Configurar a lista de autorização de AP de controladores sem fio Catalyst 9800

Contents

Introdução

Este documento descreve como configurar a política de autenticação do ponto de acesso (AP) da controladora Wireless LAN do Catalyst 9800.

Informações de Apoio

Para autorizar um Ponto de Acesso (AP), o endereço MAC Ethernet do AP precisa ser autorizado no banco de dados local com o Controlador LAN Wireless 9800 ou em um servidor RADIUS (Remote Authentication Dial-In User Service) externo.

Esse recurso garante que somente os pontos de acesso (APs) autorizados possam se unir a um controlador de LAN sem fio Catalyst 9800. Este documento não aborda o caso de APs de malha (série 1500) que exigem uma entrada de filtro mac para se unir ao controlador, mas não rastreiam o fluxo de autorização de AP típico (consulte as referências).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- WLC 9800
- Acesso via interface de linha de comando (CLI) aos controladores sem fio

Componentes Utilizados

WLC 9800 v16.12

AP 1810W

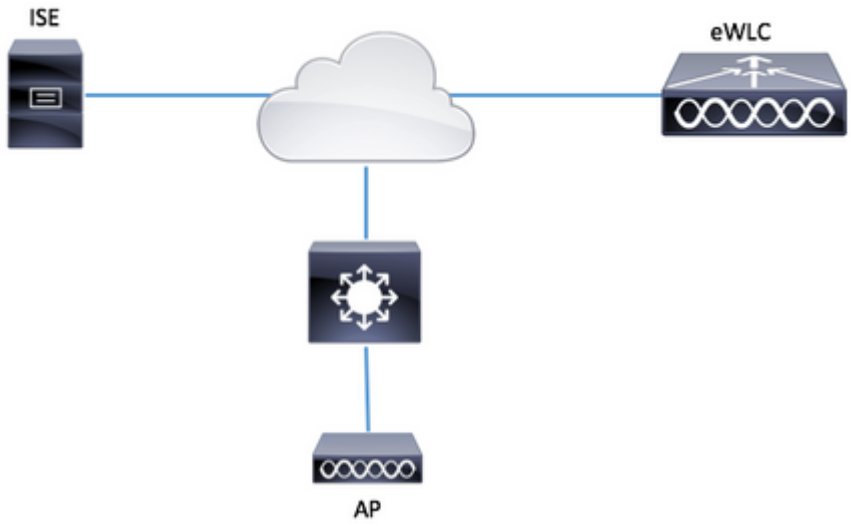
AP 1700

Identity Service Engine (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



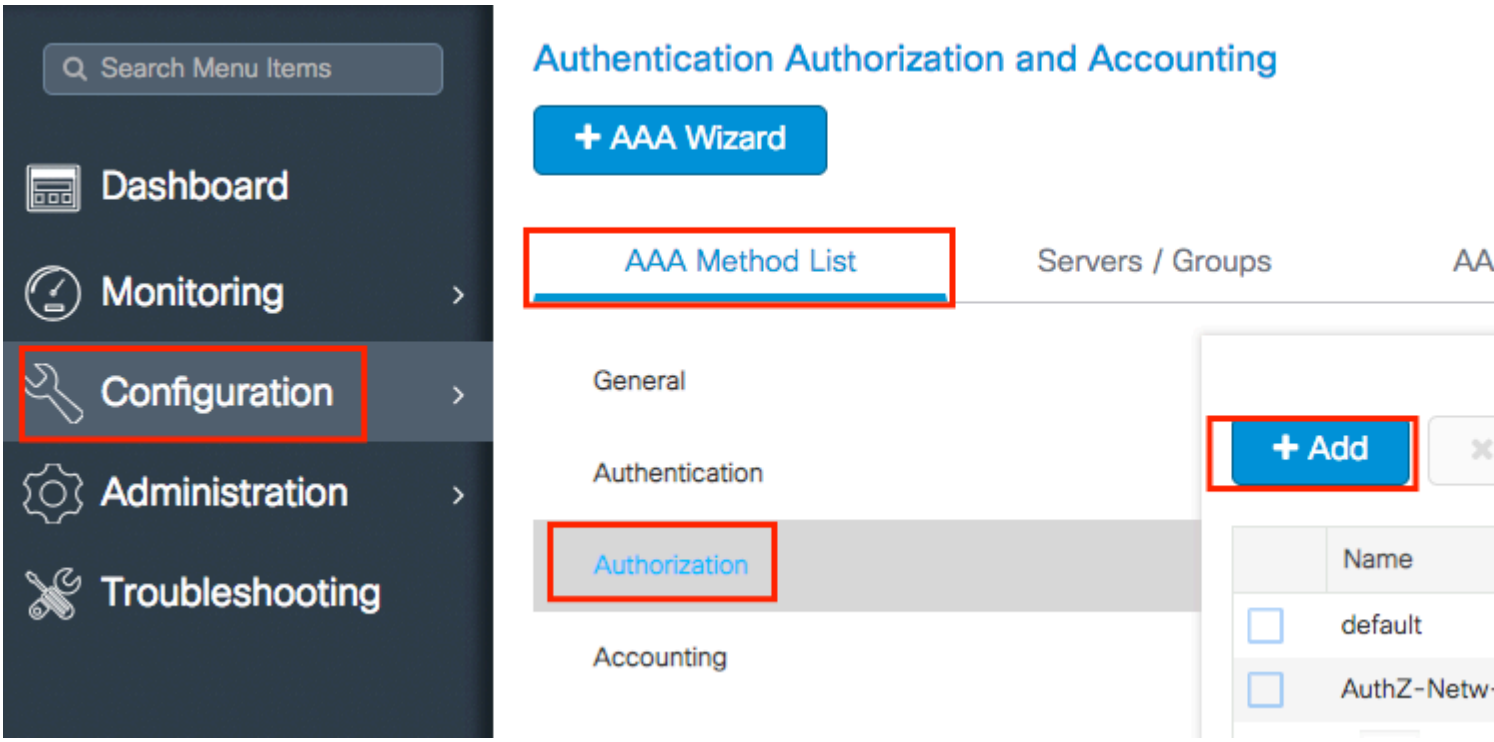
Configurações

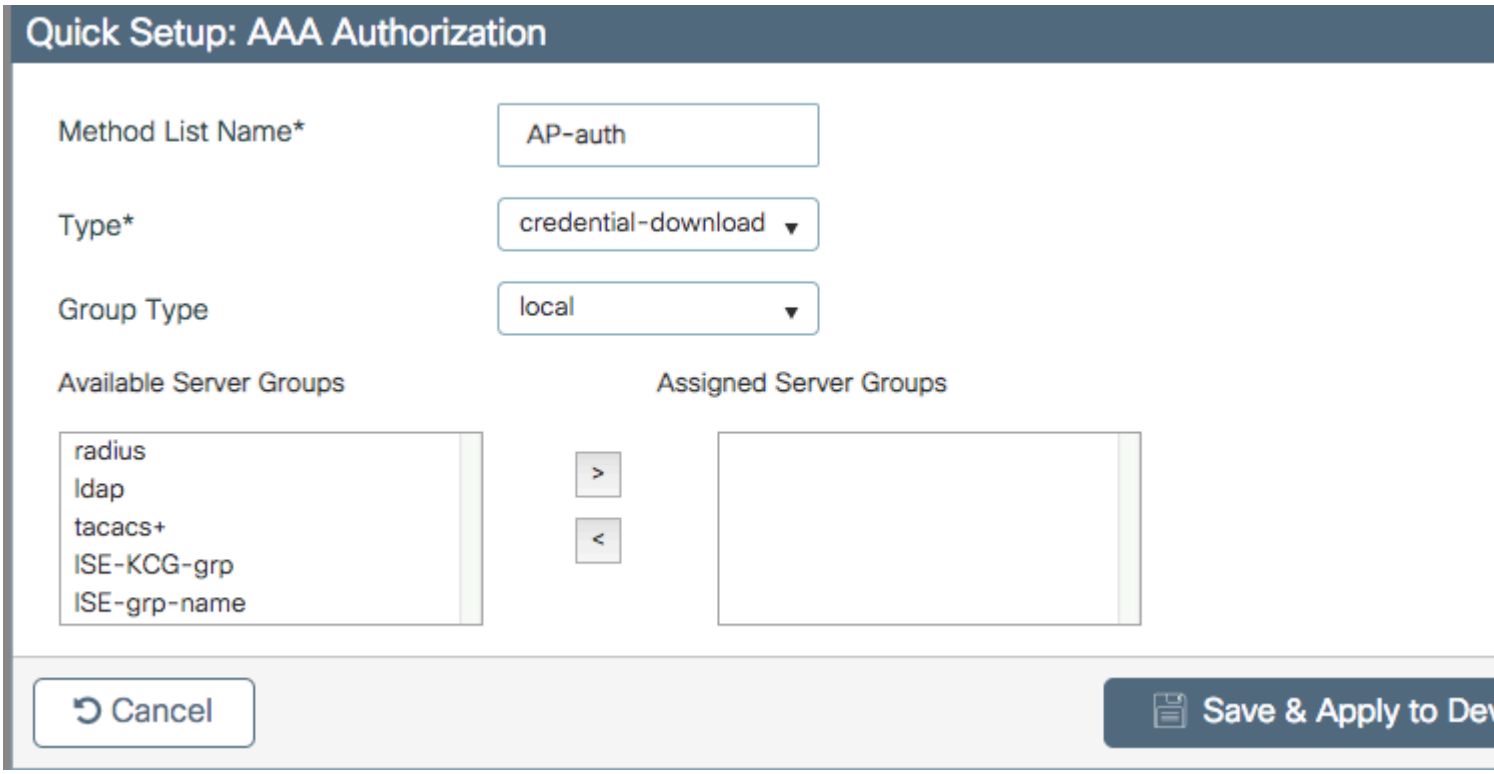
Lista de autorização MAC AP - Local

O endereço MAC dos APs autorizados é armazenado localmente na WLC 9800.

Etapa 1. Crie uma lista de métodos de download de credenciais de autorização local.

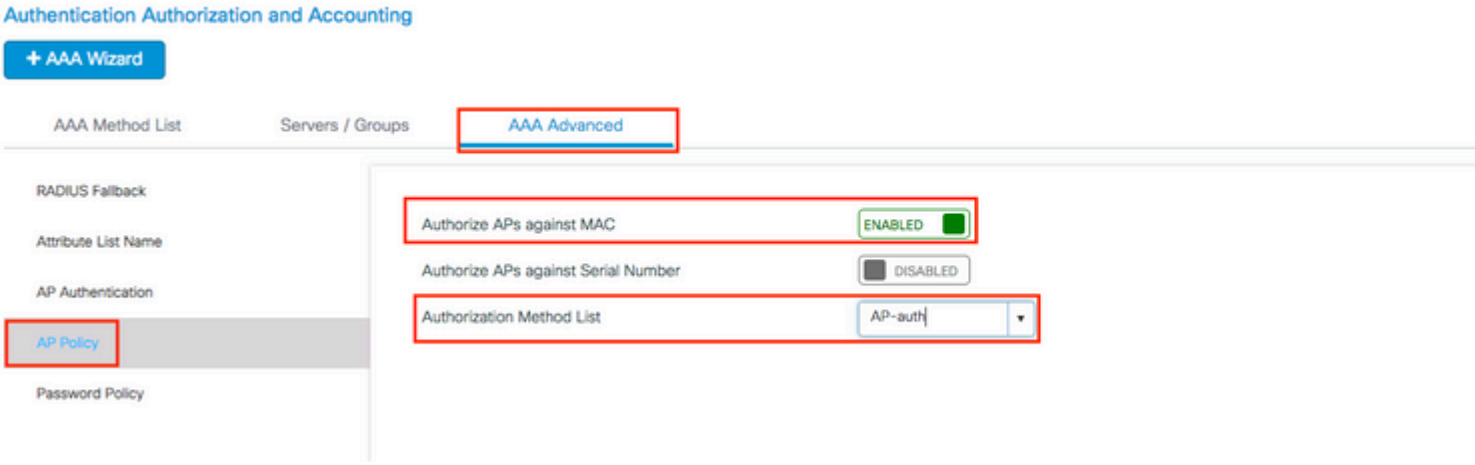
Navegue até **Configuration > Security > AAA > AAA Method List > Authorization > + Add**





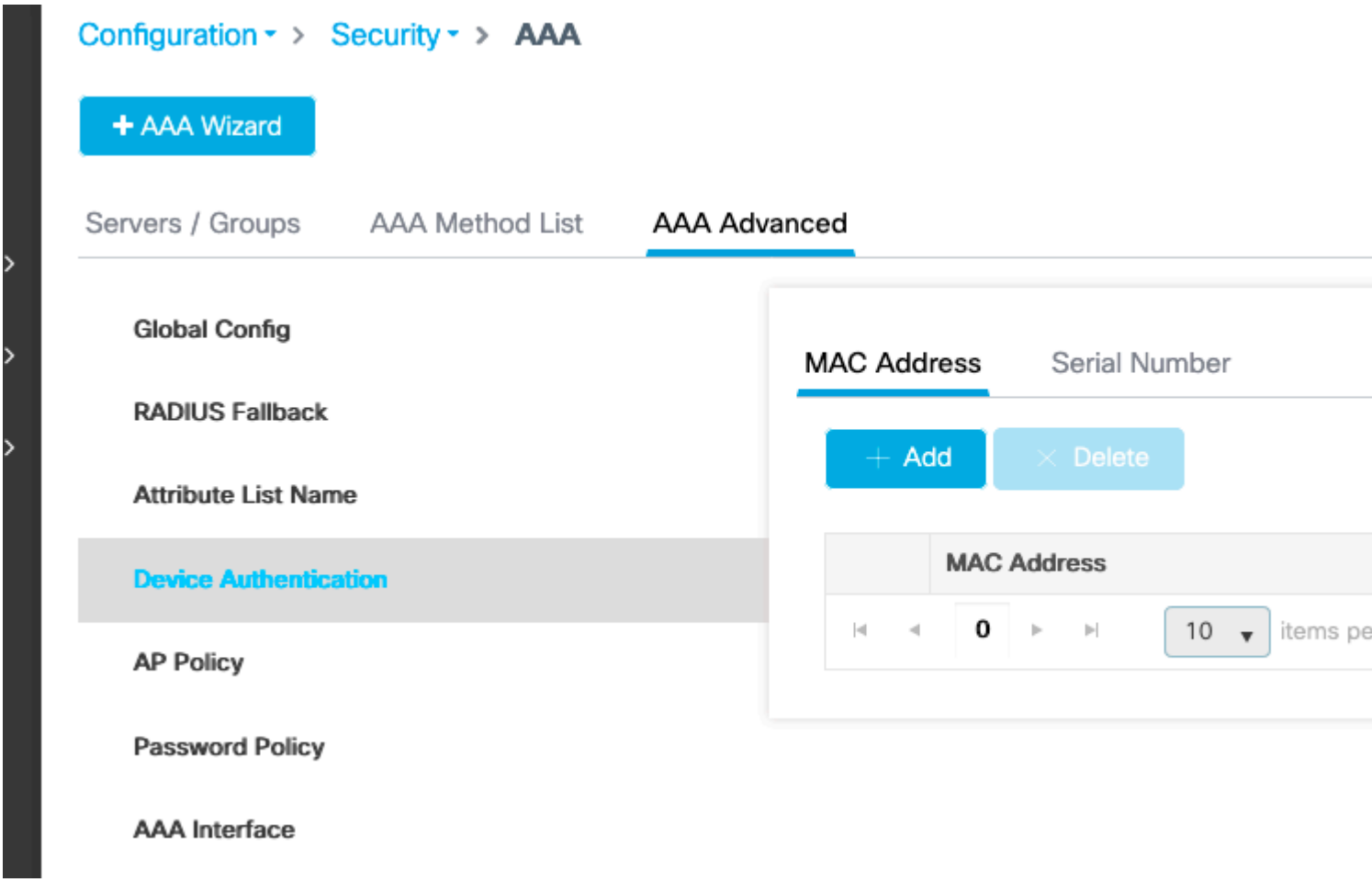
Etapa 2. Ative a autorização MAC do AP.

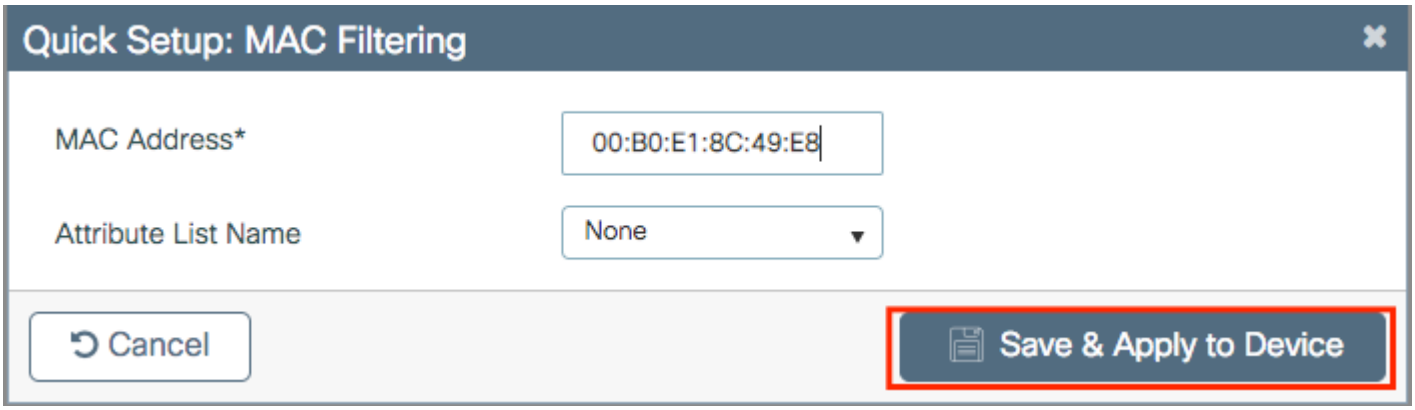
Navegue até **Configuração > Segurança > AAA > AAA Advanced > AP Policy.** Ative **Authorize APs against MAC** e selecione a **Authorization Method List** criada na Etapa 1.



Etapa 3. Adicione o endereço MAC Ethernet do AP.

Navegue até **Configuration > Security > AAA > AAA Advanced > Device Authentication > MAC Address > + Add**





> **Observação**: o endereço MAC Ethernet do AP deve ser em um desses formatos quando inserida na interface do usuário da Web (xx:xx:xx:xx:xx:xx (ou) xxxx.xxxx.xxxx (ou) xx-xx-xx-xx-xx-xx) na versão 16.12. Na versão 17.3, eles devem estar no formato xxxxxxxxxxxx sem nenhum separador. O formato CLI é sempre xxxxxxxxxxx em qualquer versão (na versão 16.12, a interface de usuário da Web remove os separadores na configuração). O bug da Cisco ID CSCv43870 permite o uso de qualquer formato na CLI ou na interface do usuário da Web em versões posteriores.

CLI:

```
# config t
# aaa new-model
# aaa authorization credential-download <AP-auth> local

# ap auth-list authorize-mac
# ap auth-list method-list <AP-auth>

# username <aaaabbbbcccc> mac
```

Lista de Autorização MAC AP - Servidor RADIUS externo

Configuração da WLC 9800

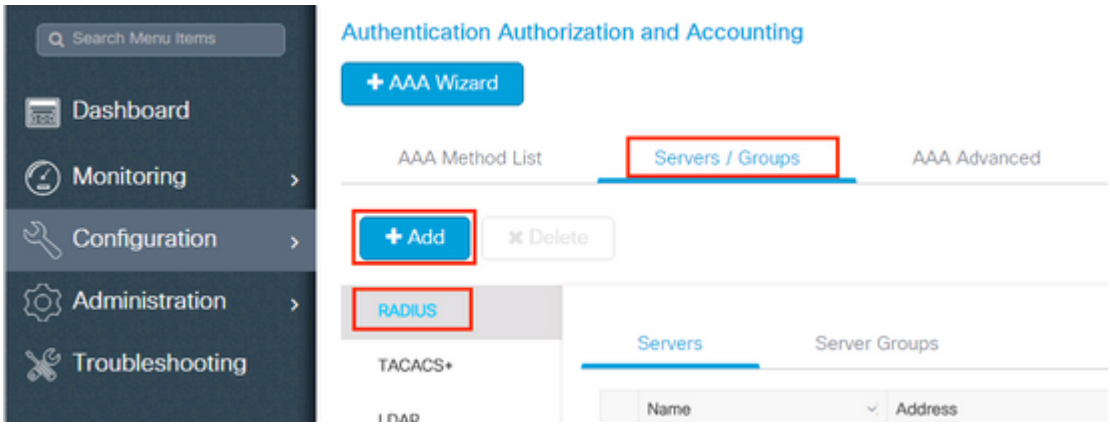
O endereço MAC dos APs autorizados é armazenado em um servidor RADIUS externo, neste exemplo, o ISE.

No ISE, você pode registrar o endereço MAC dos APs como nomes de usuário/senha ou como endpoints. Ao longo das etapas, você é instruído a selecionar o uso de uma maneira ou de outra.

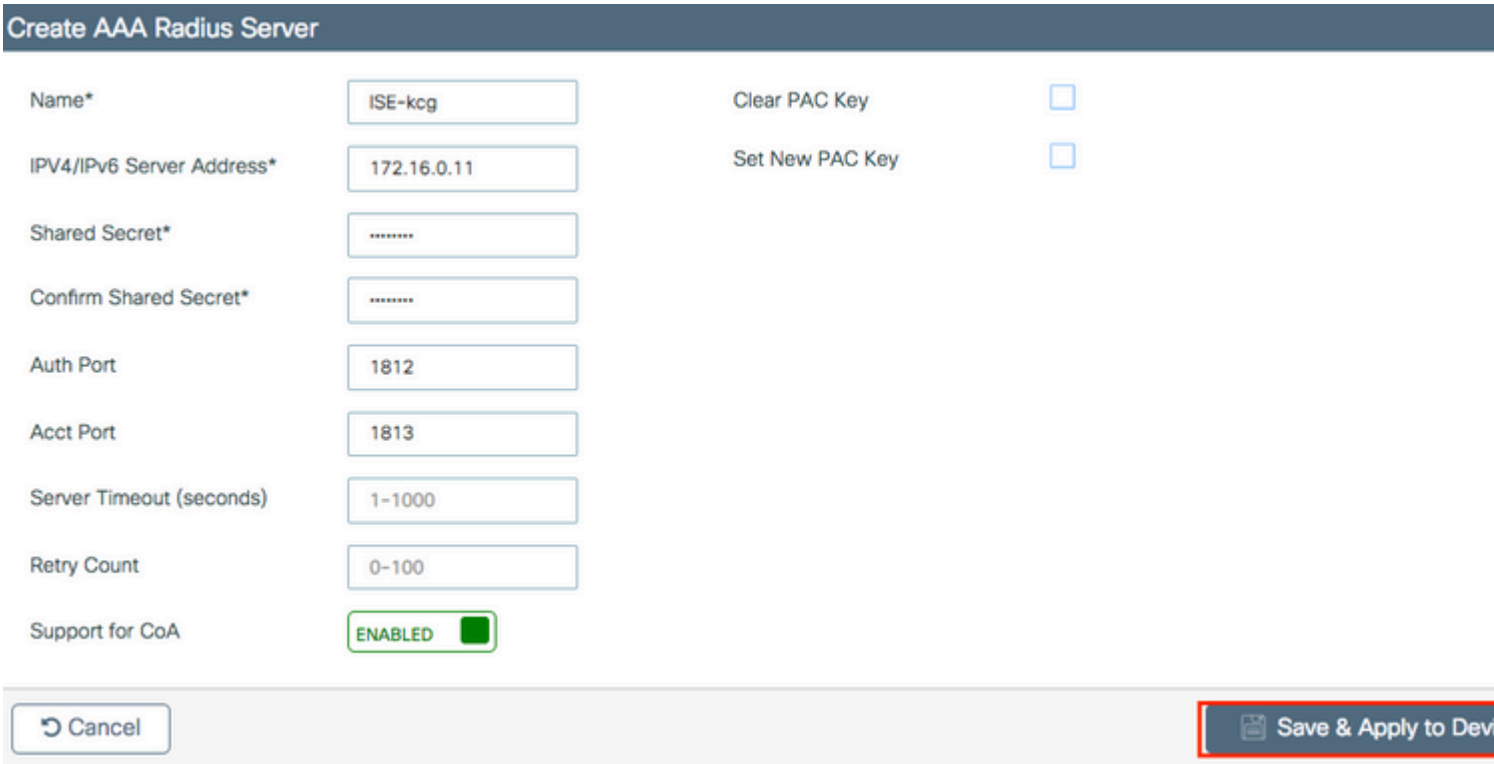
GUI:

Etapa 1. Declarar o servidor RADIUS

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



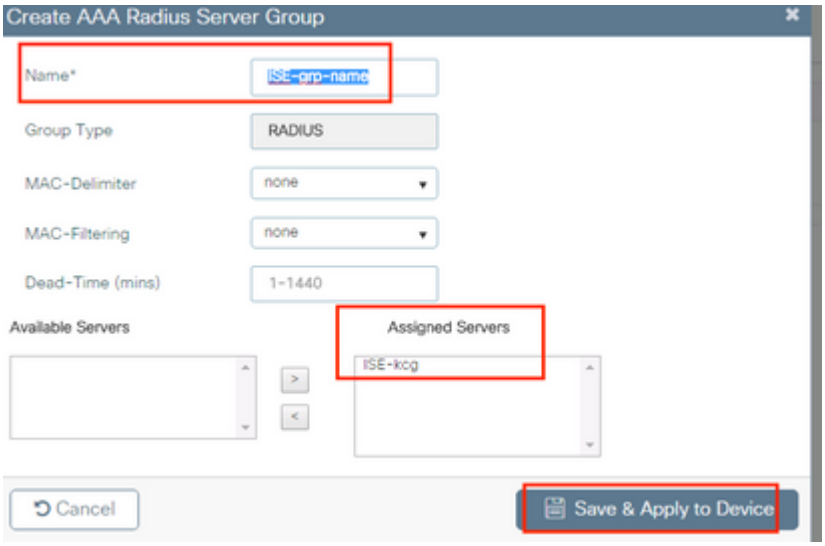
Verifique se o suporte para CoA está ativado, caso você planeje usar a autenticação da Web central (ou qualquer tipo de segurança que exija o CoA) no futuro.



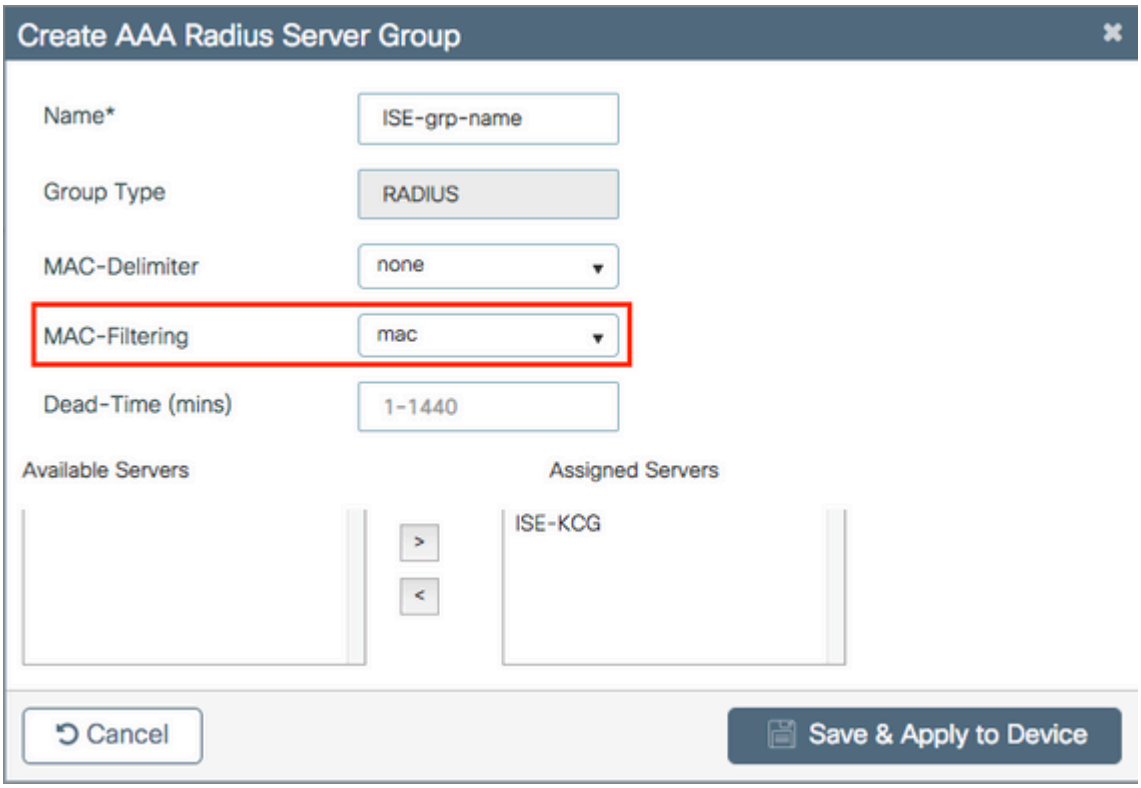
Etapa 2. Adicionar o servidor RADIUS a um grupo RADIUS

Navegue até **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add**

Para que o ISE autentique o endereço MAC do AP como nomes de usuário, deixe a Filtragem MAC como nenhum.

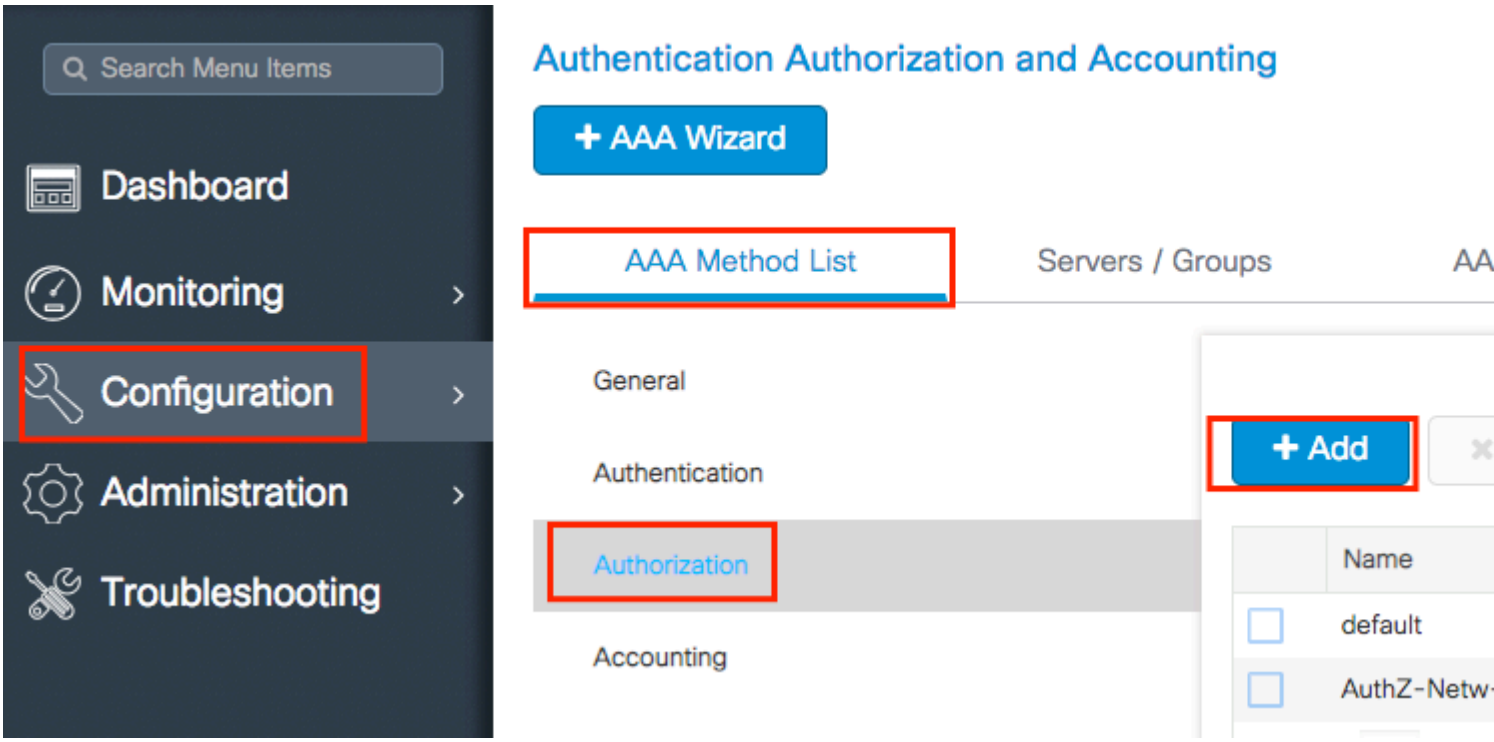


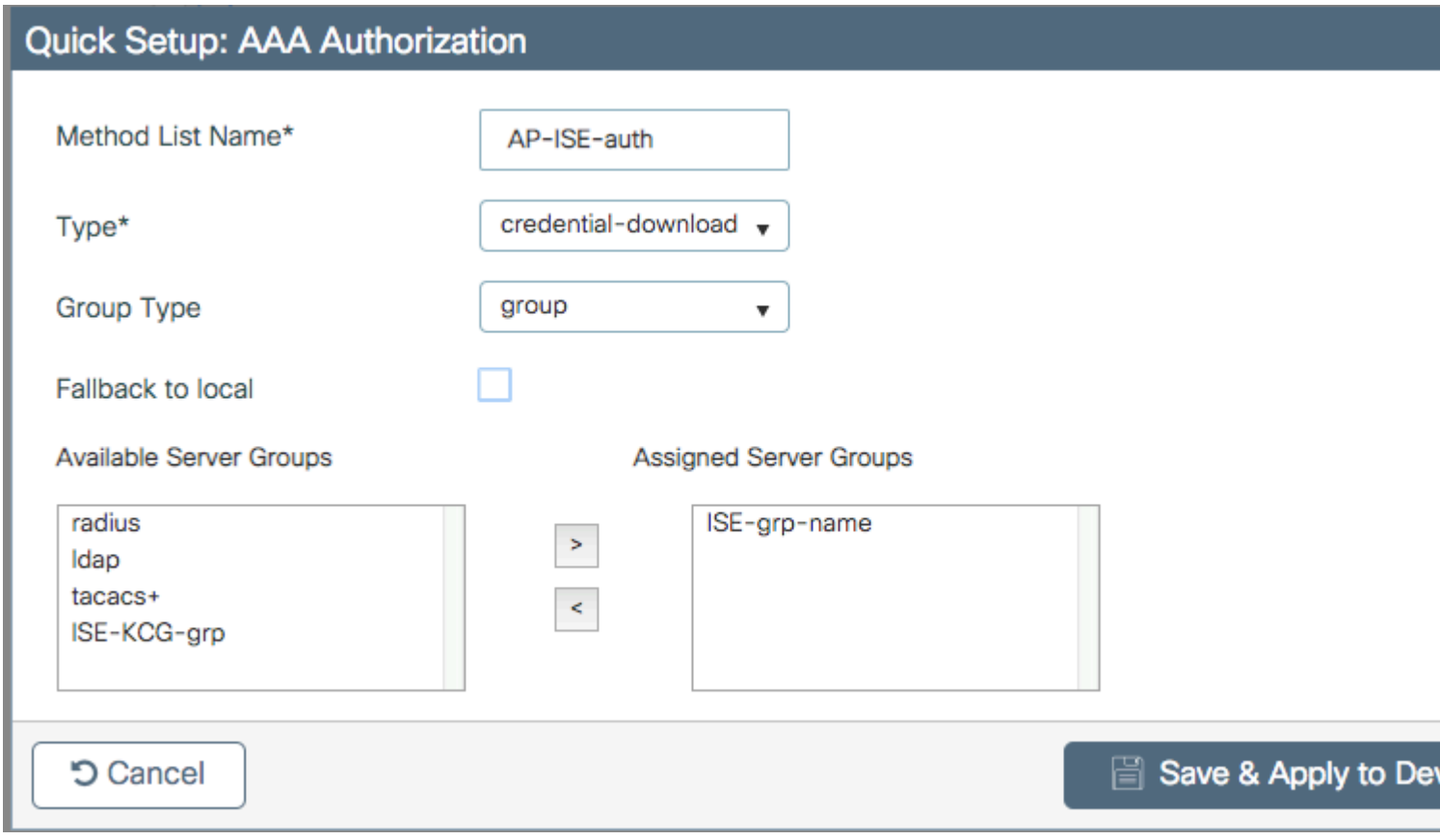
Para que o ISE autentique o endereço MAC do AP quando os endpoints mudarem a filtragem MAC para MAC.



Etapa 3. Crie uma lista de métodos de download de credenciais de autorização.

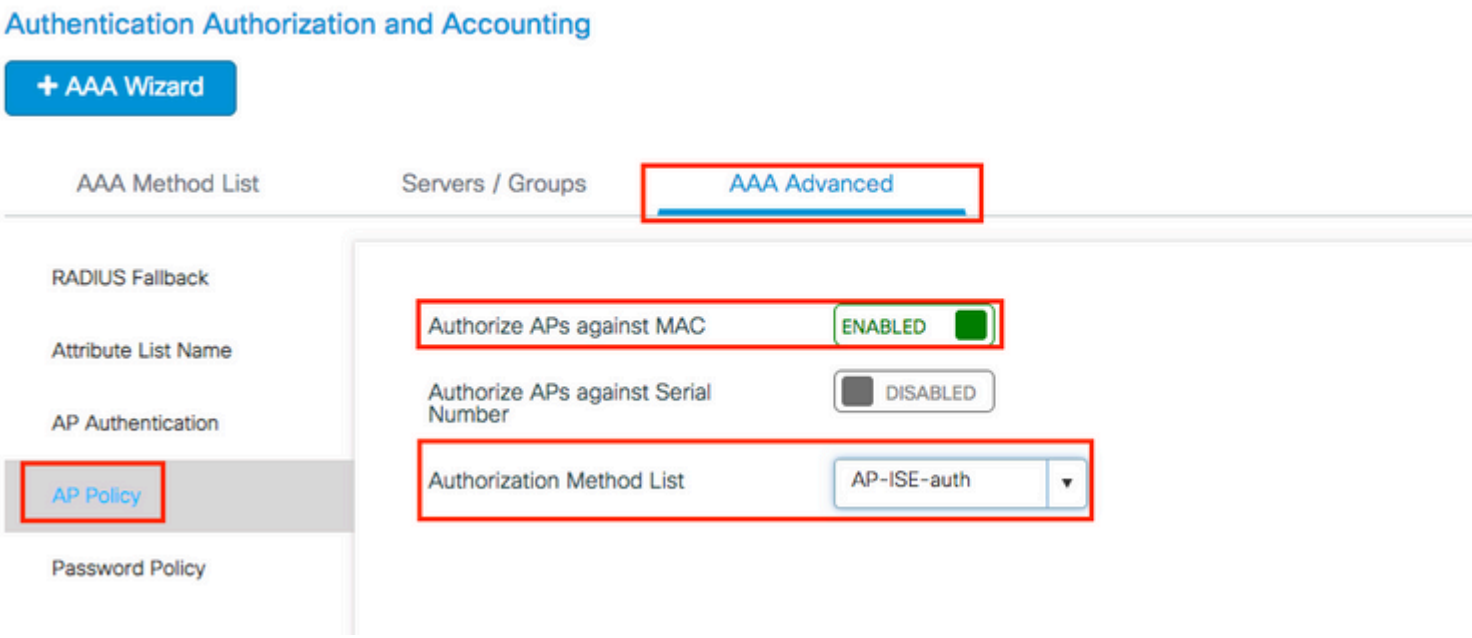
Navegue até **Configuration > Security > AAA > AAA Method List > Authorization > + Add**





Etapa 4. Ative a autorização MAC do AP.

Navegue até **Configuração > Segurança > AAA > AAA Advanced > AP Policy.** Ative **Authorize APs against MAC** e selecione a **Authorization Method List** criada na Etapa 3.



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 credential-download <AP-auth> group <radius-grp-name>
# ap auth-list authorize-mac
# ap auth-list method-list <AP-ISE-auth>
```

Configuração do ISE

Etapa 1. Para adicionar a WLC 9800 ao ISE:

Declarar WLC 9800 no ISE

Escolha configurar com base na autenticação o endereço MAC dos APs com as etapas necessárias:

Configure USE para autenticar o endereço MAC como pontos finais

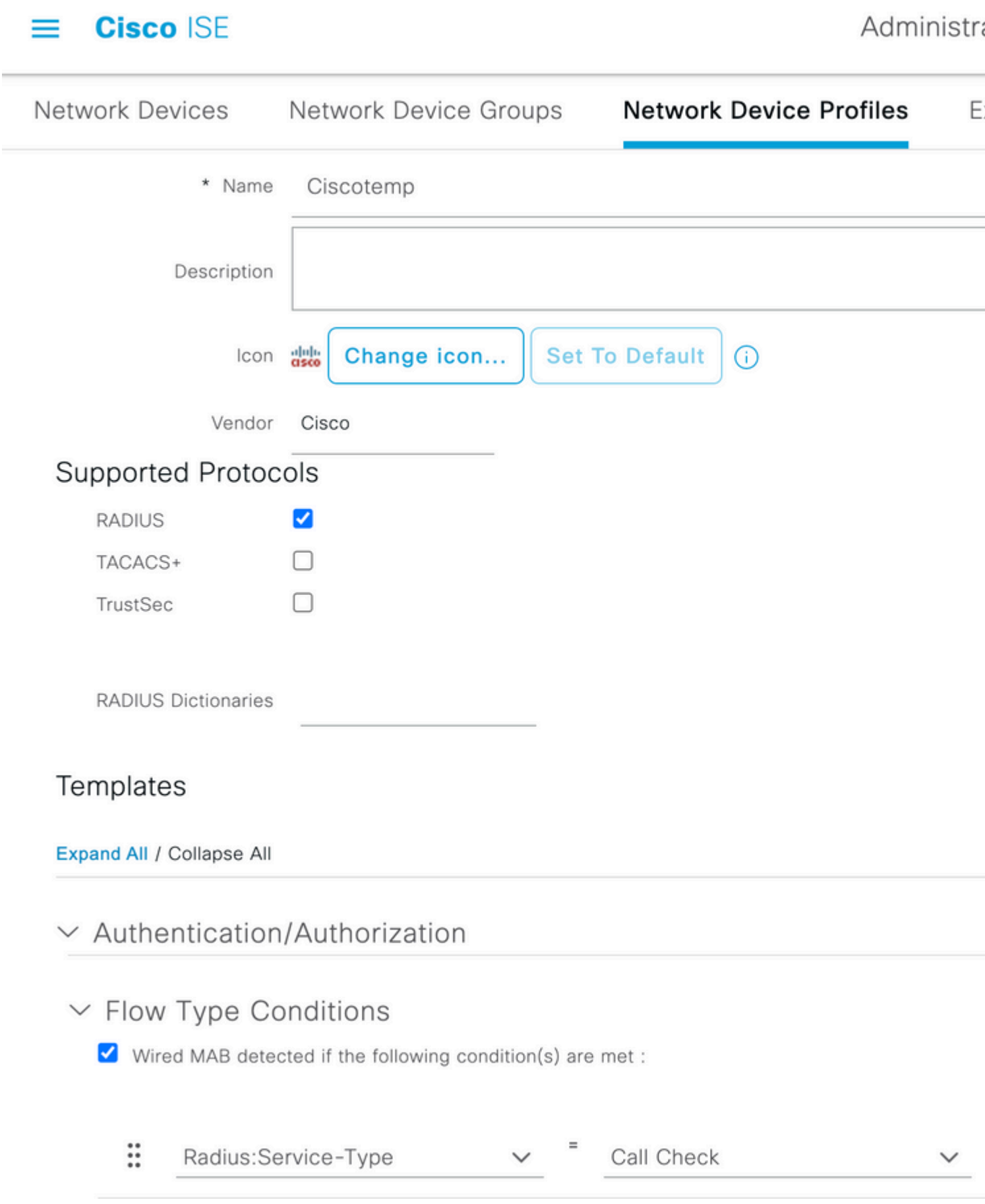
Configurar o ISE para autenticar o endereço MAC como nome de usuário/senha

Configurar o ISE para autenticar o endereço MAC como endpoints

Etapa 2. (Opcional) Criar um grupo de identidade para Pontos de Acesso

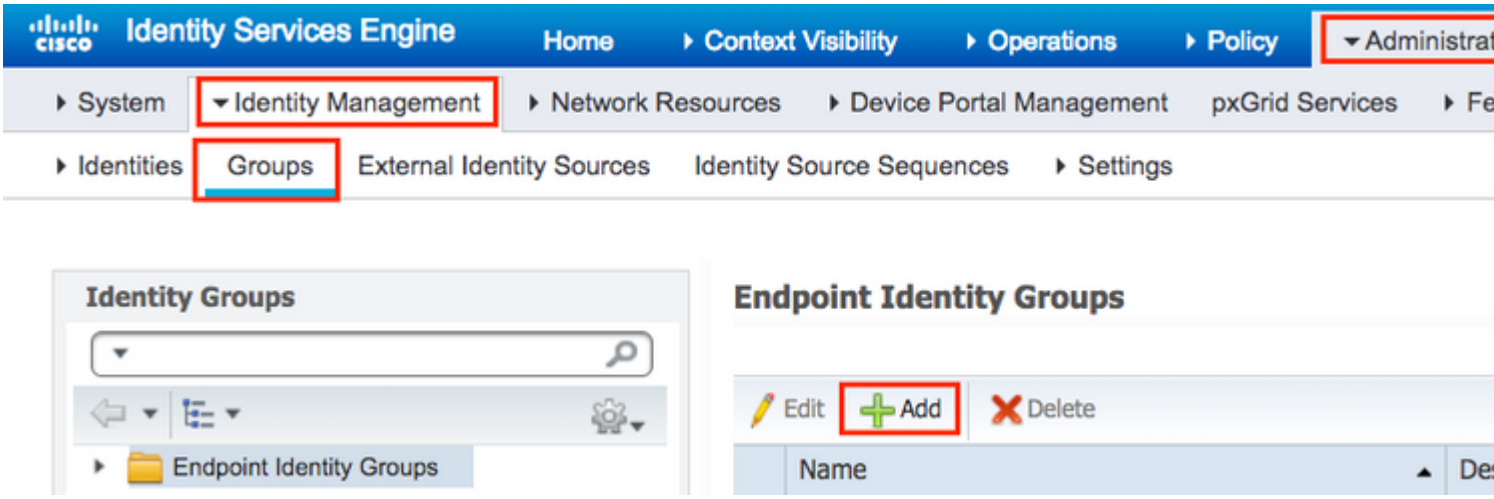
Como o 9800 não envia o atributo NAS-port-Type com autorização de AP, bug Cisco IDCSCvy74904), o ISE não reconhece uma autorização de AP como um fluxo de trabalho de MAB e, portanto, não é possível autenticar um AP se o endereço MAC do AP for colocado na lista de endpoints, a menos que você modifique os fluxos de trabalho de MAB para não exigir o atributo do tipo de porta NAS no ISE.

Navegue até **Administrator > Network device profile** e crie um novo perfil de dispositivo. Ative o RADIUS e adicione service-type=call-check para MAB com fio. Você pode copiar o restante do perfil original da Cisco, a ideia é não ter nenhuma condição "no-port-type" para o MAB com fio.

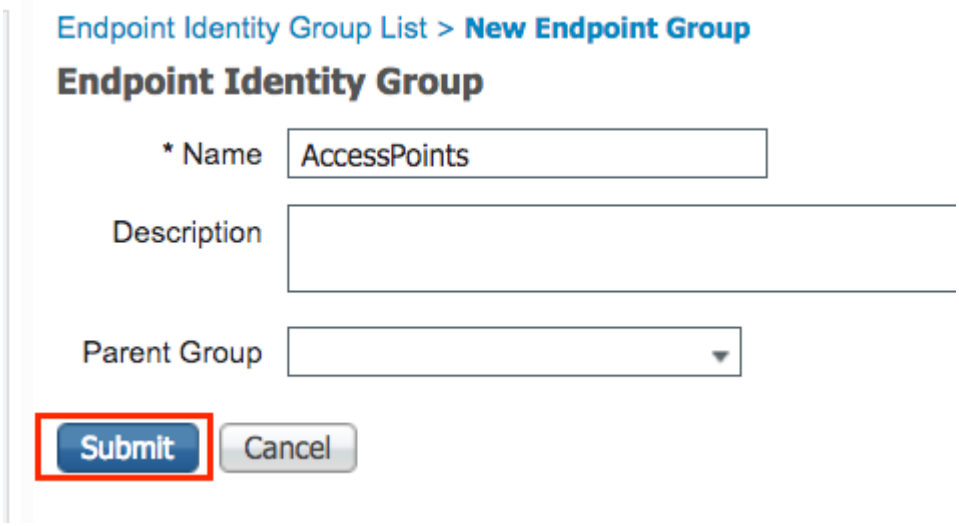


Volte para a entrada do dispositivo de rede do 9800 e defina seu perfil para o perfil de dispositivo recém-criado.

Navegue até **Administração > Gerenciamento de identidades > Grupos > Grupos de identidade de endpoint > Adicionar.**

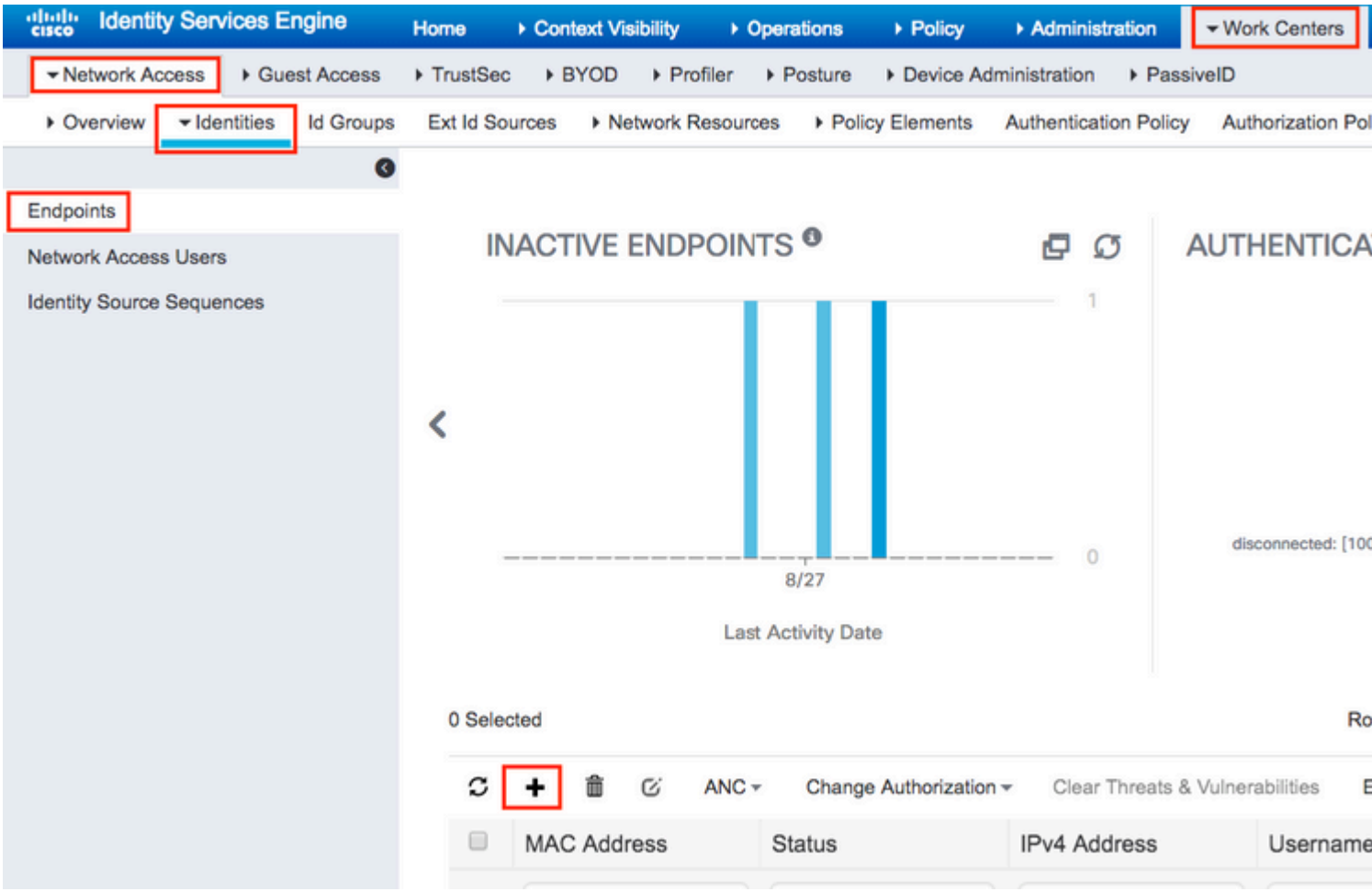


Escolha um nome e clique em **Enviar.**

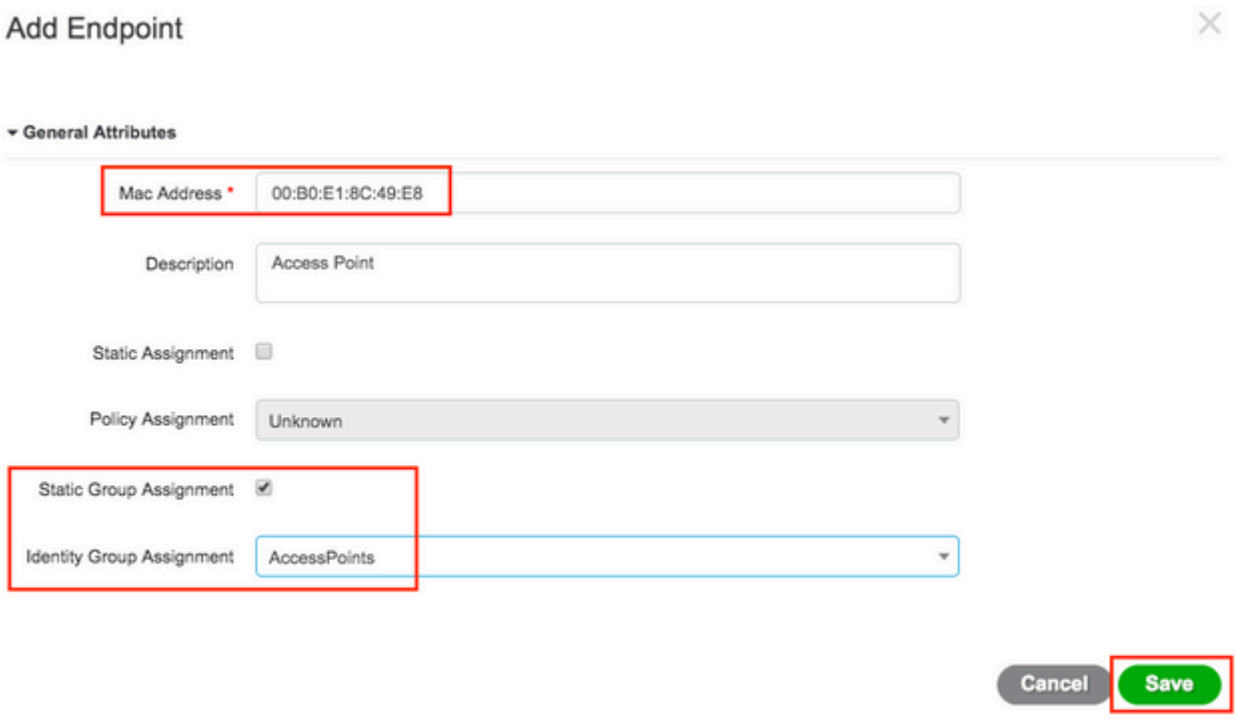


Etapa 3. Adicione o endereço MAC Ethernet do AP ao seu grupo de identidade de ponto final.

Navegue até **Centros de trabalho > Acesso à rede > Identidades > Endpoints > +**



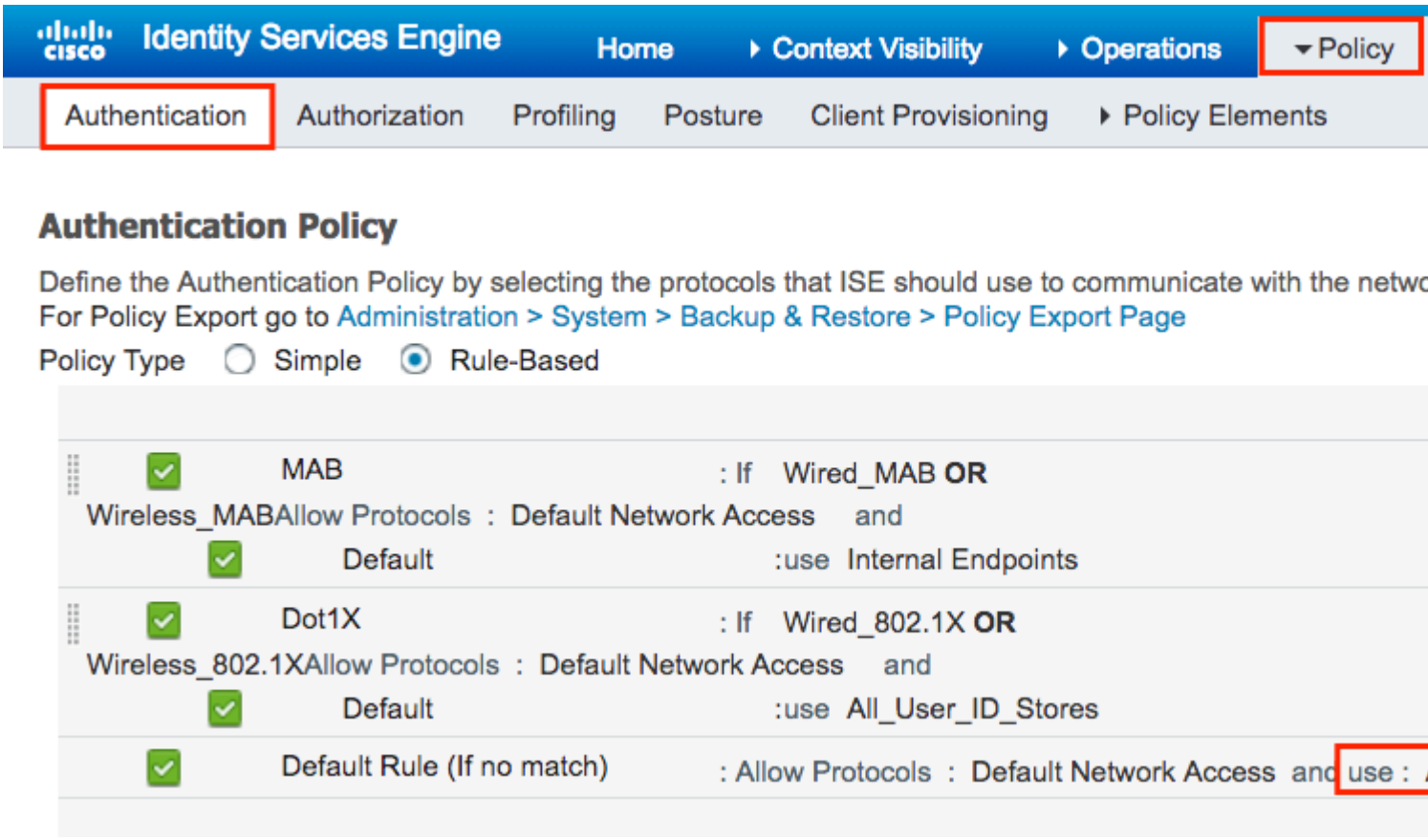
Insira as informações necessárias.



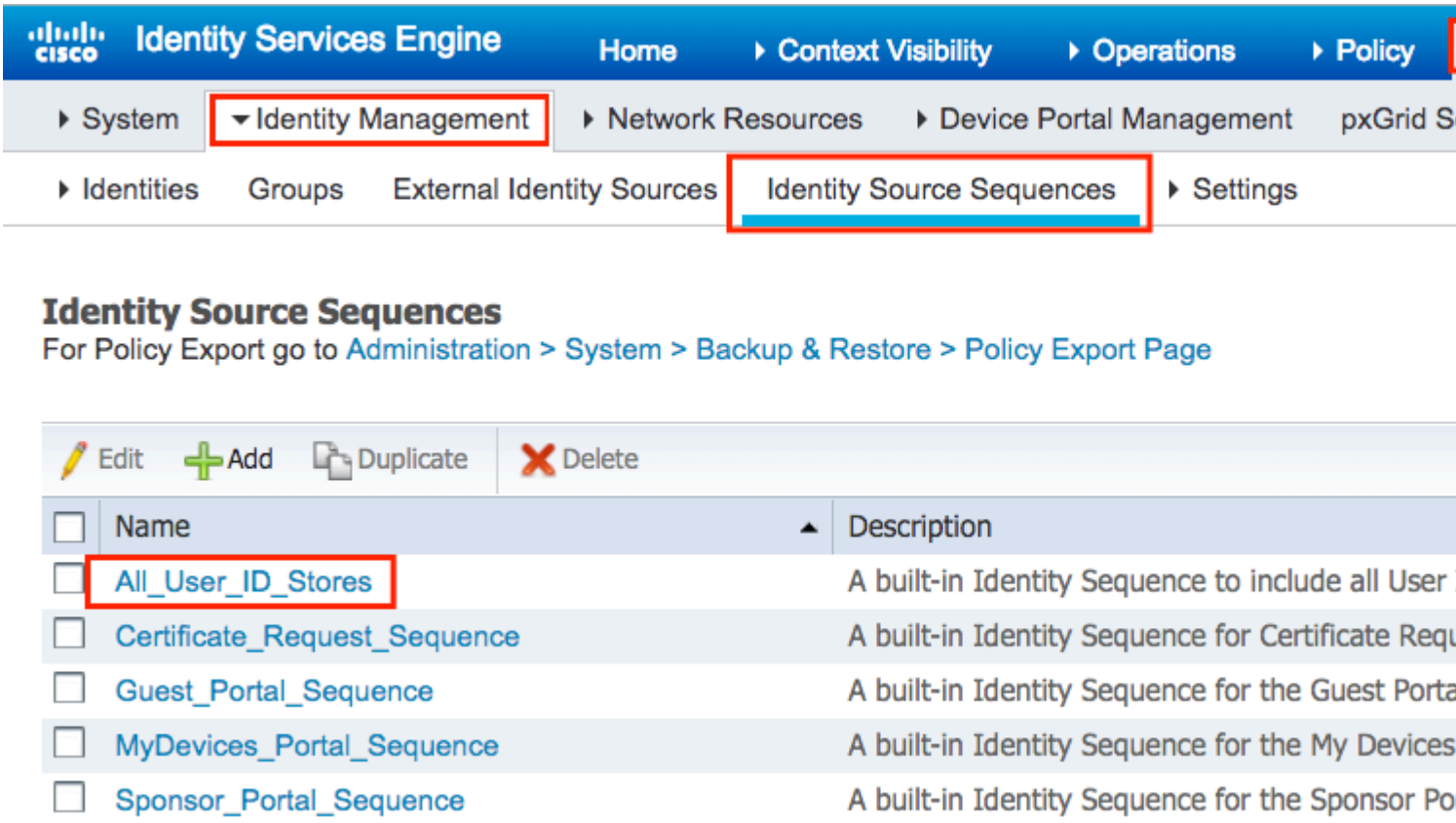
Etapa 4. Verifique se o armazenamento de identidade usado na regra de autenticação padrão contém os

pontos de extremidade internos.

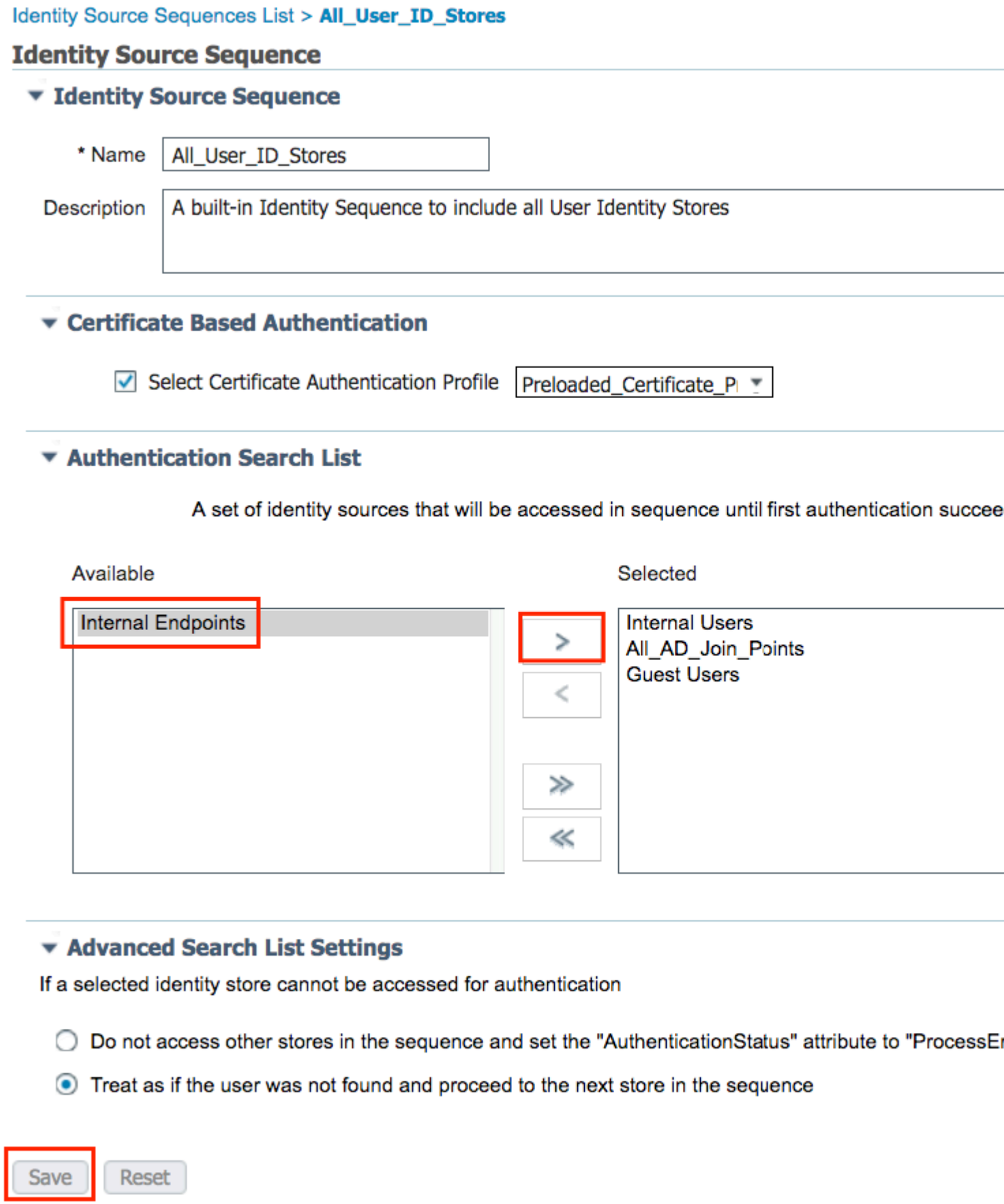
A. Navegue até **Policy** > **Authentication** e anote o Identity store.



B. Navegue até **Administração** > **Gerenciamento de identidades** > **Sequências de origem de identidade** > **Nome da identidade.**



C. Certifique-se de que endpoints internos pertençam a ele; caso contrário, adicione-o.



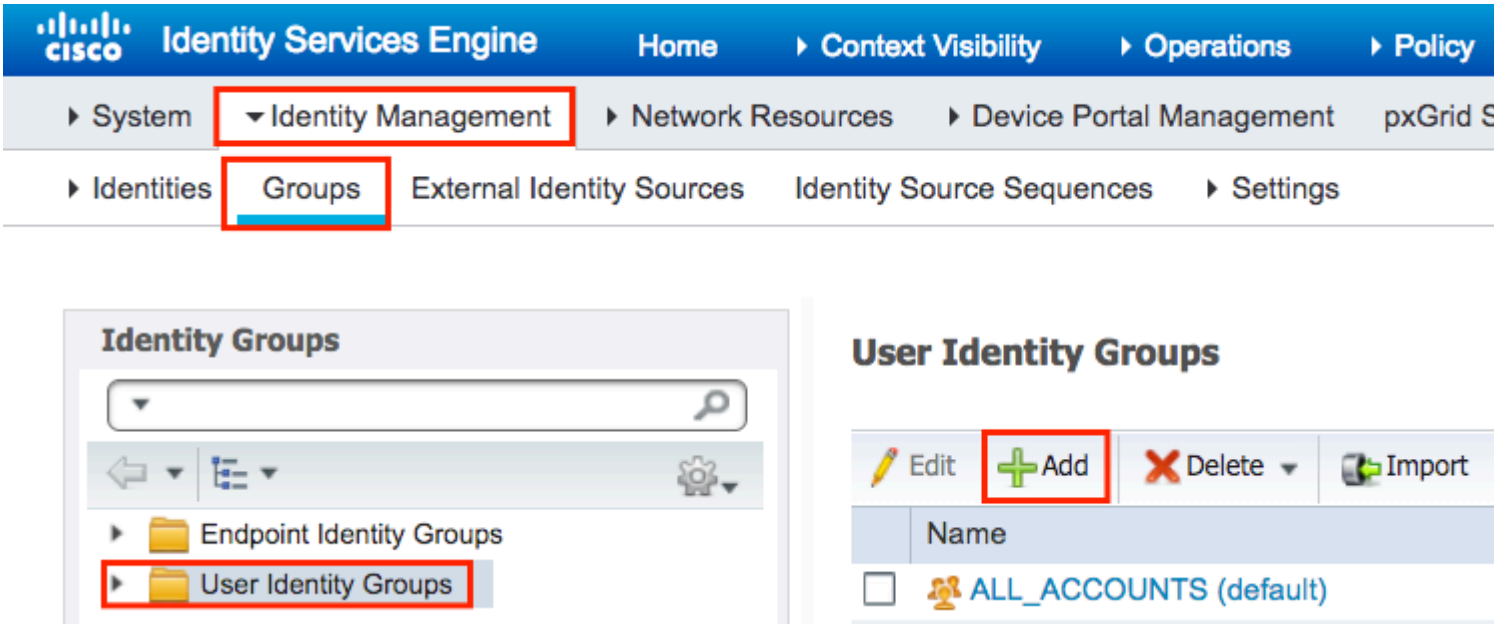
Configurar o ISE para autenticar o endereço MAC como nome de usuário/senha

Este método não é recomendado, pois requer políticas de senha mais baixas para permitir a mesma senha que o nome de usuário.

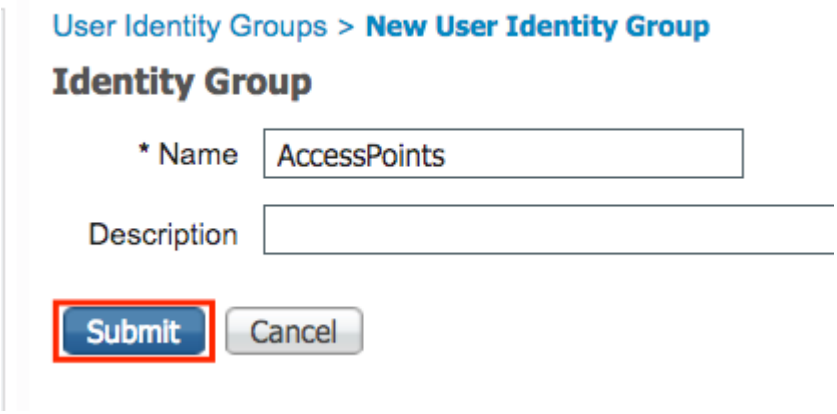
No entanto, pode ser uma solução alternativa caso você não possa modificar seu perfil de dispositivo de rede

Etapa 2. (Opcional) Criar um grupo de identidade para Pontos de Acesso

Navegue até **Administração > Gerenciamento de identidades > Grupos > Grupos de identidades do usuário > + Adicionar.**

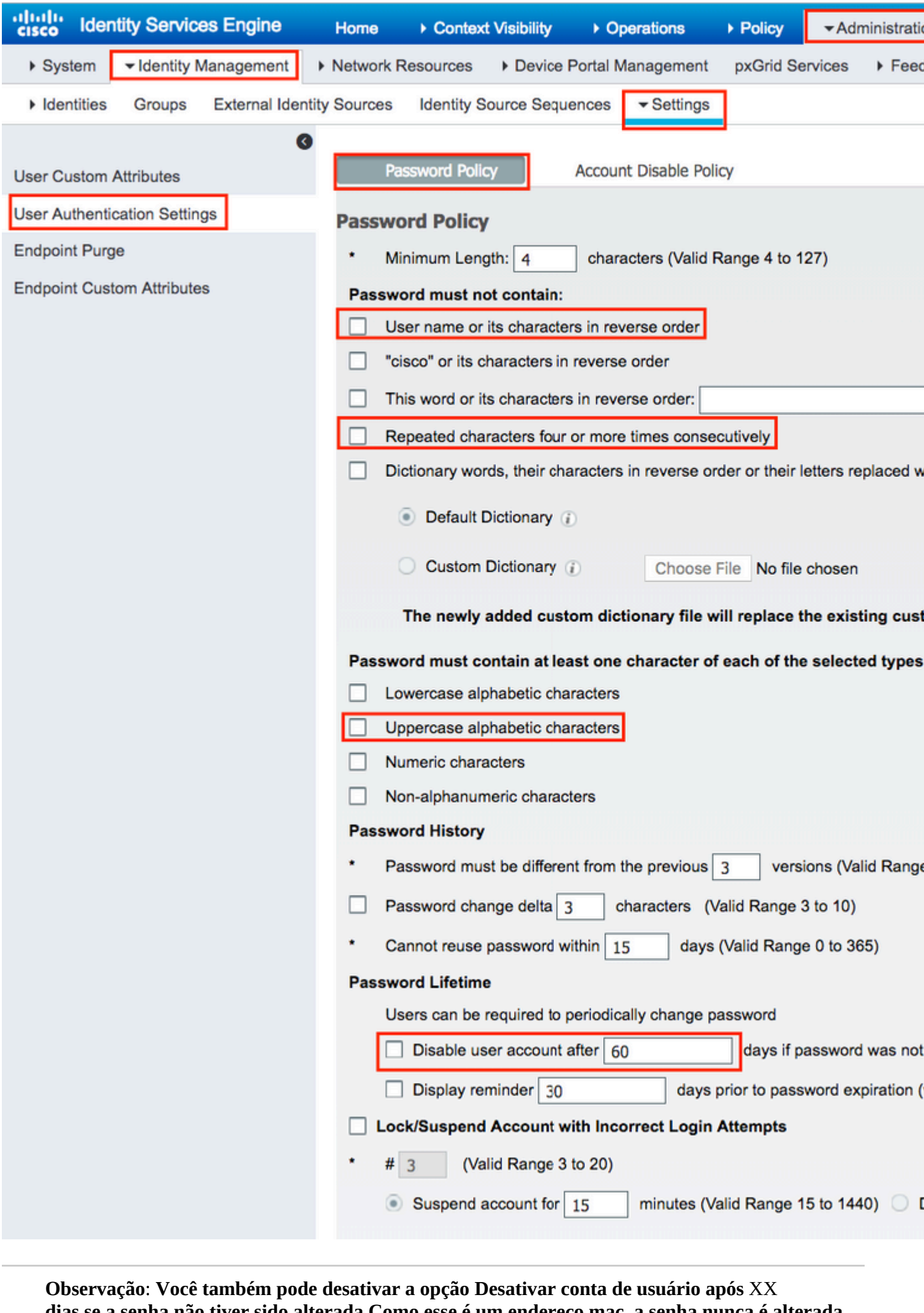


Escolha um nome e clique em **Enviar.**



Etapa 3. Verifique se a política de senha atual permite adicionar um endereço mac como nome de usuário e senha.

Navegue para **Administração > Gerenciamento de identidades > Configurações > Configurações de autenticação de usuário > Política de senha** e verifique se pelo menos estas opções estão desabilitadas:

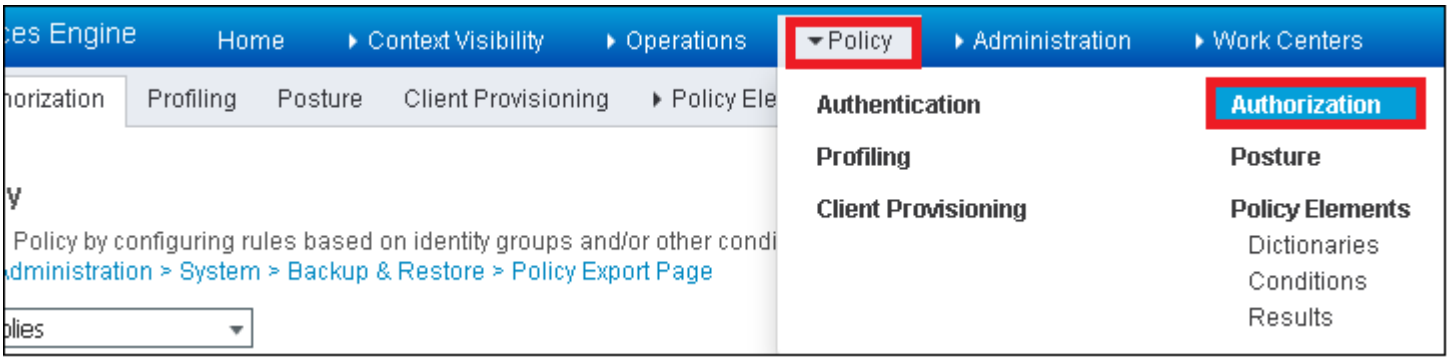


Observação: **Você também pode desativar a opção Desativar conta de usuário após** XX **dias se a senha não tiver sido alterada Como esse é um endereço mac, a senha nunca é alterada**

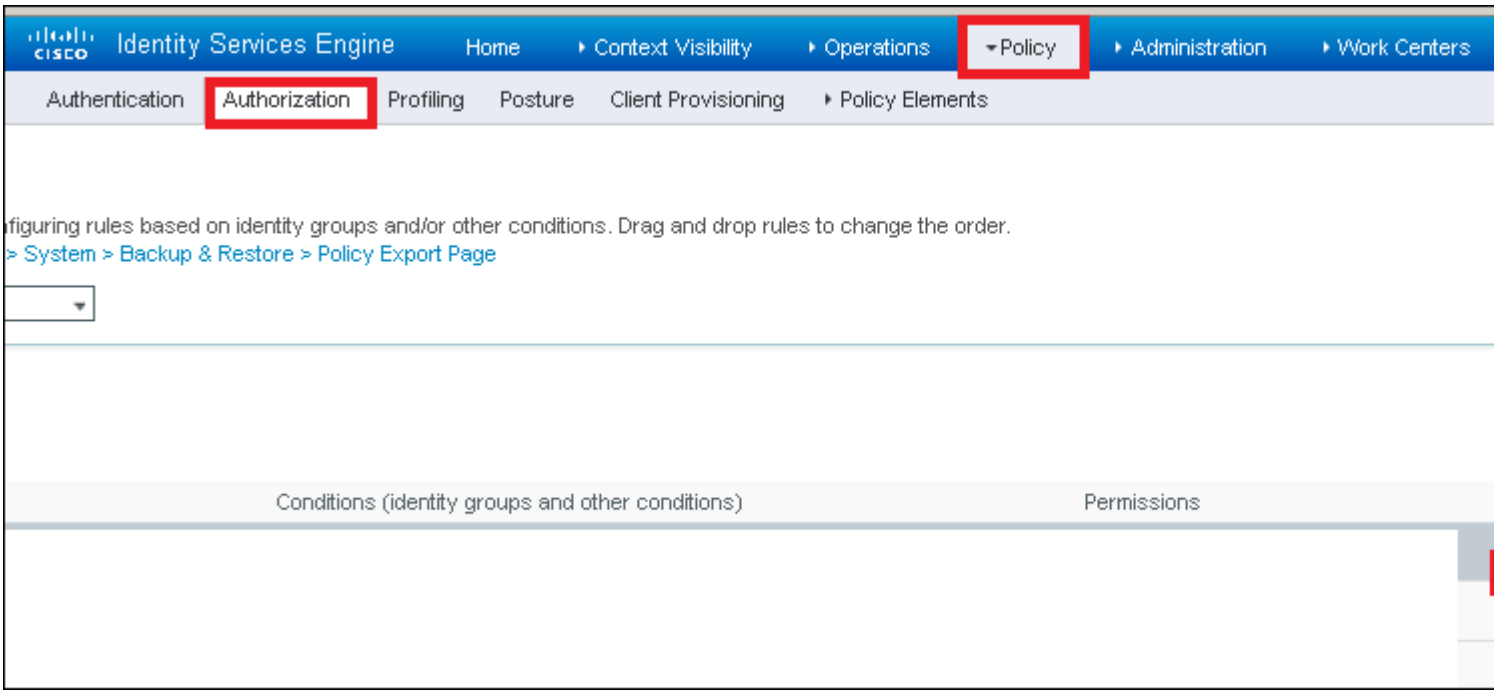
O campo Senha deve ser o endereço MAC ethernet do AP, todos em letras minúsculas e nenhum separador.

Política de autorização para autenticar APs

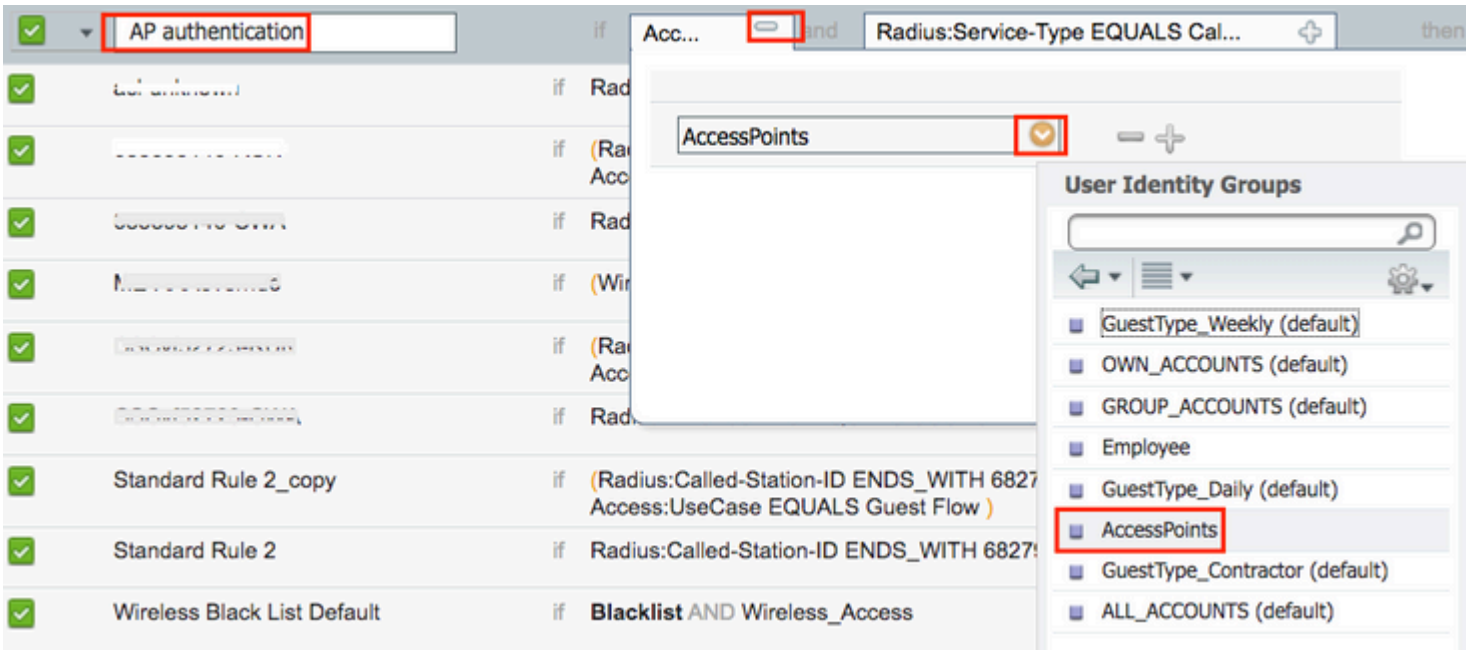
Navegue **paraPolítica > Autorização** conforme mostrado na imagem.



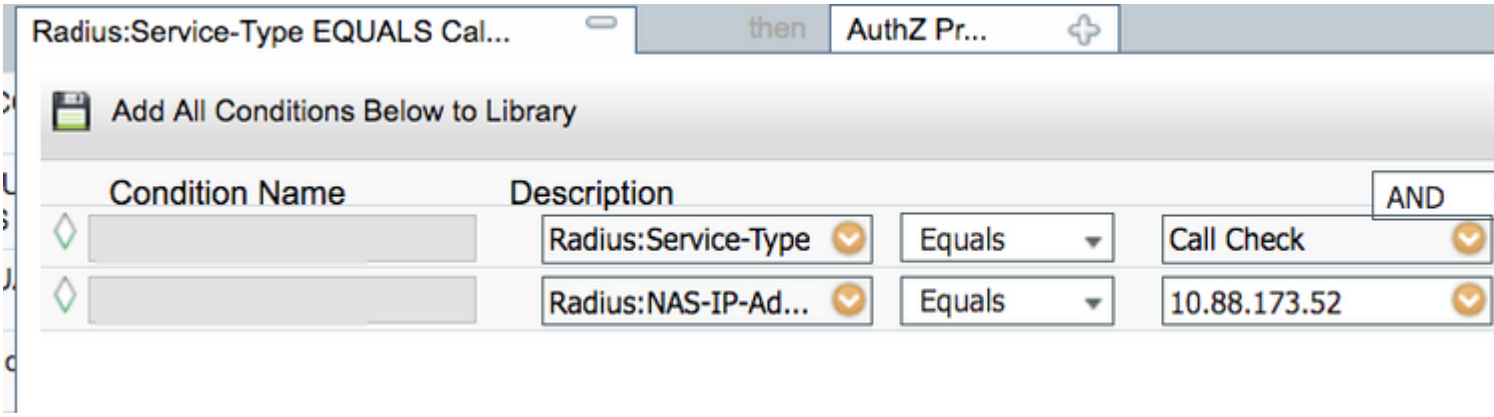
Inserir uma nova regra conforme mostrado na imagem.



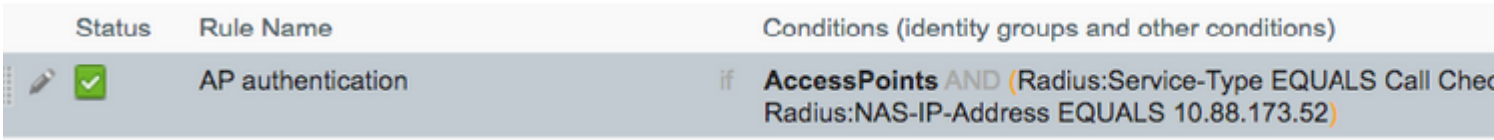
Primeiro, selecione um nome para a regra e o grupo Identidade onde o Ponto de acesso está armazenado (Pontos de acesso). Selecione **User Identity Groups** se decidir autenticar o endereço MAC como nome de usuário e senha ou **Endpoint Identity Groups** se decidir autenticar o endereço MAC do AP como pontos de extremidade.



Depois disso, selecione outras condições que fazem com que o processo de autorização se encaixe nessa regra. Neste exemplo, o processo de autorização atinge essa regra se usar o tipo de serviço Call Check e a solicitação de autenticação vier do endereço IP 10.88.173.52.



Por fim, selecione o perfil de autorização atribuído aos clientes que atingiram essa regra, clique emConcluídoe salve-o como mostrado na imagem.



Observação: os APs que já se uniram na controladora não perdem sua associação. Se, no entanto, após a habilitação da lista de autorização, eles perderem a comunicação com o controlador e tentarem se unir novamente, eles passarão pelo processo de autenticação. Se os endereços mac não estiverem listados localmente ou no servidor RADIUS, eles não poderão se unir de volta à controladora.

Verificar

Verifique se a WLC 9800 habilitou a lista de autenticação de AP

<#root>

```
# show ap auth-list
```

```
Authorize APs against MAC : Disabled
Authorize APs against Serial Num : Enabled
Authorization Method List : <auth-list-name>
```

Verifique a configuração de raio:

<#root>

```
#
```

```
show run aaa
```

Troubleshooting

A WLC 9800 fornece recursos de rastreamento SEMPRE ATIVOS. Isso garante que todas as mensagens de erros relacionados à junção de AP, de aviso e de nível de aviso sejam constantemente registradas e você possa exibir registros de uma condição de incidente ou falha após sua ocorrência.

Observação: o volume de logs gerados varia de 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 por meio dessas etapas (certifique-se de registrar a sessão em um arquivo de texto).

Etapa 1. Verifique a hora atual do controlador para que você possa acompanhar os registros no tempo de volta 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 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 Trace 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 habilitadas (endereço mac, endereço ip, etc.). Isso aumentaria 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 de rádio 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 Ative (RA), que fornece rastreamentos no nível de depuração para todos os processos que interagem com a condição especificada (endereço mac do cliente, neste caso).

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

```
# 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). Como alternativa, você pode aumentar esse tempo para até 2.085.978.494 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 na sessão de terminal, pois tudo é armazenado em buffer internamente para ser exibido mais tarde.

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>
```

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_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Etapa 9. Colete o arquivo da atividade do endereço MAC. Você pode copiar o registro de rastreamento de RA 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_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.d
```

Mostre o conteúdo:

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

Etapa 10. Se a causa do problema ainda não for evidente, colete os registros internos, que são uma visualização mais detalhada dos registros de nível de depuração. Não é necessário depurar o cliente novamente, pois só examinamos mais detalhadamente os logs de depuração já coletados e armazenados internamente.

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

Observação: a saída desse comando retorna rastros para todos os níveis de registro 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 Troubleshooting.

Referências

Unir APs de malha ao WLC 9800

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.