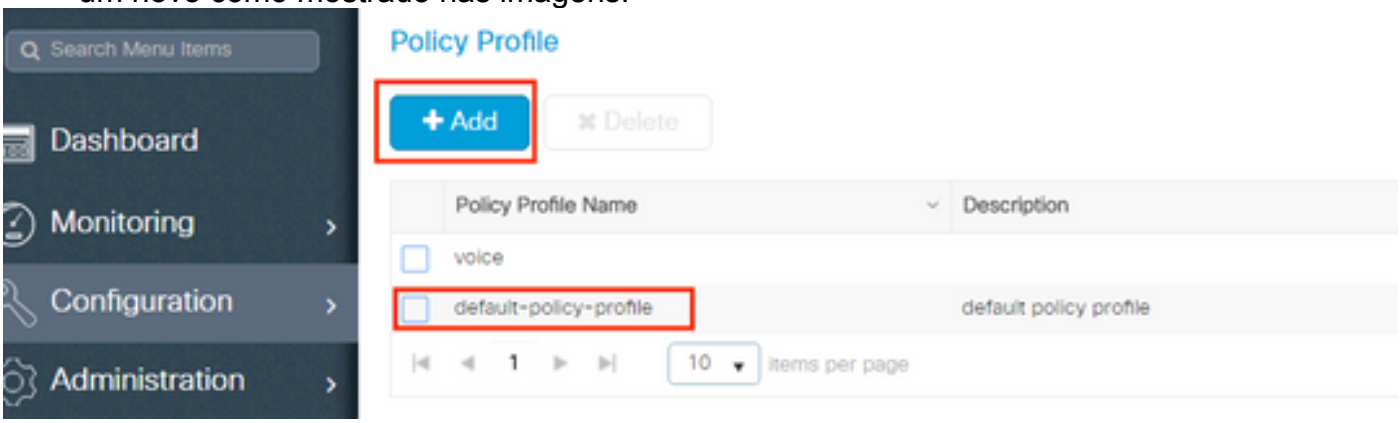
Etapa 4. Configurar o perfil de política

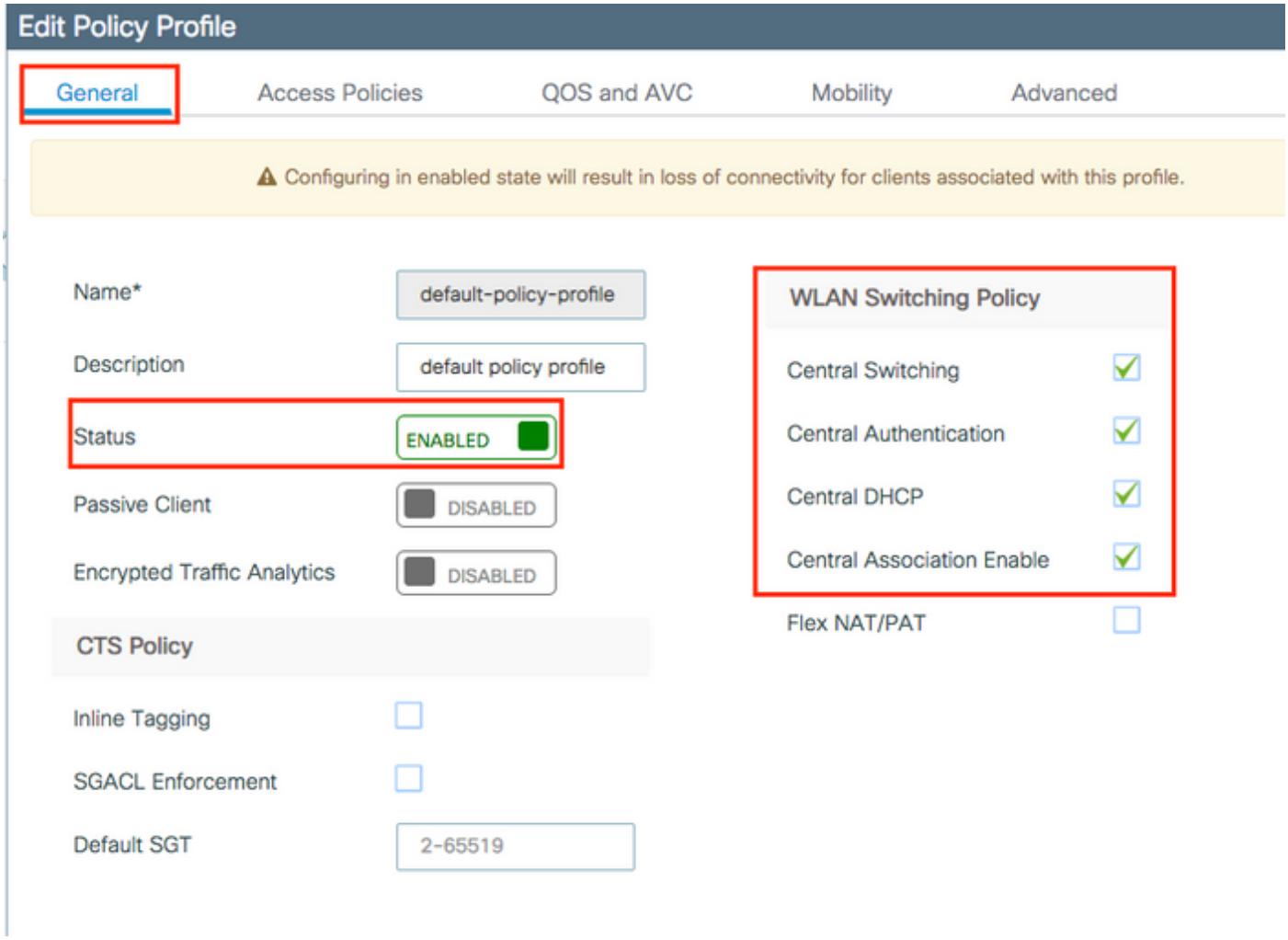
Este procedimento explica como configurar o perfil de política no WLC.

Conclua estes passos:

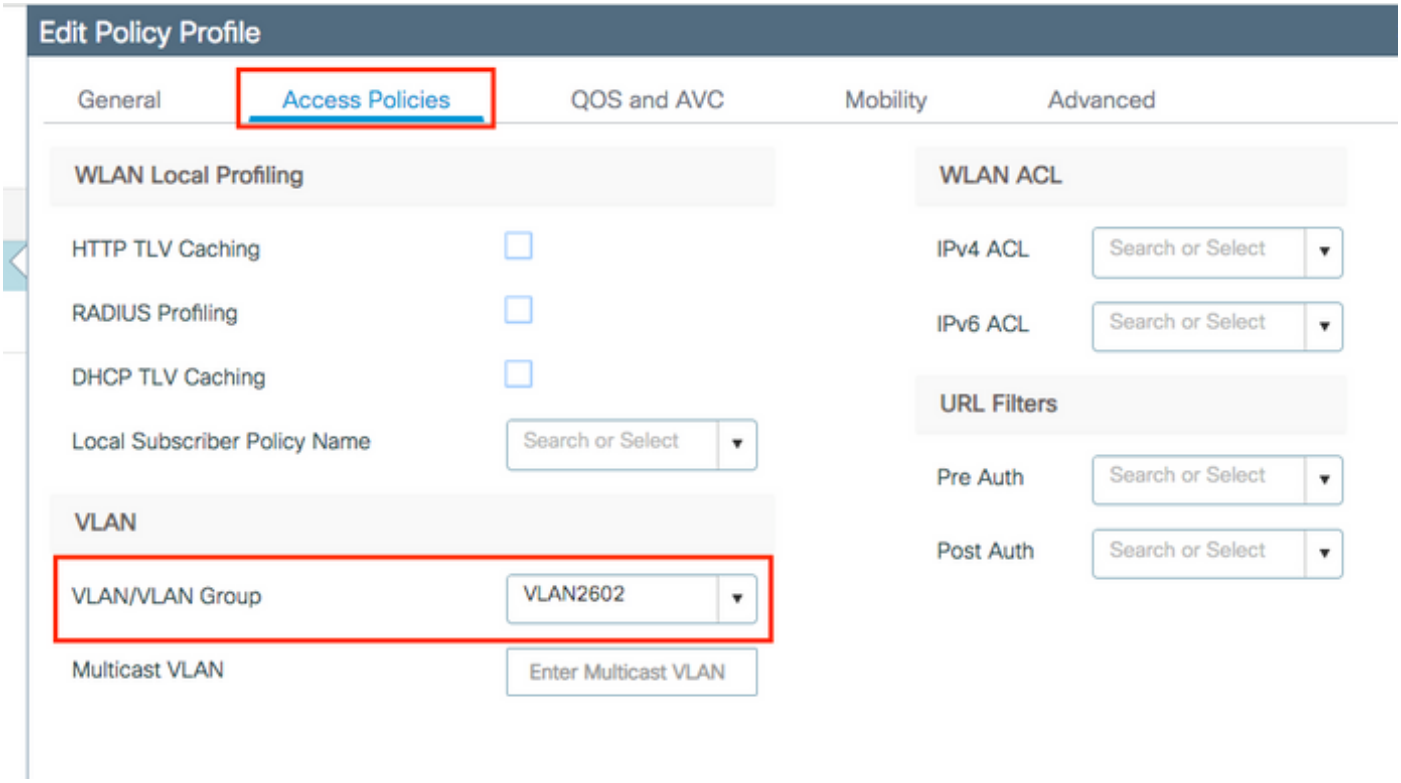
1. Navegar para **Configuration > Tags & Profiles > Policy Profile** e configurar **default-policy-profile** ou criar

um novo como mostrado nas imagens:



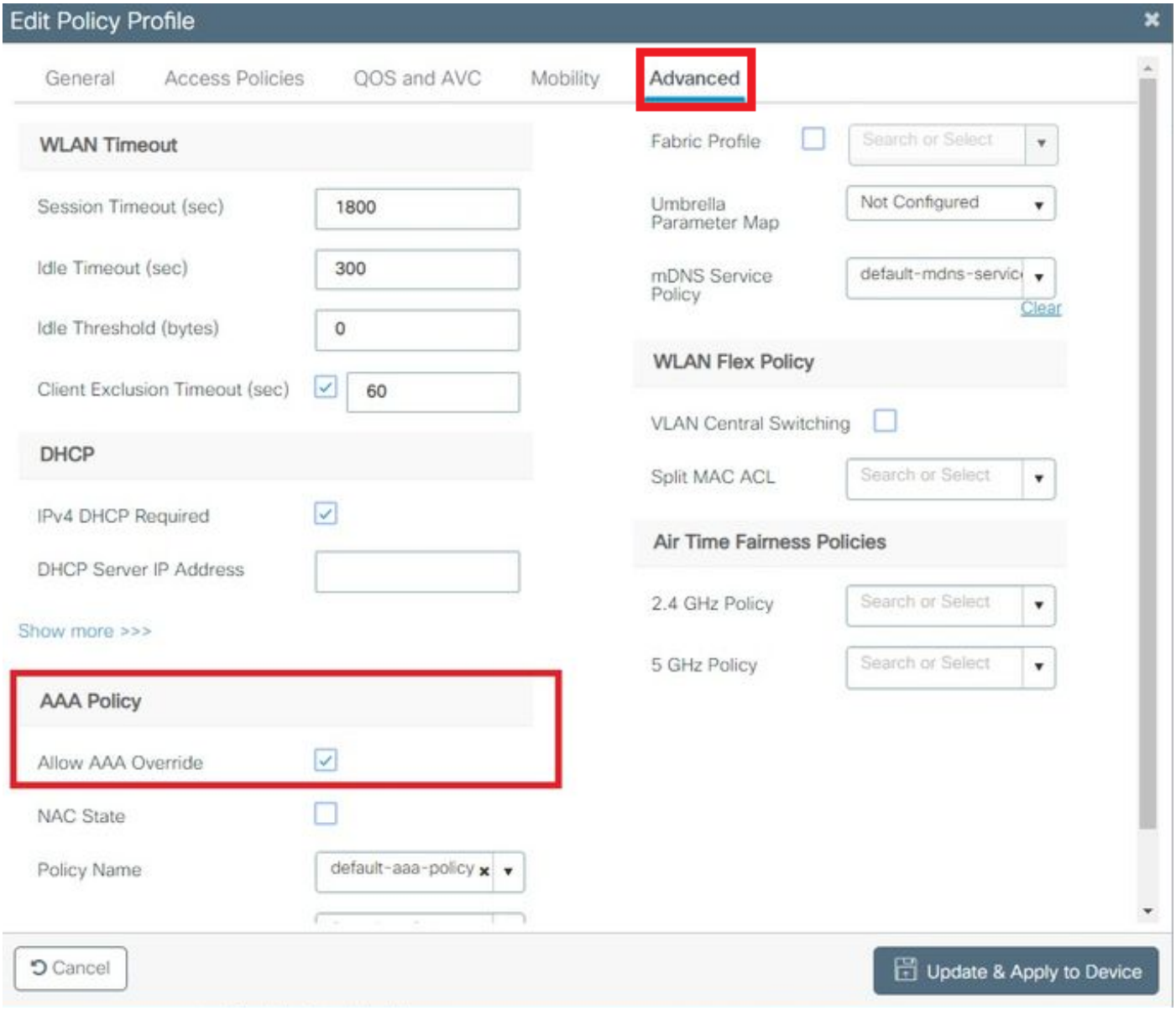


2. Nos **Access Policies** atribua a VLAN à qual os clientes sem fio estão atribuídos quando se conectam a esta WLAN por padrão, como mostrado na imagem:



Note: No exemplo fornecido, é tarefa do servidor RADIUS atribuir um cliente sem fio a uma VLAN específica na autenticação bem-sucedida, portanto, a VLAN configurada no perfil de política pode ser uma VLAN de buraco negro, o servidor RADIUS substitui esse mapeamento e atribui o usuário que vem através dessa WLAN à VLAN especificada no campo do usuário Tunnel-Group-Private-ID no servidor RADIUS.

3. Nos **Advance** , habilite o **Allow AAA Override** para substituir a configuração da WLC quando o servidor RADIUS retornar os atributos necessários para colocar o cliente na VLAN apropriada, como mostrado na imagem:

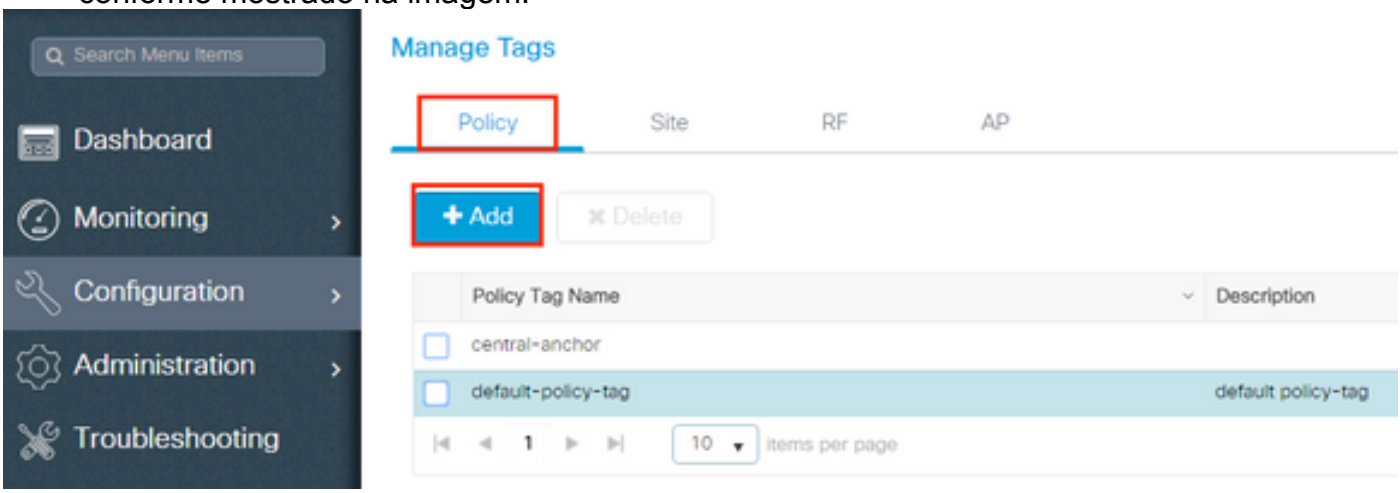


Etapa 5. Configurar a etiqueta de política

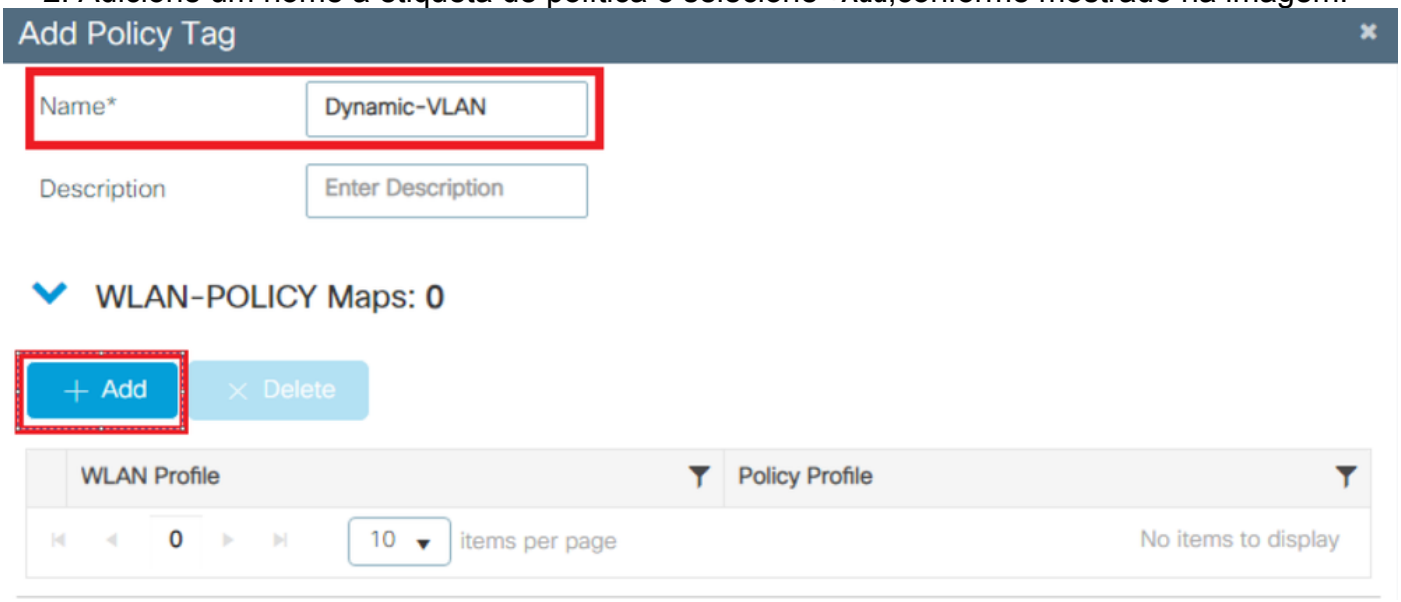
Este procedimento explica como configurar a tag Policy no WLC.

Conclua estes passos:

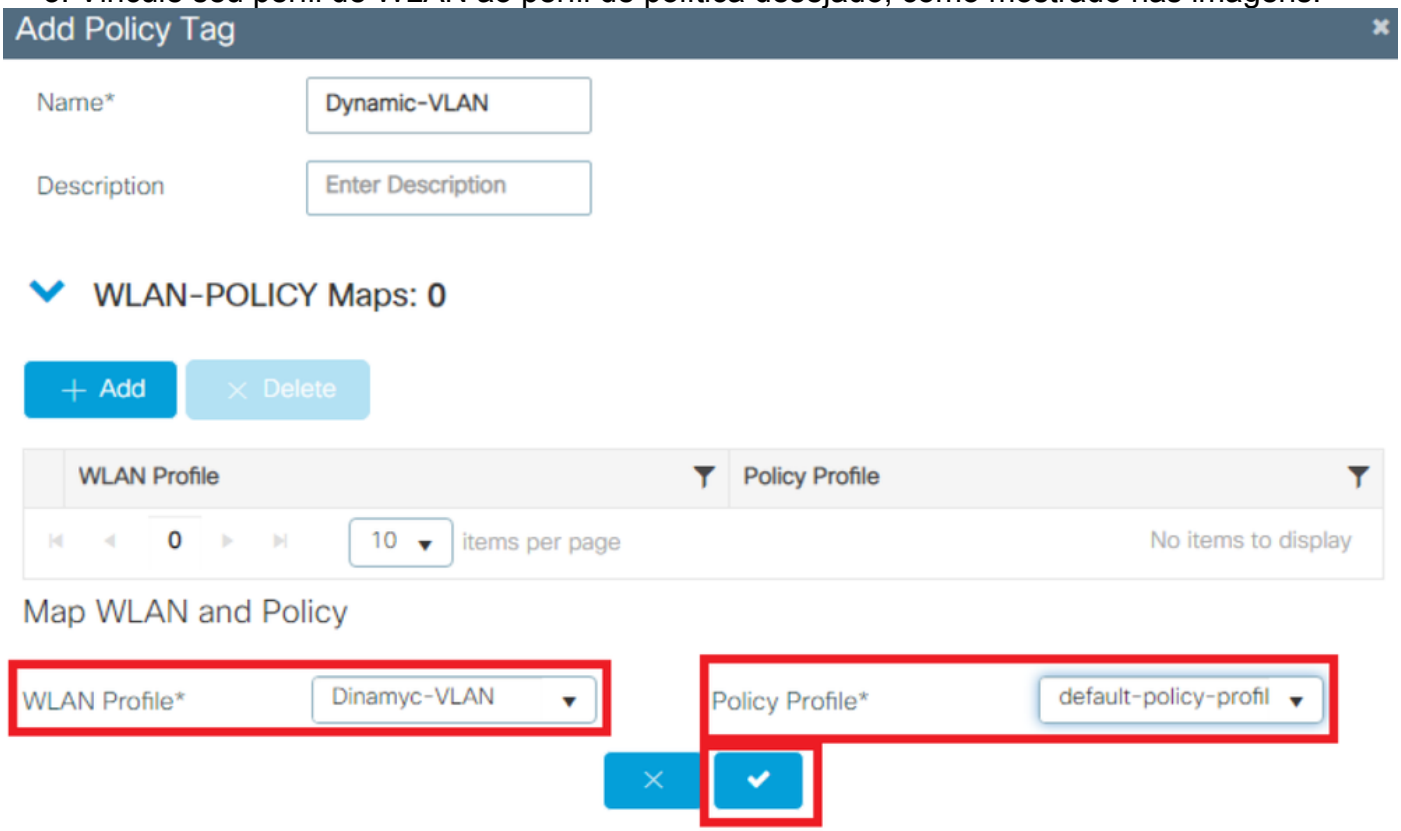
1. Navegar para **Configuration > Tags & Profiles > Tags > Policy** e adicione um novo, se necessário, conforme mostrado na imagem:

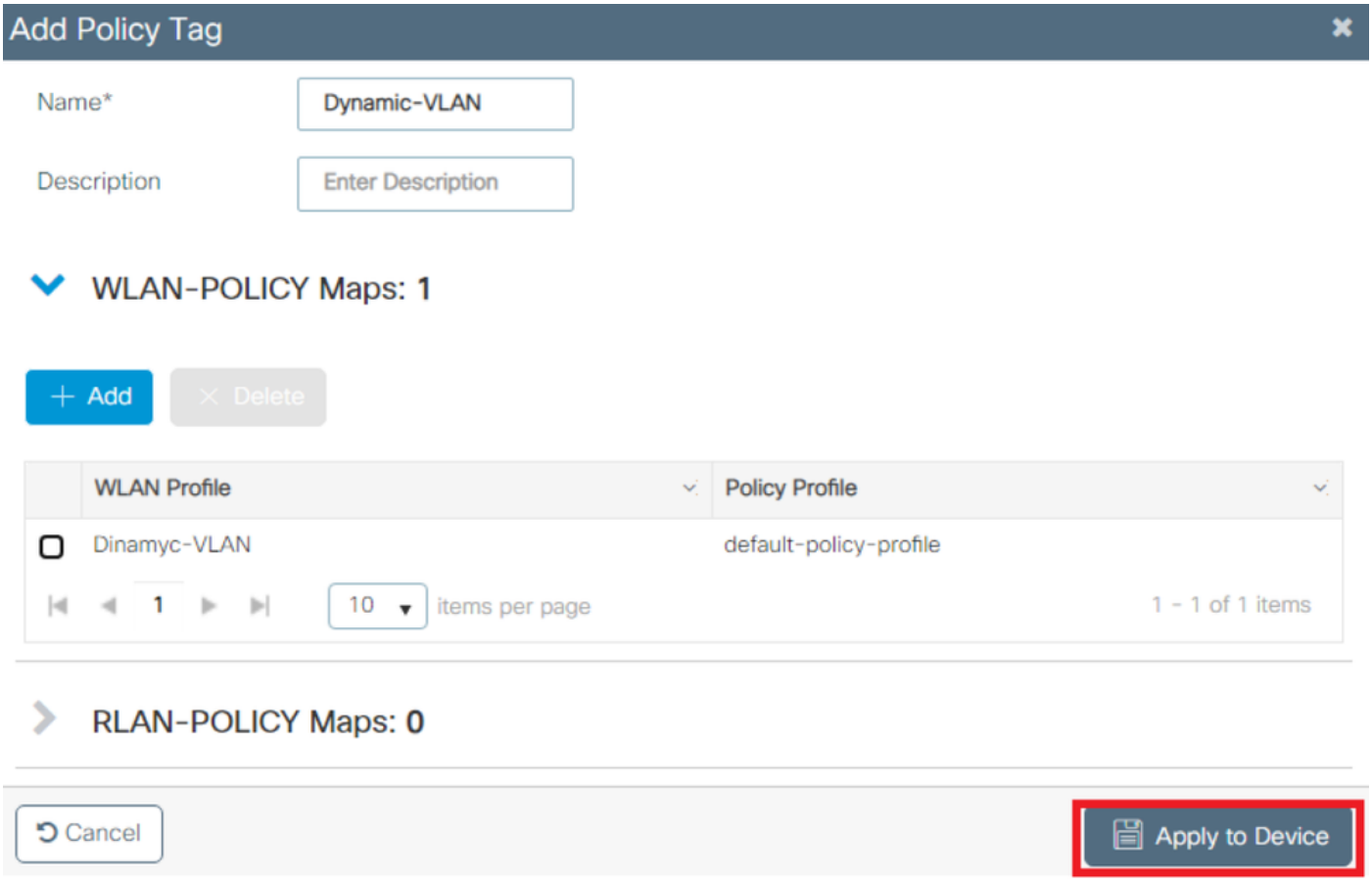


2. Adicione um nome à etiqueta de política e selecione **+Add**,conforme mostrado na imagem:



3. Vincule seu perfil de WLAN ao perfil de política desejado, como mostrado nas imagens:



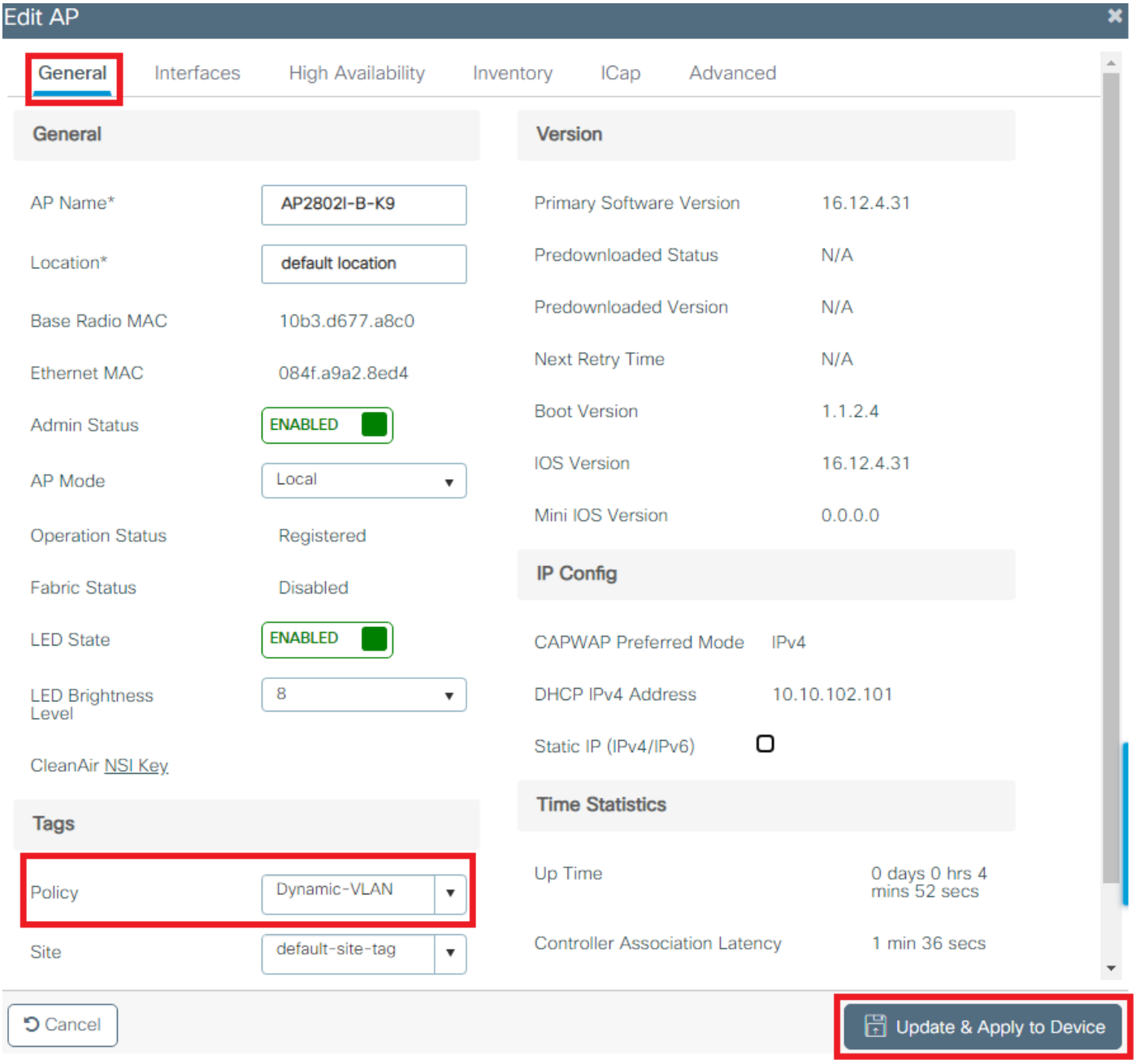


Etapa 6. Atribuir a etiqueta de política a um AP

Este procedimento explica como configurar a tag Policy no WLC.

Conclua estes passos:

1. Navegar para **Configuration > Wireless > Access Points > AP Name > General Tags** atribua a marca de política relevante e selecione **Update & Apply to Device** conforme mostrado na imagem:



Caution: Lembre-se de que quando a etiqueta de política em um AP é alterada, ela descarta sua associação à WLC e se junta novamente.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

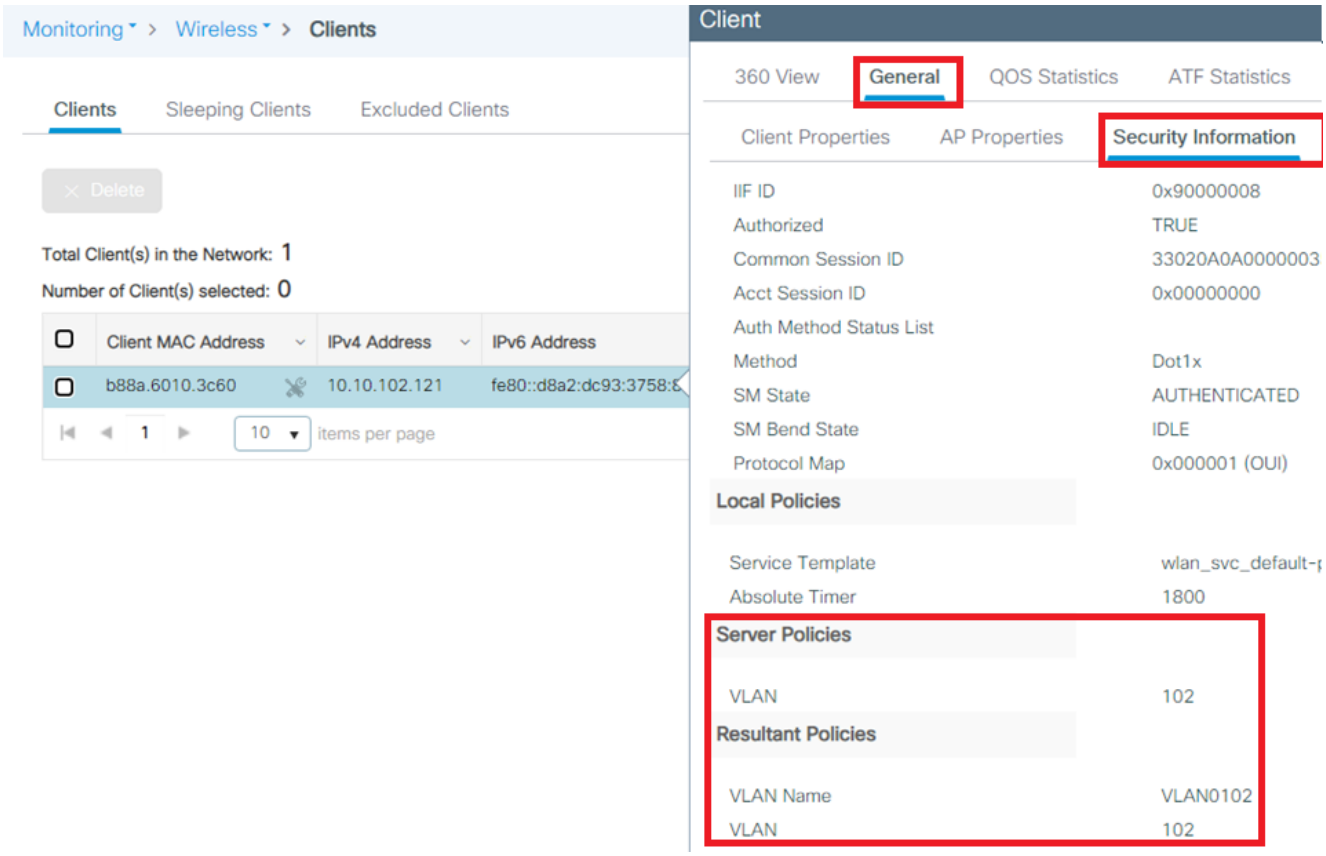
Teste a conexão com o Windows 10 e o suplicante nativo, depois que você for solicitado a inserir um nome de usuário e uma senha, insira as informações do usuário mapeado para uma VLAN no ISE.

No exemplo anterior, observe que jonathga-102 está atribuído à VLAN102 conforme especificado no servidor RADIUS. Este exemplo usa este nome de usuário para receber autenticação e ser atribuído a uma VLAN pelo servidor RADIUS:

Quando a autenticação for concluída, você precisará verificar se o cliente está atribuído à VLAN

adequada de acordo com os atributos RADIUS enviados. Conclua estes passos para realizar esta tarefa:

1. Na GUI do controlador, navegue para **Monitoring > Wireless > Clients > Select the client MAC address > General > Security Information** e procure o campo VLAN conforme mostrado na imagem:



Nessa janela, você pode observar que esse cliente está atribuído à VLAN102 de acordo com os atributos RADIUS configurados no servidor RADIUS.Na CLI, você pode usar o comando **show wireless client summary detail** para exibir as mesmas informações mostradas na imagem:

```
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. Épossível ativar o **Radioactive traces** para garantir a transferência bem-sucedida dos atributos RADIUS para a WLC. Para fazer isso, siga estas etapas: Na GUI do controlador, navegue para **Troubleshooting > Radioactive Trace > +Add**.Digite o endereço Mac do cliente sem fio.Selecionar **Start**.Conecte o cliente à WLAN.Navegar para **Stop > Generate > Choose 10 minutes > Apply to Device > Select the trace file to download the log**.

Esta parte da saída de rastreamento garante uma transmissão bem-sucedida dos 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

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Guia do usuário final