

WLAN FlexConnect com sobreposição de AAA 802.1x nos Catalyst 9800 Wireless Controllers

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração](#)

[Configuração AAA em WLC 9800](#)

[Configuração da WLAN](#)

[Definir AP como modo FlexConnect](#)

[Configuração do Switch](#)

[Configuração do perfil de política](#)

[Configuração da etiqueta de política](#)

[Atribuição de tag de política](#)

[Configuração do ISE](#)

[Verificar](#)

[Troubleshoot](#)

Introduction

Este documento descreve como configurar um controlador de LAN sem fio elástico (WLC 9800) com access points (APs) do modo FlexConnect e uma WLAN (Wireless Local Area Network) 802.1x comutada localmente com substituição de Autenticação, Autorização e Contabilidade (AAA - Virtual Local Area Network).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- modo de configuração de WLC 9800
- FlexConnect

Componentes Utilizados

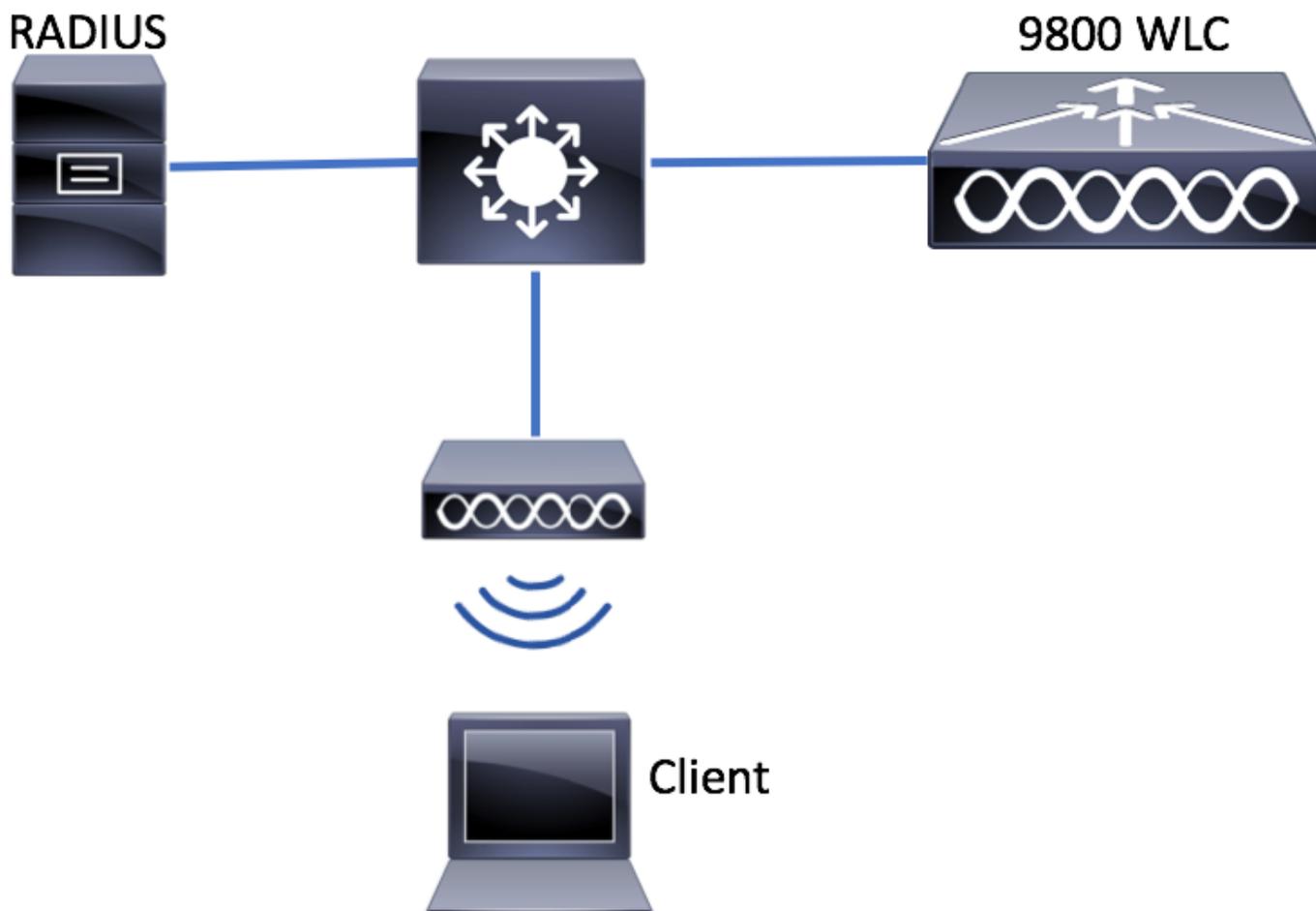
As informações neste documento são baseadas nestas versões de software e hardware:

- WLC 9800 v16.10

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.

Configurar

Diagrama de Rede



Configuração

Configuração AAA em WLC 9800

Você pode seguir as instruções deste link:

[Configuração AAA em WLC 9800](#)

Configuração da WLAN

Você pode seguir as instruções deste link:

[Configuração da WLAN](#)

Definir AP como modo FlexConnect

Diferentemente da configuração do AireOS, na WLC 9800 não é possível configurar o modo local ou flexconnect do AP diretamente. Siga estas etapas para configurar um AP no modo FlexConnect.

GUI

Etapa 1. Configure um perfil Flex.

Navegar para **Configuração > Marcas e perfis > Flex** e modifique o **perfil flex padrão** ou clique em **+Adicionar** para criar um novo.

The screenshot shows the 'Flex Profile' configuration page. On the left, a navigation sidebar has 'Configuration' highlighted with a red box. The main content area is titled 'Flex Profile' and features a '+ Add' button (highlighted in red) and a 'Delete' button. Below these is a table with the following data:

Flex Profile Name	Description
<input type="checkbox"/> default-flex-profile	default profile

At the bottom of the table, there are navigation controls showing '1' items per page and a '10' items per page dropdown.

The screenshot shows the 'Add Flex Profile' form with the 'General' tab selected. The form contains the following fields and options:

Field	Value	Option
Name*	new-flex-profile	Multicast Overridden Interface <input type="checkbox"/>
Description	New flex profile	Fallback Radio Shut <input type="checkbox"/>
Native VLAN ID	2601	ARP Caching <input checked="" type="checkbox"/>
HTTP Proxy Port	0	Efficient Image Upgrade <input checked="" type="checkbox"/>
HTTP-Proxy IP Address	0.0.0.0	CTS Inline Tagging <input type="checkbox"/>
		Office Extend AP <input type="checkbox"/>
		Join Minimum Latency <input type="checkbox"/>

At the bottom, there is a 'Cancel' button and a 'Save & Apply to Device' button (highlighted in red).

Etapa 2. Adicione as VLANs necessárias (as VLANs padrão da WLAN ou as VLANs removidas do ISE).

Nota: Na etapa 3 da seção **Configuração do perfil de política**, você seleciona a VLAN padrão atribuída ao SSID. Se você usar um nome de VLAN nessa etapa, certifique-se de usar o mesmo nome de vlan na configuração do perfil Flex, caso contrário, os clientes não poderão se conectar à WLAN.

Edit Flex Profile

General

Local Authentication

Policy ACL

VLAN

+ Add

✕ Delete

VLAN Name

ID

ACL Name



0



10



items per page

No items to display

Você também pode adicionar ACLs específicas por VLAN.

VLAN Name*

vlan2602

VLAN Id*

2602

ACL Name

Select ACL



✓ Save

↺ Cancel

Opcionalmente, atribua um grupo de servidores Radius para permitir que os APs FlexConnect executem a autenticação local.

Edit Flex Profile

General **Local Authentication** Policy ACL VLAN

Radius Server Group LEAP

EAP Fast Profile PEAP

TLS

RADIUS

Users

Username

10 items per page

No items to display

Etapa 3. Configurar uma etiqueta de site.

Navegue até **Configuration > Tags & Profiles > Tags > Site**. Modifique a **marca de site padrão** (que é a marca atribuída por padrão a todos os APs) ou crie uma nova (Clique em **+Adicionar** para criar uma nova).

Manage Tags

Policy **Site** RF AP

Site Tag Name

default-site-tag

10 items per page

Certifique-se de desabilitar a opção **Enable Local Site**, caso contrário a opção **Flex Profile** não estará disponível.

Add Site Tag

Name*

Description

AP Join Profile

Flex Profile

Enable Local Site

Note: Qualquer AP que obtenha uma Etiqueta de Site com **Ativar Site Local** ativado é configurado como modo local. Da mesma forma, qualquer AP que obtenha uma Etiqueta de Site com **Ativar Local** desabilitado é configurado como modo flexconnect.

Etapa 4. Faça um AP associado à WLC 9800 e atribua a tag Site configurada na Etapa 2.

Navegue até **Configuration > Wireless > Access Points > AP name** e defina a tag Site. Em seguida, clique em **Atualizar e aplicar ao dispositivo** para definir a alteração.

Access Points

All APS

Number of AP(s): 1

AP Name	AP Model	Base Radio MAC	AP Mode	Adm Stat
AP1702-05	AIR-CAP1702I-A-K9	00:c0:00:00:00:00	Local	En

Edit AP

General

AP Name*

Location*

Base Radio MAC

Ethernet MAC

Admin Status

AP Mode

Operation Status

Fabric Status

Tags

Policy

Site

RF

Observação: lembre-se de que, depois de alterar a marca em um AP, ela perde sua associação com a WLC 9800 e se junta novamente em cerca de 1 minuto.

Etapa 5. Quando o AP se juntar novamente, observe que o modo AP é Flex

The screenshot displays the Cisco ISE GUI. On the left is a navigation sidebar with options: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main area is titled 'Access Points' and shows a table with one AP: AP1702-05, model AIR-CAP1702I-A-K9, Base Radio MAC 00:c8:8b:26:2c:d0, and AP Mode Flex. Below the table are expandable sections for Radios 802.11a/n/ac, Radios 802.11b/g/n, and Dual-Band Radios. On the right, the 'Edit AP' page is open, showing the 'General' tab with fields for AP Name (AP1702-05), Location (default location), Base Radio MAC (00:c8:8b:26:2c:d0), Ethernet MAC (00:f2:8b:89:c2:ac), Admin Status (Enabled), AP Mode (Flex), Operation Status (Registered), and Fabric Status (Disabled). The 'AP Mode' field is highlighted with a red box in both views.

CLI

```
# config t
# wireless profile flex new-flex-profile
# arp-caching
# description "New flex profile"
# native-vlan-id 2601

# config t
# wireless tag site new-flex-site
# flex-profile new-flex-profile
# no local-site
# site-tag new-flex-site

# config t
# ap <eth-mac-address>
# site-tag new-flex-site
Associating site-tag will cause associated AP to reconnect
# exit

#show ap name <ap-name> config general | inc AP Mode
AP Mode                               : FlexConnect
```

Configuração do Switch

Configure a interface do switch à qual o AP está conectado.

```
# config t
# interface <int-id>
# switchport trunk native vlan 2601
# switchport mode trunk
# spanning-tree portfast trunk
# end
```

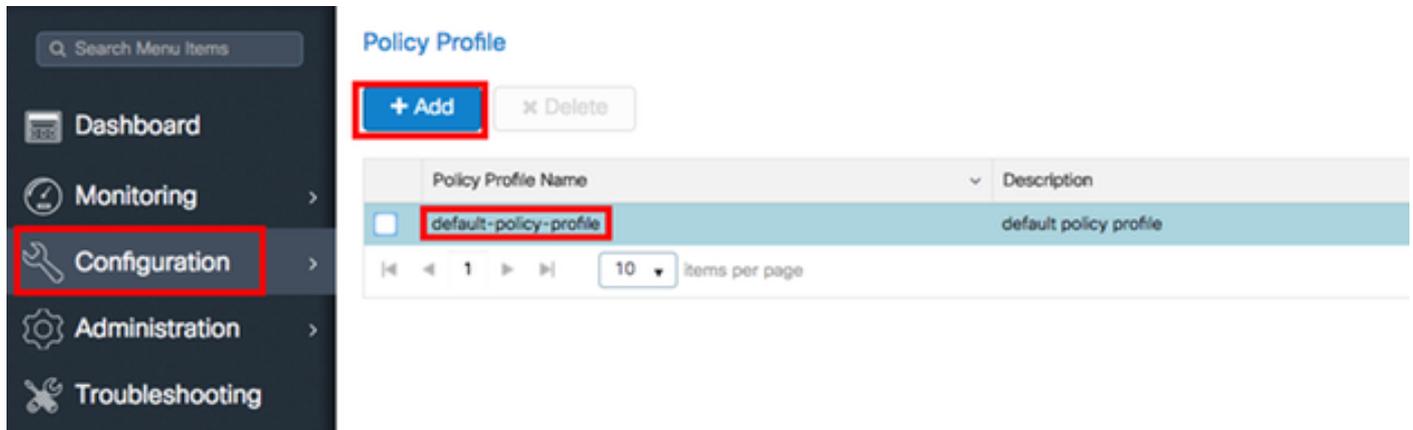
Configuração do perfil de política

Dentro de um perfil de política, você pode decidir a qual VLAN atribui os clientes, entre outras configurações (como Lista de controles de acesso [ACLs], Qualidade de serviço [QoS], Âncora de mobilidade, Temporizadores e assim por diante).

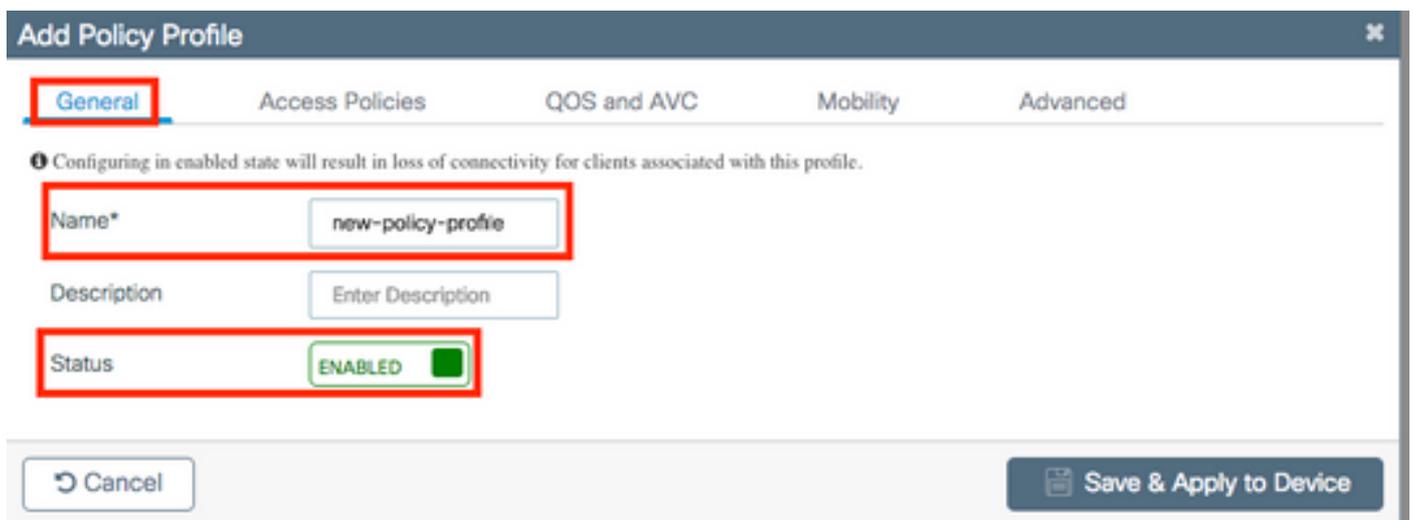
GUI

Etapa 1. Configure o perfil de política a ser atribuído à WLAN.

Navegue até **Configuration > Tags & Profiles > Policy** e crie um novo ou modifique o **default-policy-profile**.



Etapa 2. Na **guia Geral**, atribua um nome ao perfil de política e altere o status para **ATIVADO**.



Etapa 3. Na **guia Políticas de acesso**, atribua a VLAN à qual os clientes sem fio estão atribuídos quando se conectam a esta WLAN por padrão.

Você pode selecionar um nome de VLAN na lista suspensa ou digitar manualmente uma id de vlan.

Observação: se você selecionar um nome de vlan no menu suspenso, verifique se ele corresponde ao nome de vlan usado na etapa 2 da seção **Definir AP como modo FlexConnect**.

Add Policy Profile

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

WLAN Local Profiling

Local HTTP Profiling

Radius HTTP Profiling

Local DHCP Profiling

Local Subscriber Policy Name

VLAN

VLAN/VLAN Group

or

Edit Policy Profile

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

WLAN Local Profiling

Local HTTP Profiling

Radius HTTP Profiling

Local DHCP Profiling

Local Subscriber Policy Name

VLAN

VLAN/VLAN Group

Etapa 4. Navegue até a **guia Avançado** e ative as opções **Ativar e Permitir Substituição de AAA**. A **Comutação Central** deve ser desativada.

A **autenticação central** deve ser habilitada se você quiser que o processo de autenticação seja executado centralmente pela WLC 9800. Desative-o se desejar que os APs FlexConnect autentiquem os clientes sem fio.

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

DHCP Enable

DHCP Server IP Address

DHCP Opt82 Enable

DHCP Opt82 Ascii

DHCP Opt82 RID

DHCP Opt82 Format

DHCP AP MAC

DHCP SSID

DHCP AP ETH MAC

DHCP AP NAME

DHCP Policy Tag

DHCP AP Location

DHCP VLAN ID

AAA Policy

Allow AAA Override

NAC State

Policy Name

Fabric Profile

WLAN Switching Policy

Central Switching

Central Authentication

Central DHCP

Central Association Enable

Flex NAT/PAT

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Cancel

Update & Apply to Device

CLI

```
# config t
# wireless profile policy new-policy-profile # central association # vlan <vlan-id or vlan-name>
```

no shutdown

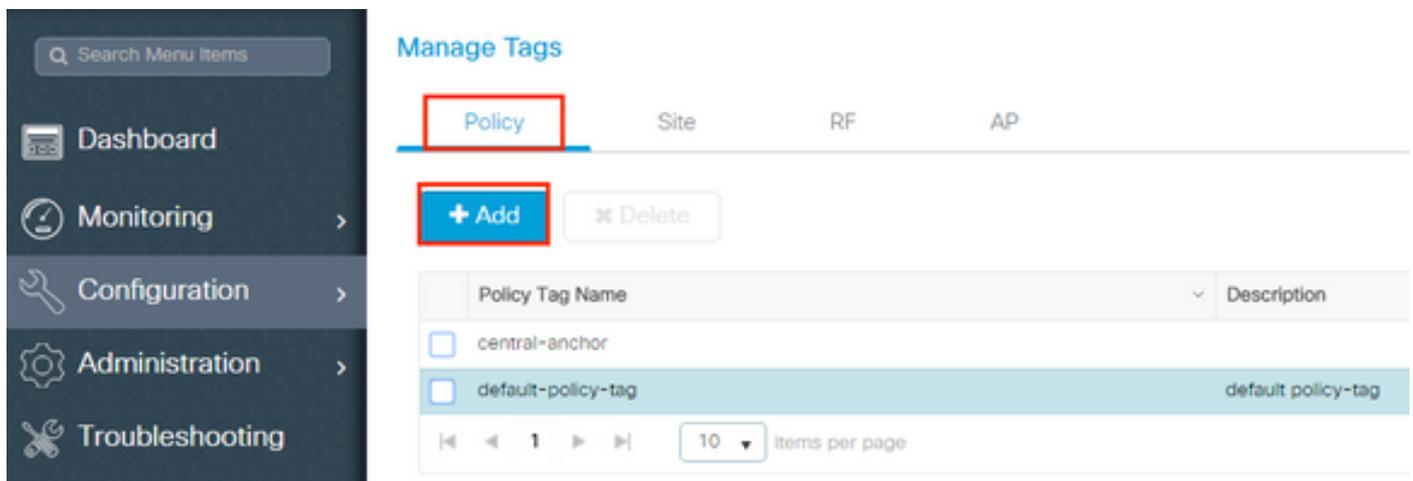
Configuração da etiqueta de política

A etiqueta de política é usada para vincular o SSID ao perfil de política. Você pode criar uma nova etiqueta de política ou usar a marca de política padrão.

Observação: a tag default-policy mapeia automaticamente qualquer SSID com uma ID de WLAN entre 1 e 16 para o perfil de política padrão. Não pode ser modificado nem excluído. Se você tiver uma WLAN com ID 17 ou superior, a tag default-policy não poderá ser usada.

GUI:

Navegue até **Configuration > Tags & Profiles > Tags > Policy** e adicione um novo se necessário.

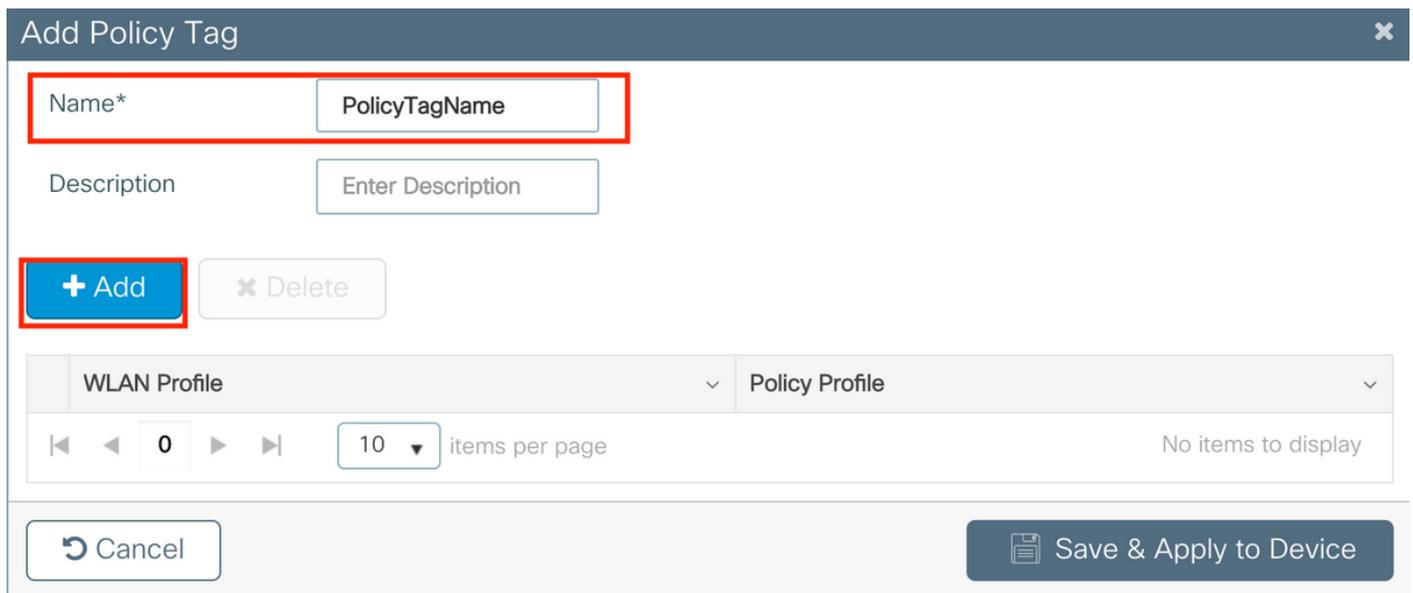


The screenshot shows the 'Manage Tags' interface. On the left is a navigation sidebar with options: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main area is titled 'Manage Tags' and has four tabs: Policy, Site, RF, and AP. The 'Policy' tab is selected and highlighted with a red box. Below the tabs are '+ Add' and 'x Delete' buttons, with the '+ Add' button highlighted in red. A table below shows existing tags:

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

At the bottom of the table, there are navigation arrows and a dropdown menu set to '10 items per page'.

Vincule seu perfil de WLAN ao perfil de política desejado.



The screenshot shows the 'Add Policy Tag' dialog box. It has a title bar with a close button (X). The form contains:

- A 'Name*' field with the value 'PolicyTagName' entered, highlighted with a red box.
- A 'Description' field with the placeholder text 'Enter Description'.
- '+ Add' and 'x Delete' buttons, with the '+ Add' button highlighted in red.
- Two dropdown menus: 'WLAN Profile' and 'Policy Profile', both currently empty.
- Navigation arrows and a dropdown menu set to '10 items per page'.
- The text 'No items to display' on the right side.
- 'Cancel' and 'Save & Apply to Device' buttons at the bottom.

Add Policy Tag ✕

Name*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
◀ ◁ 0 ▷ ▶ <input style="width: 50px;" type="text" value="10"/> items per page No items to display	

Map WLAN and Policy

WLAN Profile*
Policy Profile*

✕
✓

↶ Cancel
📄 Save & Apply to Device

Add Policy Tag ✕

Name*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> prof-name	default-policy-profile
◀ ◁ 1 ▷ ▶ <input style="width: 50px;" type="text" value="10"/> items per page 1 - 1 of 1 items	

↶ Cancel
📄 Save & Apply to Device

CLI:

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

Atribuição de tag de política

Atribuir a marca de política ao AP

GUI

Para atribuir a marca a um AP, navegue para **Configuration > Wireless > Access Points > AP Name > General Tags (Configuração > Sem fio > Pontos de acesso > Nome do AP > Marcas gerais)**, faça a atribuição necessária e clique em **Update & Apply to Device (Atualizar e aplicar ao dispositivo)**.

The screenshot shows the 'Edit AP' configuration page with the following details:

General	Version
AP Name* AP1702-05	Primary Software Version 16.0.0.0
Location* default location	Predownloaded Status N/A
Base Radio MAC 00:c0:00:00:00:00	Predownloaded Version N/A
Ethernet MAC 00:c0:00:00:00:00	Next Retry Time N/A
Admin Status Enabled	Boot Version 15.0.0.0
AP Mode Flex	iOS Version 15.0
Operation Status Registered	Mini iOS Version 0.0.0.0
Fabric Status Disabled	

Tags

Policy	new-policy-tag
Site	new-flex-site
RF	default-rf-tag

IP Config

IP Address	172.16.0.200
Static IP	<input type="checkbox"/>

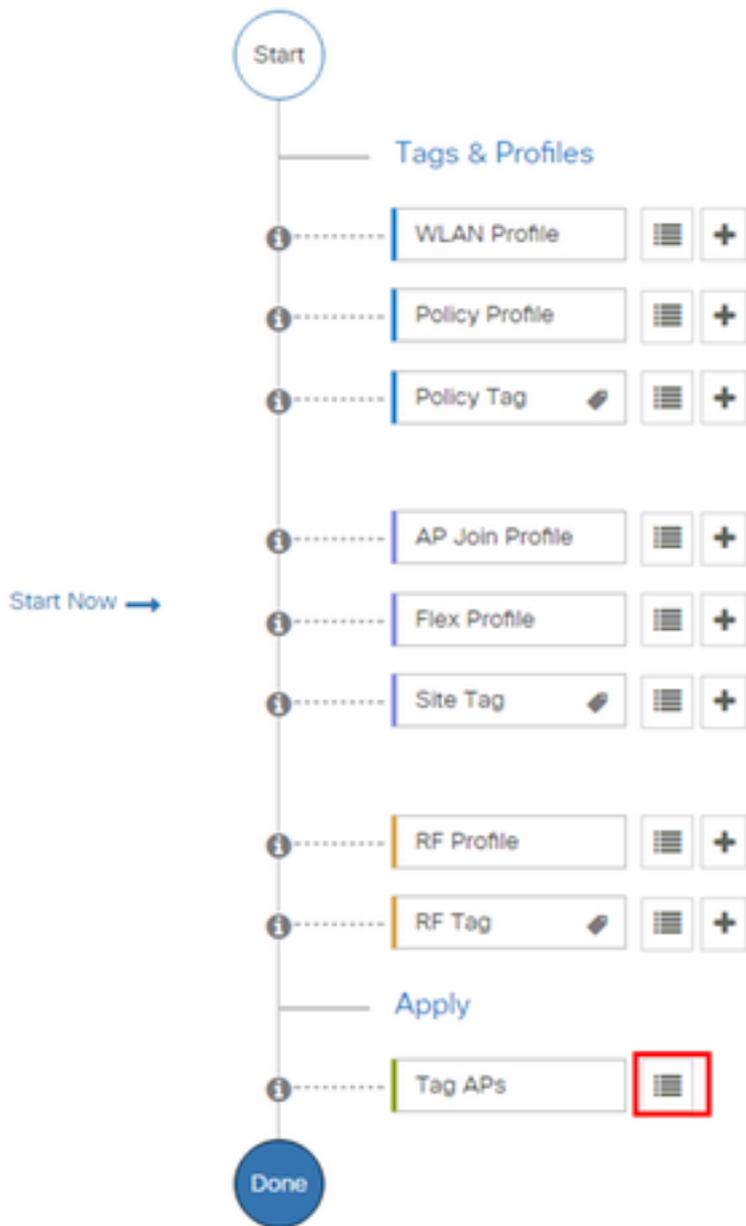
Time Statistics

Up Time	1 days 1 hrs 44 mins 59 secs
Controller Associated Time	0 days 5 hrs 32 mins 5 secs
Controller Association Latency	0 days 20 hrs 11 mins 24 secs

Buttons: Cancel, Update & Apply to Device

Observação: lembre-se de que, depois de alterar a etiqueta de política em um AP, ela perde sua associação ao WLC 9800 e se junta novamente em cerca de 1 minuto.

Para atribuir a mesma etiqueta de política a vários APs, navegue para **Configuration > Wireless > Wireless Setup > Start Now > Apply (Configuração > Sem fio > Configuração sem fio > Iniciar agora > Aplicar)**.



Selecione os APs aos quais deseja atribuir a marca e clique em + Tag APs

+ Tag APs

Number of APs: 3
Selected Number of APs: 3

<input checked="" type="checkbox"/>	AP Name	AP Model	AP MAC	AP Mode	Admin Status	Operation Status	Policy Tag	Site Tag
<input checked="" type="checkbox"/>	AP3802-02-WS	AIR-AP3802I-A-K9	C0-40-00-10-11-00	Local	Enabled	Registered	default-policy-tag	default-site-tag
<input checked="" type="checkbox"/>	AP3802-01	AIR-AP3802I-B-K9	20-40-00-10-11-00	Local	Enabled	Registered	default-policy-tag	default-site-tag
<input checked="" type="checkbox"/>	AP3802-02	AIR-AP3802I-B-K9	C0-40-00-10-11-00	Local	Enabled	Registered	default-policy-tag	default-site-tag

10 items per page 1 - 3 of 3 items

Selecione a etiqueta desejada e clique em **Salvar e aplicar ao dispositivo**

Tag APs [X]

Tags

Policy: default-policy-tag ▼

Site: SiteTag1 ▼

RF: default-rf-tag ▼

Cancel Save & Apply to Device

CLI

```
# config t
# ap <ethernet-mac-addr>
# policy-tag <policy-tag-name>
# end
```

Configuração do ISE

Para a configuração do ISE v1.2, verifique este link:

[Configuração do ISE](#)

Verificar

Você pode usar esses comandos para verificar a configuração atual

```
# show run wlan
# show run aaa
# show aaa servers
# show ap config general
# show ap name <ap-name> config general
# show ap tag summary
# show ap name <AP-name> tag detail
# show wlan { summary | id | name | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
```

Troubleshoot

O WLC 9800 oferece recursos de rastreamento SEMPRE ACESO. Isso garante que todos os erros relacionados à conectividade do cliente, mensagens de nível de aviso e de aviso sejam constantemente registradas e você pode exibir registros de um incidente ou condição de falha depois que ele ocorreu.

Note: Dependendo do volume de registros sendo gerado, você pode voltar algumas horas para vários dias.

Para visualizar os rastreamentos que a WLC 9800 coletou por padrão, você pode se conectar via SSH/Telnet à WLC 9800 e seguir estas etapas (certifique-se de que está fazendo o log da sessão em um arquivo de texto).

Etapa 1. Verifique a hora atual do controlador para que você possa rastrear os registros no tempo até quando o problema ocorreu.

```
# show clock
```

Etapa 2. Colete syslogs do buffer do controlador ou do syslog externo conforme indicado pela configuração do sistema. Isso fornece uma visão rápida da integridade e dos erros do sistema, se houver.

```
# show logging
```

Etapa 3. Verifique se alguma condição de depuração está ativada.

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop
```

```
IOSXE Packet Tracing Configs:
```

```
Packet Infra debugs:
```

```
Ip Address _____ | _____ Port
```

Note: Se você vir alguma condição listada, isso significa que os rastreamentos estão sendo registrados no nível de depuração para todos os processos que encontram as condições habilitadas (endereço mac, endereço ip etc.). Isso aumentaria o volume de registros. Portanto, é recomendável limpar todas as condições quando não a depuração ativa

Etapa 4. Supondo que o endereço mac em teste não estivesse listado como uma condição na Etapa 3, colete os rastreamentos de nível de aviso sempre ativo para o endereço mac específico.

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file  
always-on-<FILENAME.txt>
```

Você pode exibir o conteúdo da sessão ou pode copiar o arquivo para um servidor TFTP externo.

```
# more bootflash:always-on-<FILENAME.txt>  
or  
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

Depuração Condicional e Rastreamento Ativo de Rádio

Se os rastreamentos sempre ativos não fornecerem informações suficientes para determinar o disparo para o problema em investigação, você poderá ativar a depuração condicional e capturar o rastreamento de rádio ativo (RA), que fornecerá rastreamentos de nível de depuração para todos os processos que interagem com a condição especificada (endereço mac do cliente neste caso). Para habilitar a depuração condicional, siga estas etapas.

Etapa 5. Verifique se não há condições de depuração habilitadas.

```
# clear platform condition all
```

Etapa 6. Ative a condição de depuração para o endereço mac do cliente sem fio que você deseja monitorar.

Esses comandos começam a monitorar o endereço mac fornecido por 30 minutos (1800 segundos). Você também pode aumentar esse tempo para até 2085978494 segundos.

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

Observação: para monitorar mais de um cliente por vez, execute o comando `debug wireless mac <aaaa.bbbb.ccc>` por endereço mac.

Nota: Você não vê a saída da atividade do cliente na sessão de terminal, pois tudo é colocado em buffer internamente para ser visualizado posteriormente.

Passo 7. Reproduza o problema ou comportamento que você deseja monitorar.

Etapa 8. Interrompa as depurações se o problema for reproduzido antes que o tempo padrão ou configurado do monitor esteja esgotado.

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

Depois que o monitor-time tiver transcorrido ou a depuração sem fio tiver sido interrompida, a WLC 9800 gera um arquivo local com o nome:

```
ra_trace_MAC_aaaabbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year
```

Etapa 9. Colete o arquivo da atividade de endereço MAC. Você pode copiar o arquivo .log do rastro para um servidor externo ou exibir a saída diretamente na tela.

Verifique o nome do arquivo de rastreamento RA

```
# dir bootflash: | inc ra_trace
```

Copie o arquivo para um servidor externo:

```
# copy bootflash:ra_trace_MAC_aaaabbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log  
tftp://a.b.c.d/ra-FILENAME.txt
```

Exibir o conteúdo:

```
# more bootflash:ra_trace_MAC_aaaabbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Etapa 10. Se a causa raiz ainda não for óbvia, colete os logs internos, que são uma visão mais detalhada dos logs de nível de depuração. Você não precisa depurar o cliente novamente, pois estamos somente analisando detalhadamente os logs de depuração que já foram coletados e armazenados internamente.

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> }  
to-file ra-internal-<FILENAME>.txt
```

Note: Essa saída de comando retorna rastreamentos para todos os níveis de registro para todos os processos e é bastante volumosa. Entre em contato com o Cisco TAC para ajudar a analisar esses rastreamentos.

Você pode copiar o ra-internal-FILENAME.txt para um servidor externo ou exibir a saída diretamente na tela.

Copie o arquivo para um servidor externo:

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

Exibir o conteúdo:

```
# more bootflash:ra-internal-<FILENAME>.txt
```

Etapa 11. Remova as condições de depuração.

```
# clear platform condition all
```

Note: Certifique-se de sempre remover as condições de depuração após uma sessão de solução de problemas.