Configurar a autenticação da Web central com âncora no Catalyst 9800

Contents

Introduction

Este documento descreve como configurar e solucionar problemas de uma Central Web Authentication (CWA) no Catalyst 9800 apontando para outro Wireless LAN Controller (WLC) como âncora de mobilidade, abrangendo o destino com o AireOS ou outro 9800 WLC.

Prerequisites

Requirements

Recomenda-se que você tenha uma compreensão básica da WLC 9800, da WLC AireOS e do Cisco ISE. Supõe-se que, antes de iniciar a configuração de âncora do CWA, você já tenha criado o túnel de mobilidade entre as duas WLCs. Isso está fora do escopo deste exemplo de configuração. Se precisar de ajuda com isso, consulte o documento intitulado "Criação de túneis de mobilidade em controladores Catalyst 9800"

Componentes Utilizados

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.

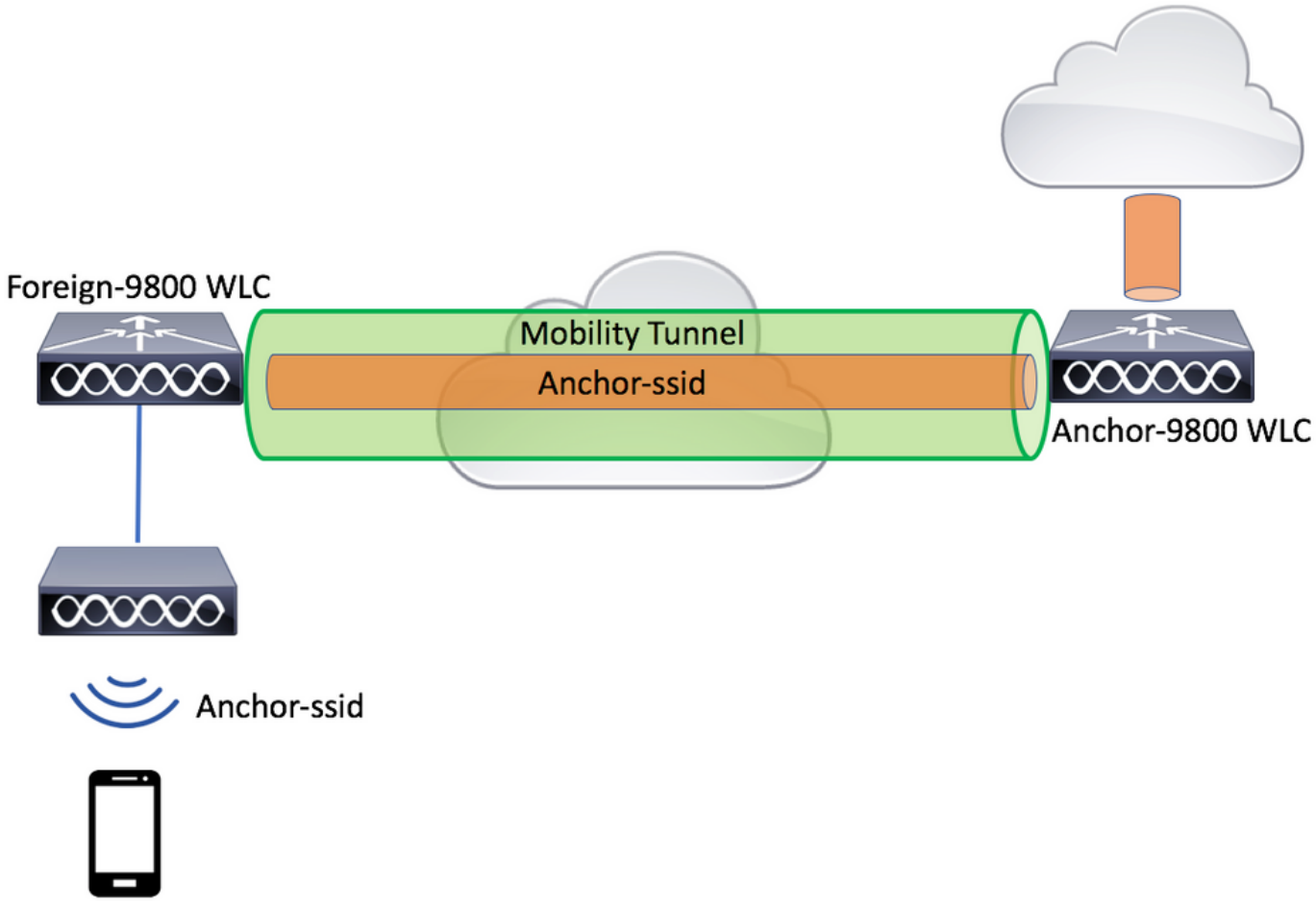
9800 17.2.1

5520 Imagem do IRCM 8.5.164

ISE 2.4

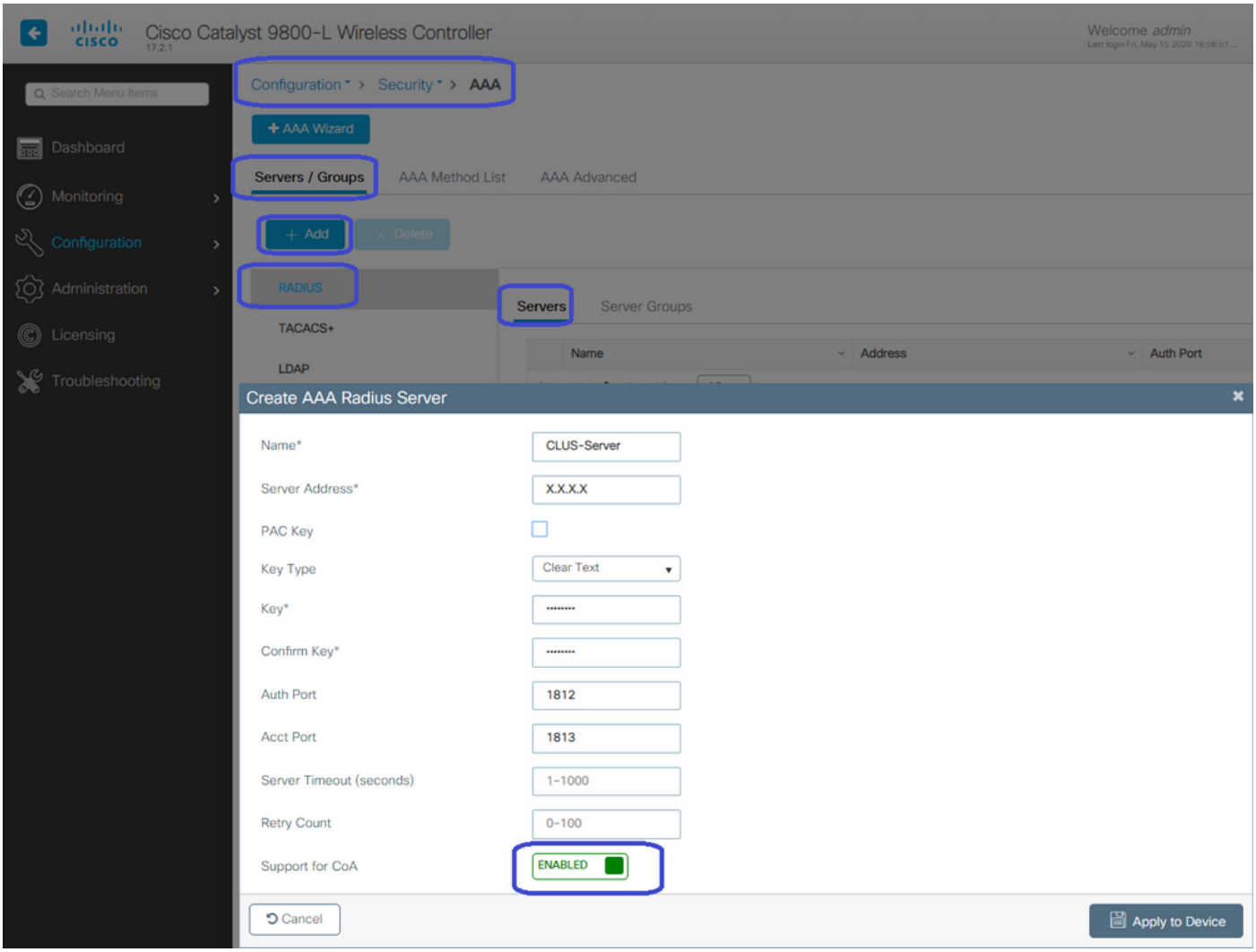
Configurar um Catalyst 9800 ancorado em outro Catalyst 9800

Diagrama de Rede

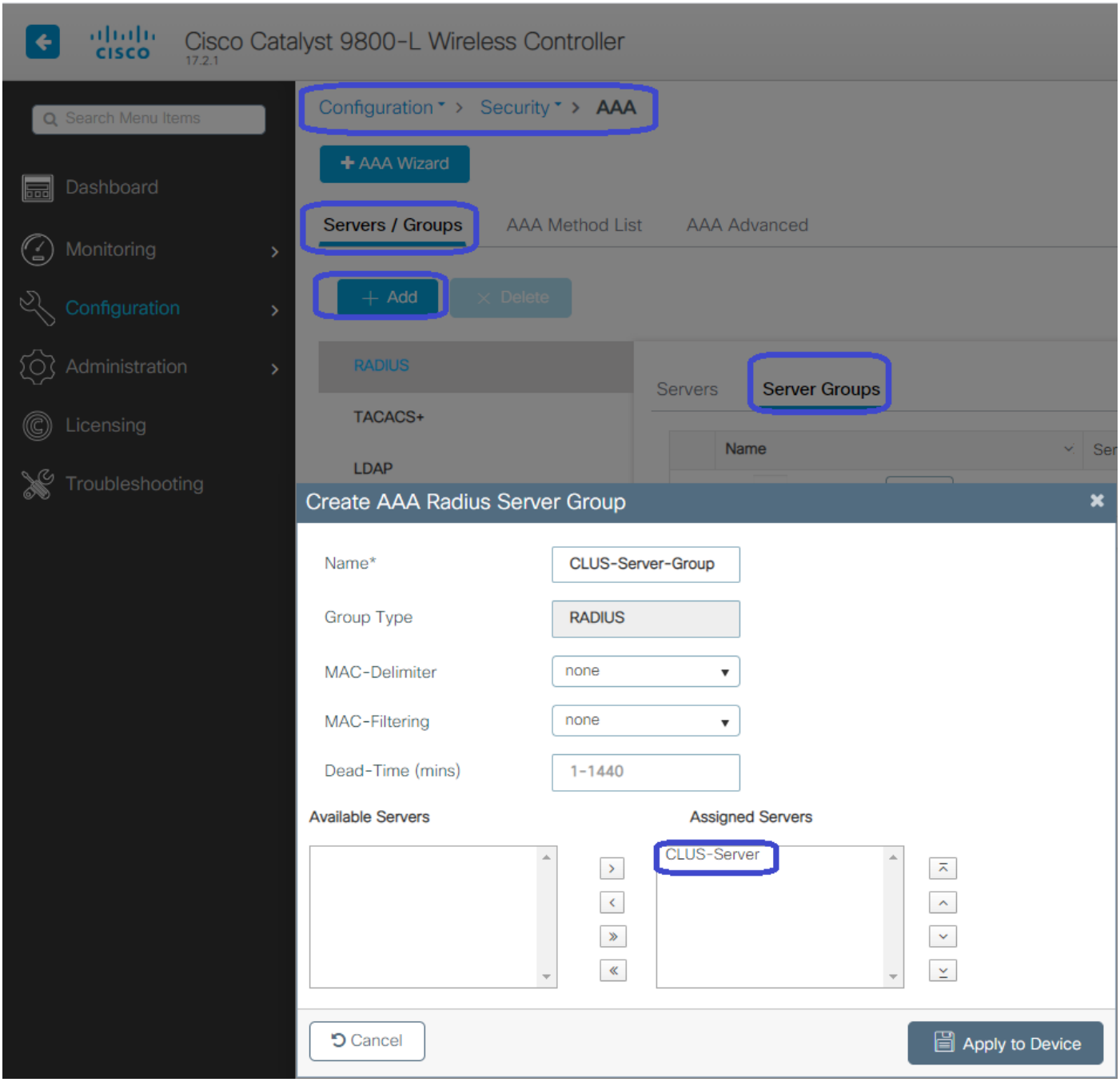


Configurar AAA em ambos os 9800s

Na âncora e no estrangeiro, você precisará primeiro adicionar o servidor RADIUS e verificar se CoA está ativado. Isso pode ser feito no menu**Configuration>Security>AAA>Servers/Groups>Servers> clique no botão Add**

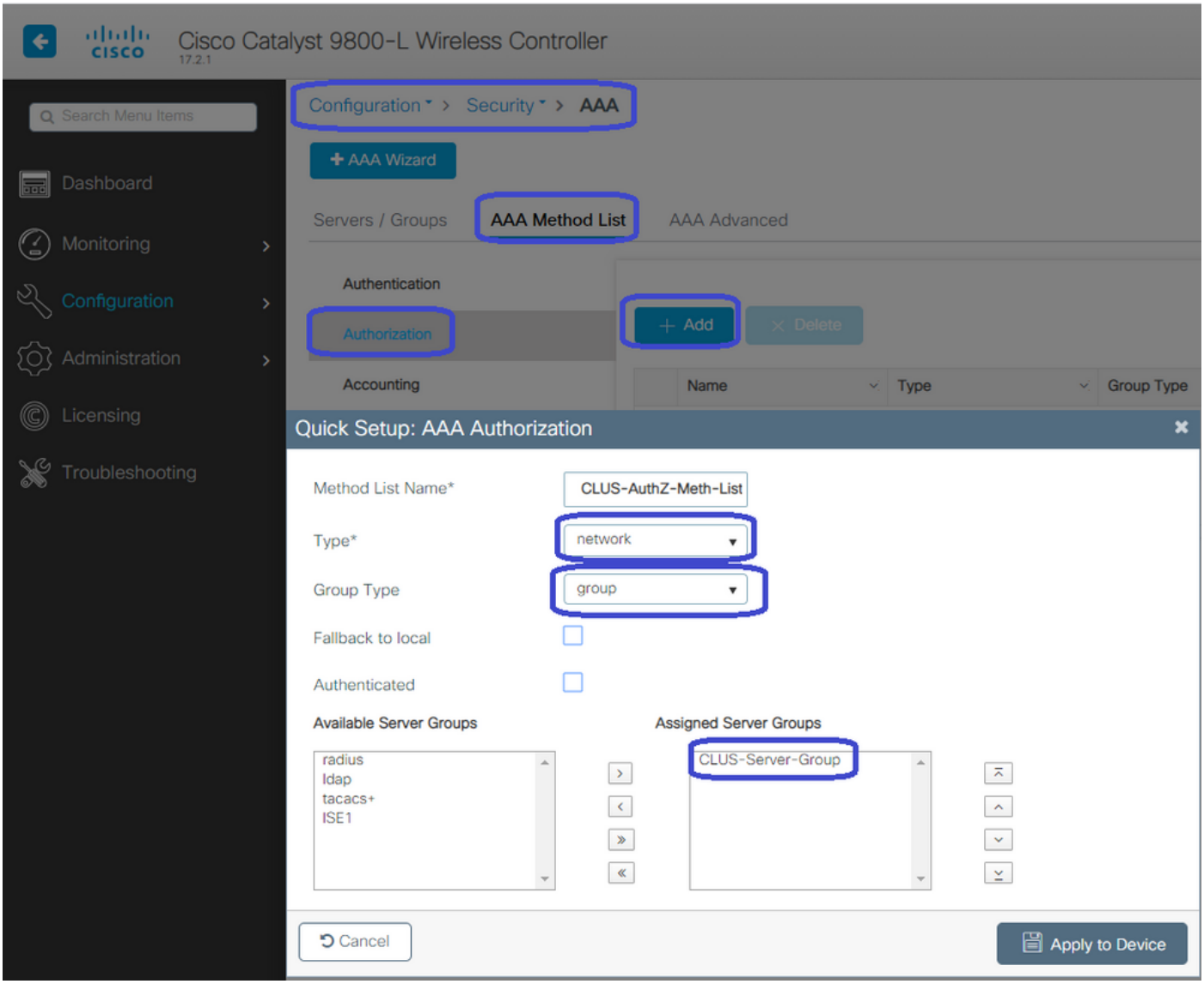


Agora você precisará criar um grupo de servidores e colocar o servidor que acabou de configurar nesse grupo. Isso é feito aqui **Configuration>Security>AAA>Servers/Groups>Server Groups>+Add**.

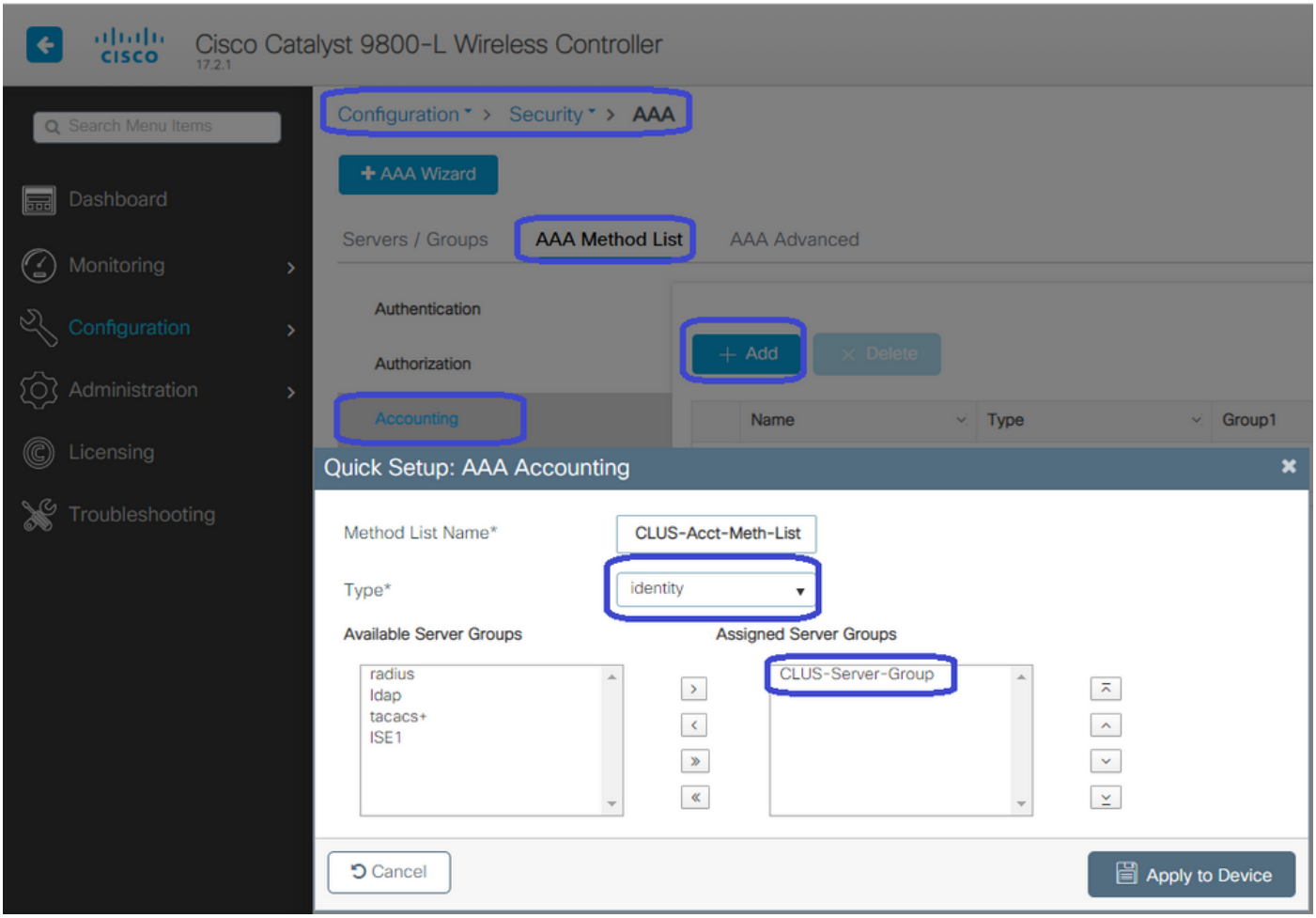


Agora, crie uma lista de métodos **de autorização** (uma lista de métodos de autenticação não é necessária para CWA) em que o tipo é rede e o tipo de grupo é grupo. Adicione o grupo de servidores da ação anterior a esta lista de métodos.

Esta configuração é feita aqui **Configuration>Security>AAA>Servers/AAA Method List>Authorization>+Add**

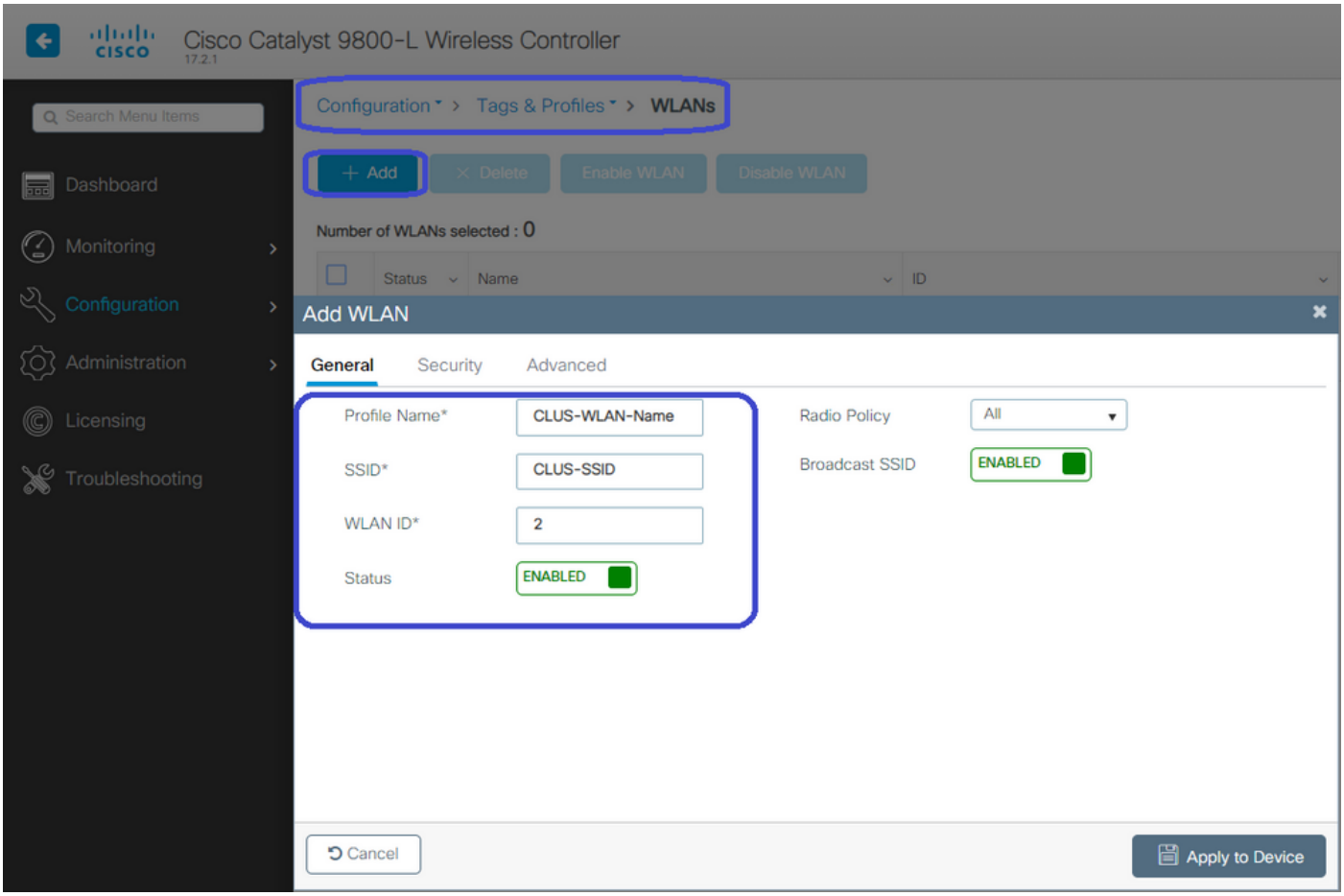


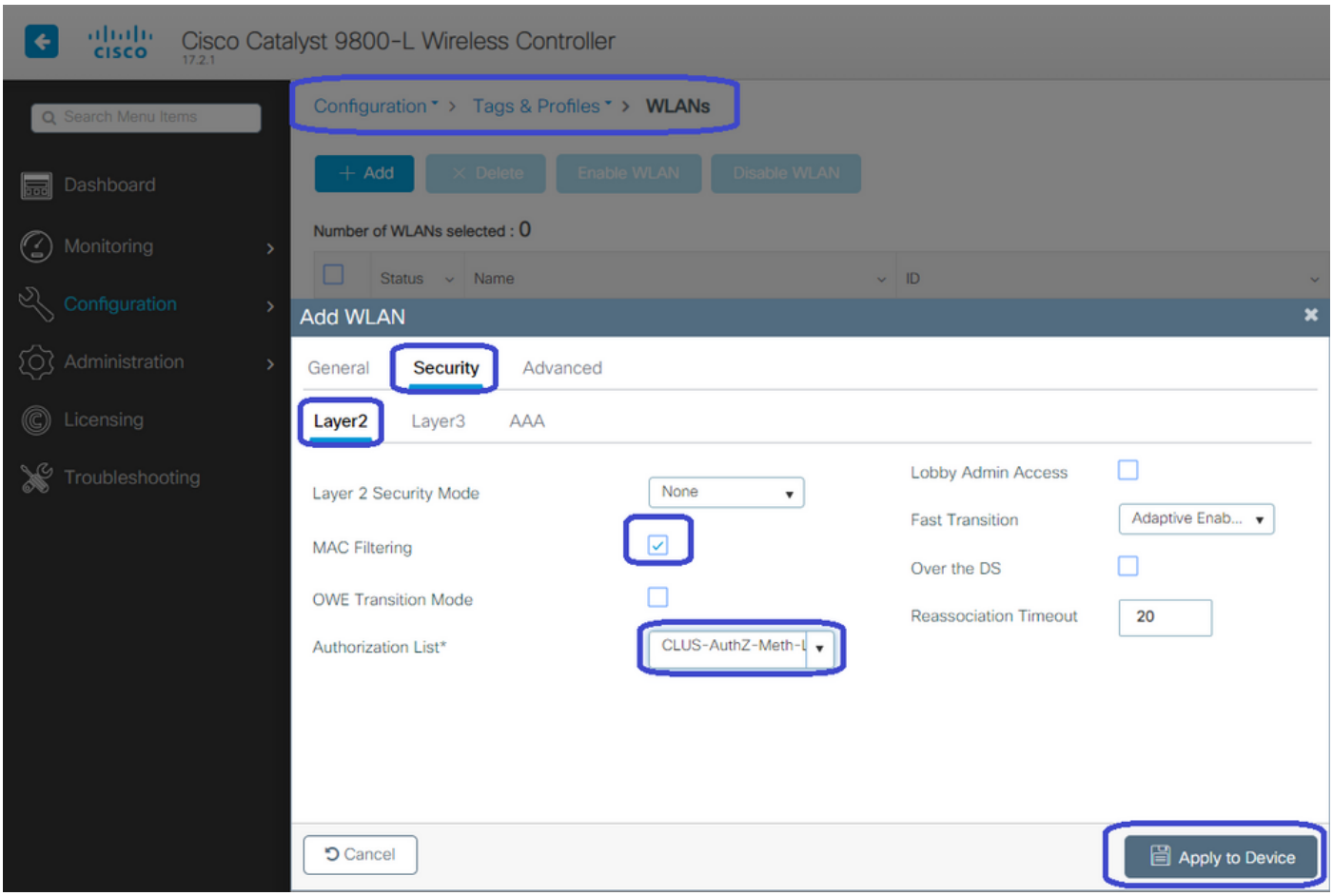
(Opcional) Crie uma lista de métodos contábeis usando o mesmo grupo de servidores da lista de métodos de autorização. A lista contábil pode ser criada aqui **Configuration>Security>AAA>Servers/AAA Method List>Accounting>+Add**



Configurar as WLANs nas WLCs

Crie e configure as WLANs em ambas as WLCs. As WLANs devem corresponder em ambos. O tipo de segurança deve ser filtragem mac e a lista de métodos de autorização da etapa anterior deve ser aplicada. Esta configuração é feita em **Configuração>Marcas e perfis>WLANs>+Adicionar**



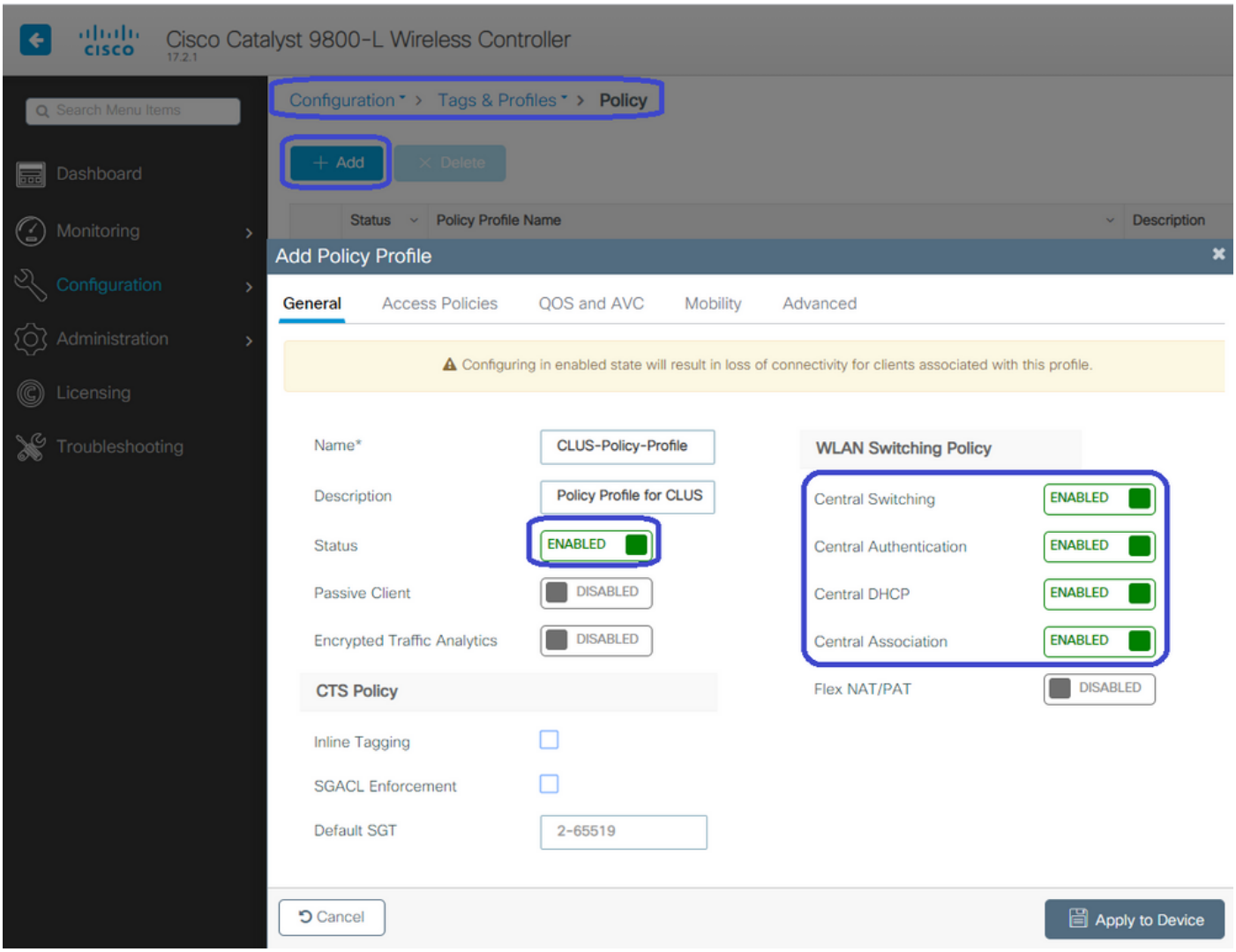


Criar o perfil de política e a marca de política na WLC externa

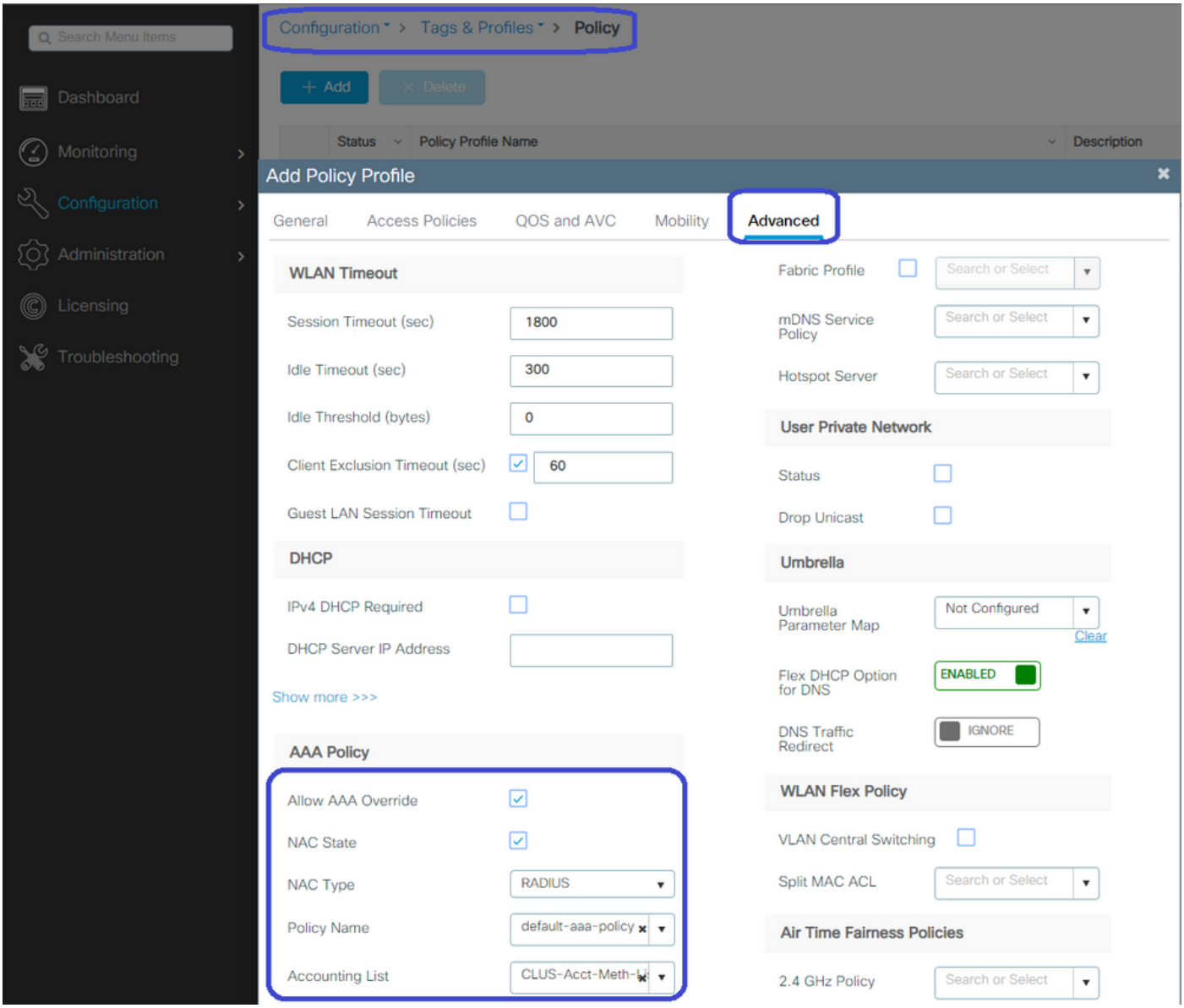
Vá para a IU da Web da WLC estrangeira.

Para criar o perfil de política, vá para **Configuration>Tags & Profiles>Policy>+Add**

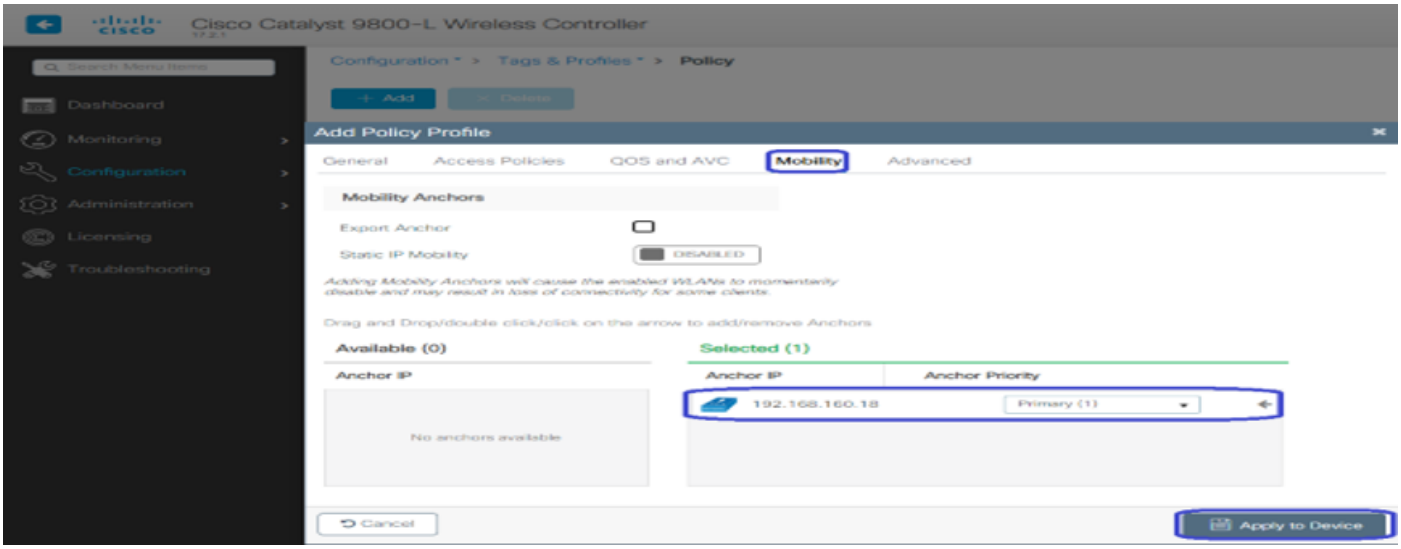
Ao ancorar, você precisa usar a comutação central.



Na guia "Avançado", a substituição de AAA e o RADIUS NAC são obrigatórios para o CWA. Aqui você também pode aplicar a lista de métodos de contabilidade se escolher fazer uma.



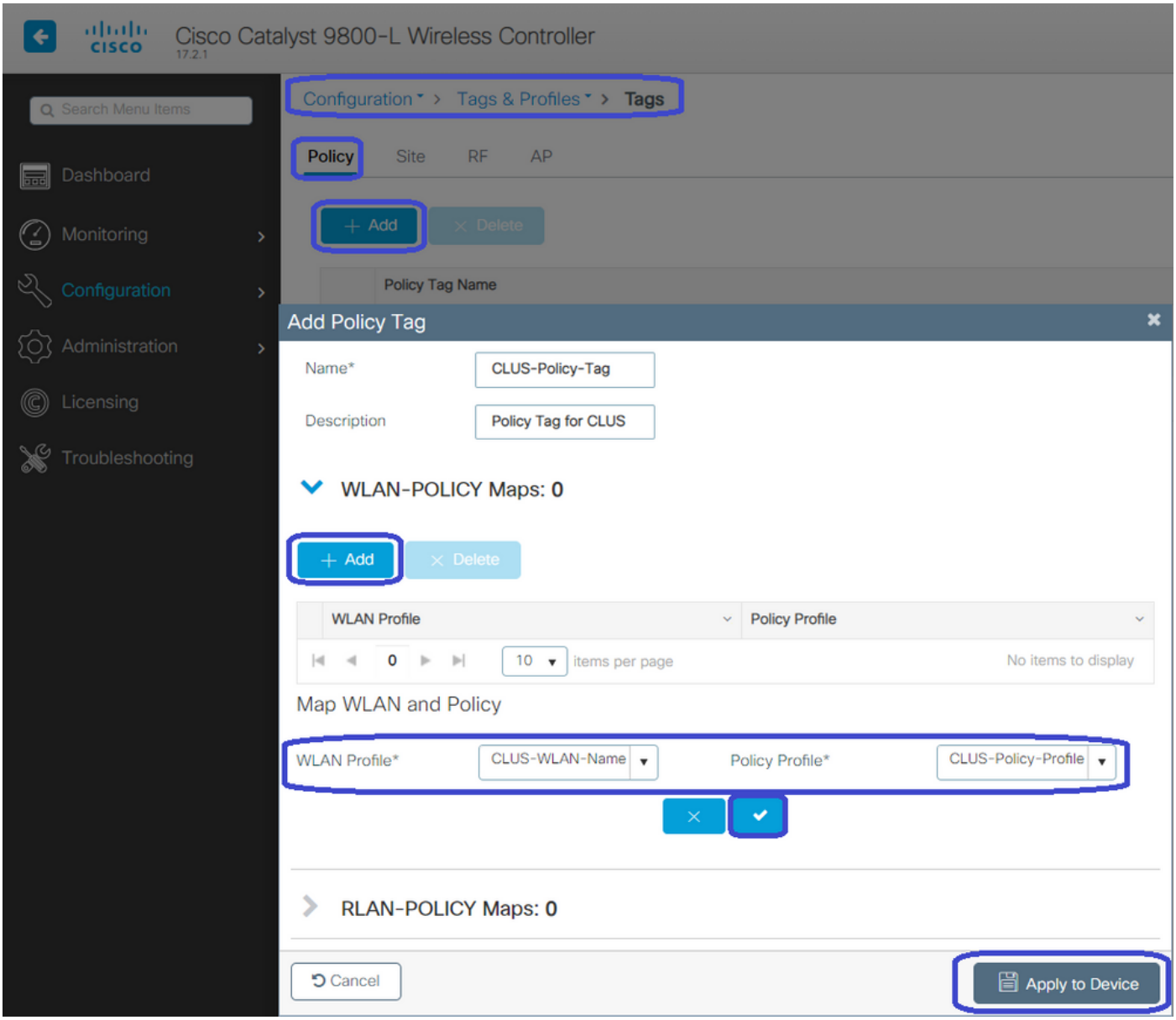
Na guia "Mobilidade", **NÃO** marque a caixa de seleção "âncora de exportação", mas adicione a WLC âncora à lista de âncoras. Certifique-se de pressionar "Apply to Device" (Aplicar ao dispositivo). Como lembrete, isso pressupõe que você já tem uma configuração de túnel de mobilidade entre os dois controladores



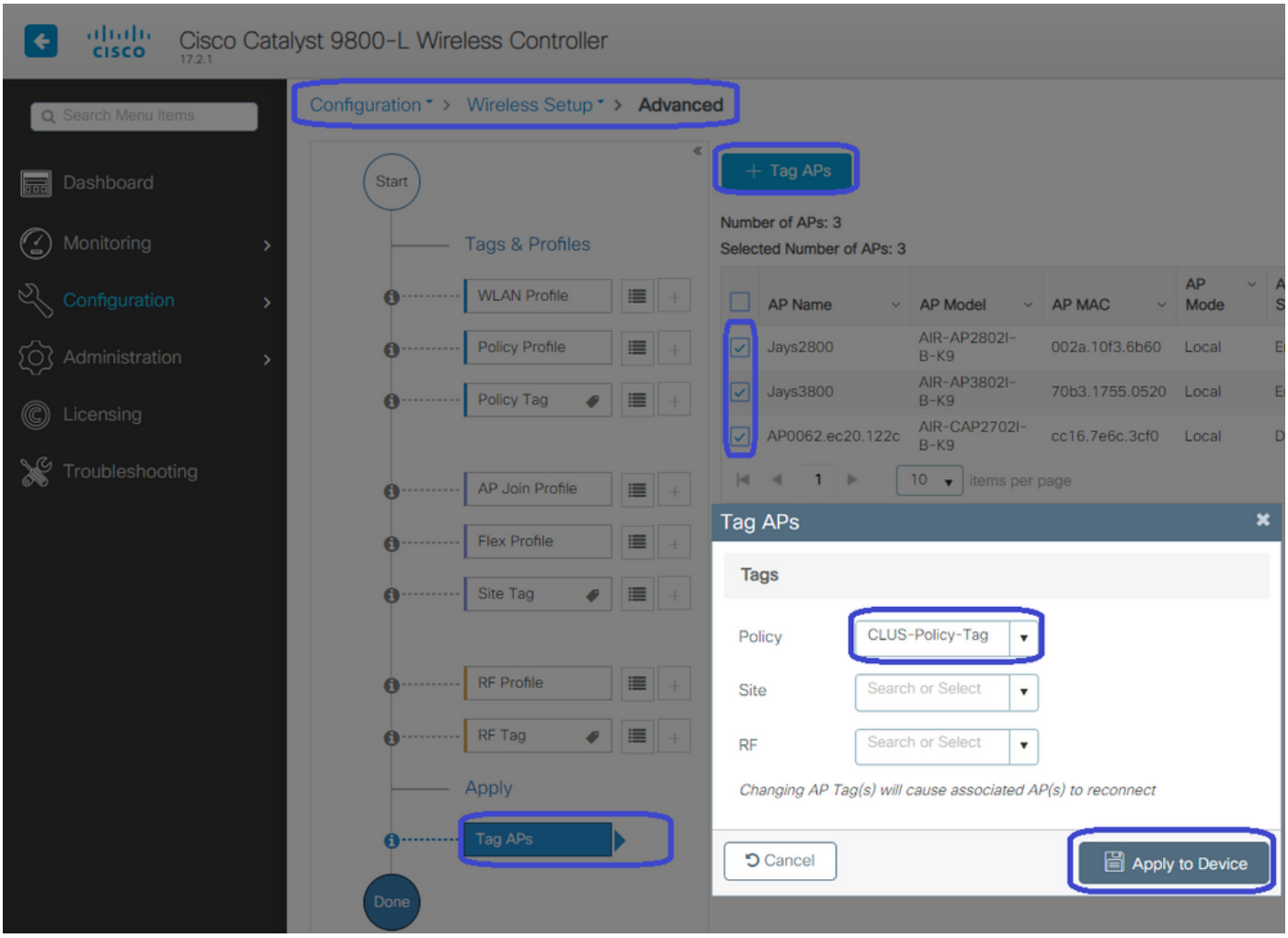
Para que os APs usem esse perfil de política, você precisará criar uma marca de política e aplicá-

la aos APs que deseja usar.

Para criar a etiqueta de política, vá para **Configuration>Tags & Profiles>Tags?Policy>+Add**



Para adicionar isso a vários APs ao mesmo tempo, vá para **Configuração>Configuração sem fio>Avançado>Iniciar agora**. Clique nas barras de marcadores ao lado de "Tag APs" e adicione a marca aos APs escolhidos.

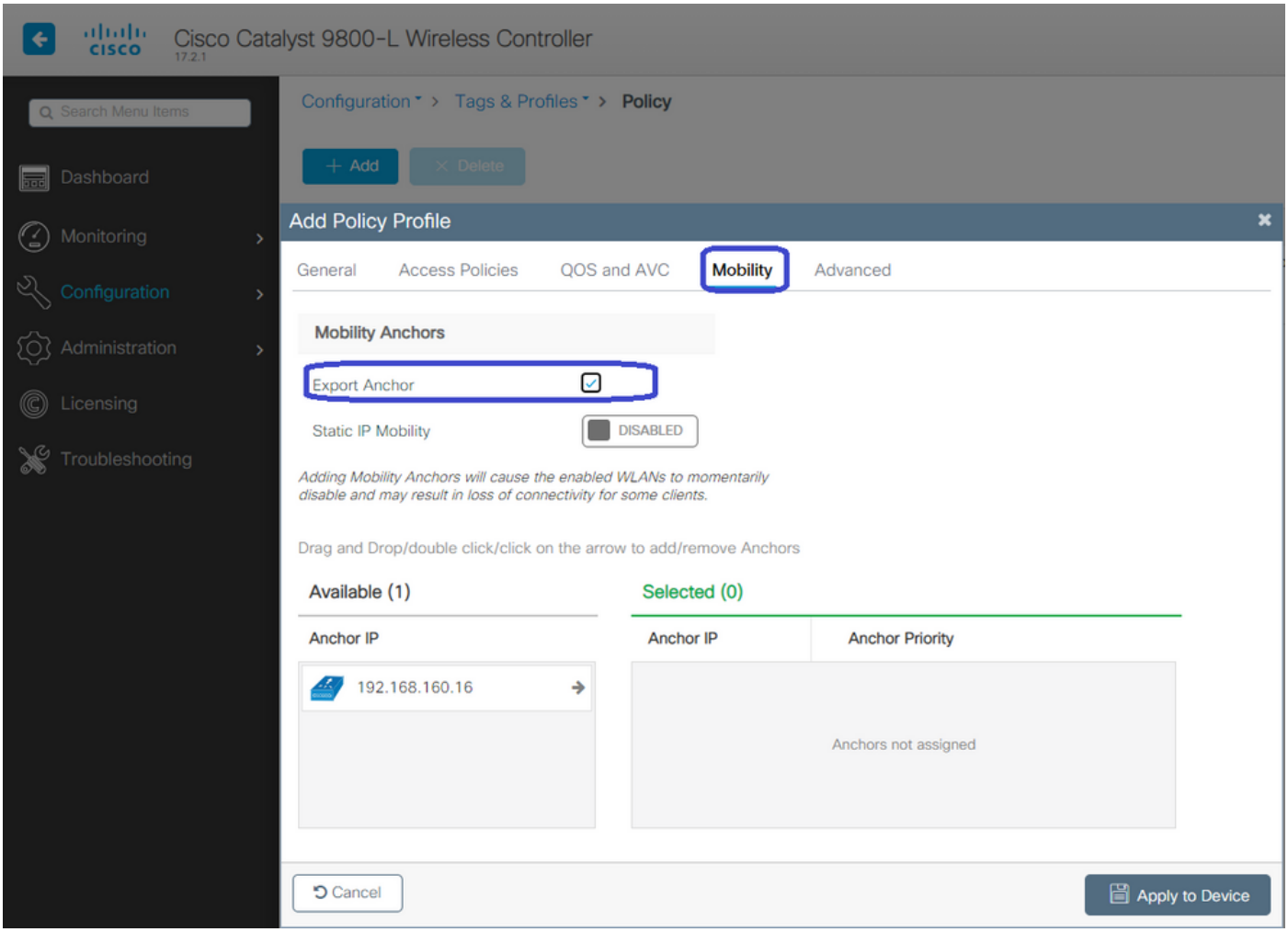


Criar o perfil de política na WLC âncora

Vá para a interface de usuário da Web do WLC âncora. Adicione o perfil de política na âncora 9800 em **Configuration>Tags & Profiles>Tags>Policy>+Add**. Certifique-se de que isso corresponda ao perfil de política feito no estrangeiro, exceto para a guia de mobilidade e a lista de contabilidade.

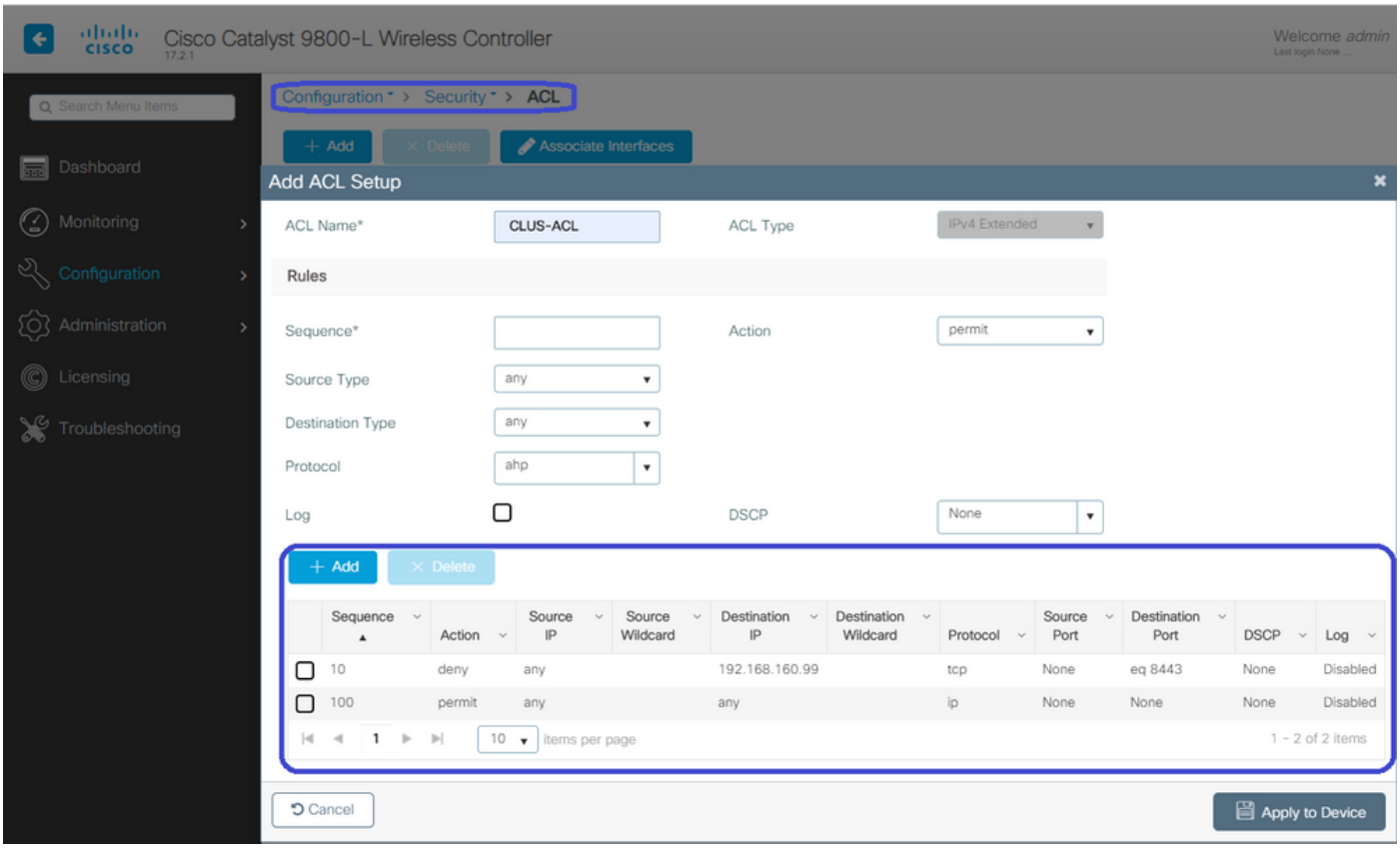
Aqui você não adiciona uma âncora, mas marca a caixa de seleção "Exportar âncora". Não adicione a lista de contabilidade aqui. Como lembrete, isso pressupõe que você já tem uma configuração de túnel de mobilidade entre os dois controladores

Note: Não há motivo para associar esse perfil a uma WLAN em uma etiqueta de política. Isso criará problemas se você fizer isso. Se quiser usar a mesma WLAN para APs nesta WLC, crie outro perfil de política para ela.



Redirecionar a configuração da ACL nos 9800s

Em seguida, você precisa criar a configuração da ACL de redirecionamento nos anos 9800. As entradas no estrangeiro não importam, pois será a WLC âncora aplicando a ACL ao tráfego. O único requisito é que ele esteja lá e tenha alguma entrada. As entradas na âncora têm que "negar" acesso ao ISE na porta 8443 e "permitir" tudo o resto. Essa ACL é aplicada somente ao tráfego que vem "dentro" do cliente, portanto as regras para o tráfego de retorno não são necessárias. O DHCP e o DNS passarão sem entradas na ACL.

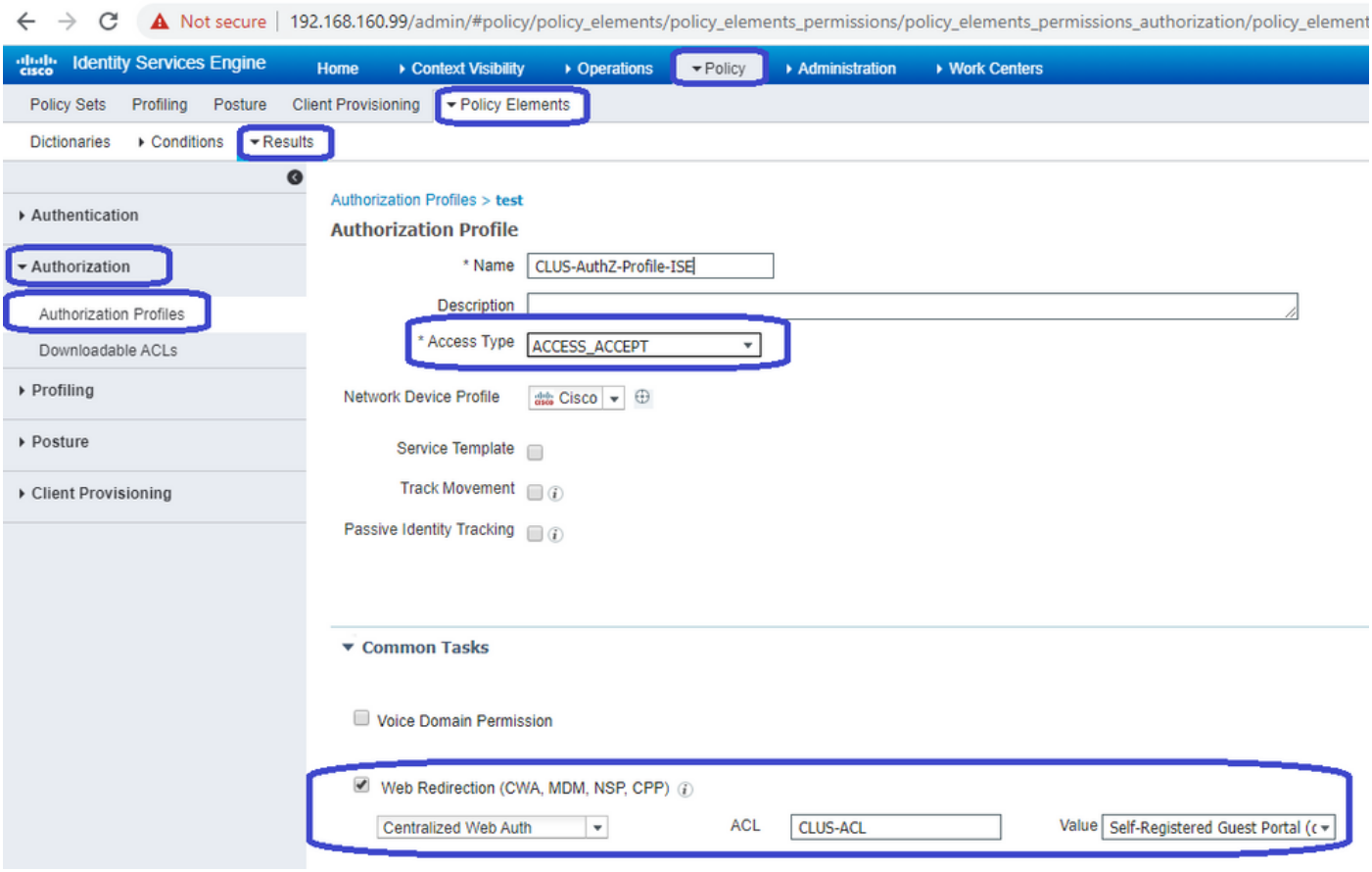


Configurar ISE

A última etapa é configurar o ISE para CWA. Há muitas opções para isso, mas este exemplo seguirá o básico e usará o portal de convidado autorregistrado padrão.

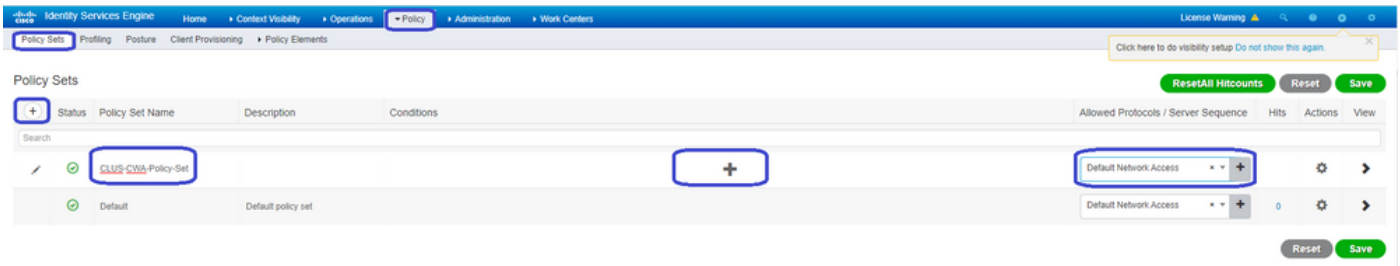
No ISE, você precisa criar um perfil de autorização, um conjunto de políticas com uma política de autenticação e uma política de autorização que use o perfil de autorização, adicionar o 9800 (estrangeiro) ao ISE como um dispositivo de rede e criar um nome de usuário e uma senha para fazer login na rede.

Para criar o perfil de autorização, vá para **Política>Elementos de política>Autorização>Resultados>Perfis de autorização>** e clique em **Adicionar**. Verifique se o tipo de acesso retornado é "access_accept" e defina os AVPs (pares de atributo-valor) que você deseja enviar de volta. Para o CWA, a ACL de redirecionamento e a URL de redirecionamento são obrigatórias, mas você também pode enviar itens como ID de VLAN e tempo limite da sessão. É importante que o nome da ACL corresponda ao nome da ACL de redirecionamento no estrangeiro e na âncora 9800.

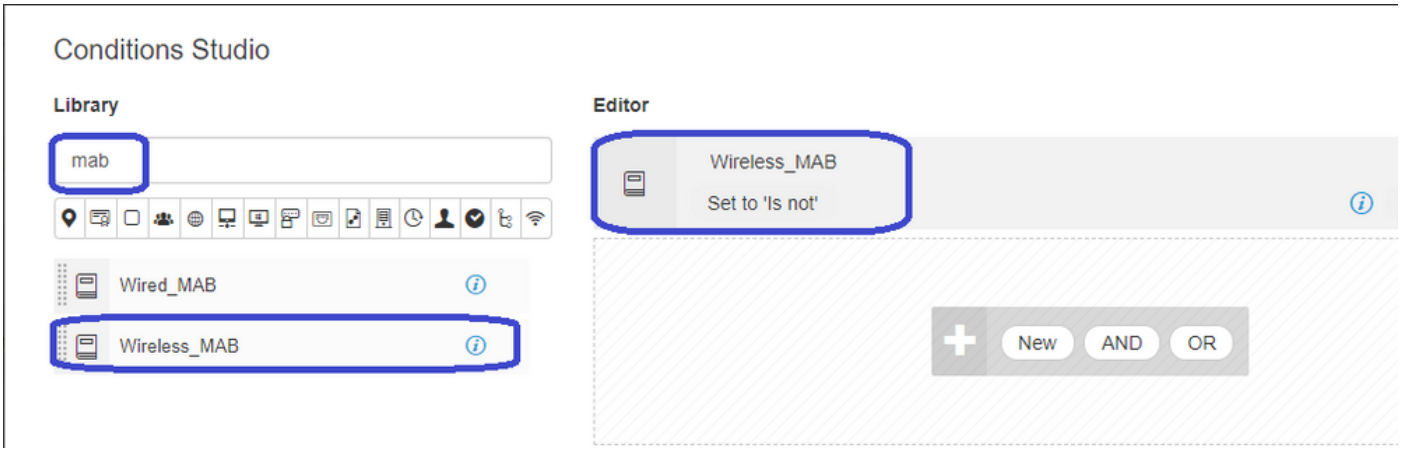


Você precisa configurar uma maneira de aplicar o perfil de autorização que acabou de criar aos clientes que passam pelo CWA. Para isso, uma maneira é criar um conjunto de políticas que ignore a autenticação ao usar MAB e aplique o perfil de autorização ao usar o SSID enviado no ID da estação chamada. Novamente, há muitas maneiras de fazer isso, de modo que se você precisa de algo mais específico ou mais seguro, que bom, essa é a maneira mais simples de fazer isso.

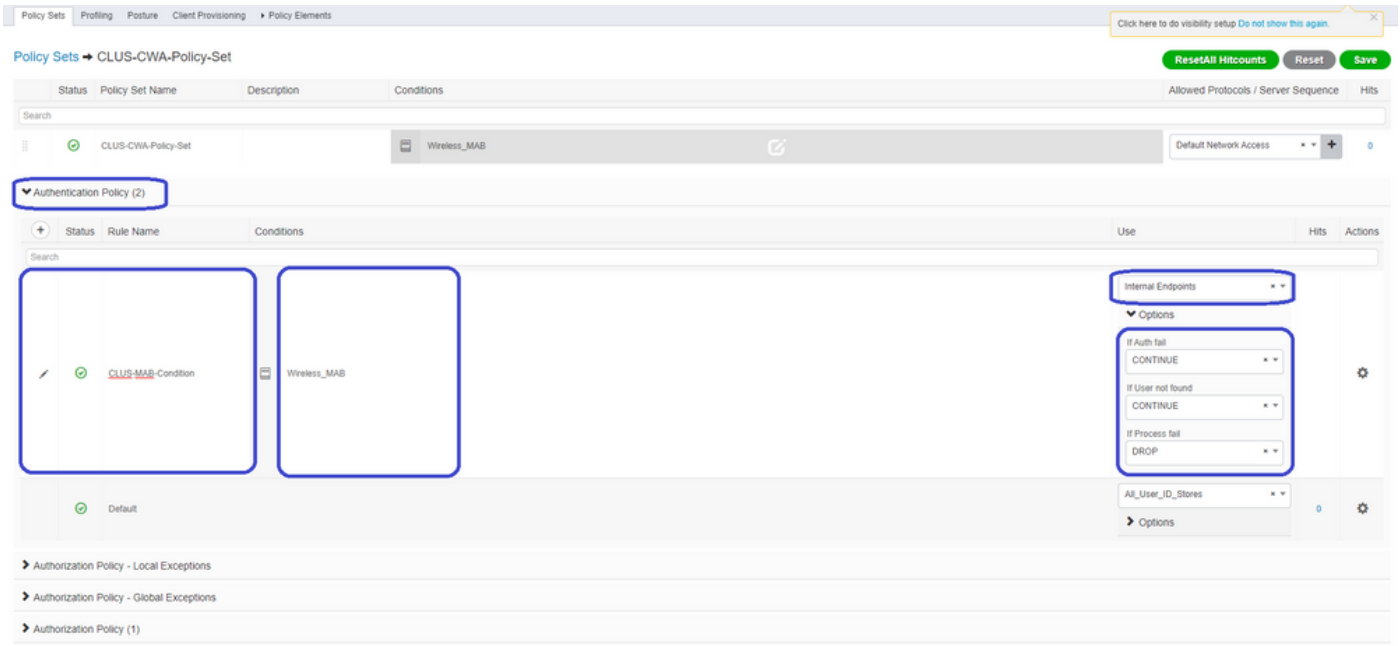
Para criar o conjunto de políticas, vá para **Policy>Policy Sets** e pressione o botão + no lado esquerdo da tela. Nomeie o novo conjunto de políticas e certifique-se de que ele esteja definido como "acesso à rede padrão" ou qualquer lista de protocolos permitida que permita "Process Host Lookup" para MAB(para verificar a lista de protocolos permitidos, vá para Policy>Policy Elements>Results>Authentication>Allowed Protocols). Agora, aperte o sinal + no meio do novo conjunto de políticas que você criou.



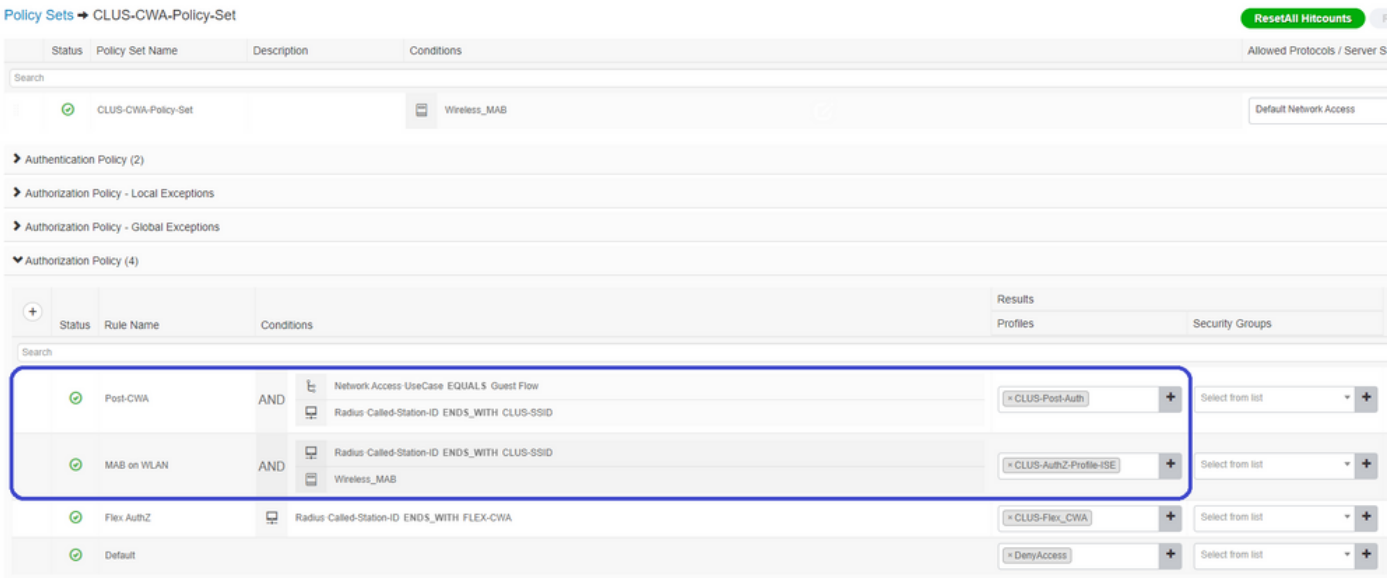
Para esse conjunto de políticas toda vez que o MAB for usado no ISE, ele passará por esse conjunto de políticas. Mais tarde, você pode fazer políticas de autorização correspondentes à ID da estação chamada para que resultados diferentes possam ser aplicados dependendo da WLAN que está sendo usada. Esse processo é muito personalizável com muitas coisas que você pode combinar.



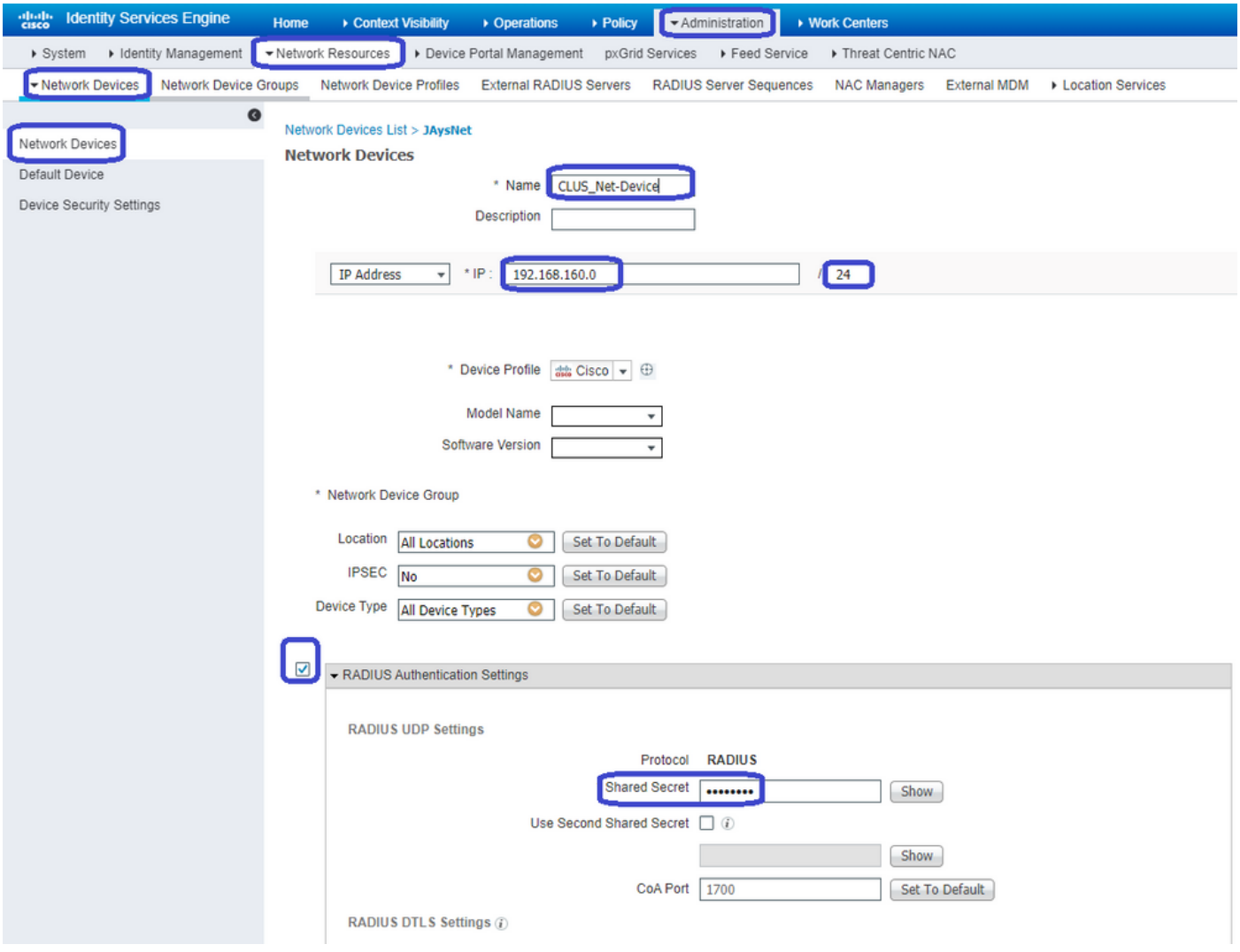
Dentro do conjunto de políticas, crie as políticas. A política de autenticação pode novamente corresponder ao MAB, mas você precisa alterar o repositório de ID para usar "endpoints internos" e precisa alterar as opções para continuar com falha de autenticação e usuário não encontrado.



Depois que a política de autenticação estiver definida, você precisará criar duas regras na política de autorização. Essa política parece uma ACL, portanto, o pedido precisa ter a regra pós-autenticação no topo e a regra de pré-autorização na parte inferior. A regra pós-autorização corresponderá aos usuários que já passaram pelo fluxo de convidado. Quer isto dizer que, se já assinaram, vão cumprir essa regra e parar por aí. Se eles não tiverem entrado, continuarão na lista e seguirão a regra de pré-autorização obtendo o redirecionamento. É uma boa ideia combinar as regras da política de autorização com o ID da estação chamada terminando com o SSID para que ele atinja somente as WLANs configuradas para fazer isso.

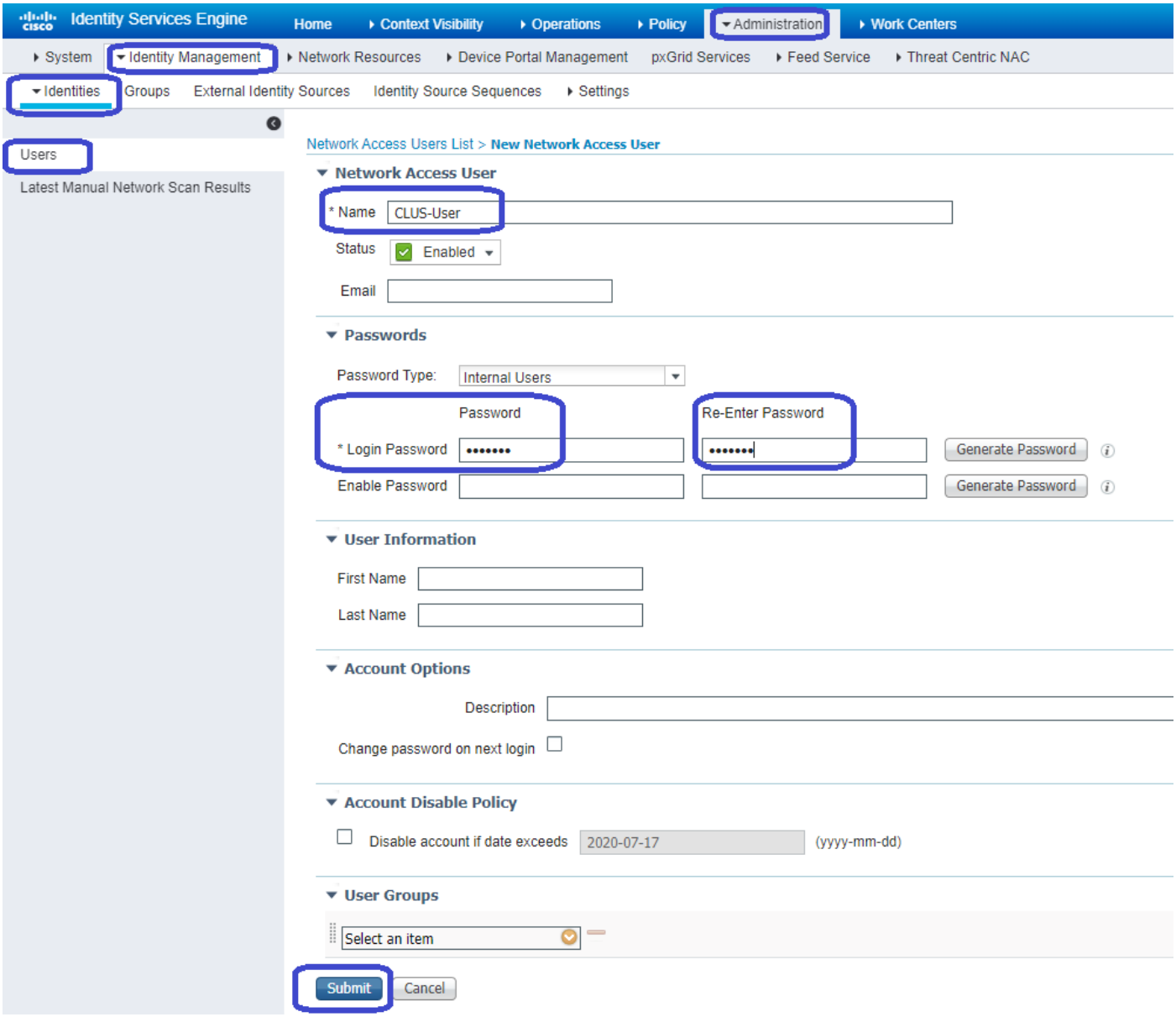


Agora que o conjunto de políticas está configurado, você precisa informar o ISE sobre o 9800 (estrangeiro) para que o ISE confie nele como um autenticador. Isso pode ser feito em **Admin>Recursos de rede>Dispositivo de rede>+**. Você precisa nomeá-lo, definir o endereço IP (ou, nesse caso, toda a sub-rede do administrador), ativar RADIUS e definir o segredo compartilhado. O segredo compartilhado no ISE deve corresponder ao segredo compartilhado no 9800 ou esse processo falhará. Depois que a configuração for adicionada, pressione o botão Enviar para salvá-la.

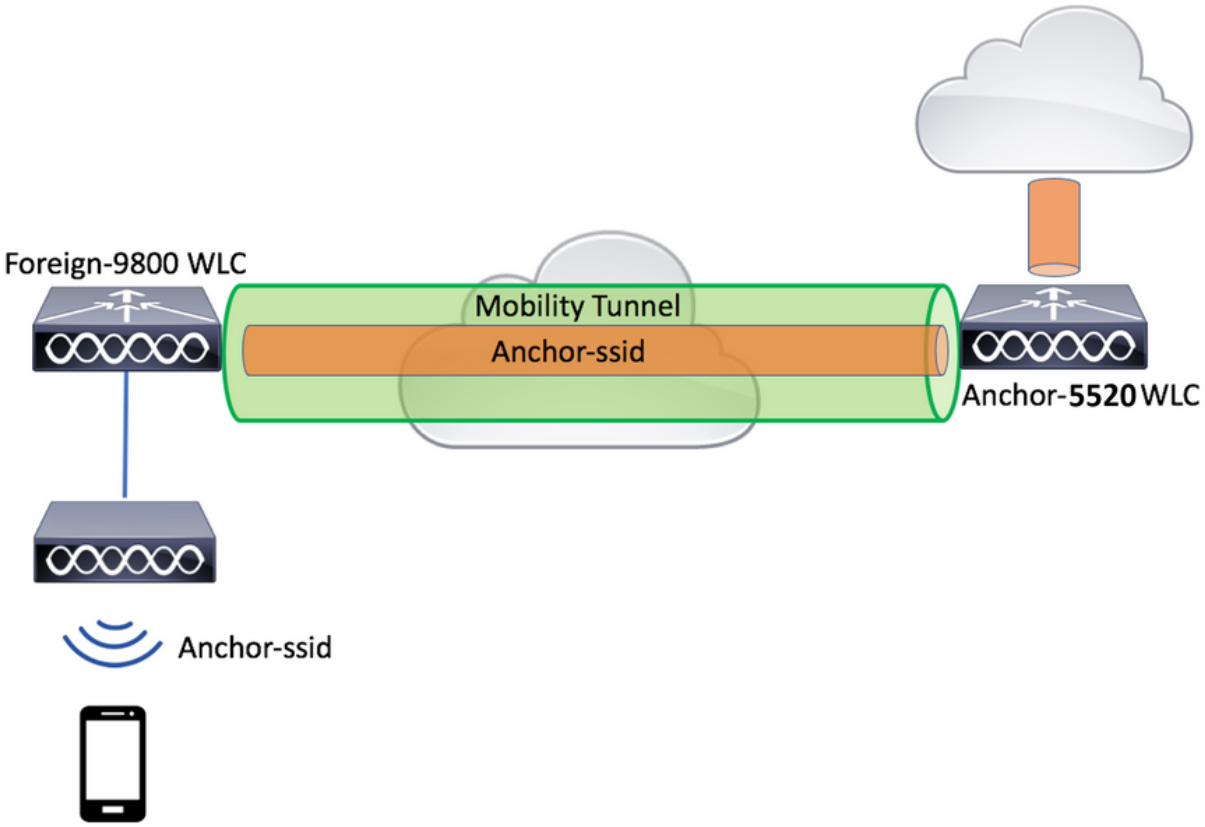


Por fim, você precisará adicionar o nome de usuário e a senha que o cliente irá inserir na página

de login para validar se ele deve ter acesso à rede. Isso é feito em **Admin>Identity Management>Identity>Users>+Add** e certifique-se de pressionar Submit (Enviar) depois de adicioná-lo. Como tudo o resto com o ISE, isso é personalizável e não precisa ser um usuário armazenado localmente, mas, novamente, é a configuração mais fácil.



Configurar um Catalyst 9800 ancorado em uma WLC AireOS

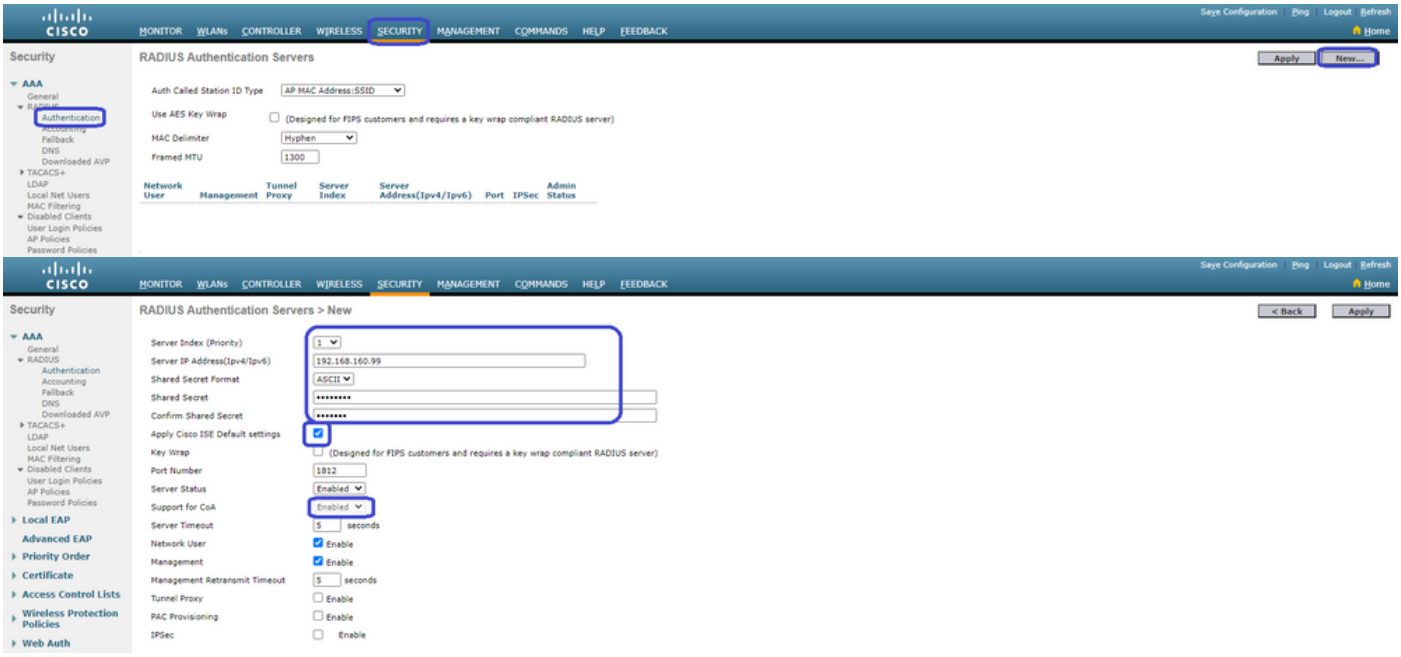


Configuração externa do Catalyst 9800

Siga as mesmas etapas discutidas anteriormente, ignorando a seção "*Create the policy profile on the anchor WLC*".

Configurações AAA na WLC AireOS âncora

Adicione o servidor à WLC indo para **Security>AAA>RADIUS>Authentication>New**. Adicione o endereço IP do servidor, o segredo compartilhado e o suporte para CoA.

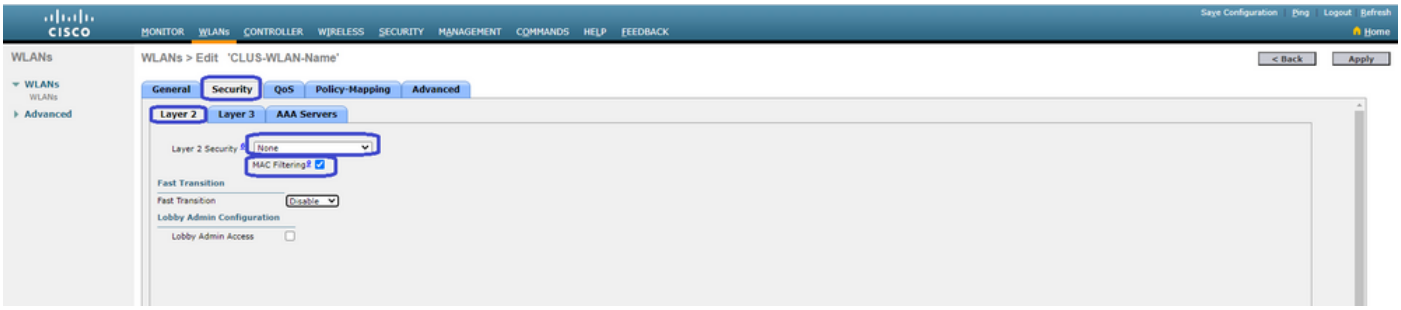


Configuração de WLAN na WLC AireOS

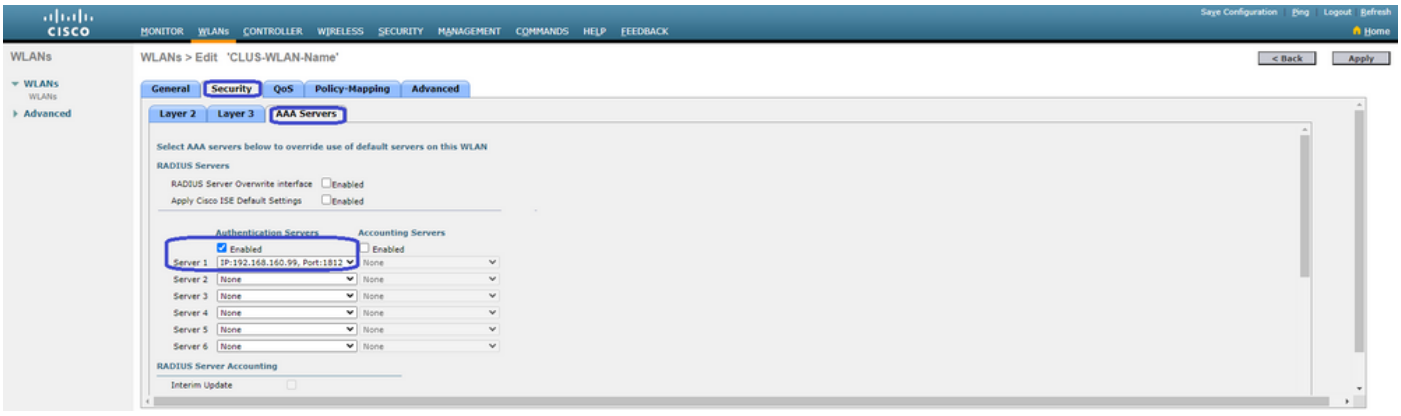
Para criar a WLAN, vá para **WLANs>Criar novo>Ir**.

Configure o nome do perfil, a ID da WLAN e o SSID e pressione "Apply" (Aplicar).

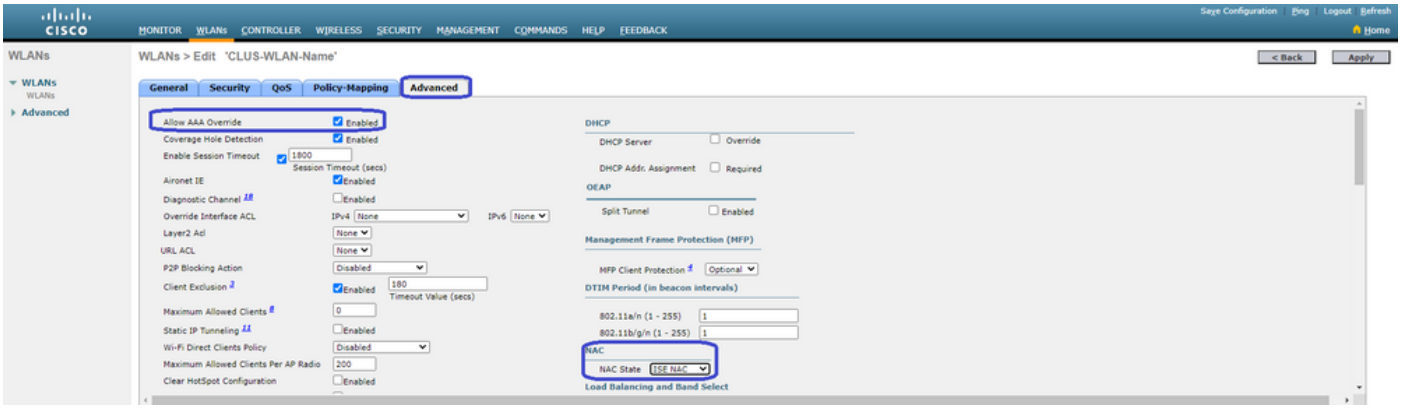
Isso deve levá-lo à configuração da WLAN. Na guia "Geral", você pode adicionar a interface que deseja que os clientes usem se não for configurar o ISE para enviá-lo nos AVPs. Em seguida, acesse a guia **Security>Layer2** e corresponda à configuração "Layer 2 Security" usada no 9800 e ative "MAC Filtering".



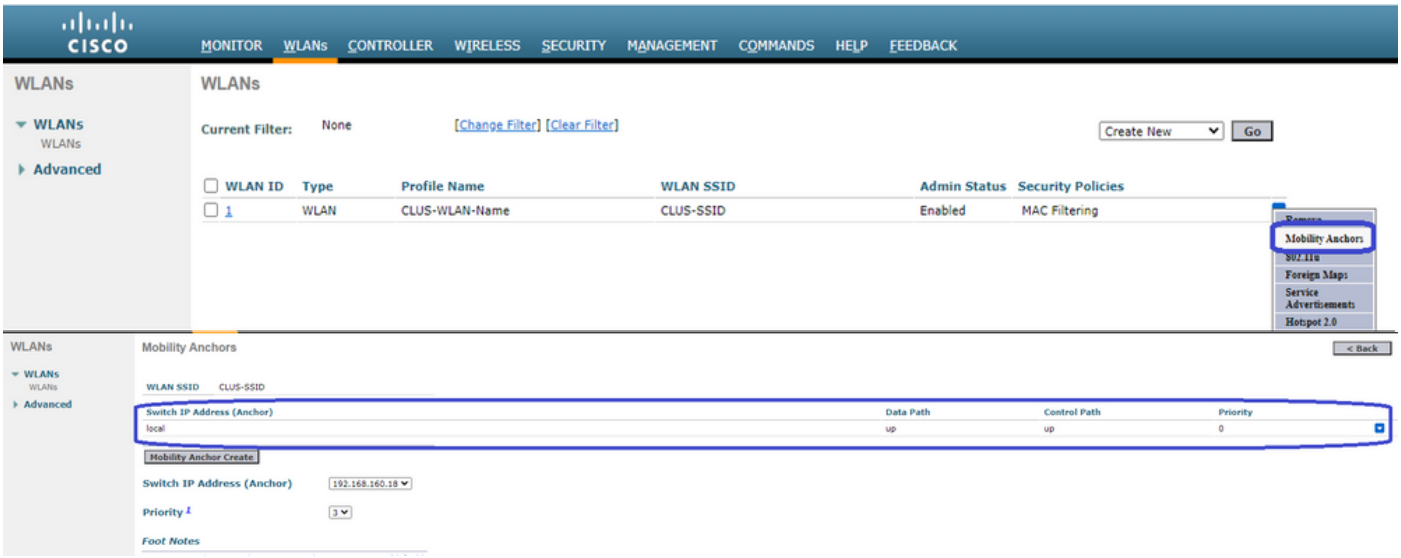
Agora vá para a guia **Security>AAA Servers** e defina o servidor ISE como o "Authentication Servers". **Não** defina nada para os "Servidores de Contabilidade". Desmarque a caixa "Enable" (Habilitar) para contabilidade.



Ainda nas configurações de WLAN, vá para a guia "Avançado" e ative "Permitir substituição de AAA", bem como altere o "Estado de NAC" para "ISE NAC"



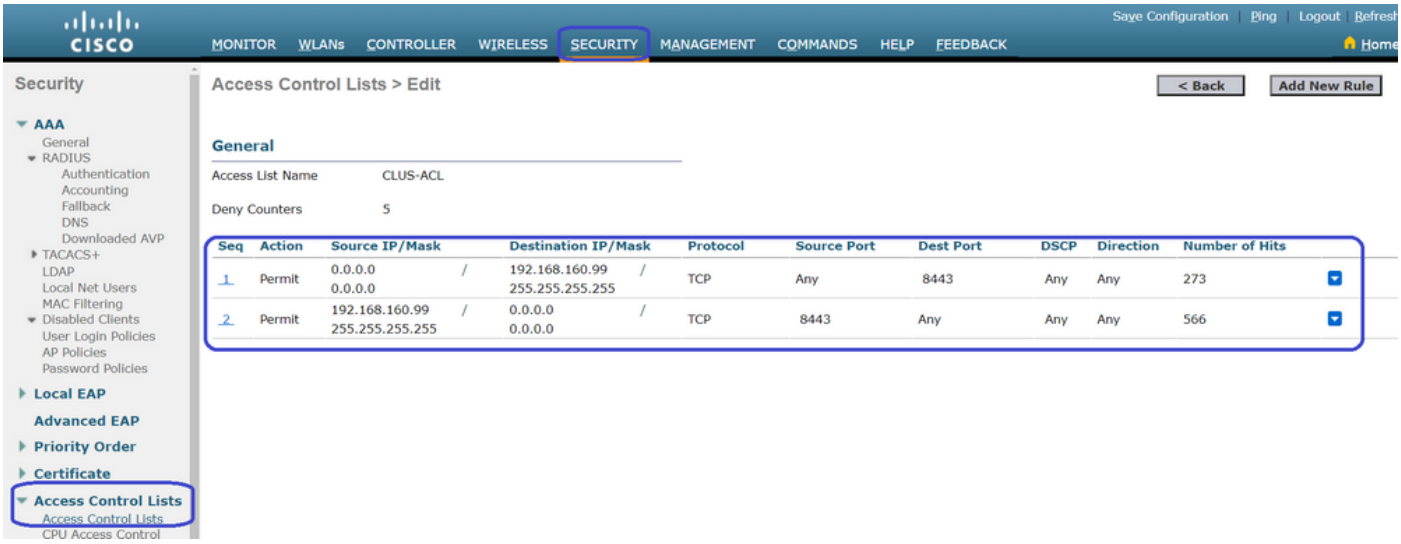
A última coisa é ancorá-la a si mesma. Para isso, volte para a página **WLANs** e passe o mouse sobre a caixa azul à direita de WLAN>Mobility Anchors. Defina "Switch IP Address (Anchor)" como local e pressione o botão "Mobility Anchor Create" (Criar âncora de mobilidade). Em seguida, deve aparecer com prioridade 0 ancorada local.



Redirecionar ACL na WLC do AireOS

Esta é a configuração final necessária na WLC AireOS. Para criar a ACL de redirecionamento, vá para **Security>Access Control Lists>Access Control Lists>New**. Insira o nome da ACL (isso deve corresponder ao que é enviado nos AVPs) e pressione "Apply" (Aplicar).

Agora, clique no nome da ACL que você acabou de criar. Clique no botão "Add New Rule" (Adicionar nova regra). Ao contrário da controladora 9800, na WLC AireOS, você configura uma instrução de permissão para tráfego que tem permissão para acessar o ISE sem ser redirecionado. DHCP e DNS são permitidos por padrão.

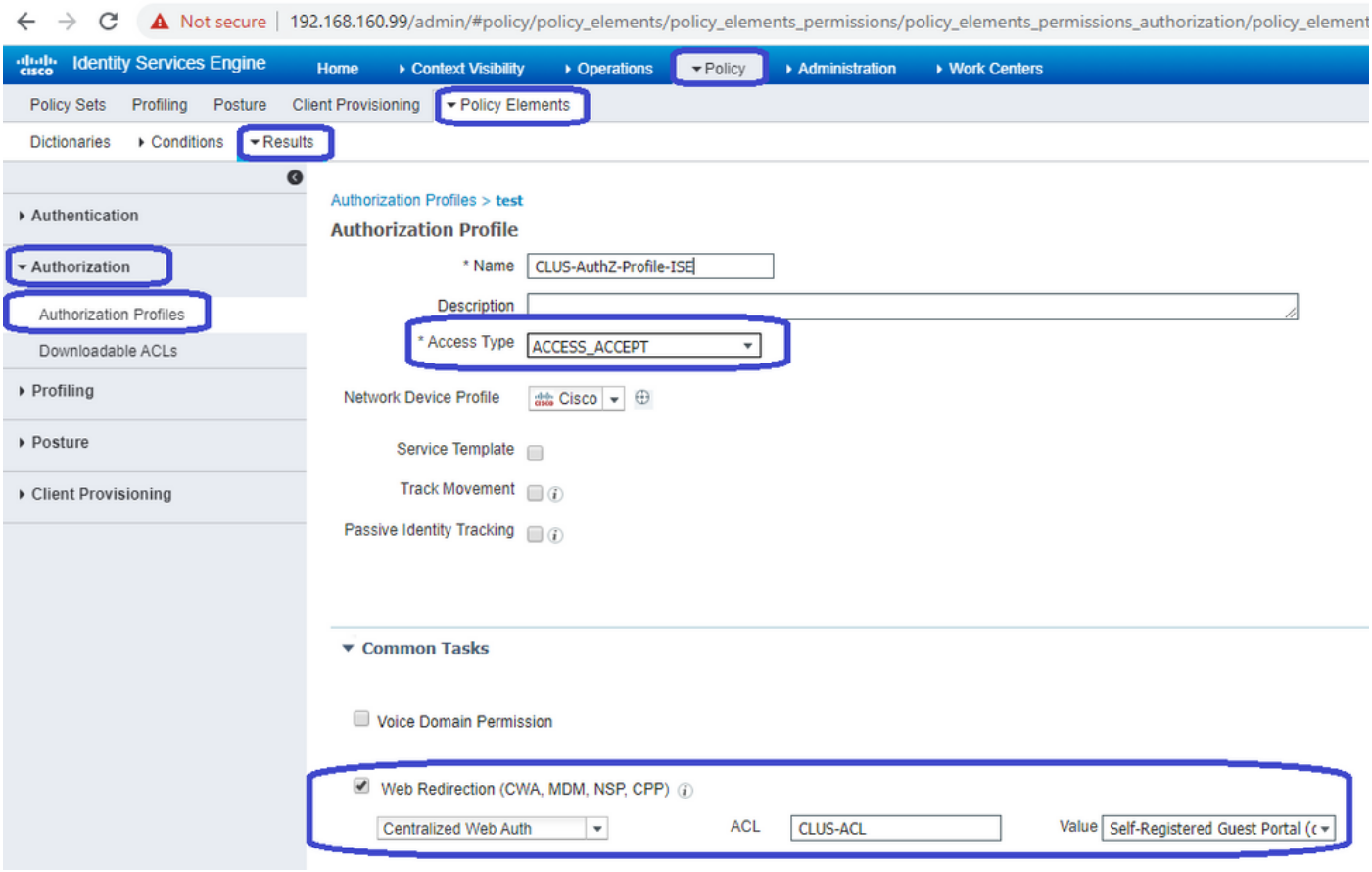


Configurar ISE

A última etapa é configurar o ISE para CWA. Há muitas opções para isso, mas este exemplo seguirá o básico e usará o portal de convidado autorregistrado padrão.

No ISE, você precisa criar um perfil de autorização, um conjunto de políticas com uma política de autenticação e uma política de autorização que use o perfil de autorização, adicionar o 9800 (estrangeiro) ao ISE como um dispositivo de rede e criar um nome de usuário e uma senha para fazer login na rede.

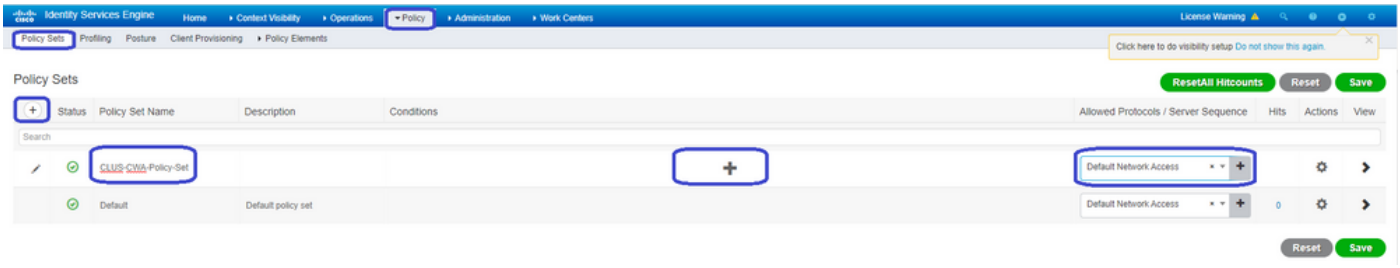
Para criar o perfil de autorização, vá **paraPolítica>Elementos de política>Autorização>Resultados>Perfis de autorização>+Adicionar**. Verifique se o tipo de acesso retornado é "access_accept" e defina os AVPs (pares de atributo-valor) que você deseja enviar de volta. Para o CWA, a ACL de redirecionamento e a URL de redirecionamento são obrigatórias, mas você também pode enviar itens como ID de VLAN e tempo limite da sessão. É importante que o nome da ACL corresponda ao nome da ACL de redirecionamento na WLC externa e âncora.



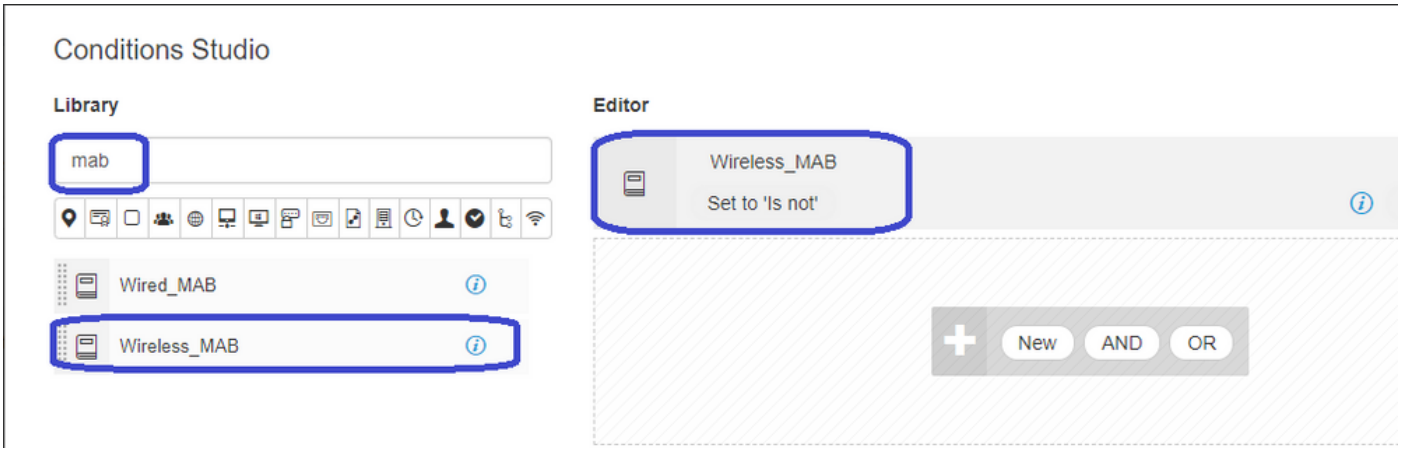
Você precisa configurar uma maneira de aplicar o perfil de autorização que acabou de criar aos clientes que passam pelo CWA.

Para isso, uma maneira é criar um conjunto de políticas que ignore a autenticação ao usar MAB e aplique o perfil de autorização ao usar o SSID enviado no ID da estação chamada. Novamente, há muitas maneiras de fazer isso, de modo que se você precisa de algo mais específico ou mais seguro, que bom, essa é a maneira mais simples de fazer isso.

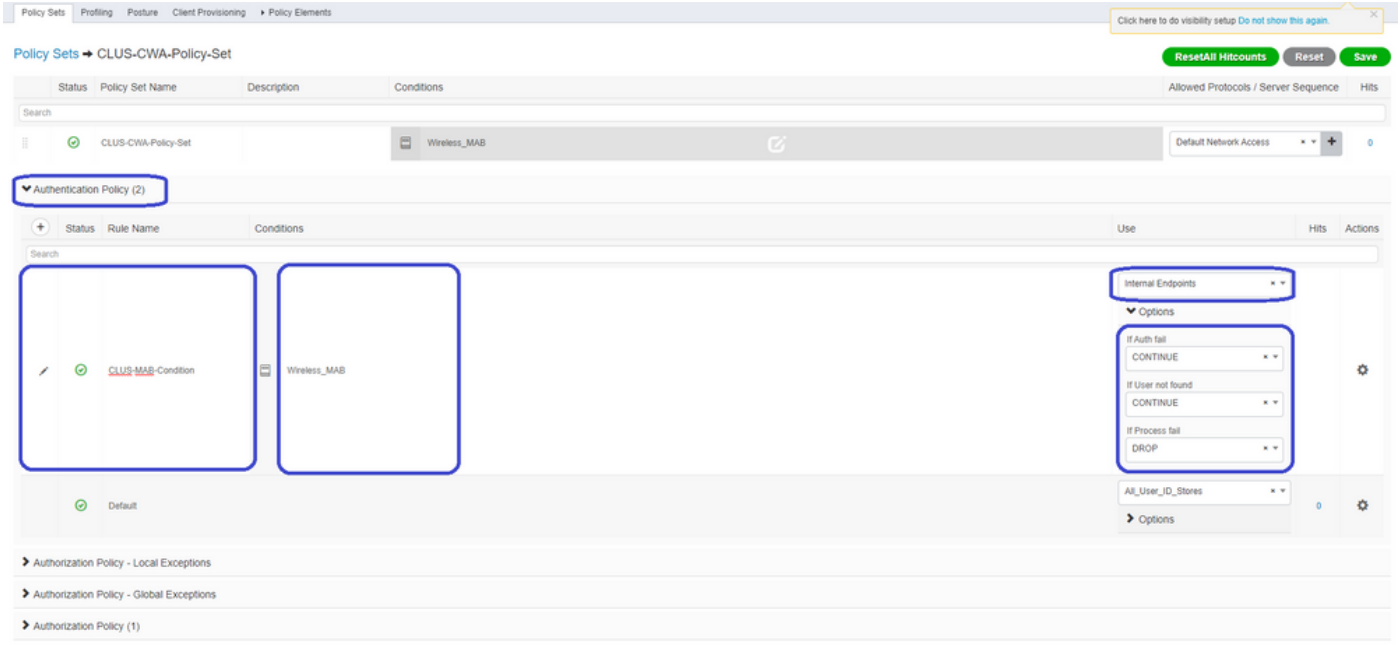
Para criar o conjunto de políticas, vá **paraPolítica>Configurações de política** e pressione o botão + no lado esquerdo da tela. Nomeie o novo conjunto de políticas e certifique-se de que ele esteja definido como "acesso à rede padrão" ou qualquer lista de protocolos permitida que permita "Process Host Lookup" para MAB(para verificar a lista de protocolos permitidos, vá para Policy>Policy Elements>Results>Authentication>Allowed Protocols). Agora, aperte o sinal + no meio do novo conjunto de políticas que você criou.



Para esse conjunto de políticas toda vez que o MAB for usado no ISE, ele passará por esse conjunto de políticas. Mais tarde, você pode fazer políticas de autorização correspondentes à ID da estação chamada para que resultados diferentes possam ser aplicados dependendo da WLAN que está sendo usada. Esse processo é muito personalizável com muitas coisas que você pode combinar

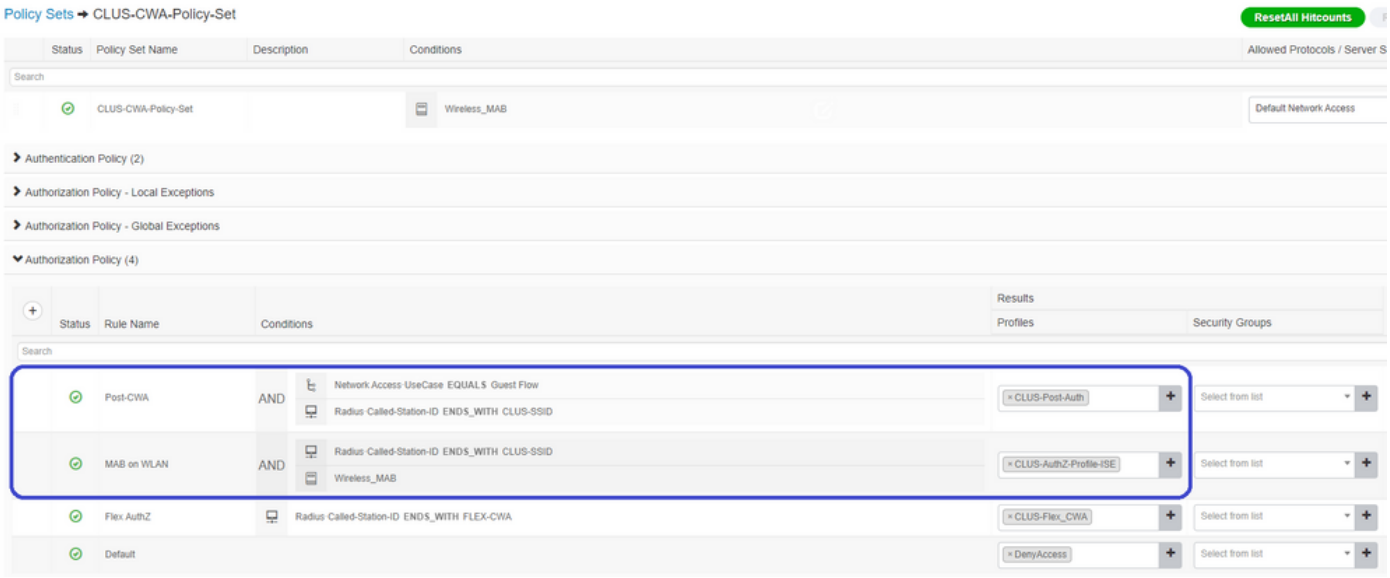


Dentro do conjunto de políticas, crie as políticas. A política de autenticação pode novamente corresponder ao MAB, mas você precisa alterar o repositório de ID para usar "endpoints internos" e precisa alterar as opções para continuar com falha de autenticação e usuário não encontrado.

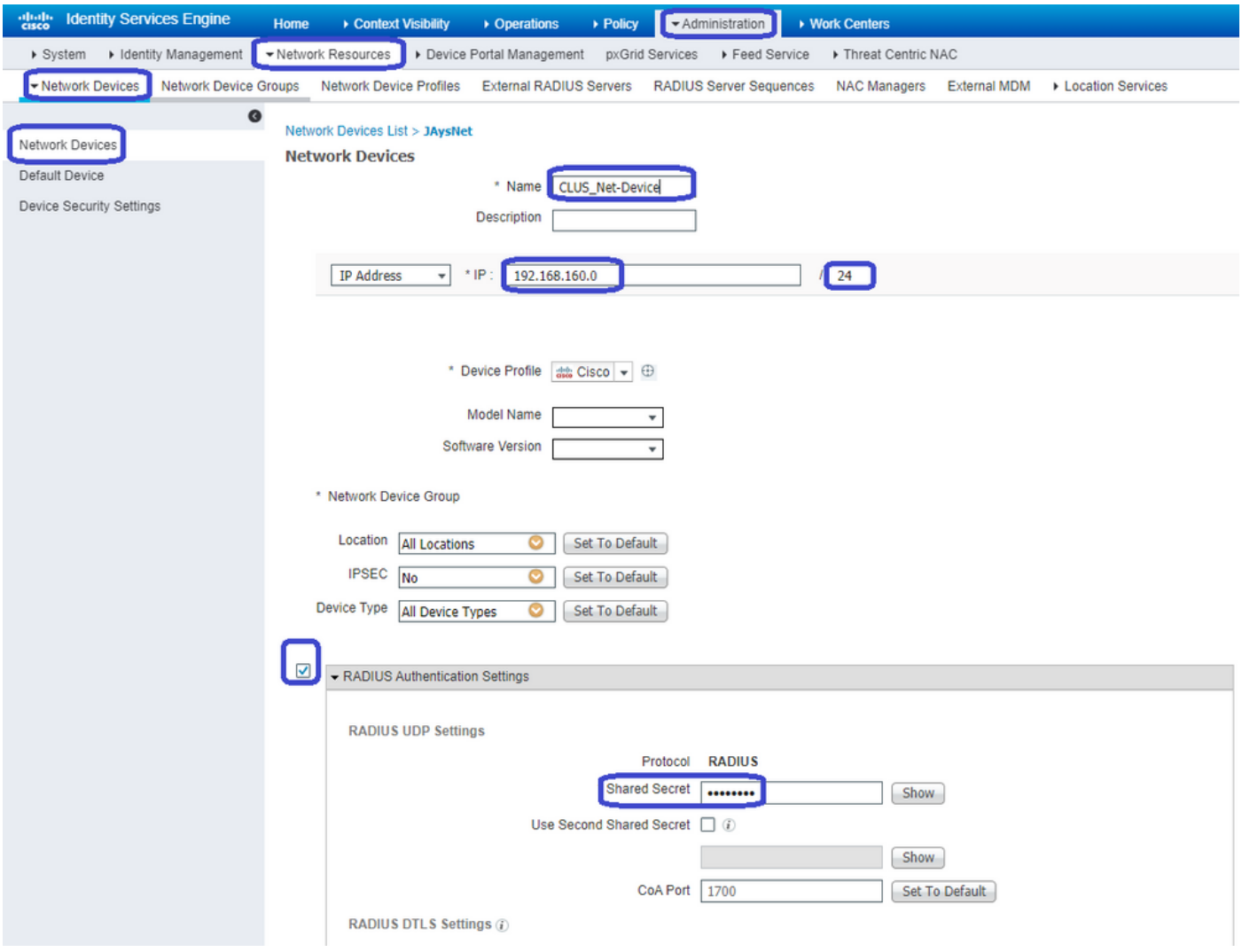


Depois que a política de autenticação estiver definida, você precisará criar duas regras na política de autorização. Essa política

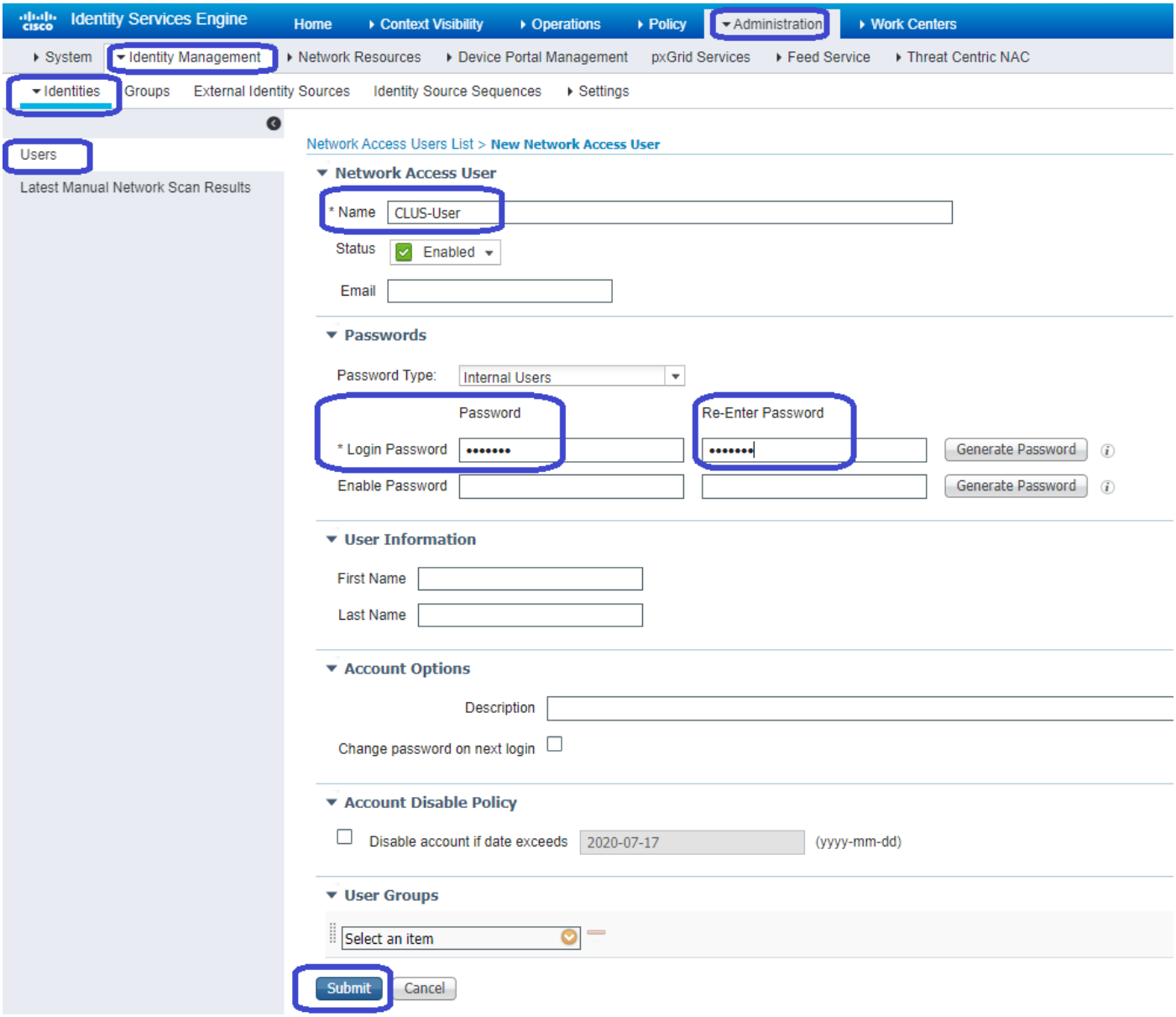
parece uma ACL, portanto, o pedido precisa ter a regra pós-autenticação no topo e a regra de pré-autorização na parte inferior. A regra pós-autorização corresponderá aos usuários que já passaram pelo fluxo de convidado. Quer isto dizer que, se já assinaram, vão cumprir essa regra e parar por aí. Se eles não tiverem entrado, continuarão na lista e seguirão a regra de pré-autorização obtendo o redirecionamento. É uma boa ideia combinar as regras da política de autorização com o ID da estação chamada terminando com o SSID para que ele atinja somente as WLANs configuradas para fazer isso.



Agora que o conjunto de políticas está configurado, você precisa informar o ISE sobre o 9800 (estrangeiro) para que o ISE confie nele como um autenticador. Isso pode ser feito em**Admin>Recursos de Rede>Dispositivo de Rede>**+ Você precisa nomeá-lo, definir o endereço IP (ou, nesse caso, toda a sub-rede do administrador), ativar RADIUS e definir o segredo compartilhado. O segredo compartilhado no ISE deve corresponder ao segredo compartilhado no 9800 ou esse processo falhará. Depois que a configuração for adicionada, pressione o botão Enviar para salvá-la.



Por fim, você precisará adicionar o nome de usuário e a senha que o cliente irá inserir na página de login para validar se ele deve ter acesso à rede. Isso é feito sob**Admin>Gerenciamento de identidade>Identidade>Usuários>+Adicionar**e certifique-se de pressionar Enviar depois de adicioná-lo. Como tudo o resto com o ISE, isso é personalizável e não precisa ser um usuário armazenado localmente, mas, novamente, é a configuração mais fácil.



Diferenças na configuração quando o AireOS WLC é o estrangeiro e o Catalyst 9800 é a âncora

Se você deseja que a WLC AireOs seja a controladora externa, a configuração é a mesma que antes, com apenas duas diferenças.

1. A contabilização de AAA nunca é feita na âncora, portanto o 9800 não teria uma lista de métodos de contabilidade e a WLC do AireOS teria a contabilidade habilitada e apontada para o ISE.
2. O AireOS precisaria ancorar no 9800 em vez de ser ele mesmo. No perfil de política, o 9800 não teria uma âncora selecionada, mas teria a caixa "Exportar âncora" marcada.
3. Éimportante observar que, quando as WLCs do AireOS exportam o cliente para o 9800, não há conceito de perfis de política, ele envia apenas o nome do perfil da WLAN. Portanto, o 9800 aplicará o Nome do perfil da WLAN enviado do AireOS ao Nome do perfil da WLAN e ao Nome do perfil da política. Isso indica que, ao ancorar de uma WLC AireOS para uma

WLC 9800, o nome do perfil de WLAN em ambas as WLCs e o nome do perfil de política na 9800 devem corresponder.

Verificar

Para verificar as configurações na WLC **9800**, execute os comandos

- AAA

```
Show Run | section aaa|radius
```

- WLAN

```
Show wlan id <wlan id>
```

- Perfil da política

```
Show wireless profile policy detailed <profile name>
```

- Marca de política

```
Show wireless tag policy detailed <policy tag name>
```

- ACL

```
Show IP access-list <ACL name>
```

- Verifique se a mobilidade está ativa com a âncora

```
Show wireless mobility summary
```

Para verificar as configurações na WLC do AireOS, execute os comandos

- AAA

```
Show radius summary
```

Note: RFC3576 é a configuração de CoA

- WLAN

```
Show WLAN <wlan id>
```

- ACL

```
Show acl detailed <acl name>
```

- Verifique se a mobilidade está alinhada com o exterior

```
Show mobility summary
```

Troubleshoot

A solução de problemas parece diferente dependendo de qual ponto do processo o cliente interrompe. Por exemplo, se a WLC nunca obtiver uma resposta do ISE no MAB, o cliente ficará preso no "Estado do Policy Manager: Associando" e não seria exportado para a âncora. Nessa situação, você solucionaria problemas somente no estrangeiro e poderia coletar um rastreamento de RA e uma captura de pacote para tráfego entre a WLC e o ISE. Outro exemplo seria que o MAB foi bem-sucedido, mas o cliente não recebe o redirecionamento. Nesse caso, você precisa certificar-se de que o estrangeiro recebeu o redirecionamento nos AVPs e o aplicou ao cliente. Você também precisa verificar a âncora para garantir que o cliente esteja lá com a ACL correta. Esse escopo de solução de problemas está fora do projeto deste documento técnico (verifique as referências de diretrizes genéricas de solução de problemas de clientes).

Para obter mais ajuda com a solução de problemas do CWA na WLC 9800, consulte o Cisco Live! apresentação DGTL-TSCENT-404

Informações sobre Troubleshooting do Catalyst 9800

Detalhes do cliente

show wireless client mac-address
Aqui você deve consultar o "Estado do Policy Manager", "Session Manager>Auth Method", "Mobility Role".

Você também pode encontrar essas informações na GUI em Monitoring>Clients

Captura de pacote incorporado

Na CLI, o comando inicia *#monitor capture <nome da captura>* e as opções vêm depois disso.

Na GUI, vá para Solução de problemas>Captura de pacotes>+Adicionar

Rastreamentos ativos por rádio

Da CLI

debug wireless mac|ip
Use a forma no do comando para pará-lo. Isso será registrado em um arquivo no flash de inicialização chamado "ra_trace", depois no endereço MAC ou IP do cliente e na data e hora.

Na GUI, vá para Troubleshoot>Radioative Trace>+Add. Adicione o endereço mac ou ip do cliente, aperte Apply e pressione start. Depois de passar pelo processo algumas vezes, pare o rastreamento, gere o log e faça o download para o dispositivo.

Informações de solução de problemas do AireOS

Detalhes do cliente

Na CLI *show client details <client mac>*

A partir do monitor GUI>Clients

Depurações do CLI

```
Debug client

Debug mobility handoff

Debug mobility config
```

Referências

Criação de túneis de mobilidade com controladores 9800

Depuração e coleta de logs sem fio no 9800