

# Configurar a autenticação 802.1X no Catalyst 9800 Wireless Controller Series

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração de WLC](#)

[Configuração de AAA em 9800 WLCs](#)

[Configuração do perfil da WLAN](#)

[Configuração de perfil de política](#)

[Configuração de marca de política](#)

[Atribuição de tag de política](#)

[Configuração do ISE](#)

[Declarar o WLConISE](#)

[Criar novo usuário no ISE](#)

[Criar perfil de autorização](#)

[Criar um conjunto de políticas](#)

[Criar Política de Autenticação](#)

[Criar Política de Autorização](#)

[Verificar](#)

[Troubleshooting](#)

[Solucionar problemas no WLC](#)

[Solução de problemas no ISE](#)

---

## Introdução

Este documento descreve como configurar uma WLAN com segurança 802.1X em um Cisco Catalyst 9800 Series Wireless Controller.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- 802.1X

### Componentes Utilizados

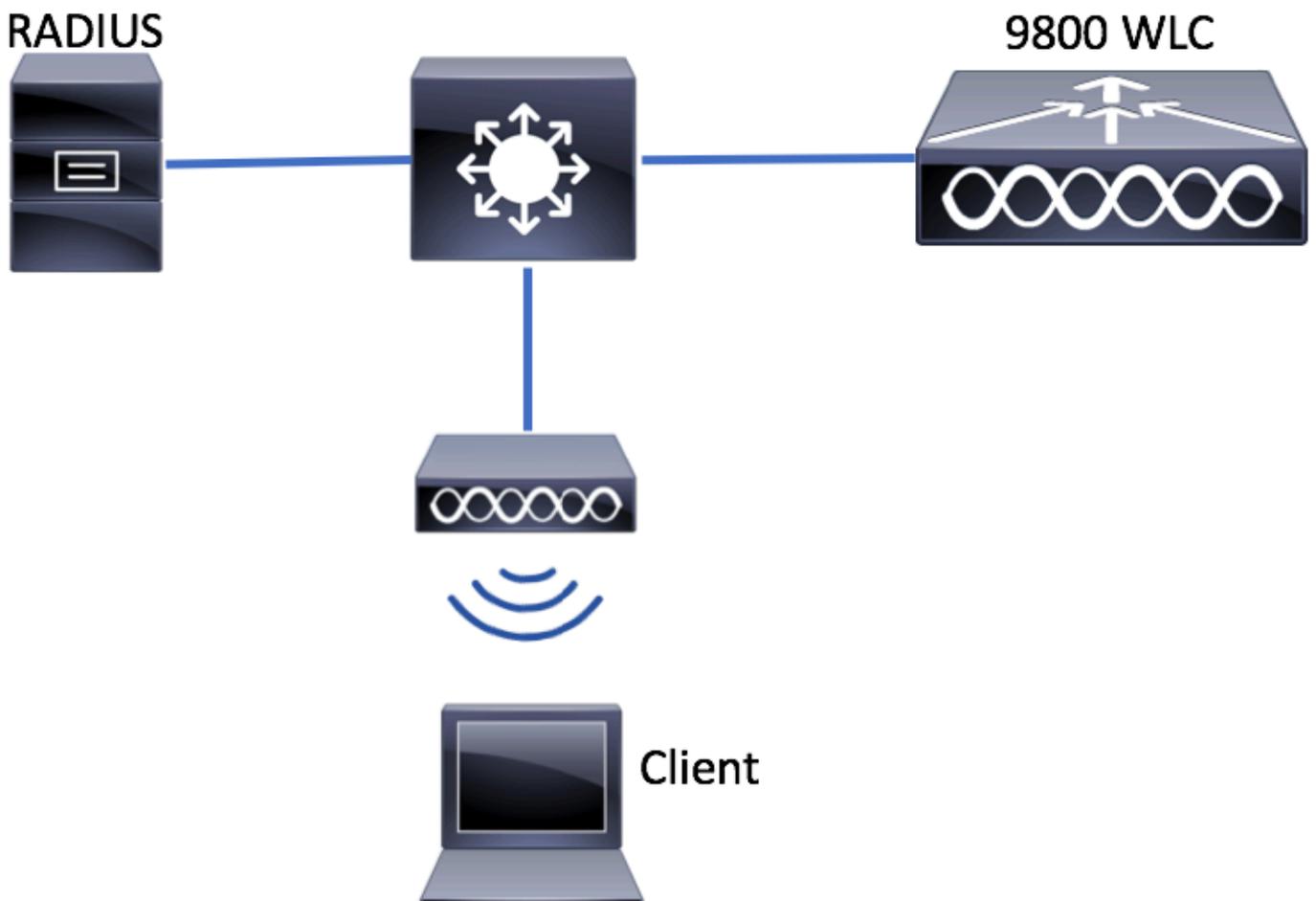
As informações neste documento são baseadas nestas versões de software e hardware:

- Série de controladores sem fio Catalyst 9800 (Catalyst 9800-CL)
- Cisco IOS® XE Gibraltar 17.3.x
- Cisco ISE 3.0

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Configurar

### Diagrama de Rede

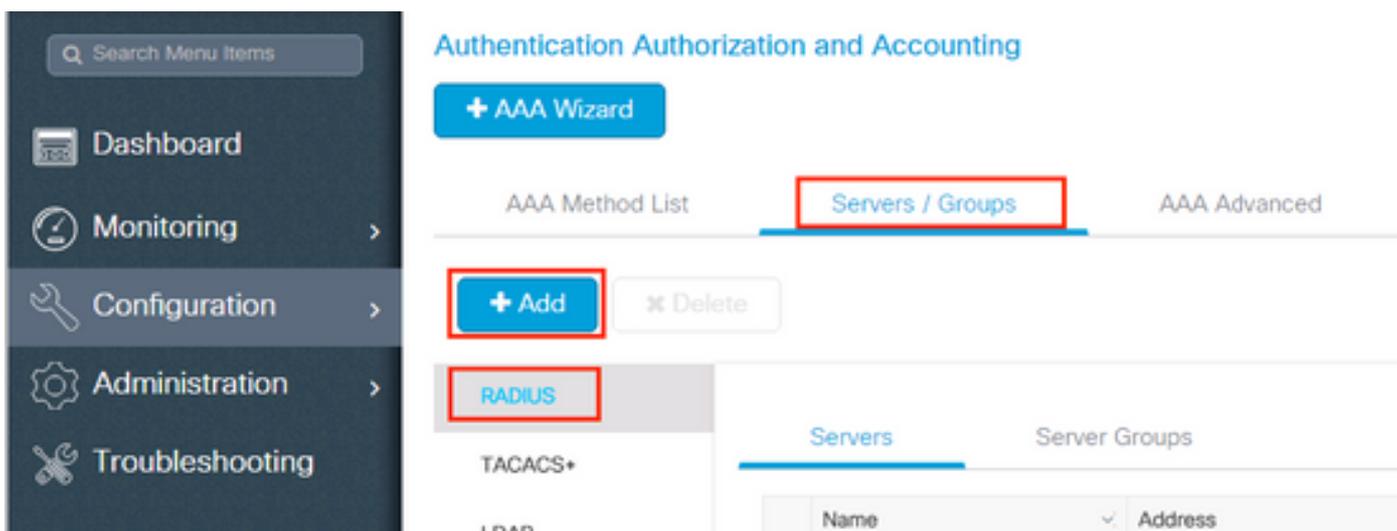


### Configuração de WLC

#### Configuração de AAA em 9800 WLCs

GUI:

Etapa 1. Declarar servidor RADIUS. Navegue **Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add** e insira as informações do servidor RADIUS.



Certifique-se de que o **Suporte para CoA** esteja habilitado se você planeja usar a Autenticação da Web Central (ou qualquer tipo de segurança que exija a Alteração de Autorização [CoA]) no futuro.

The screenshot shows the 'Create AAA Radius Server' form. It has a dark header bar with the title 'Create AAA Radius Server' and a close button. The form contains several input fields and checkboxes. The fields are: Name\* (ISE-kcg), IP V4/IP v6 Server Address\* (172.16.0.11), Shared Secret\* (masked with dots), Confirm Shared Secret\* (masked with dots), Auth Port (1812), Acct Port (1813), Server Timeout (seconds) (1-1000), and Retry Count (0-100). There are two checkboxes: 'Clear PAC Key' and 'Set New PAC Key', both of which are unchecked. The 'Support for CoA' checkbox is checked, and the text 'ENABLED' is displayed next to it. At the bottom of the form, there are two buttons: 'Cancel' and 'Save & Apply to Device' (highlighted with a red box).

Etapa 2. Adicione o servidor RADIUS a um grupo RADIUS. Navegue para **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add**. Dar um nome ao seu grupo e mova o servidor criado anteriormente na lista de **Assigned Servers**.

### Create AAA Radius Server Group

Name\*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Available Servers

Assigned Servers

Etapa 3. Crie uma lista de métodos de autenticação. Navegue até **Configuration > Security > AAA > AAA Method List > Authentication > + Add**.

The screenshot shows the 'Authentication Authorization and Accounting' configuration page. On the left is a dark sidebar with menu items: Dashboard, Monitoring, Configuration (highlighted with a red box), and Administration. The main content area has a blue header and a '+ AAA Wizard' button. Below that, 'AAA Method List' is highlighted with a red box. Underneath, the 'Authentication' tab is selected and highlighted with a red box. To the right of the 'Authentication' tab, a '+ Add' button is highlighted with a red box. A 'Servers / Groups' section is visible to the right of the main content area.

Inserir informações:

Quick Setup: AAA Authentication

Method List Name\*

Type\*

Group Type

Fallback to local

Available Server Groups

- radius
- ldap
- tacacs+
- ISE-kcg-grp

Assigned Server Groups

- ISE-grp-name

**CLI:**

```
# config t # aaa new-model # radius server <radius-server-name> # address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813 # timeout 300 # retransmit 3
# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>
# aaa authentication dot1x <dot1x-list-name> group <radius-grp-name>
```

**Observação sobre a detecção de servidor inativo AAA**

Depois de configurar o servidor RADIUS, você pode verificar se ele é considerado "ATIVO":

```
#show aaa servers | s WNCDC Platform State from WNCDC (1) : current UP Platform State from WNCDC (2) : current
```

Você pode configurar o, assim **dead criteria**, como o, **deadtime** em sua WLC, especialmente se você usar vários servidores RADIUS.

```
#radius-server dead-criteria time 5 tries 3 #radius-server deadtime 5
```

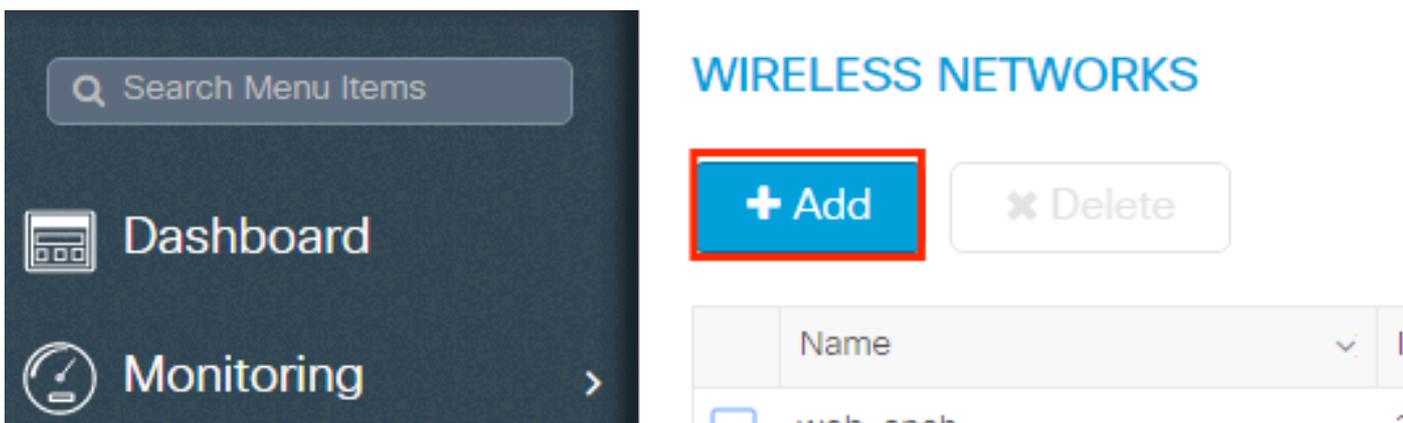
 **Observação: dead criteria** os critérios usados para marcar um servidor RADIUS como inativo. É composto por: 1. Um tempo limite (em segundos) que representa a quantidade de tempo que deve decorrer do momento em que o controlador recebeu um pacote válido do servidor RADIUS pela última vez até o momento em que o servidor é marcado como inativo. 2. Um contador, que representa o número de tempos limite consecutivos que devem ocorrer no controlador antes que o servidor RADIUS seja marcado como inativo.

 **Observação:** o **deadtime** especifica o tempo (em minutos) que o servidor permanece no status inativo depois que o dead-criteria o marca como inativo. Quando o tempo de inatividade expirar, o controlador marcará o servidor como ATIVO (ATIVO) e notificará os clientes registrados sobre a alteração de estado. Se o servidor ainda estiver inacessível depois que o estado for marcado como ATIVO e se os critérios de inatividade forem atendidos, o servidor será marcado como inativo novamente para o intervalo de tempo de inatividade.

Configuração do perfil da WLAN

## GUI:

Etapa 1. Criar a WLAN. Navegue até **Configuration > Wireless > WLANs > + Add** e configure a rede conforme necessário.



Etapa 2. Insira as informações da WLAN

### Add WLAN

**General**      Security      Advanced

Profile Name*	<input type="text" value="prof-name"/>	Radio Policy	<input type="text" value="All"/>
SSID	<input type="text" value="ssid-name"/>	Broadcast SSID	<input checked="" type="checkbox"/> ENABLED
WLAN ID*	<input type="text" value="1"/>		
Status	<input checked="" type="checkbox"/> ENABLED		

Etapa 3. Navegue até a guia Segurança e selecione o método de segurança necessário. Nesse caso, **WPA2 + 802.1x**.

**Add WLAN** [Close]

General      **Security**      Advanced

Layer2      Layer3      AAA

Layer 2 Security Mode      WPA + WPA2 ▼

MAC Filtering     

Protected Management Frame

Fast Transition      Adaptive Enab... ▼

Over the DS     

Reassociation Timeout      20

PMF      Disabled ▼

WPA Parameters

WPA Policy     

[Cancel]      [Save & Apply to Device]

**Add WLAN** [Close]

PMF      Disabled ▼

WPA Parameters

WPA Policy     

WPA2 Policy     

WPA2 Encryption

AES(CCMP128)     

CCMP256     

GCMP128     

GCMP256     

Auth Key Mgmt      802.1x ▼

[Cancel]      [Save & Apply to Device]

Etapa 4. Na **Security** > **AAA** guia, selecione o método de autenticação criado na Etapa 3 da seção AAA Configuration on 9800 WLC.

**Add WLAN**

General      **Security**      Advanced

Layer2      Layer3      **AAA**

Authentication List: list-name

Local EAP Authentication:

Cancel      Save & Apply to Device

**CLI:**

```
# config t # wlan <profile-name> <wlan-id> <ssid-name> # security dot1x authentication-list <dot1x-list-name> # no shutdown
```

Configuração de perfil de política

Dentro de um Perfil de política, você pode decidir a qual VLAN atribuir os clientes, entre outras configurações (como Lista de controles de acesso [ACLs], Qualidade de serviço [QoS], Âncora de mobilidade, Temporizadores, etc.).

Você pode usar seu perfil de política padrão ou criar um novo perfil.

**GUI:**

Navegue para **Configuration > Tags & Profiles > Policy Profile** e configure seu **default-policy-profile** ou crie um novo.

**Policy Profile**

**+ Add**      Delete

Policy Profile Name	Description
<input type="checkbox"/> voice	
<input type="checkbox"/> <b>default-policy-profile</b>	default policy profile

1 items per page

Verifique se o perfil está ativado.

Além disso, se o ponto de acesso (AP) estiver no modo local, verifique se o perfil de política tem **Central Switching** e **Central Authentication** ativados.

### Edit Policy Profile

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

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name*	default-policy-profile	<b>WLAN Switching Policy</b>	
Description	default policy profile	Central Switching	<input checked="" type="checkbox"/>
Status	ENABLED <input checked="" type="checkbox"/>	Central Authentication	<input checked="" type="checkbox"/>
Passive Client	<input type="checkbox"/> DISABLED	Central DHCP	<input checked="" type="checkbox"/>
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED	Central Association Enable	<input checked="" type="checkbox"/>
<b>CTS Policy</b>		Flex NAT/PAT	<input type="checkbox"/>
Inline Tagging	<input type="checkbox"/>		
SGACL Enforcement	<input type="checkbox"/>		
Default SGT	2-65519		

Selecione a VLAN à qual os clientes precisam ser atribuídos na guia **Access Policies**.

## Edit Policy Profile

General

**Access Policies**

QOS and AVC

Mobility

Advanced

### WLAN Local Profiling

HTTP TLV Caching

RADIUS Profiling

DHCP TLV Caching

Local Subscriber Policy Name

Search or Select



### VLAN

VLAN/VLAN Group

VLAN2602



Multicast VLAN

Enter Multicast VLAN

### WLAN ACL

IPv4 ACL

Search or Select



IPv6 ACL

Search or Select



### URL Filters

Pre Auth

Search or Select



Post Auth

Search or Select



Se você planeja ter atributos de retorno ISE no Access-Accept como atribuição de VLAN, habilite a substituição de AAA na **Advanced** guia:

✕
Edit Policy Profile

---

General
Access Policies
QOS and AVC
Mobility
Advanced

**WLAN Timeout**

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

**DHCP**

IPv4 DHCP Required

DHCP Server IP Address

[Show more >>>](#)

**AAA Policy**

Allow AAA Override

NAC State

Policy Name

Fabric Profile

Umbrella Parameter Map

mDNS Service Policy  [Clear](#)

**WLAN Flex Policy**

VLAN Central Switching

Split MAC ACL

**Air Time Fairness Policies**

2.4 GHz Policy

5 GHz Policy

↶ Cancel

↵
Update & Apply to Device

**CLI:**

```
# config # wireless profile policy <policy-profile-name>
# aaa-override # central switching # description "<description>" # vlan <vlanID-or-VLAN_name> # no shutdown
```

**Configuração de marca de política**

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

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

**GUI:**

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

Search Menu Items

Dashboard

Monitoring >

Configuration >

Administration >

Troubleshooting

### Manage Tags

Policy Site RF AP

+ Add x Delete

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

1 10 items per page

Vincule o perfil de WLAN ao perfil de política desejado.

### Add Policy Tag

Name\* PolicyTagName

Description Enter Description

+ Add x Delete

WLAN Profile Policy Profile

0 10 items per page No items to display

Cancel Save & Apply to Device

**Add Policy Tag** ✕

Name\*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
<span>◀ ◁ 0 ▷ ▶</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">10</span> items per page <span style="float: right;">No items to display</span>	

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 ▷ ▶ 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

Atribua a marca de política aos APs necessários.

**GUI:**

Para atribuir a marca a um AP, navegue para **Configuration > Wireless > Access Points > AP Name > General Tags**, atribuir a marca de política relevante e clique em **Update & Apply to Device**.

The screenshot shows the 'Edit AP' configuration window with the 'General' tab selected. The 'Policy' dropdown menu is highlighted with a red box, showing 'default-policy-tag' as the selected option. Other fields include AP Name (AP3802-02-WS), Location (default location), Base Radio MAC (00:42:68:c6:41:20), Ethernet MAC (00:42:68:a0:d0:22), Admin Status (Enabled), AP Mode (Local), Operation Status (Registered), and Fabric Status (Disabled). The 'Version' section shows Primary Software Version (10.0.200.50), Predownloaded Status (N/A), Predownloaded Version (N/A), Next Retry Time (N/A), Boot Version (1.0.0), IOS Version (10.0.200.52), and Mini IOS Version (0.0.0.0). The 'IP Config' section shows IP Address (172.16.0.207) and Static IP (unchecked). The 'Time Statistics' section shows Up Time (9 days 1 hrs 17 mins 24 secs), Controller Associated Time (0 days 3 hrs 26 mins 41 secs), and Controller Association Latency (8 days 21 hrs 50 mins 33 secs). At the bottom, the 'Update & Apply to Device' button is highlighted with a red box.

 **Observação:** lembre-se de que quando a marca de política em um AP é alterada, ele descarta sua associação com a WLC 9800 e se junta alguns momentos depois.

Para atribuir a mesma Policy Tag a vários APs, navegue até **Configuration > Wireless Setup > Advanced > Start Now > Apply**.

Start

## Tags & Profiles



WLAN Profile



Policy Profile



Policy Tag



AP Join Profile



Start Now →



Flex Profile



Site Tag



RF Profile



RF Tag



## Apply



Tag APs



Done

consiste em um conjunto de atributos que são retornados quando uma condição é correspondida. O perfil de autorização determina se o cliente tem acesso ou não à rede, envia Listas de Controle de Acesso (ACLs), substituições de VLAN ou qualquer outro parâmetro. O perfil de autorização mostrado neste exemplo envia uma aceitação de acesso para o cliente e atribui o cliente à VLAN 1416.

Etapa 1. Navegue **Policy > Policy Elements > Results > Authorization > Authorization Profiles** e clique no **Add** botão.

The screenshot displays the Cisco ISE web interface. The breadcrumb navigation path is **Policy > Policy Elements > Results > Authorization > Authorization Profiles**. The 'Results' tab is selected in the top navigation bar. The left sidebar shows the 'Authorization' menu expanded to 'Authorization Profiles'. The main content area is titled 'Standard Authorization Profiles' and includes a table of existing profiles.

<input type="checkbox"/>	Name	Profile	Description
<input type="checkbox"/>	Authz_Profile_IPSK	Cisco	
<input type="checkbox"/>	Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices. Ensure that you configu
<input type="checkbox"/>	Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.

Etapa 2. Insira os valores conforme mostrado na imagem. Aqui podemos retornar atributos de substituição AAA como VLAN, por exemplo. A WLC 9800 aceita os atributos de túnel 64, 65, 81, que usam o ID ou o nome da VLAN, e aceita também o uso do **AirSpace-Interface-Name** atributo.

Cisco ISE Policy - Policy Elements Evaluation Mode 85 Days

Dictionarys Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > PermitAccessVlan1416

Authorization Profile

\* Name PermitAccessVlan1416

Description

\* Access Type ACCESS\_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

Common Tasks

Security Group

VLAN Tag ID 1 Edit Tag ID/Name 1416

Voice Domain Permission

Advanced Attributes Settings

Select an item

Attributes Details

Access Type = ACCESS\_ACCEPT

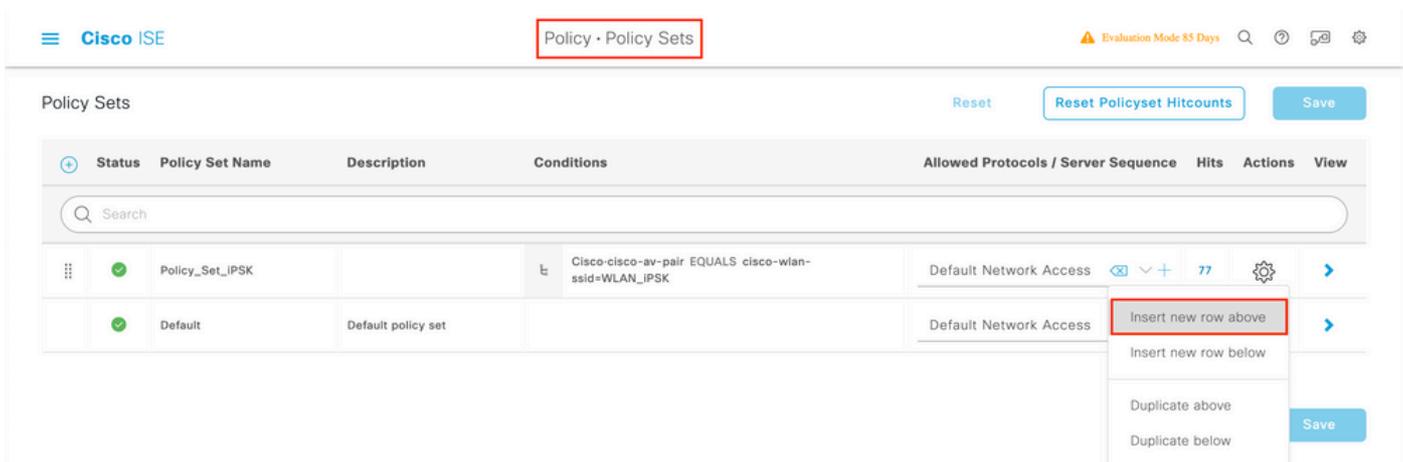
Tunnel-Private-Group-ID = 1:1416

Tunnel-Type = 1:13

Tunnel-Medium-Type = 1:6

## Criar um conjunto de políticas

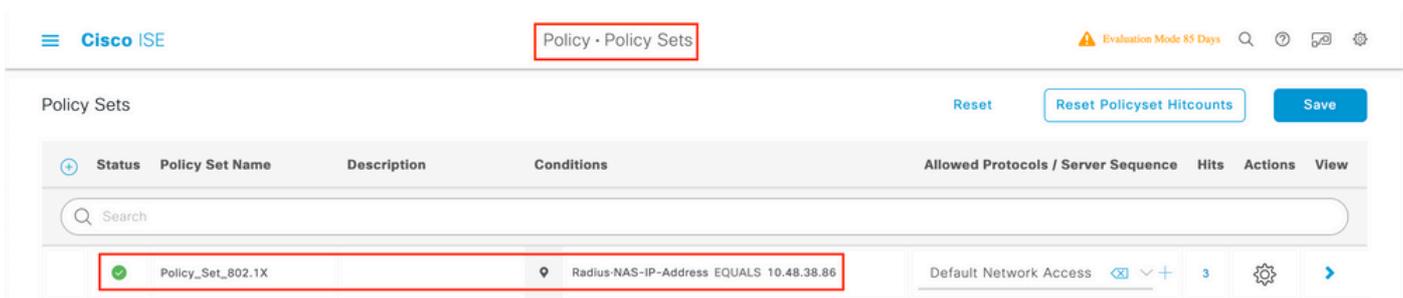
Um conjunto de políticas define uma coleção de regras de Autenticação e Autorização. Para criar um, vá para **Policy > Policy Sets**, clique na engrenagem do primeiro conjunto de políticas na lista e selecione **Insert new row above** como mostrado nesta imagem:



Configure um nome e crie uma condição para este Conjunto de políticas. Neste exemplo, a condição específica que correspondamos ao tráfego que vem da WLC:

Radius:NAS-IP-Address EQUALS X.X.X.X // X.X.X.X is the WLC IP address

Verifique se **Default Network Access** está selecionado em **Allowed Protocols / Server Sequence**.



### Criar Política de Autenticação

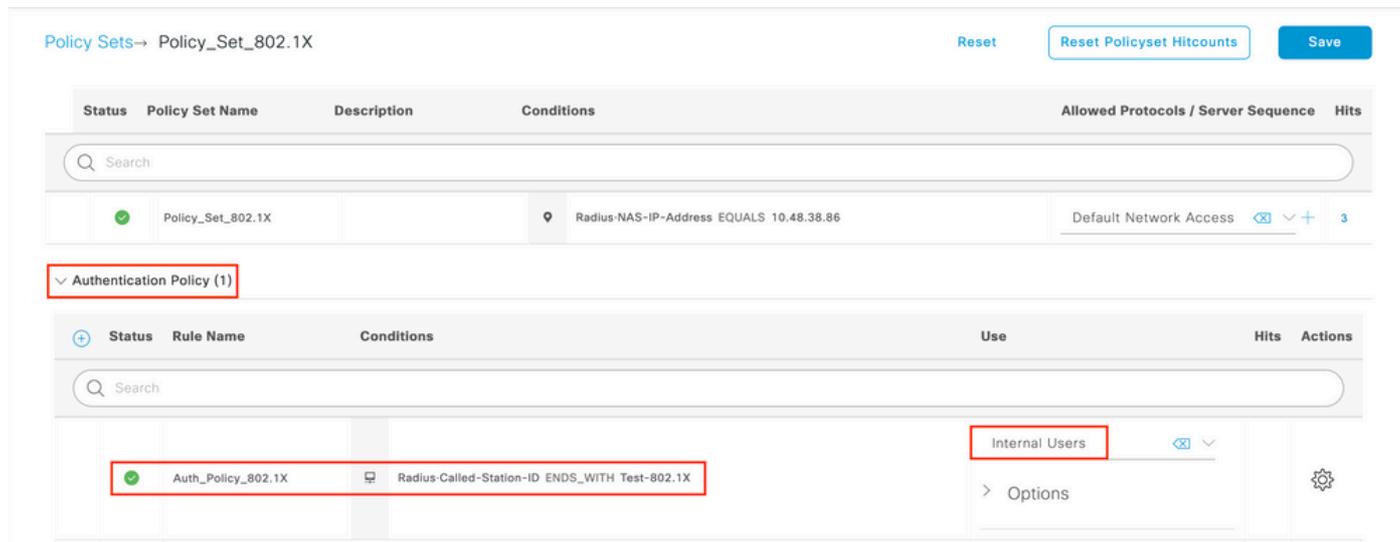
Para configurar as políticas de Autenticação e Autorização, você precisa inserir a configuração do Conjunto de Políticas. Isso pode ser feito se você clicar na seta azul à direita da **Policy Set** linha:



**As políticas de autenticação** são usadas para verificar se as credenciais dos usuários estão corretas (verifique se o usuário realmente é quem diz ser). Em **Authenticaton Policy**, crie uma política de autenticação e configure-a como mostrado nesta imagem. A condição para a política usada neste exemplo é:

RADIUS:Called-Station-ID ENDS\_WITH <SSID> // <SSID> is the SSID of your WLAN

Além disso, escolha **Internal Users** na Use guia Authentication Policy.

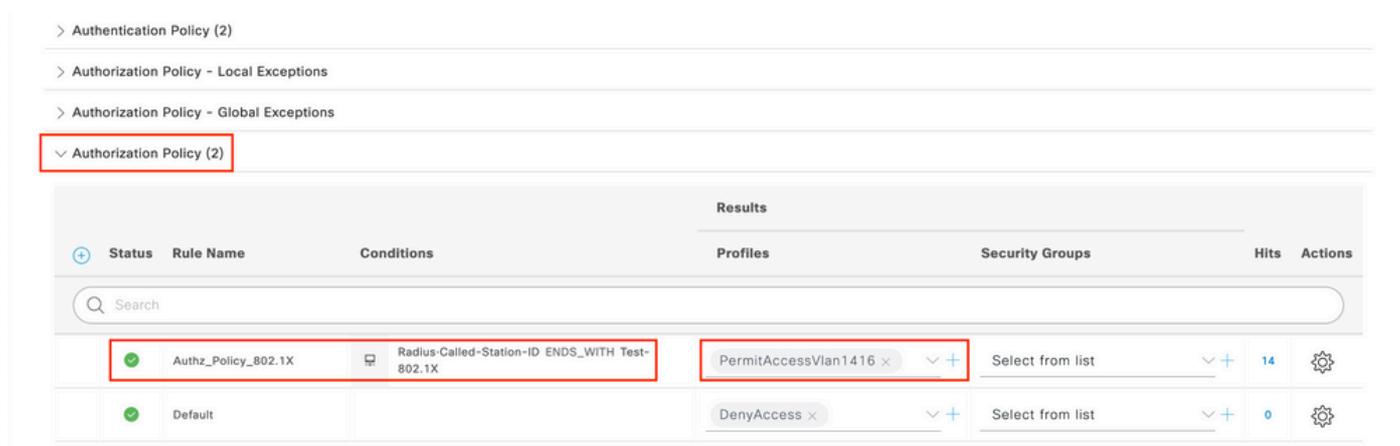


### Criar Política de Autorização

Na mesma página, vá para **Authorization Policy** e crie uma nova. A condição para esta Diretiva de Autorização é:

RADIUS:Called-Station-ID ENDS\_WITH <SSID> // <SSID> is the SSID of your WLAN

Na **Result > Profiles** guia dessa diretiva, selecione a **Authorization Profile** que você criou anteriormente. Isso faz com que o ISE envie os atributos corretos para a WLC se o usuário estiver autenticado.



Neste ponto, toda a configuração da WLC e do ISE está concluída, você pode tentar se conectar a um cliente.

Para obter mais informações sobre as políticas de permissão de protocolos do ISE, consulte o capítulo: Manage Authentication Policies from the Cisco Identity Services Engine Administrator Guide [Manage Authentication Policies](#)

Para obter mais informações sobre as fontes de identidade do ISE, consulte o capítulo: Manage Users and External Identity Sources no Cisco Identity Services Engine Administrator Guide: [Identity Sources](#)

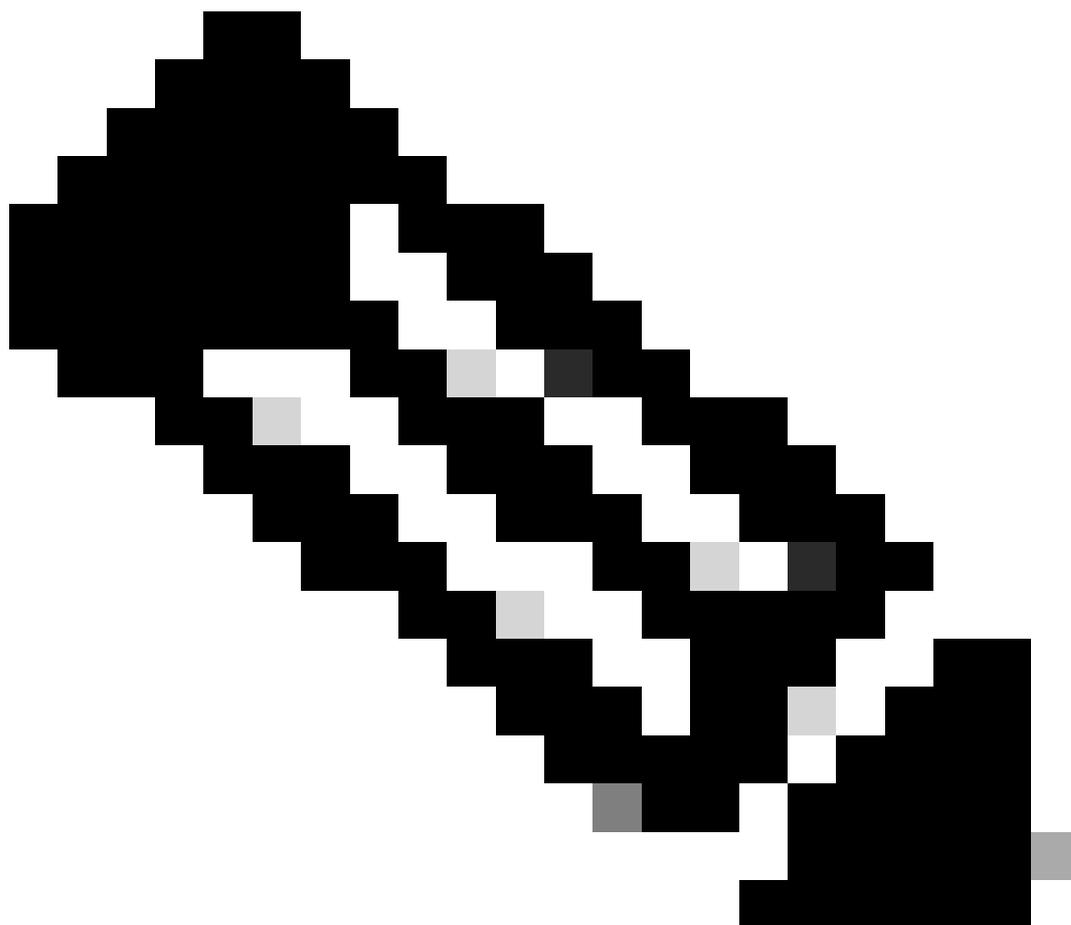
Verificar

Você pode usar estes comandos para verificar sua configuração atual:

```
# show run wlan // WLAN configuration # show run aaa // AAA configuration (server, server group, methods) # show aaa servers // Configured AAA servers
# show ap tag summary // Tag information for AP'S
# show wlan { summary | id | name | all } // WLAN details
# show wireless tag policy detailed <policy-tag name> // Detailed information on given policy tag
# show wireless profile policy detailed <policy-profile name> // Detailed information on given policy profile
```

Troubleshooting

---



---

**Observação:** o uso de balanceadores de carga externos é adequado. No entanto, certifique-se de que o balanceador de carga funcione por cliente usando o atributo RADIUS calling-station-id. Dependendo da porta de origem UDP não é um mecanismo suportado para equilibrar solicitações RADIUS do 9800.

---

## Solucionar problemas no WLC

A WLC 9800 fornece recursos de rastreamento **SEMPRE ATIVOS**. Isso garante que todos os erros, avisos e mensagens de nível de aviso relacionados à conectividade do cliente sejam constantemente registrados e que você possa exibir registros de uma condição de incidente ou falha após sua ocorrência.

Depende do volume de logs gerados, mas normalmente você pode voltar de algumas horas a vários dias.

Para visualizar os rastreamentos que a WLC 9800 coletou por padrão, você pode se conectar via SSH/Telnet à WLC 9800 e executar estas etapas: (Certifique-se de registrar a sessão em um arquivo de texto).

Etapa 1. Verifique a hora atual da WLC para que você possa rastrear os logs no tempo de volta para quando o problema ocorreu.

```
# show clock
```

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

```
# show logging
```

Etapa 3. Verifique se as condições de depuração estão ativadas.

```
# show debugging IOSXE Conditional Debug Configs: Conditional Debug Global State: Stop IOSXE Packet Tracing Configs: Packet Infra debugs: Ip Ad
```

---

 **Observação:** se você vir qualquer condição listada, isso significa que os rastreamentos são registrados no nível de depuração para todos os processos que encontram as condições ativadas (endereço mac, endereço ip e assim por diante). Isso aumenta o volume de registros. Portanto, recomenda-se limpar todas as condições quando não estiver depurando ativamente.

---

Etapa 4. Suponha que o endereço mac em teste não esteja 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 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 radioativo

Se os rastreamentos sempre ativos não fornecerem informações suficientes para determinar o disparador do problema sob investigação, você poderá habilitar a depuração condicional e capturar o rastreamento de Radio Ativo (RA), que fornece rastreamentos em nível de depuração para todos os processos que interagem com a condição especificada (endereço mac do cliente, neste caso). Você pode fazer isso por meio da GUI ou da CLI.

#### CLI:

Para habilitar a depuração condicional, execute 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.

Esse comando começa a monitorar o endereço mac fornecido por 30 minutos (1800 segundos). Opcionalmente, você pode aumentar esse tempo para 2085978494 segundos.

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

---

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

---

---

 MAC.

---

 **Observação:** você não vê a saída da atividade do cliente em uma sessão de terminal, pois tudo é armazenado em buffer internamente para ser exibido posteriormente.

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

Etapa 8. Interrompa as depurações se o problema for reproduzido antes do tempo de monitor padrão ou configurado decorrer.

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

Depois que o monitor-time tiver passado ou a conexão sem fio de depuração for interrompida, o 9800 WLC gerará um arquivo local com o nome:

```
ra_trace_MAC_aaaabbbccccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

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

Verifique o nome do arquivo de rastreamentos de RA:

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

Copie o arquivo para um servidor externo:

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

Mostre o conteúdo:

```
# more bootflash:ra_trace_MAC_aaaabbbccccc_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 visualização mais detalhada dos logs de nível de depuração. Você não precisa depurar o cliente novamente, pois examinamos em detalhes 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
```

---

 **Observação:** a saída desse comando retorna rastros para todos os níveis de log de 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
```

Mostre o conteúdo:

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

Etapa 11. Remova as condições de depuração.

```
# clear platform condition all
```

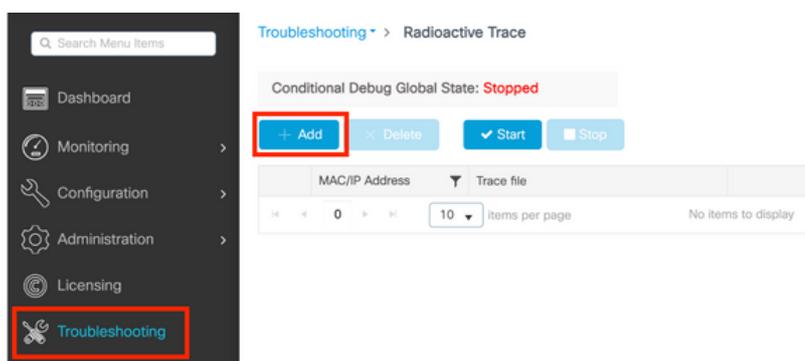
---

 **Observação:** certifique-se de sempre remover as condições de depuração após uma sessão de solução de problemas.

---

## GUI:

Etapa 1. Vá para **Troubleshooting > Radioactive Trace > + Add** e especifique o endereço MAC/IP do(s) cliente(s) para o(s) qual(is) deseja solucionar problemas.



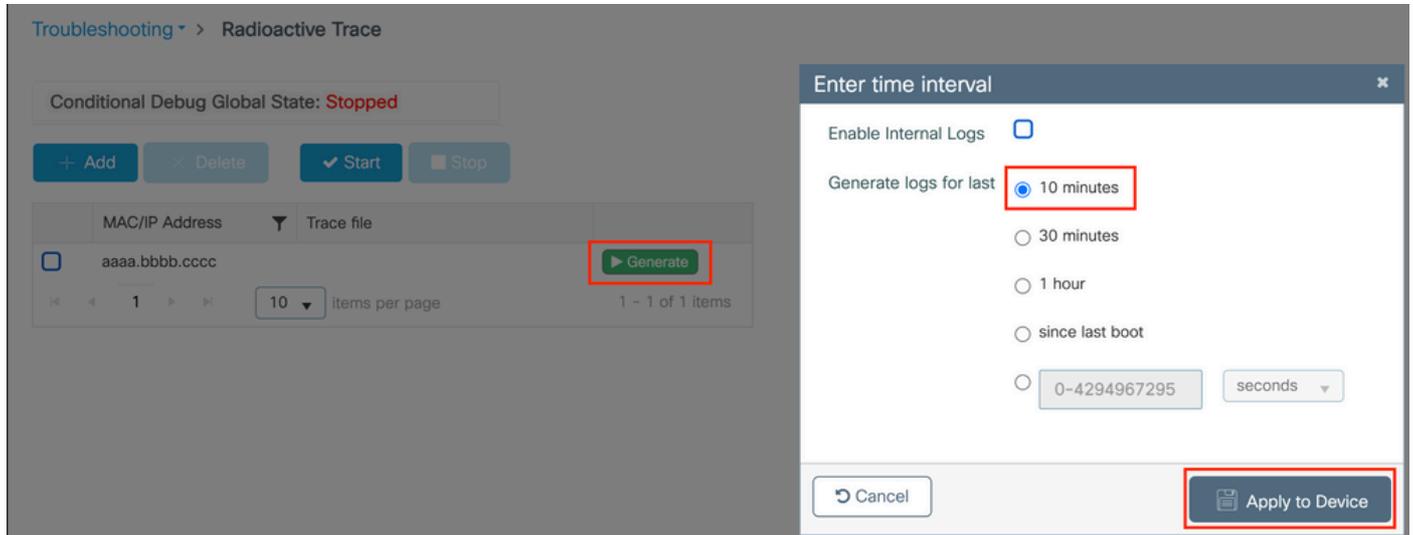
The screenshot displays the Cisco GUI interface for the 'Radioactive Trace' feature. On the left, a dark sidebar menu contains various navigation options, with 'Troubleshooting' highlighted by a red box. The main content area shows the 'Radioactive Trace' configuration page. At the top, the breadcrumb navigation reads 'Troubleshooting > Radioactive Trace'. Below this, a status indicator shows 'Conditional Debug Global State: Stopped'. A row of control buttons includes '+ Add', 'Delete', 'Start', and 'Stop', with the '+ Add' button highlighted by a red box. Below the buttons is a table with two columns: 'MAC/IP Address' and 'Trace file'. The table is currently empty, displaying '0' items and 'No items to display'.

Etapa 2. Clique em Iniciar.

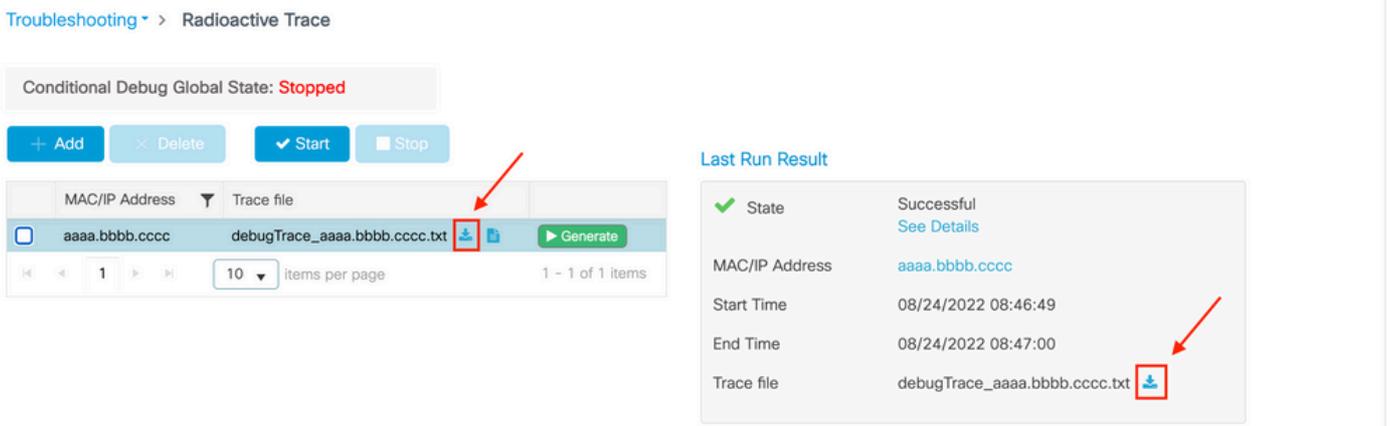
Etapa 3. Reproduza o problema.

Etapa 4. Clique em **Stop**.

Etapa 5. Clique no **Generate** botão, selecione o intervalo de tempo para o qual deseja obter os logs e clique em **Apply to Device**. In this example, the logs for the last 10 minutes are requested.



Etapa 6. Faça o download do rastreamento radioativo no seu computador, clique no botão de download e inspecione-o.



### Solução de problemas no ISE

Se você tiver problemas com a autenticação do cliente, poderá verificar os logs no servidor ISE. Vá para **Operations > RADIUS > Live Logs** e veja a lista de solicitações de autenticação, bem como o conjunto de políticas correspondente, o resultado de cada solicitação e assim por diante. Você pode obter mais detalhes se clicar na lupa sob a **Details** guia de cada linha, como mostrado na imagem:

Live Logs

Live Sessions

Misconfigured Supplicants 0

Misconfigured Network Devices 0

RADIUS Drops 0

Client Stopped Responding 2

Repeat Counter 0

Refresh: Never | Show: Latest 20 records | Within: Last 3 hours

Refresh | Reset Repeat Counts | Export To

Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...	IP Address	Netwo
Aug 23, 2022 06:18:42.5...	<span style="color: blue;">●</span>		0	user1	08:BE:AC:27:85:...	Unknown	Policy_Set...	Policy_Set...	PermitAcc...	10.14.16.112,...	
Aug 23, 2022 09:45:48.1...	<span style="color: red;">●</span>			user1	BC:D0:74:2B:6D:...						9800-W

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.