

Configurar o SSID de autenticação MAC nos controladores sem fio Catalyst 9800

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração AAA em WLC 9800](#)

[Autenticar clientes com servidor externo](#)

[Autenticar clientes localmente](#)

[Configuração de WLAN](#)

[Configuração de perfil de política](#)

[Configuração de marca de política](#)

[Atribuição de tag de política](#)

[Registre localmente o endereço MAC na WLC para a autenticação local](#)

[Insira o endereço MAC no banco de dados do endpoint do ISE](#)

[Criar uma Regra de Autenticação](#)

[Criação de Regra de Autorização](#)

[Verificar](#)

[Troubleshooting](#)

[Depuração condicional e rastreamento radioativo](#)

Introdução

Este documento descreve como configurar uma rede local sem fio (WLAN) com segurança de autenticação MAC no Cisco Catalyst 9800 WLC.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Endereço MAC
- Controladores sem fio Cisco Catalyst 9800 Series
- Identity Service Engine (ISE)

Componentes Utilizados

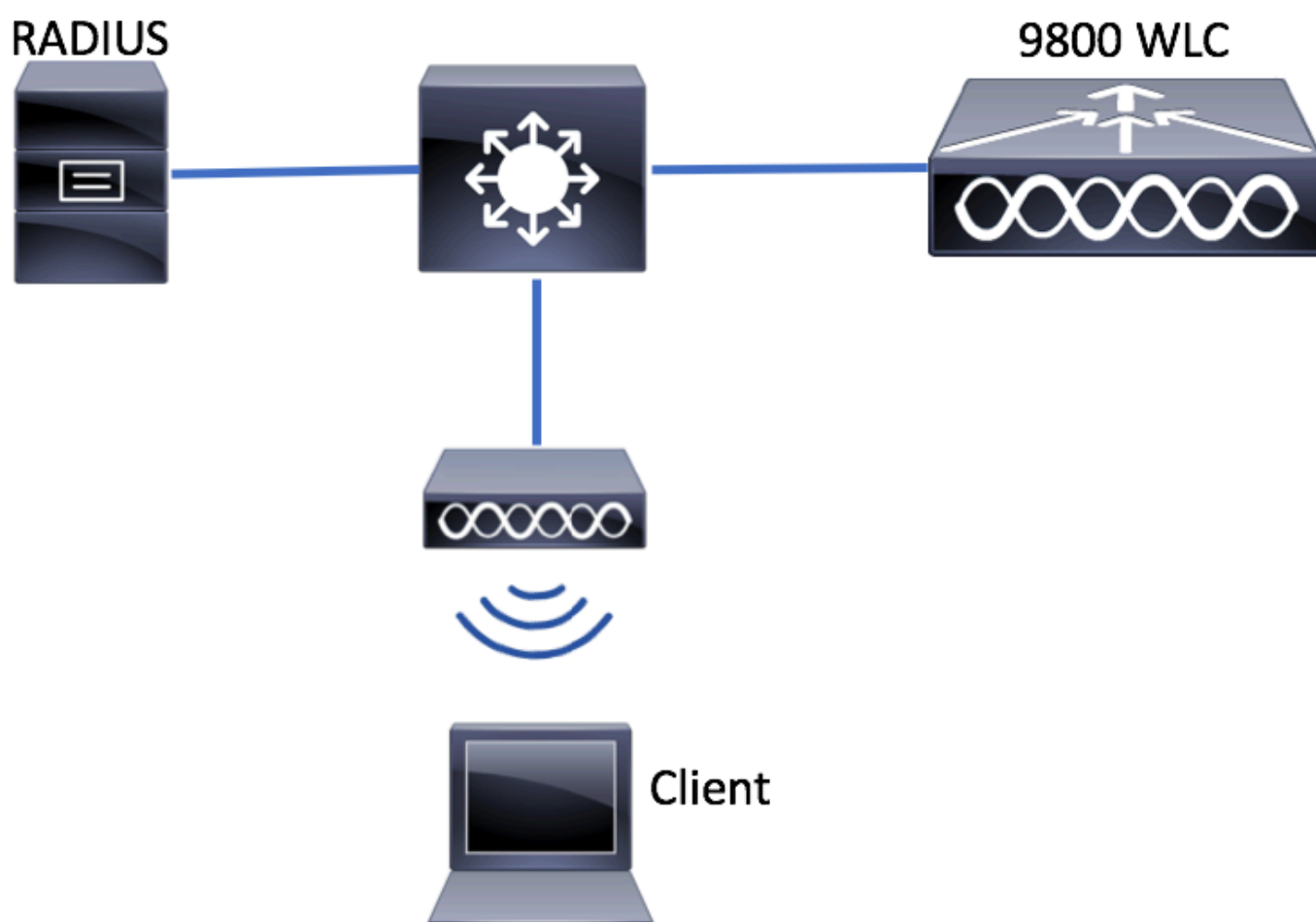
As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco IOS® XE Gibraltar v16.12
- ISE v2.2

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 AAA no 9800 WLC

Autenticar clientes com servidor externo

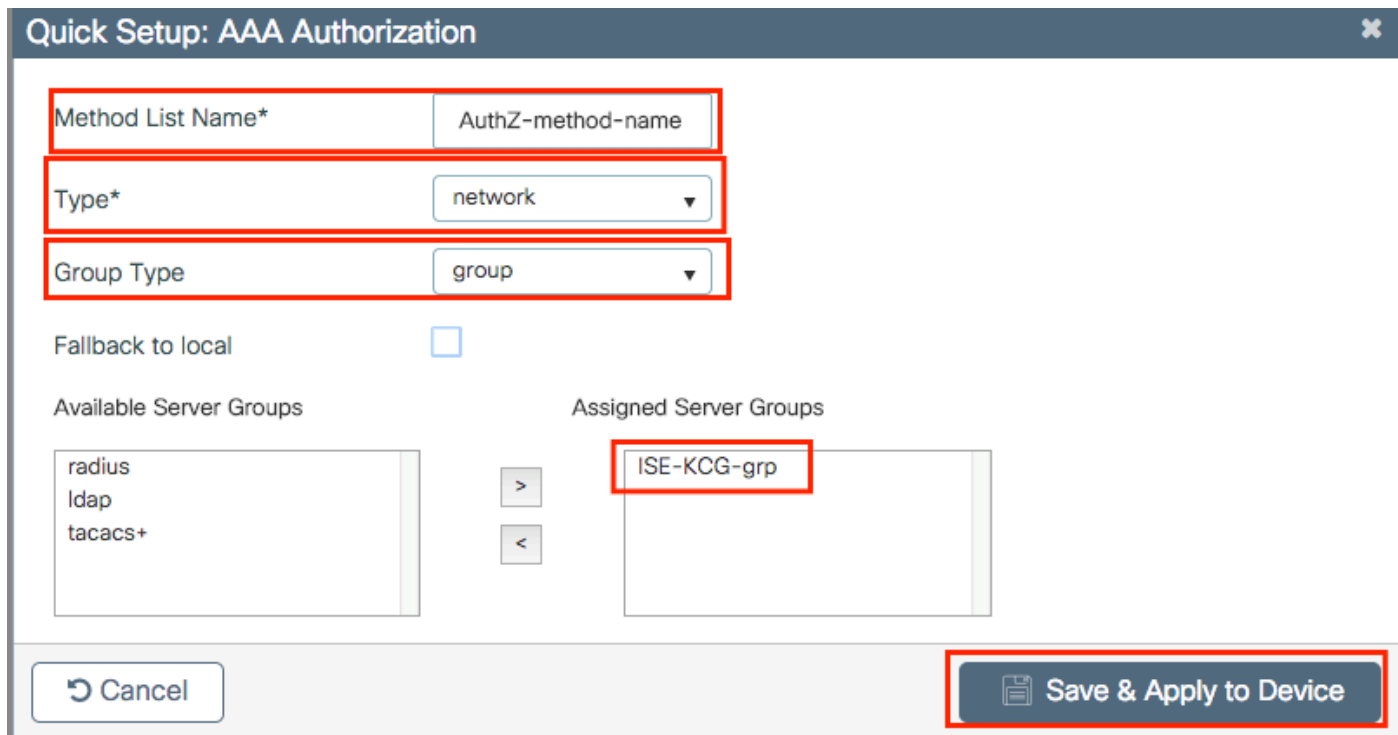
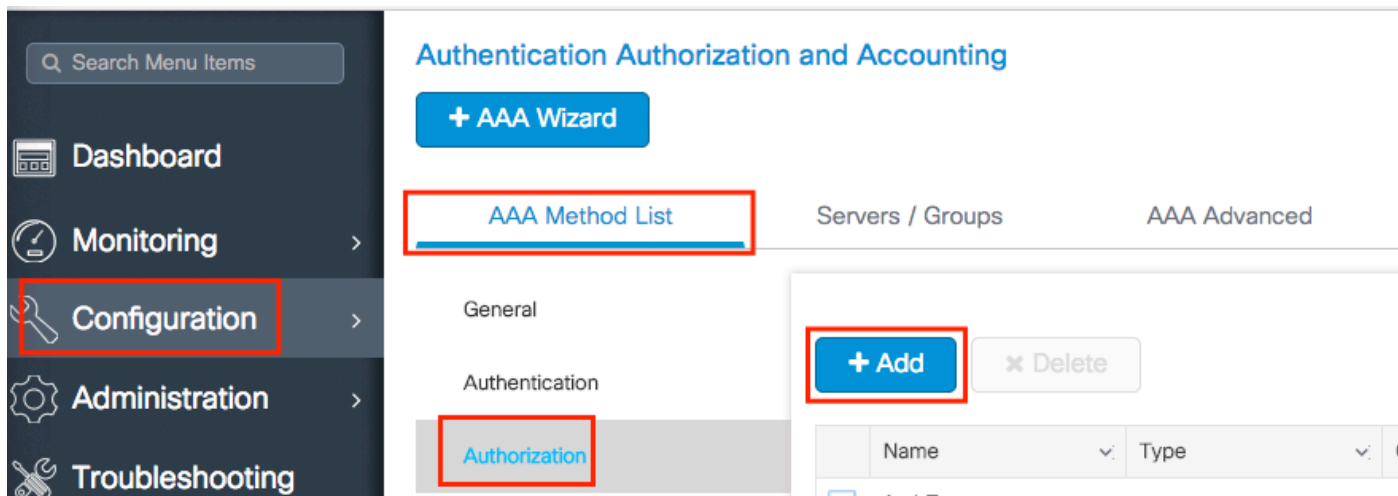
GUI:

Leia as Etapas 1-3 da seção 'Configuração AAA em 9800 WLCs' neste link:

Configuração de AAA em WLC 9800 Series

Etapa 4. Crie um método de rede de autorização.

Navegue até Configuration > Security > AAA > AAA Method List > Authorization > + Adde crie-o.



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
# key <shared-key>
```

```
# exit
```

```
# aaa group server radius <radius-grp-name>
```

```
# server name <radius-server-name>
```

```
# exit
```

```
# aaa server radius dynamic-author
```

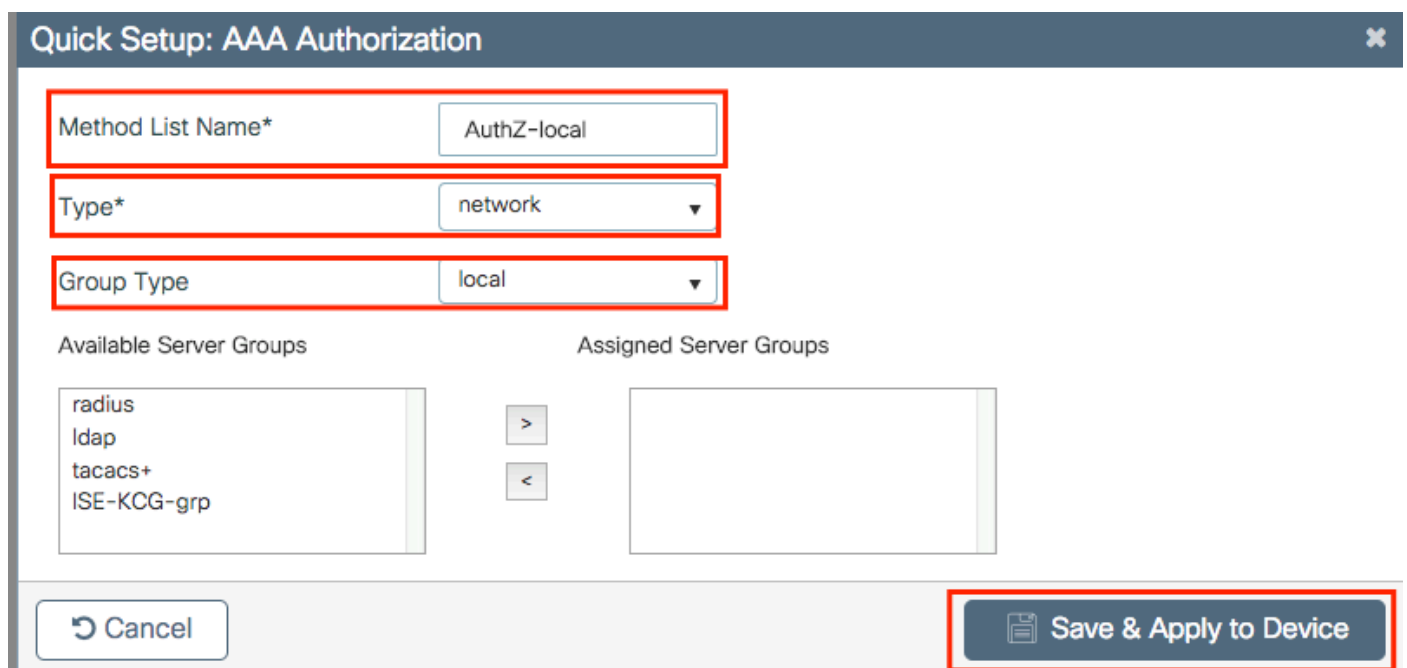
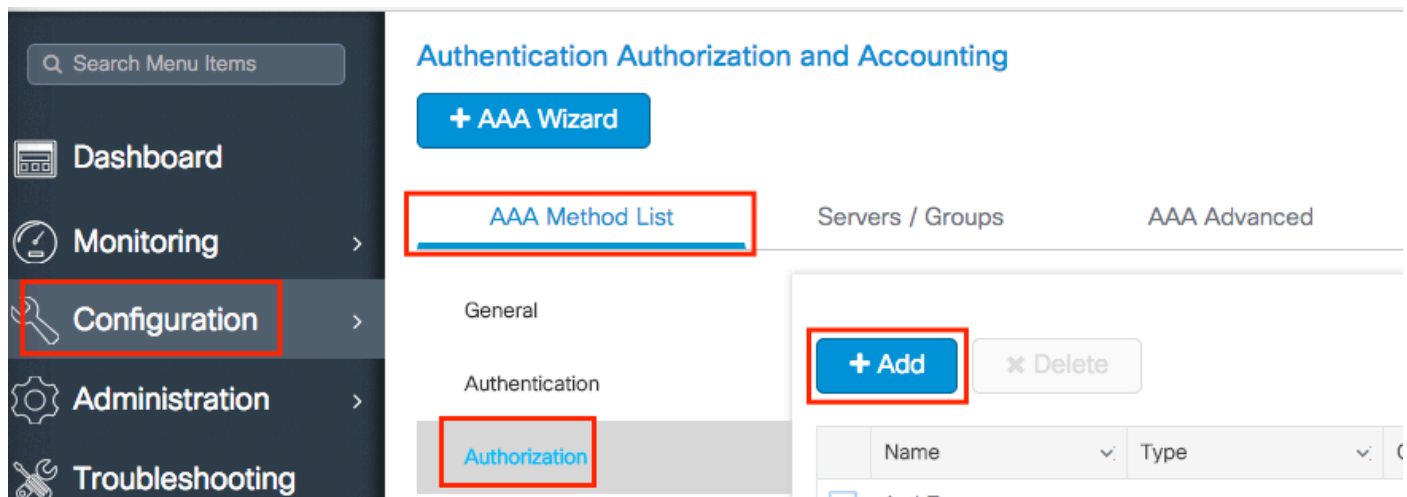
```
# client <radius-server-ip> server-key <shared-key>
```

```
# aaa authorization network <AuthZ-method-name> group <radius-grp-name>
```

Autenticar clientes localmente

Crie um método de rede de autorização local.

Navegue até **Configuration > Security > AAA > AAA Method List > Authorization > + Add** e crie-o.



CLI:

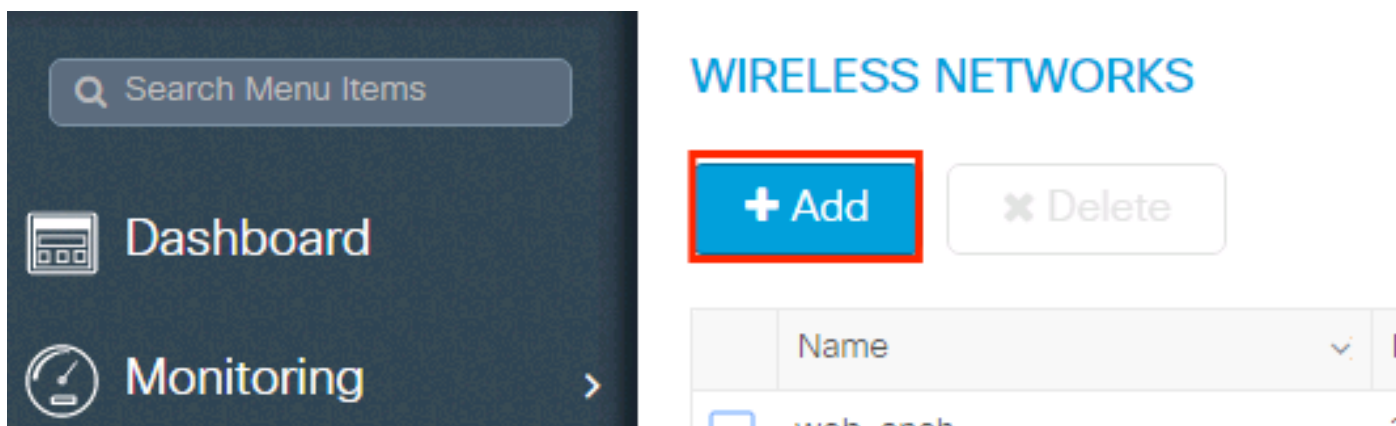
```
# config t
# aaa new-model
# aaa authorization network AuthZ-local local
```

Configuração de WLAN

GUI:

Etapa 1. Criar a WLAN.

Navegue até a rede `Configuration > Wireless > WLANs > + Add` e configure-a conforme necessário.



Etapa 2. Insira as informações da WLAN.

✕
Add WLAN

General
Security
Advanced

Profile Name*	<input type="text" value="mac-auth"/>	Radio Policy	<input type="text" value="All"/>
SSID	<input type="text" value="mac-auth"/>	Broadcast SSID	ENABLED <input checked="" type="checkbox"/>
WLAN ID*	<input type="text" value="3"/>		
Status	ENABLED <input checked="" type="checkbox"/>		

↶ Cancel

📄
Save & Apply to Device

Etapa 3. Navegue até a **Security** guia e desative **Layer 2 Security Mode** e ative **MAC Filtering**. Em **Authorization List**, escolha o método de autorização criado na etapa anterior. Em seguida, clique em **Save & Apply to Device**.

✕
Add WLAN

General
Security
Advanced

Layer2
Layer3
AAA

Layer 2 Security Mode	<input type="text" value="None"/>	Fast Transition	<input type="text" value="Adaptive Enab..."/>
MAC Filtering	<input checked="" type="checkbox"/>	Over the DS	<input checked="" type="checkbox"/>
Authorization List*	<input type="text" value="AuthZ-method-name"/>	Reassociation Timeout	<input type="text" value="20"/>

↶ Cancel

📄
Save & Apply to Device

CLI:

```
# config t
# wlan <profile-name> <wlan-id> <ssid-name>
# mac-filtering <authZ-network-method>
# no security wpa akm dot1x
# no security wpa wpa2 ciphers aes
# no shutdown
```

Configuração de perfil de política

Você deve habilitar `aaa-override` no perfil de política para garantir que a filtragem de mac por SSID funcione bem.

[Configuração do perfil de política no 9800 WLC](#)

Configuração de marca de política

[Marca de política no 9800 WLC](#)

Atribuição de tag de política

[Atribuição de marcação de política no 9800 WLC](#)

Registre o endereço MAC permitido.

Registre localmente o endereço MAC na WLC para a autenticação local

Navegue até `Configuration > Security > AAA > AAA Advanced > AP Authentication > + Add`.

The screenshot displays the Cisco WLC configuration interface. On the left, a dark sidebar contains menu items: Dashboard, Monitoring, Configuration (highlighted with a red box), Administration, and Troubleshooting. The main content area is titled 'Authentication Authorization and Accounting' and features a '+ AAA Wizard' button. Below this, there are tabs for 'AAA Method List', 'Servers / Groups', and 'AAA Advanced' (highlighted with a red box). Under 'AAA Advanced', there are sections for 'RADIUS Fallback', 'Attribute List Name', 'AP Authentication' (highlighted with a red box), and 'Password Policy'. The 'AP Authentication' section is expanded to show a table with columns 'MAC Address' and 'Serial Number'. The table contains two entries: 'aabbccdeeff' and 'e4b3187c3058'. A '+ Add' button (highlighted with a red box) and a 'x Delete' button are located above the table. At the bottom of the table, there is a pagination control showing '1' of 10 items per page.


Escreva o endereço mac em todas as letras minúsculas sem um separador e clique em `Save & Apply` to

Device.

Quick Setup: MAC Filtering

MAC Address*

Attribute List Name

 Observação: nas versões anteriores à 17.3, a interface do usuário da Web alterou qualquer formato MAC digitado no formato 'sem separador' mostrado na ilustração. Na versão 17.3 e posterior, a interface do usuário da Web respeita qualquer design inserido e, portanto, é essencial não inserir nenhum separador. Bug de aprimoramento O bug da Cisco ID [CSCv43870](https://tools.cisco.com/bugcenter/bug/?bugID=CSCv43870) rastreia o suporte de vários formatos para autenticação MAC.

CLI:

```
# config t
# username <aabbccddeeff> mac
```

Insira o endereço MAC no banco de dados do endpoint do ISE

Etapa 1. (Opcional) Crie um novo grupo de endpoints.

Navegue até Work Centers > Network Access > Id Groups > Endpoint Identity Groups > + Add.

Identity Services Engine

Home | Context Visibility | Operations | Policy | Administration | Work Centers

Network Access | Guest Access | TrustSec | BYOD | Profiler | Posture | Device Administration | PassiveID

Overview | Identities | Id Groups | Ext Id Sources | Network Resources | Policy Elements | Authentication Policy | Authorization Po

Identity Groups

Endpoint Identity Groups

Edit + Add X Delete

Identity Groups

Endpoint Identity Group List > **New Endpoint Group**

Endpoint Identity Group

* Name

Description

Parent Group

Etapa 2. Navegue até Work Centers > Network Access > Identities > Endpoints > +Add.

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > **Work Centers**

Network Access > Guest Access > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID

Overview > **Identities** > Id Groups > Ext Id Sources > Network Resources > Policy Elements > Authentication Policy > Authorization Policy > Troubleshoot

Endpoints

Network Access Users
Identity Source Sequences

INACTIVE ENDPOINTS ⓘ

AUTHENTICATION STATUS ⓘ

No data available

Last Activity Date

Change Authorization Change Clear Threats & Vulnerabilities Export Import

Add Endpoint

▼ General Attributes

Mac Address * aa:bb:cc:dd:ee:ff

Description

Static Assignment

Policy Assignment Unknown

Static Group Assignment

Identity Group Assignment MACaddressgroup

Cancel Save

Configuração do ISE

Adicionar o 9800 WLC ao ISE.

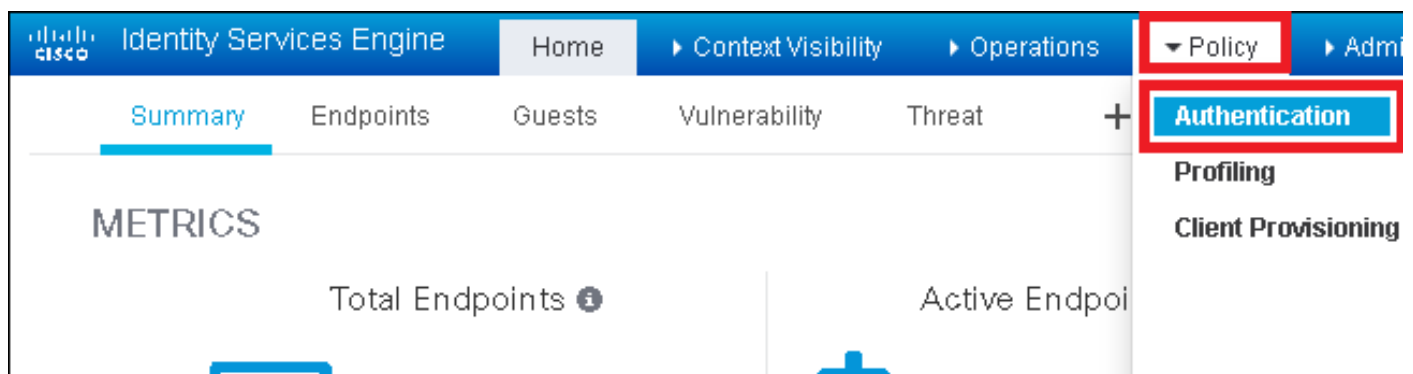
Leia as instruções neste link: [Declare WLC to ISE](#).

Criar uma Regra de Autenticação

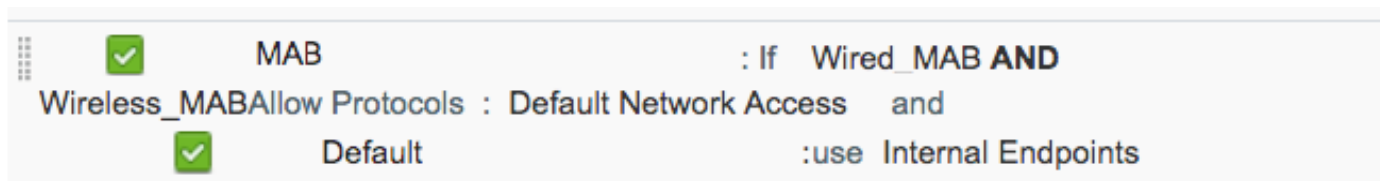
As regras de autenticação são usadas para verificar se as credenciais dos usuários estão corretas (verifique se o usuário realmente é quem diz ser) e limitar os métodos de autenticação que podem ser usados por ele.

Etapa 1. Navegue até **Policy > Authentication** como mostrado na imagem.

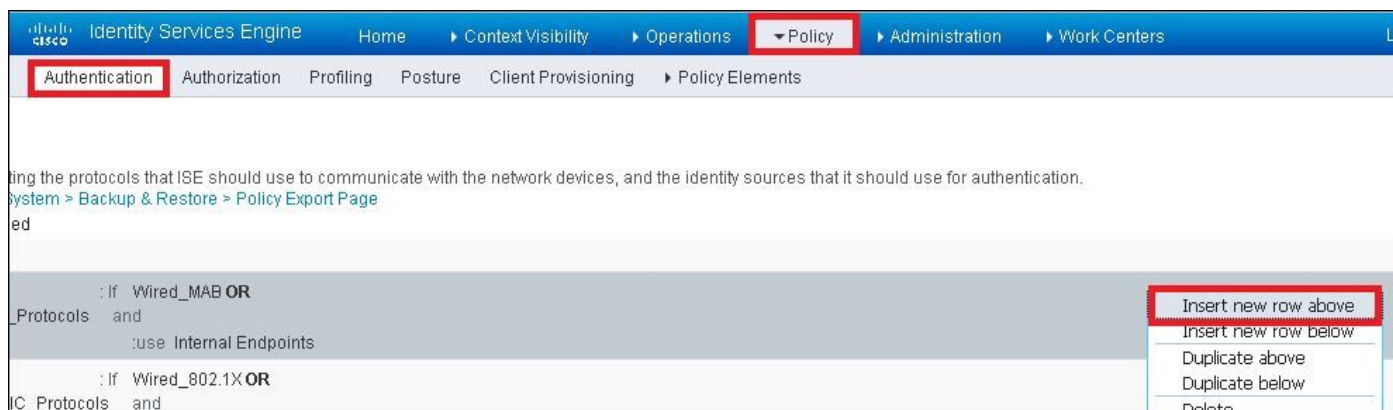
Confirme se a regra MAB padrão existe no ISE.



Etapa 2. Verifique se a regra de autenticação padrão para MAB já existe:



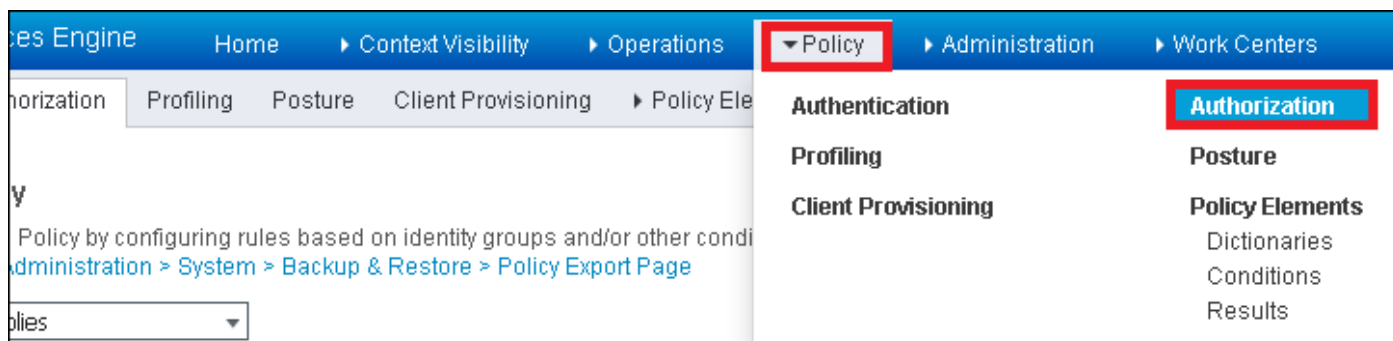
Caso contrário, você poderá adicionar um novo quando clicar em **Insert new row above**.



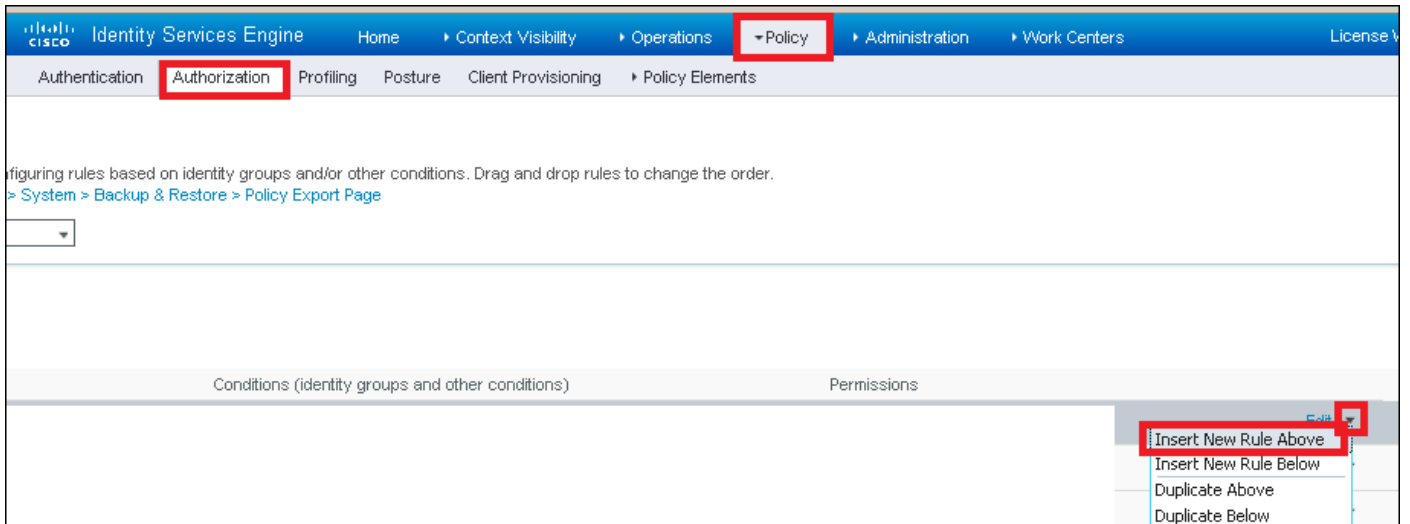
Criação de Regra de Autorização

A regra de autorização é responsável por determinar qual resultado de permissões (qual perfil de autorização) é aplicado ao cliente.

Etapa 1. Navegue até **Policy > Authorization** como mostrado na imagem.

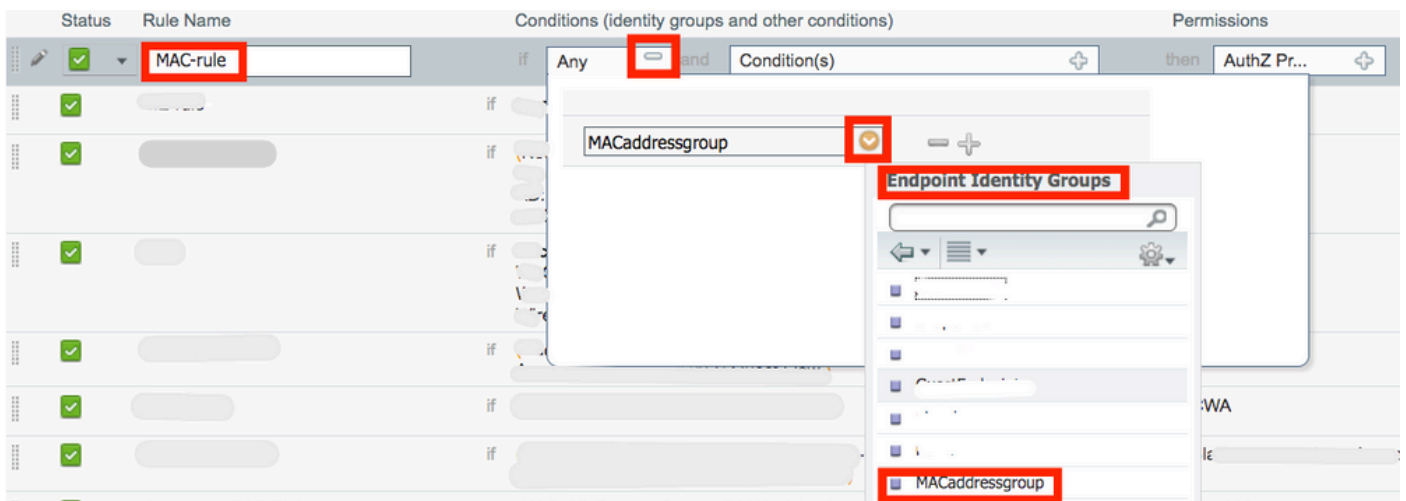


Etapa 2. Inserir uma nova regra conforme mostrado na imagem.

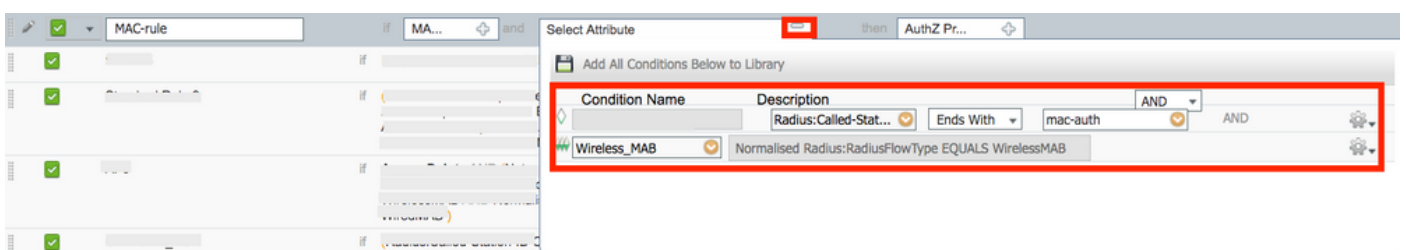


Etapa 3. Insira os valores.

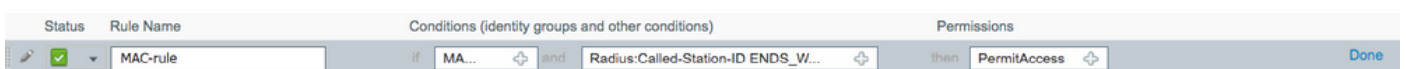
Primeiro, escolha um nome para a regra e o grupo Identidade onde o ponto final está armazenado (MACaddressgroup), como mostrado na imagem.



Depois disso, escolha outras condições que fazem o processo de autorização para se enquadrar nessa regra. Neste exemplo, o processo de autorização atinge esta regra se usar o MAB sem fio e seu ID de estação chamado (o nome do SSID) termina com mac-auth como mostrado na imagem.



Finalmente, escolha o perfil de Autorização que é atribuído, nesse caso, PermitAccess aos clientes que atingiram essa regra. Clique Done e salve-o.




Verificar

Você pode usar estes comandos para verificar a configuração atual:

```
# show wlan { summary | id | name | all }
# 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>
```

Troubleshooting

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.

 Observação: embora dependa do volume de logs gerados, 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 ler essas etapas (certifique-se de registrar a sessão em um arquivo de texto).

Etapa 1. Verifique a hora atual do controlador para que você possa controlar os registros desde a hora até quando o problema ocorreu.

```
# show clock
```

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

```
# 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 Address _____ Port
-----|-----
```

 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. Se o endereço MAC no teste não estiver 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-
```

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). Para habilitar a depuração condicional, leia 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.

Estes comandos começam a monitorar o endereço MAC fornecido por 30 minutos (1.800 segundos). Como alternativa, você pode aumentar esse tempo para até 2.085.978.494 segundos.

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

 Note: Para monitorar mais de um cliente por vez, execute o comando `debug wireless mac` por endereço mac.

 Observação: você não vê a saída da atividade do cliente na sessão do terminal, pois tudo é armazenado 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 de monitoramento padrão ou configurado acabe.

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

Quando o tempo do monitor tiver decorrido ou a depuração sem fio tiver sido interrompida, a WLC 9800 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 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.
```

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 depuração. Não é necessário depurar o cliente novamente, pois você só precisa dar uma olhada mais detalhada nos 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 r
```

 **Observação:** a saída desse comando retorna rastros para todos os níveis de registro de todos os processos e é bastante volumosa. Envie 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 Troubleshooting.

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.