Configurar a Autenticação da Web Local com Autenticação Externa

Contents

Informações Relacionadas

Introdução

Este documento descreve como configurar a Autenticação Web Local com Autenticação Externa em uma WLC 9800 e no ISE.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- 9800 Configuração de Wireless LAN Controllers (WLC)
- Pontos de Acesso Lightweight (LAPs)
- Como instalar e configurar um servidor Web externo Identity Services Engine (ISE).
- Como instalar e configurar servidores DHCP e DNS.

Componentes Utilizados

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

- 9800-40 WLC Cisco IOS® XE, versão 17.18.4a com APSP1 e APSP2
- Identity Services Engine (ISE), versão 3.2.0.542
- Access point Cisco® Wireless 9172I Series Wi-Fi 7, versão 17.18.4.202

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.

Autenticação da Web

A autenticação da Web é um recurso de segurança da camada 3 que permite que usuários convidados tenham acesso à rede.

Esse recurso foi projetado para fornecer acesso de convidado fácil e seguro a SSIDs abertos, sem a necessidade de configurar um perfil de usuário, e também pode funcionar com métodos de segurança de Camada 2.

A finalidade da autenticação da Web é permitir que dispositivos não confiáveis (convidados) acessem a rede com privilégios de acesso à rede limitados, por meio de uma WLAN de convidado que pode ser configurada com mecanismos de segurança e que a segurança da rede não seja comprometida. Para que os usuários convidados tenham acesso à rede, eles precisam se autenticar com êxito, ou seja, precisam fornecer as credenciais corretas ou aceitar a Política de uso aceitável (AUP) para obter acesso à rede.

A autenticação da Web é um benefício para as empresas porque promove a fidelidade do usuário, torna a empresa compatível com o uso de um aviso de isenção que o usuário convidado deve aceitar e permite que a empresa interaja com os visitantes.

Para implantar a autenticação da Web, deve-se levar em consideração como o portal convidado e a autenticação são tratados. Há dois métodos comuns:

- Autenticação Web local (LWA): Um método de redirecionamento de usuários convidados para um portal diretamente do WLC. O redirecionamento e a ACL pré-WebAuth são configurados localmente na WLC.
- Autenticação da Web central (CWA): Um método de redirecionamento de usuários convidados em que o URL de redirecionamento e a ACL de redirecionamento são configurados centralmente em um servidor externo (por exemplo, ISE) e comunicados à WLC via RADIUS. Na autenticação da Web central, o URL de redirecionamento e a ACL de redirecionamento estão centralmente localizados em um servidor externo (como o RADIUS). O servidor RADIUS é aquele que manipula a autenticação, ele envia instruções para a WLC. No CWA, o WLC não requer um certificado de autenticação da Web local, apenas um certificado é necessário no portal da Web central e requer um servidor de autenticação central, como o ISE. Para ler o CWA com mais detalhes, navegue para Configurar a autenticação da Web central (CWA) no Catalyst 9800 WLC e ISE.

Na Autenticação da Web Local, o portal da Web pode estar presente na WLC ou em um servidor externo. No LWA com Autenticação Externa, o portal da Web está presente no WLC. No LWA com Servidor Web Externo, o portal Web está presente em um servidor externo (como o Cisco DNA Spaces). Um exemplo de LWA com Servidor Web Externo é descrito em detalhes em: Configurar o portal cativo do DNA Spaces com o Catalyst 9800 WLC.

Diagrama dos diferentes métodos de autenticação da Web:

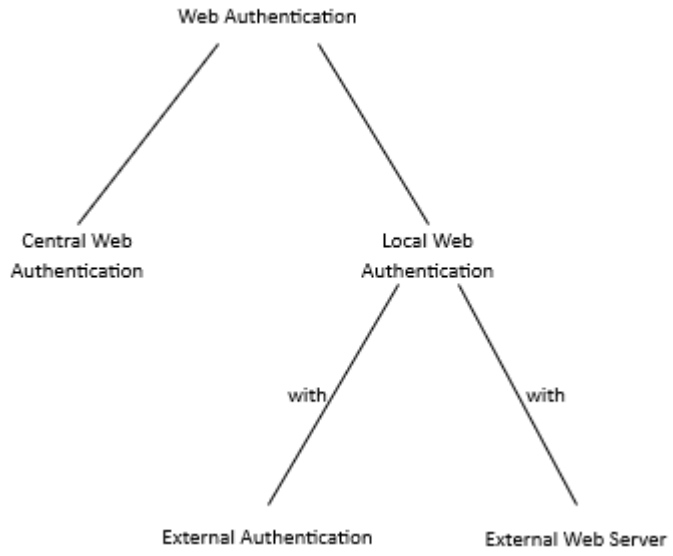


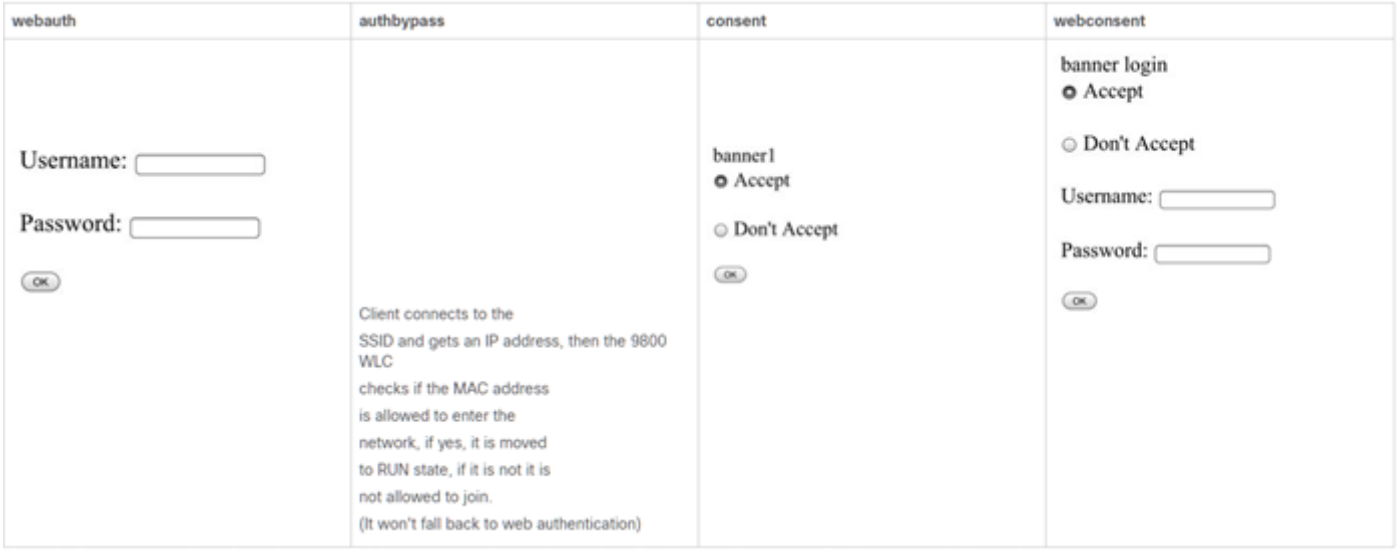
Diagrama dos diferentes métodos de autenticação da Web

Note: Se você estiver implantando APs Wi-Fi 7 com autenticação da Web em uma WLC 9800, certifique-se de estar executando uma versão recomendada do Cisco IOS XE, como 17.18.4a ou posterior.

Tipos de autenticação

Há quatro tipos de autenticação para autenticar o usuário convidado:

- Webauth: Insira o nome de usuário e a senha.
- Consentimento (passagem pela Web): Aceite AUP.
- Autbypass: Autenticação baseada no endereço MAC do dispositivo de usuário convidado.
- Consentimento da Web: Uma combinação entre nome de usuário/senha e aceitar AUP.



Quatro tipos de autenticação para autenticar o usuário convidado

Banco de Dados para Autenticação

As credenciais para autenticação podem ser armazenadas em um servidor LDAP, localmente no WLC ou no servidor RADIUS.

- Banco de dados local: As credenciais (nome de usuário e senha) são armazenadas localmente na WLC.
- Banco de dados LDAP: As credenciais são armazenadas no banco de dados back-end LDAP. A WLC consulta o servidor LDAP para obter as credenciais de um usuário específico no banco de dados.
- Banco de dados RADIUS: As credenciais são armazenadas no banco de dados back-end do RADIUS. A WLC consulta o servidor RADIUS quanto às credenciais de um usuário específico no banco de dados.

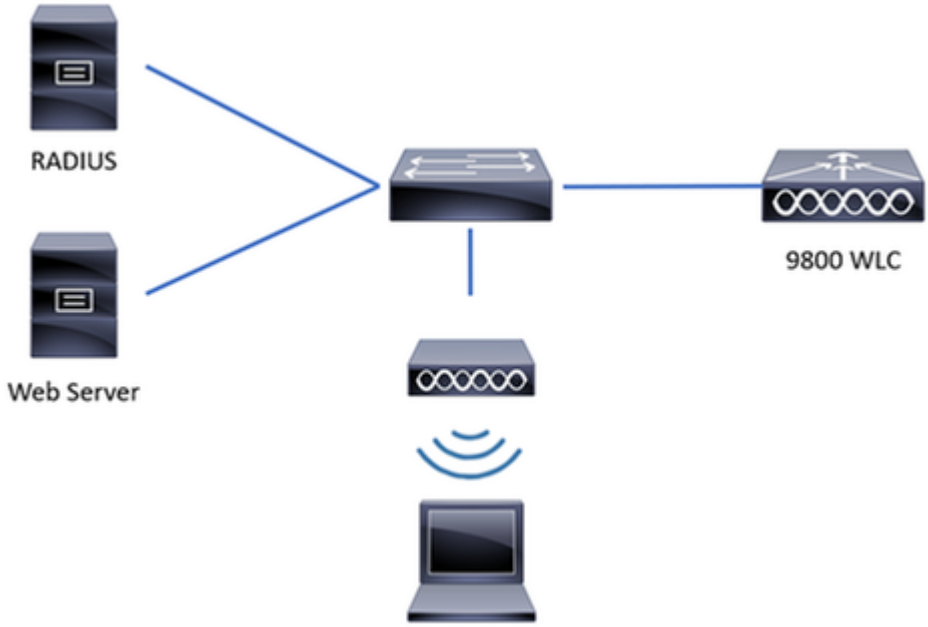
Autenticação da Web Local

Na autenticação da Web local, o usuário convidado é redirecionado para um portal da Web diretamente da WLC.

O portal da Web pode estar na WLC ou em outro servidor. O que ele torna local é o fato de que o URL de redirecionamento e a ACL que corresponde ao tráfego devem estar na WLC (não no local do portal da Web). No LWA, quando um usuário convidado se conecta à WLAN convidada, a WLC intercepta a conexão do usuário convidado e as redireciona para a URL do portal da Web,

onde o usuário convidado é solicitado a se autenticar. Quando o usuário convidado digita as credenciais (nome de usuário e senha), a WLC captura as credenciais. A WLC autentica o usuário convidado com um servidor LDAP, servidor RADIUS ou banco de dados local (banco de dados presente localmente na WLC). No caso do servidor RADIUS (um servidor externo como o ISE), ele pode ser usado não também para armazenar credenciais, mas também para fornecer opções para registro de dispositivo e autoprovisionamento. No caso de um servidor Web externo, como o Cisco DNA Spaces, o portal da Web está presente. No LWA, há um certificado no WLC e outro no portal da Web.

A imagem representa a topologia genérica do LWA:



Topologia Genérica de LWA

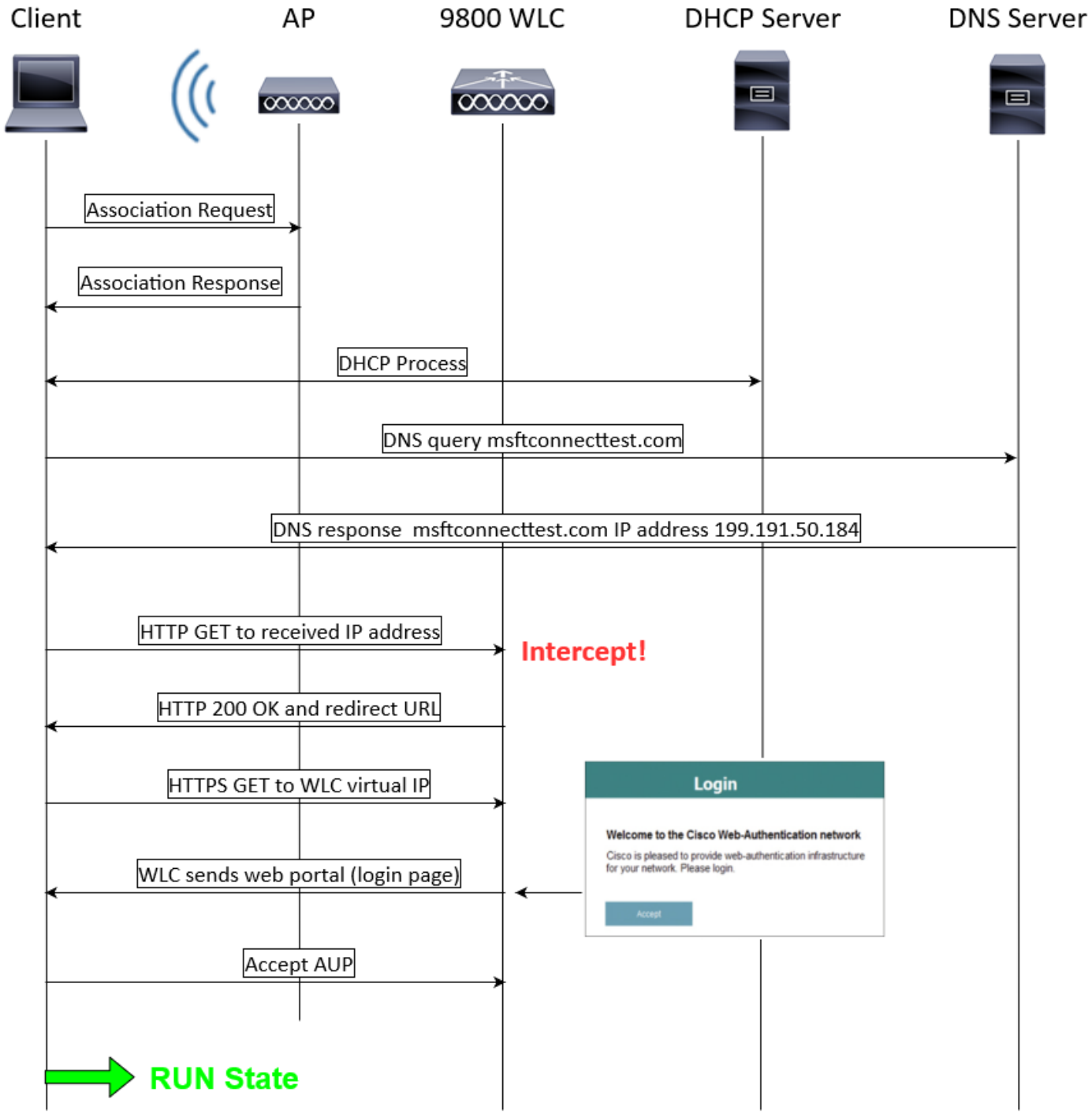
Dispositivos na topologia de rede do LWA:

- Cliente: Envia solicitações ao servidor DHCP e DNS, solicita acesso à WLAN convidada e responde a solicitações da WLC.
- Ponto de acesso: Conectado a um switch, transmite a WLAN convidada e fornece conexão sem fio a dispositivos de usuários convidados. Ele também permite pacotes DHCP e DNS antes que o usuário convidado seja autenticado (antes de inserir credenciais válidas).
- WLC: Gerencia os APs e clientes. A WLC hospeda a URL de redirecionamento e a ACL que corresponde ao tráfego. Intercepta solicitações HTTP dos usuários convidados, redireciona-os para um portal da Web (página de logon) onde os usuários convidados precisam se autenticar. Ele captura as credenciais e autentica os usuários convidados e envia solicitações de acesso a um servidor externo, servidor LDAP ou banco de dados local para confirmar se as credenciais são válidas.
- Servidor de autenticação: Responde às solicitações de acesso da WLC com access accept/reject. O servidor de autenticação valida as credenciais do usuário convidado e

notifica a WLC se as credenciais são válidas ou não. Se as credenciais forem válidas, o usuário convidado será autorizado a acessar a rede (o servidor de autenticação fornece opções para registro de dispositivo e autoprovisionamento). Se as credenciais não forem válidas, o acesso à rede será negado ao usuário convidado.

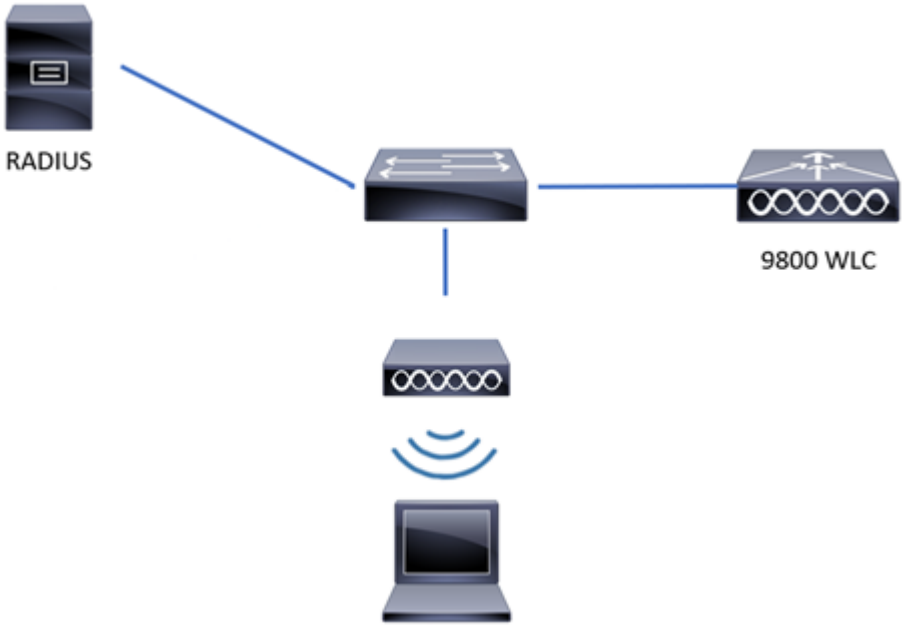
Fluxo LWA:

- O usuário convidado se associa a um AP que transmite a WLAN convidada.
- O usuário convidado passa pelo processo DHCP para obter um endereço IP.
- O usuário convidado deseja fazer uma verificação de conectividade com a Internet no portal cativo. Se for um dispositivo Apple, ele tenta o portal cativo Apple; se for um dispositivo Android, ele tenta o portal cativo Android; se for um dispositivo Windows, ele tentará usar o portal de teste de conexão do Windows.
- O usuário convidado envia uma consulta DNS para solicitar o endereço IP do portal cativo. O servidor DNS responde à consulta com o endereço IP correspondente.
- O usuário convidado envia uma mensagem HTTP GET ao endereço IP do portal cativo.
- A WLC intercepta essa mensagem e responde ao usuário convidado com HTTP 200 OK e o URL de redirecionamento.
- O usuário convidado envia uma mensagem HTTPS GET ao IP virtual da WLC e a WLC responde com o portal da Web.
- O usuário convidado é solicitado a inserir credenciais de autenticação no portal da Web.
- O portal da Web redireciona o usuário de volta para a WLC com as credenciais fornecidas (se um portal da Web externo for usado).
- A WLC autentica o usuário convidado através de um banco de dados local ou envia uma consulta ao servidor RADIUS ou LDAP, para confirmar se as credenciais estão corretas (se o tipo de autenticação for webconsent ou webauth).
- Se as credenciais estiverem corretas, a WLC autenticará o usuário convidado e ele entrará no estado RUN. Se as credenciais estiverem erradas, a WLC excluirá o usuário convidado.
- A WLC redireciona o cliente de volta ao URL original que foi inserido no navegador da Web.



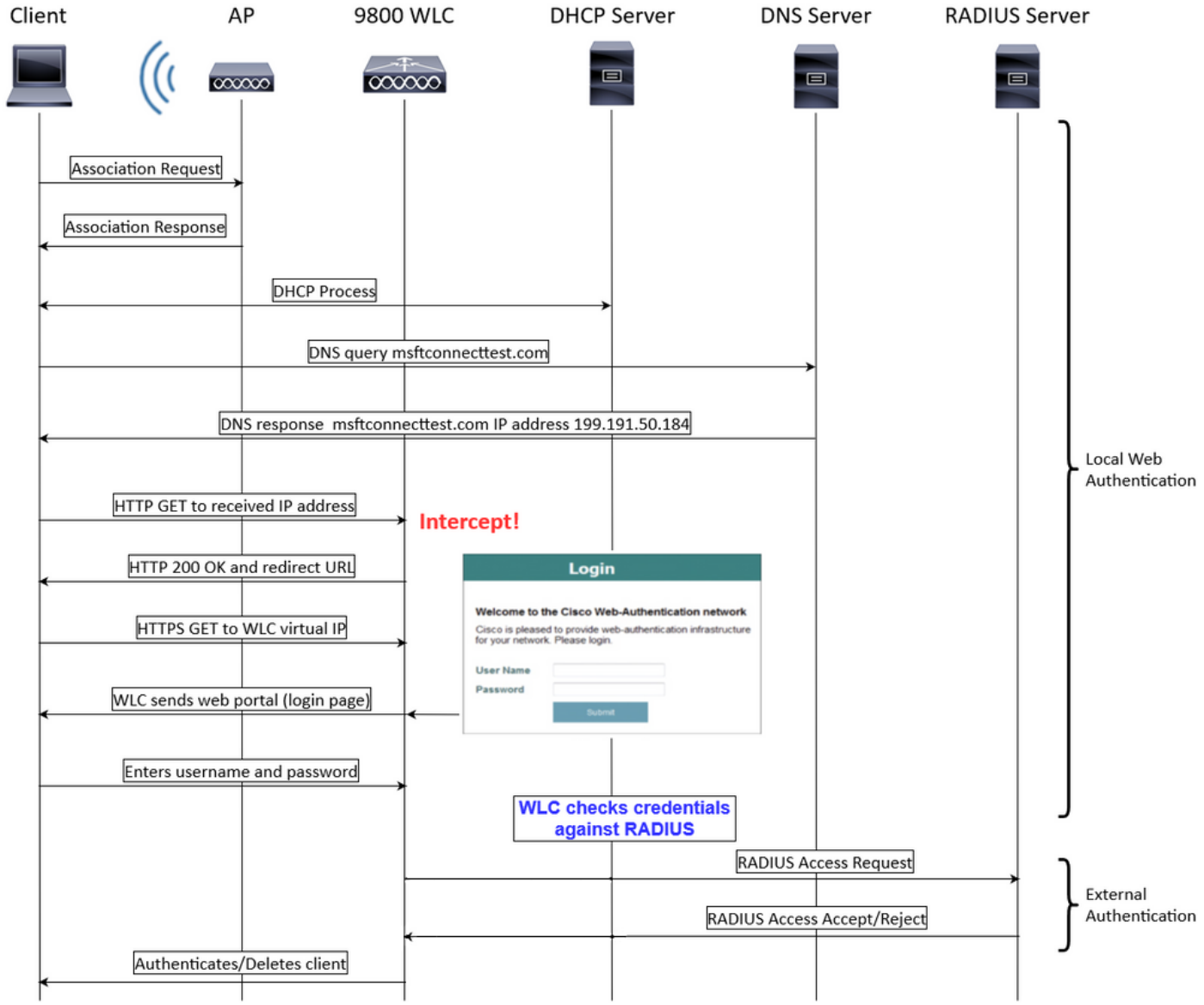
Fluxo LWA

Autenticação da Web Local com Autenticação Externa



Topologia Genérica do LWA-EA

LWA-EA é um método de LWA em que o portal da Web e a URL de redirecionamento estão localizados na WLC e as credenciais são armazenadas em um servidor externo, como o ISE. A WLC captura as credenciais e autentica o cliente através de um servidor RADIUS externo. Quando o usuário convidado insere credenciais, a WLC verifica as credenciais em relação ao RADIUS, envia uma solicitação de acesso RADIUS e recebe uma aceitação/rejeição de acesso RADIUS do servidor RADIUS. Em seguida, se as credenciais estiverem corretas, o usuário convidado entrará no estado EXECUTAR. Se as credenciais estiverem incorretas, o usuário convidado será excluído pela WLC.



Fluxo LWA-EA

Configurar

Diagrama de Rede

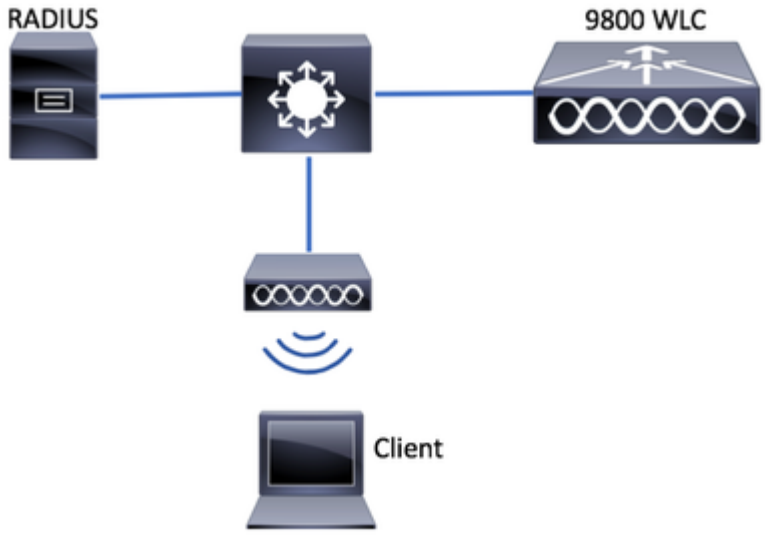


Diagrama de Rede

Note: Este exemplo de configuração cobre somente a comutação/autenticação central. A configuração do switching local flexível possui requisitos ligeiramente diferentes para configurar a autenticação da Web.

Configurar a autenticação da Web local com autenticação externa na CLI

Configurar o servidor AAA e o grupo de servidores

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#radius server RADIUS
9800WLC(config-radius-server)#address ipv4 <ip address> auth-port 1812 acct-port 1813
9800WLC(config-radius-server)#key cisco
9800WLC(config-radius-server)#exit
9800WLC(config)#aaa group server radius RADIUSGROUP
9800WLC(config-sg-radius)#server name RADIUS
9800WLC(config-sg-radius)#end
```

Configurar Autenticação e Autorização Local

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#aaa new-model
```

```
9800WLC(config)#aaa authentication login LWA_AUTHENTICATION group RADIUSGROUP
9800WLC(config)#aaa authorization network LWA_AUTHORIZATION group RADIUSGROUP
9800WLC(config)#end
```

Configure Parameter Maps

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)# parameter-map type webauth global
9800WLC(config-params-parameter-map)#virtual-ip ipv4 192.0.2.1
9800WLC(config-params-parameter-map)#trustpoint <trustpoint name>
9800WLC(config-params-parameter-map)#end
```

Configurar parâmetros de segurança da WLAN

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wlan LWA_EA 1 LWA_EA
9800WLC(config-wlan)#no security wpa
9800WLC(config-wlan)#no security wpa wpa2
9800WLC(config-wlan)#no security wpa wpa2 ciphers aes
9800WLC(config-wlan)#no security wpa akm dot1x
9800WLC(config-wlan)#security web-auth
9800WLC(config-wlan)#security web-auth authentication-list LWA_AUTHENTICATION
9800WLC(config-wlan)#security web-auth parameter-map global
9800WLC(config-wlan)#no shutdown
9800WLC(config-wlan)#end
```

Criar Perfil de Diretiva sem Fio

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wireless profile policy POLICY_PROFILE
9800WLC(config-wireless-policy)#vlan <vlan name>
9800WLC(config-wireless-policy)#no shutdown
9800WLC(config-wireless-policy)#end
```

Criar uma Marca de Diretiva

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wireless tag policy POLICY_TAG
```

```
9800WLC(config-policy-tag)#wlan LWA_EA policy POLICY_PROFILE
9800WLC(config-policy-tag)# end
```

Atribuir uma etiqueta de política a um AP

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#ap <MAC address>
9800WLC(config-ap-tag)#policy-tag POLICY_TAG
9800WLC(config-ap-tag)#end
```

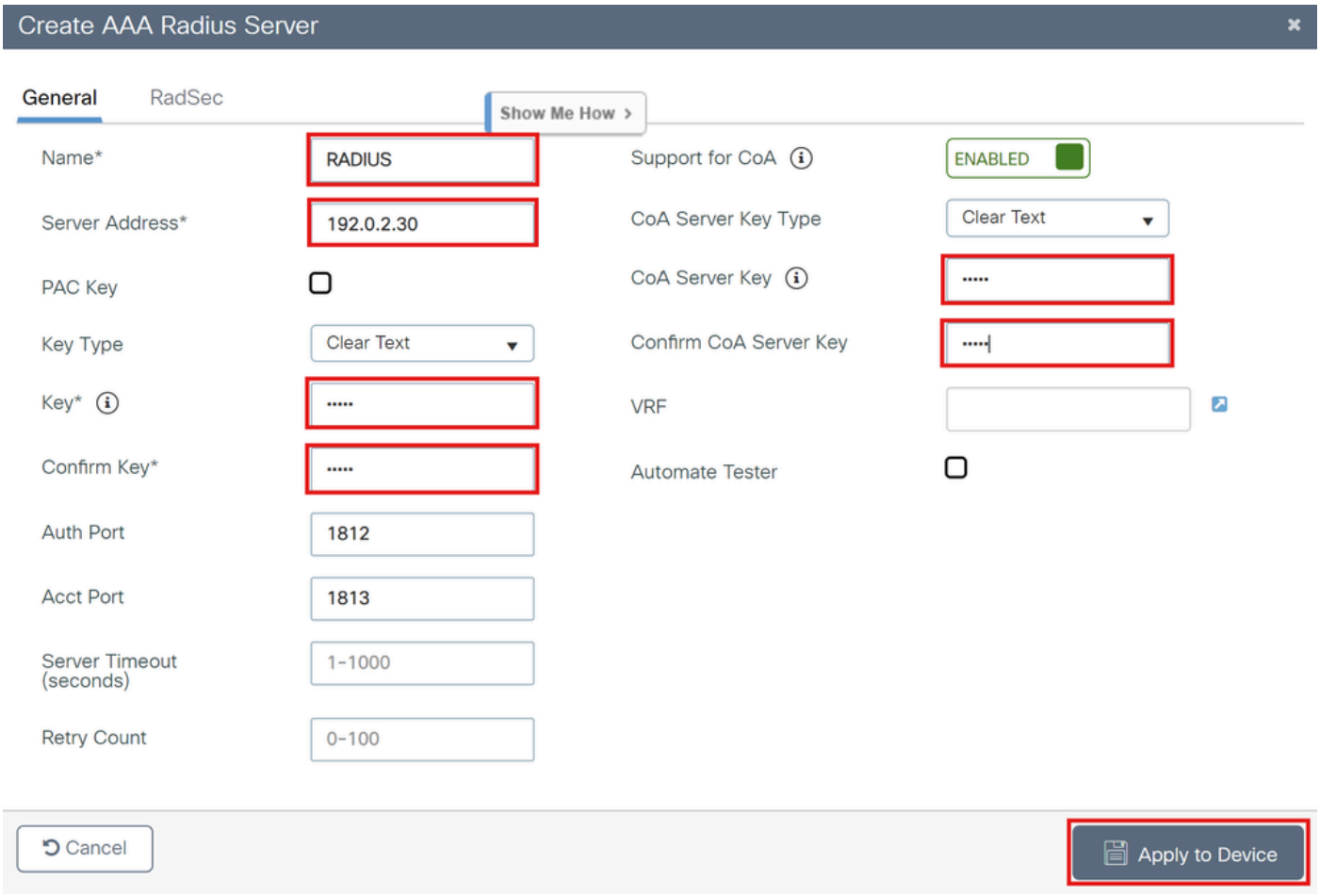
Para concluir a configuração no lado do ISE, vá para a seção Configuração do ISE.

Configurar a Autenticação da Web Local com Autenticação Externa na WebUI

Configuração de AAA no 9800 WLC

Etapa 1. Adicionar o servidor ISE à configuração da WLC 9800.

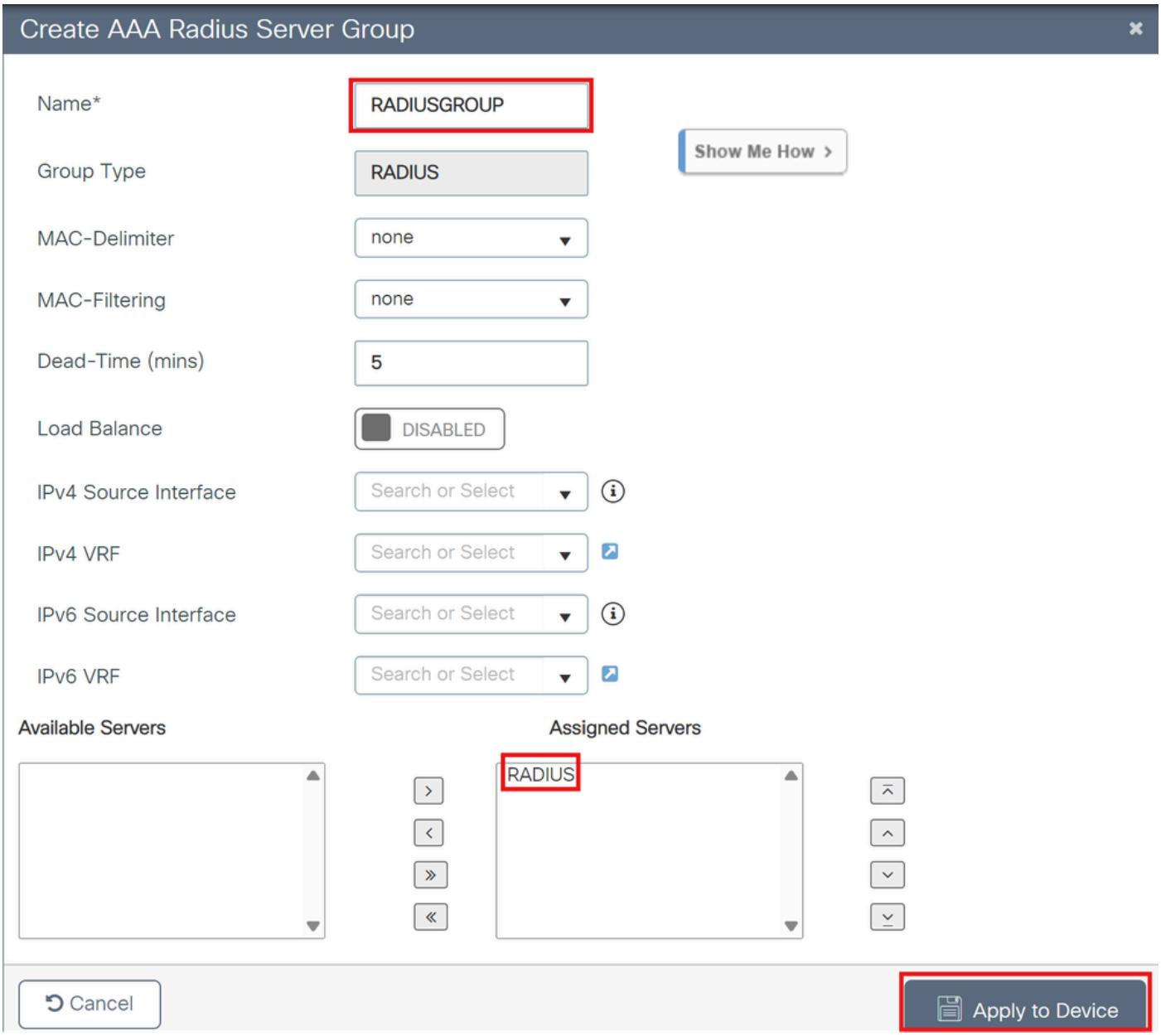
Navegue para Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add e insira as informações do servidor RADIUS como mostrado na imagem:



Configuração de AAA no 9800 WLC

Etapa 2. Adicionar o grupo de servidores RADIUS.

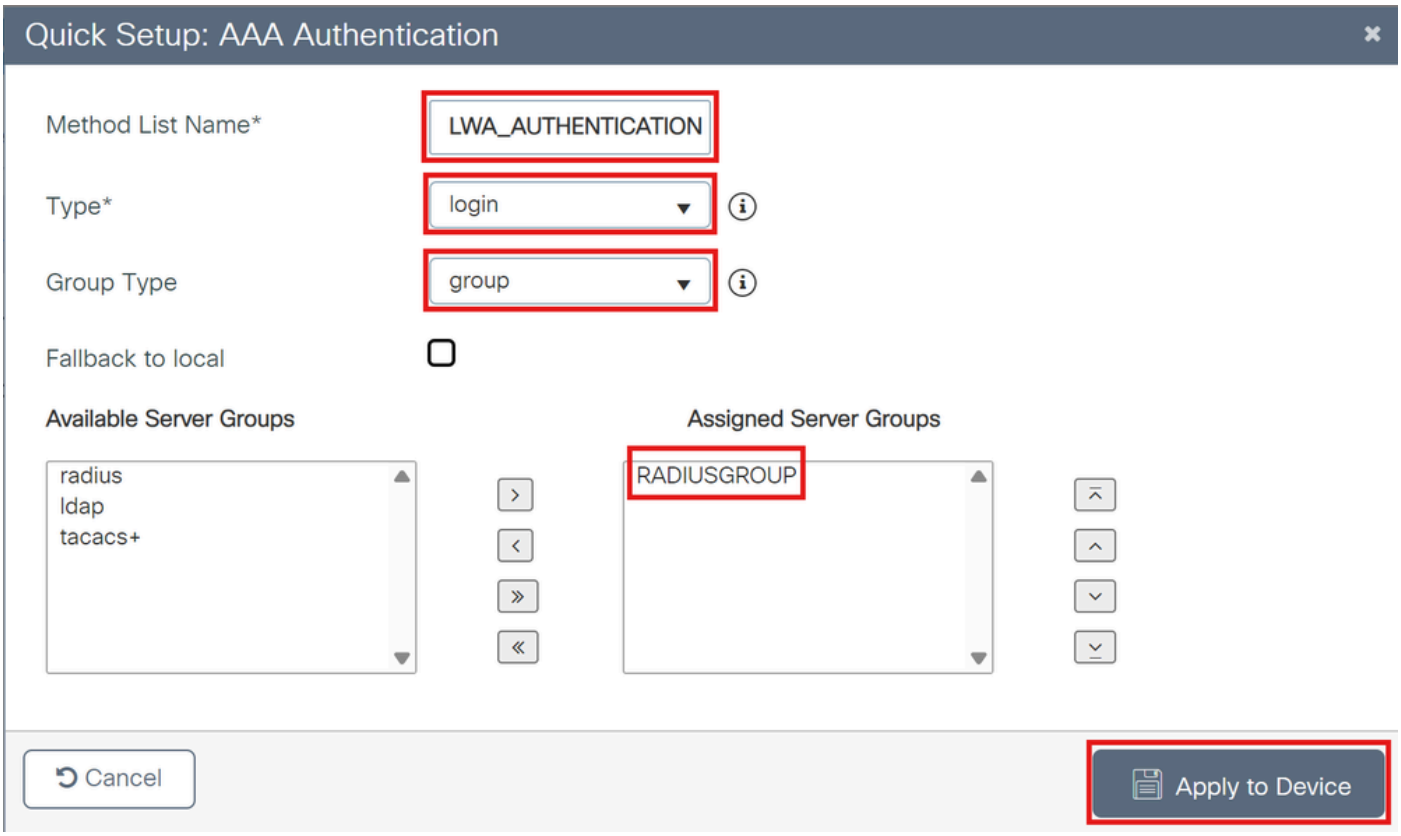
Navegue para Configuration > Security > AAA > Servers/Groups > RADIUS > Servers Group > + Add e insira as informações do grupo de servidores RADIUS:



Adicionar o grupo de servidores RADIUS

Etapa 3. Crie uma lista de métodos de autenticação.

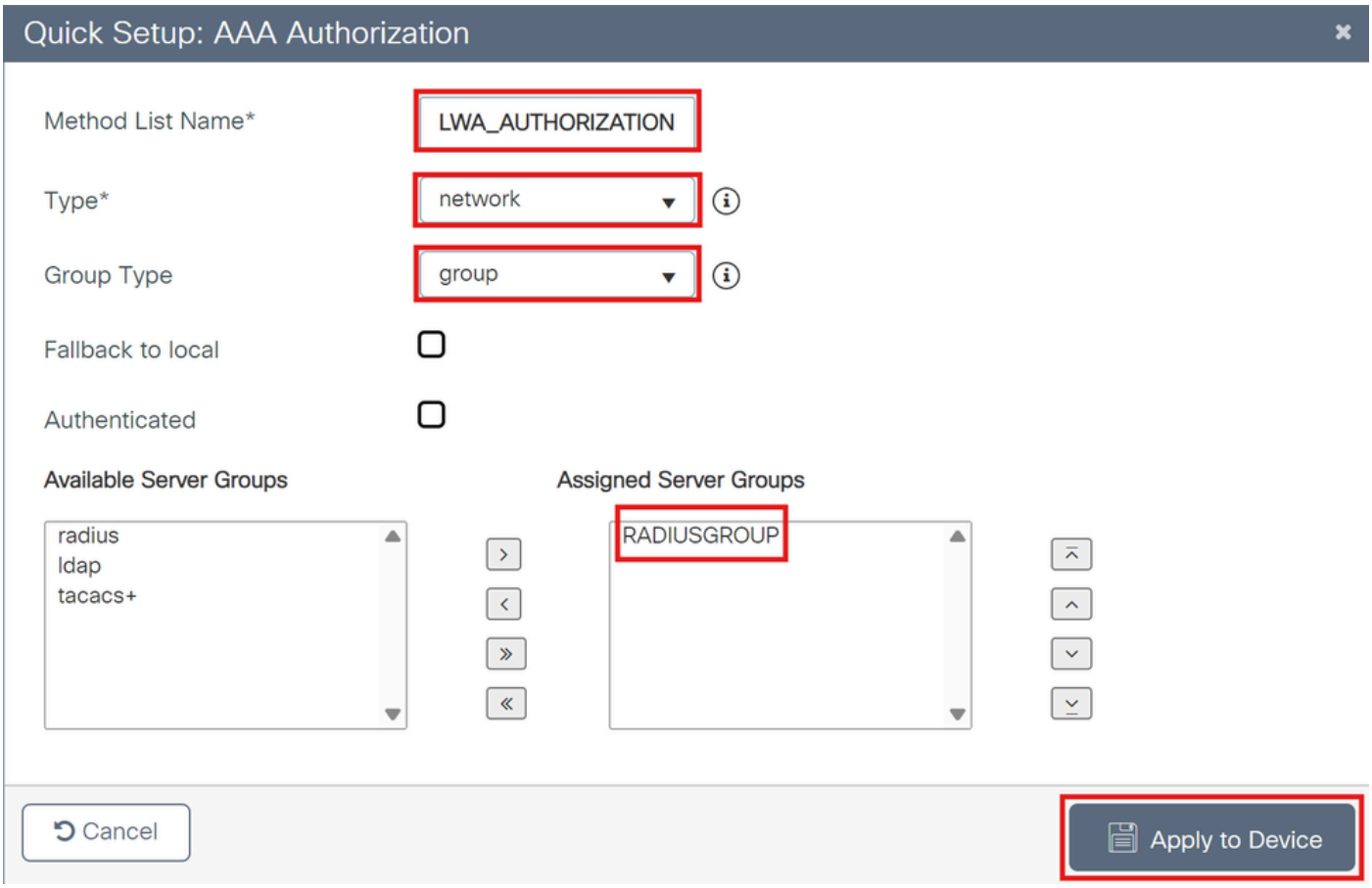
Navegue até Configuration > Security > AAA > AAA Method List > Authentication > + Add:



Criar uma lista de métodos de autenticação

Etapa 4. Criar uma lista de métodos de autorização.

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

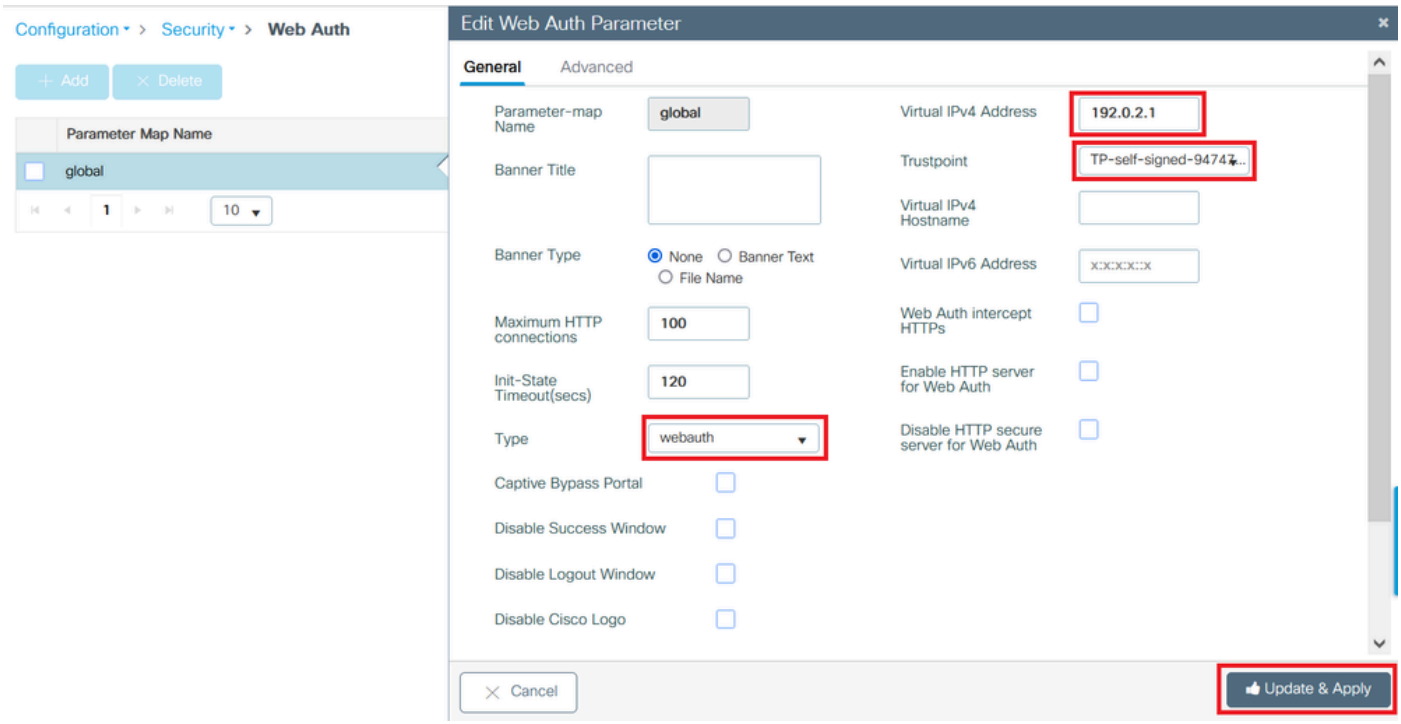


Crie uma lista de métodos de autorização

Configuração do WebAuth

Crie ou edite um mapa de parâmetros. Selecione o tipo como webauth, o endereço IPv4 virtual deve ser um endereço não usado na rede para evitar conflitos de endereços IP e adicione um ponto de confiança.

Navegue até Configuration > Security > Web Auth > + Add ou selecione um mapa de parâmetros:

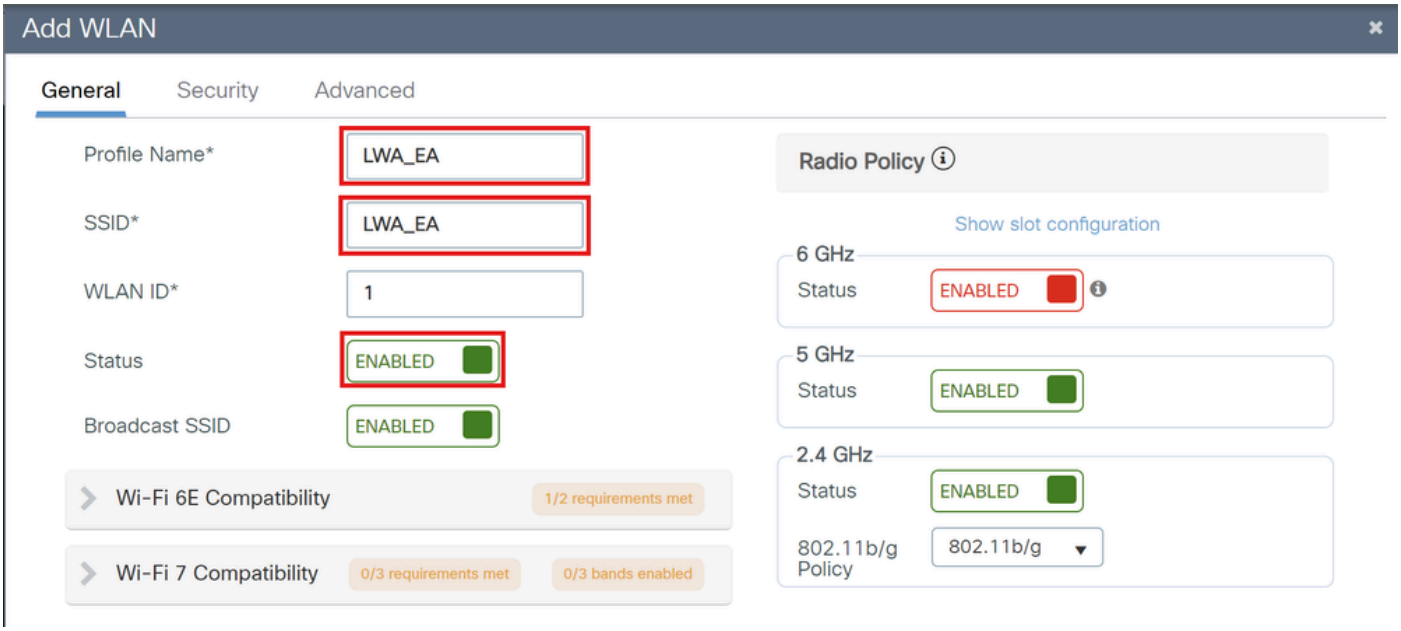


Configuração do WebAuth

Configuração de WLAN

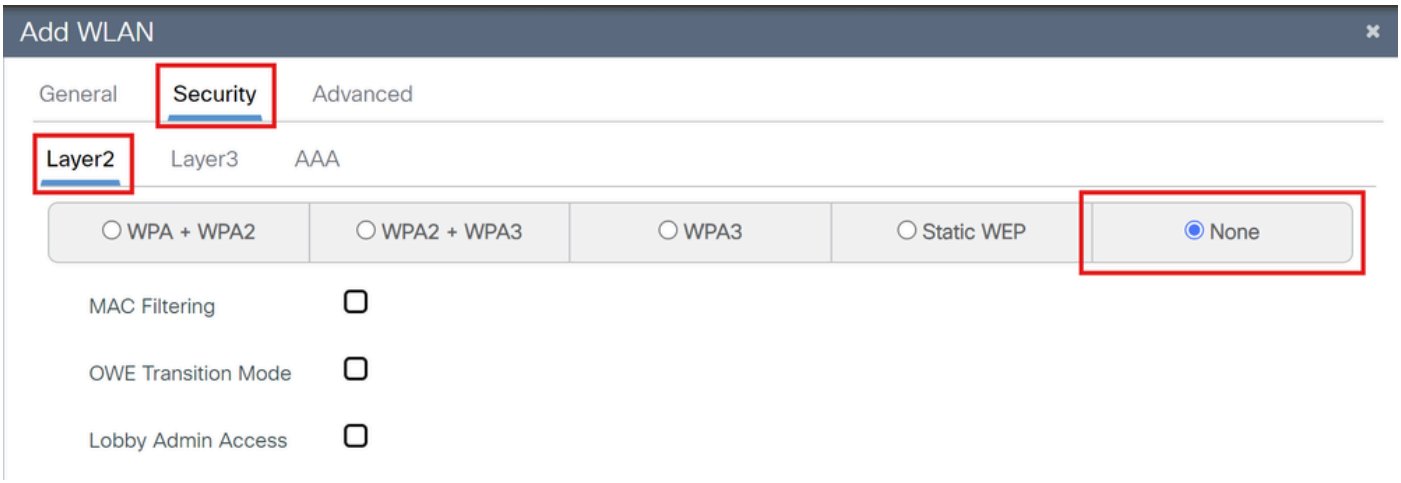
Etapa 1. Criar a WLAN.

Navegue até Configuração > Marcas e perfis > WLANs > + Adicionar e configure a rede conforme necessário.



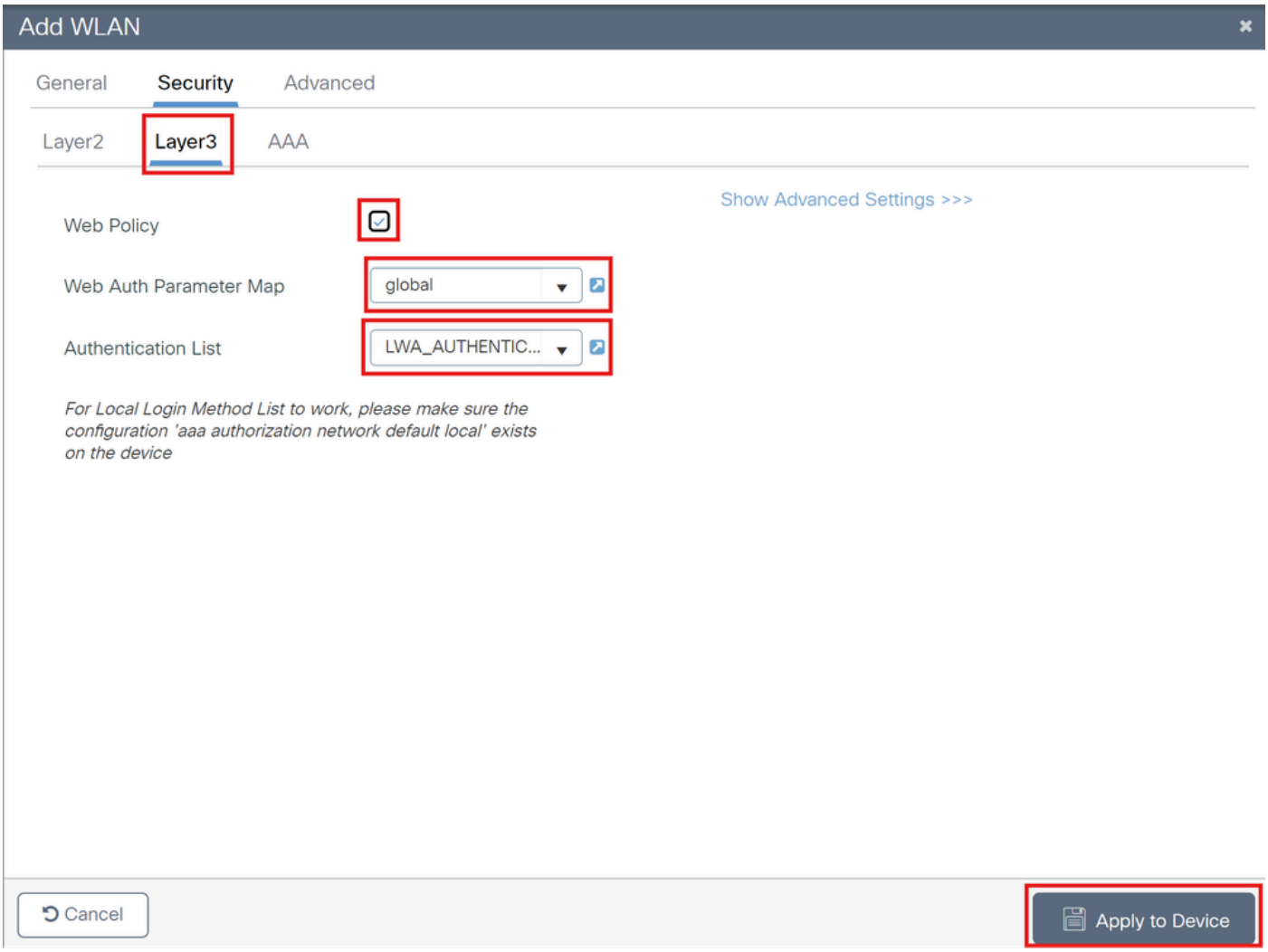
Criar a WLAN

Etapa 2. Navegue até Security > Layer2 e, no Layer 2 Security Mode, selecione None.



Crie a segurança da WLAN

Etapa 3. Navegue até Security > Layer3 e, em Web Policy, marque a caixa, em Web Auth Parameter Map selecione o nome do parâmetro e, em Authentication List, selecione a lista de autenticação criada anteriormente.



A WLAN é exibida na lista de WLANs:

WLAN criada

Configuração de perfil de política

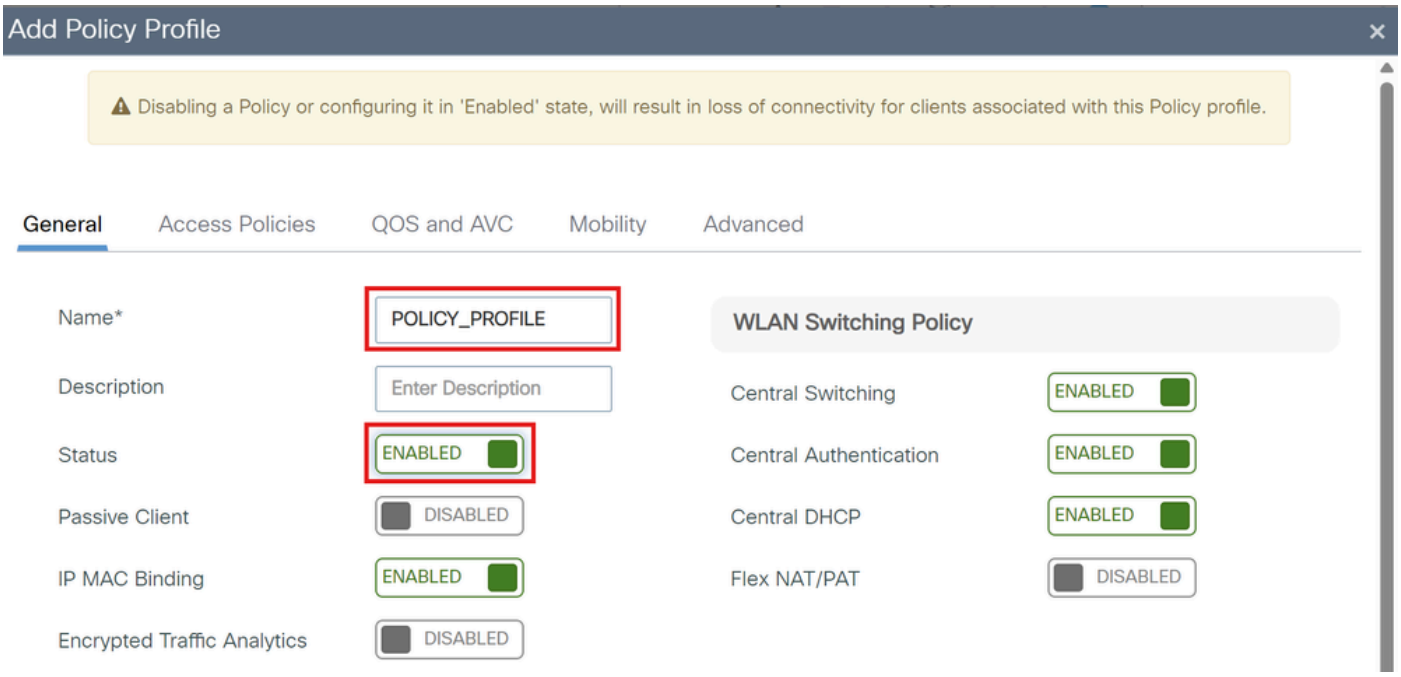
Dentro de um perfil de política, você pode selecionar a VLAN que atribui os clientes, entre outras configurações.

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

Etapa 1. Crie um novo Perfil de Política.

Navegue até Configuration > Tags & Profiles > Policy e configure seu perfil de política padrão ou crie um novo.

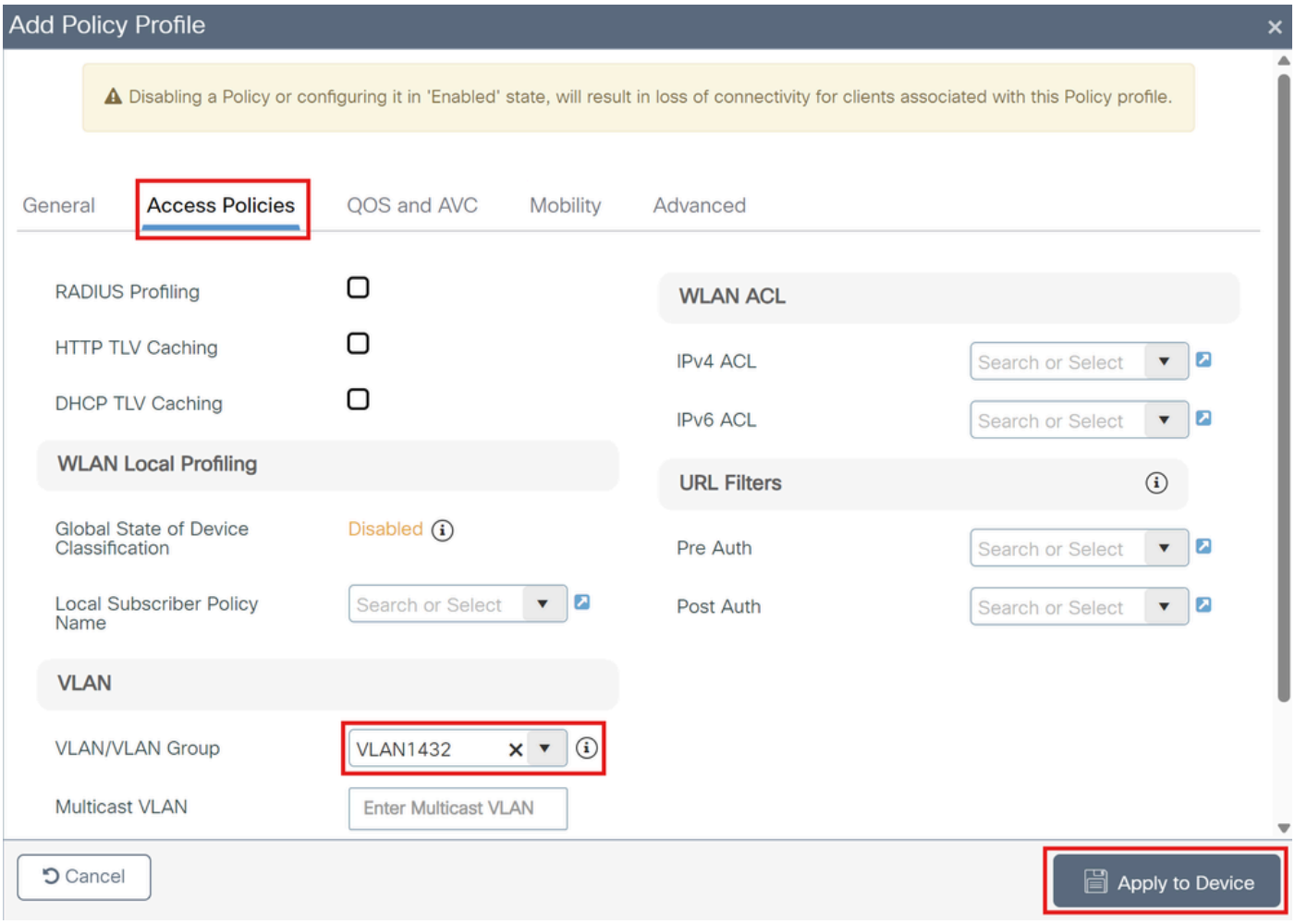
Verifique se o perfil está ativado.



Criar um novo perfil de política

Etapa 2. Selecione a VLAN.

Navegue até a guia Políticas de acesso e selecione o nome da VLAN no menu suspenso ou digite manualmente a VLAN-ID.



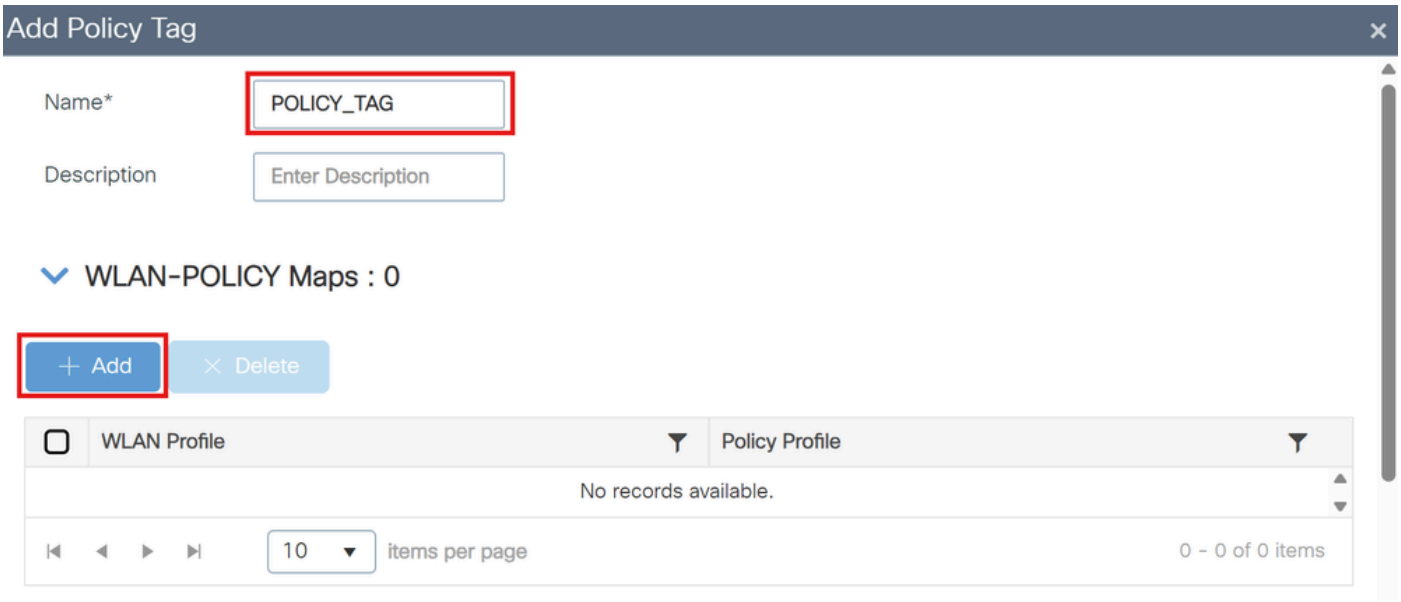
Selecione a VLAN

Configuração de marca de política

Dentro da marca de política, você vincula a SSID ao perfil de política. Você pode criar uma nova marca de política ou usar a marca default-policy.

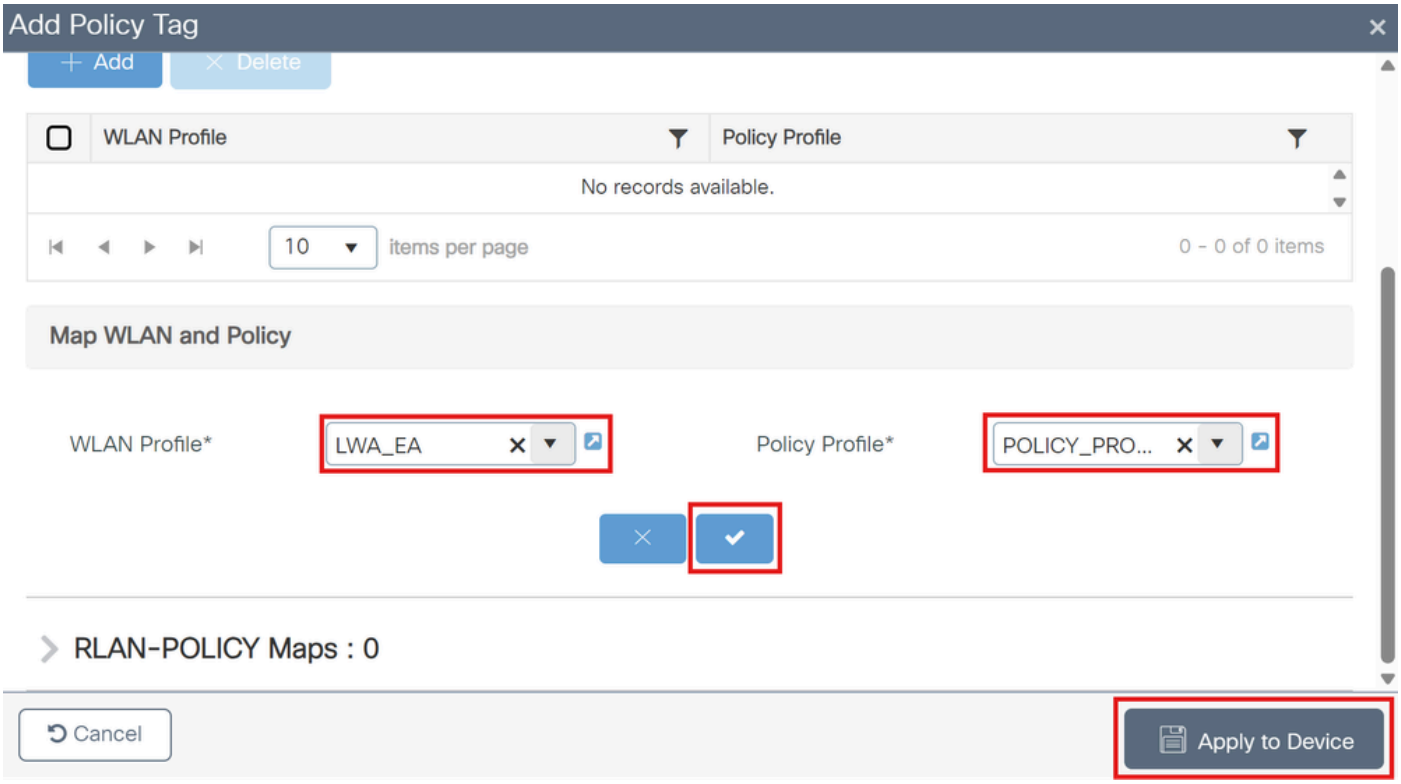
Navegue até Configuração > Marcas e perfis > Marcas > Política e adicione uma nova, se necessário, conforme mostrado na imagem.

Selecione + Adicionar:



Configuração de marca de política

Vincule o perfil de WLAN ao perfil de política desejado:

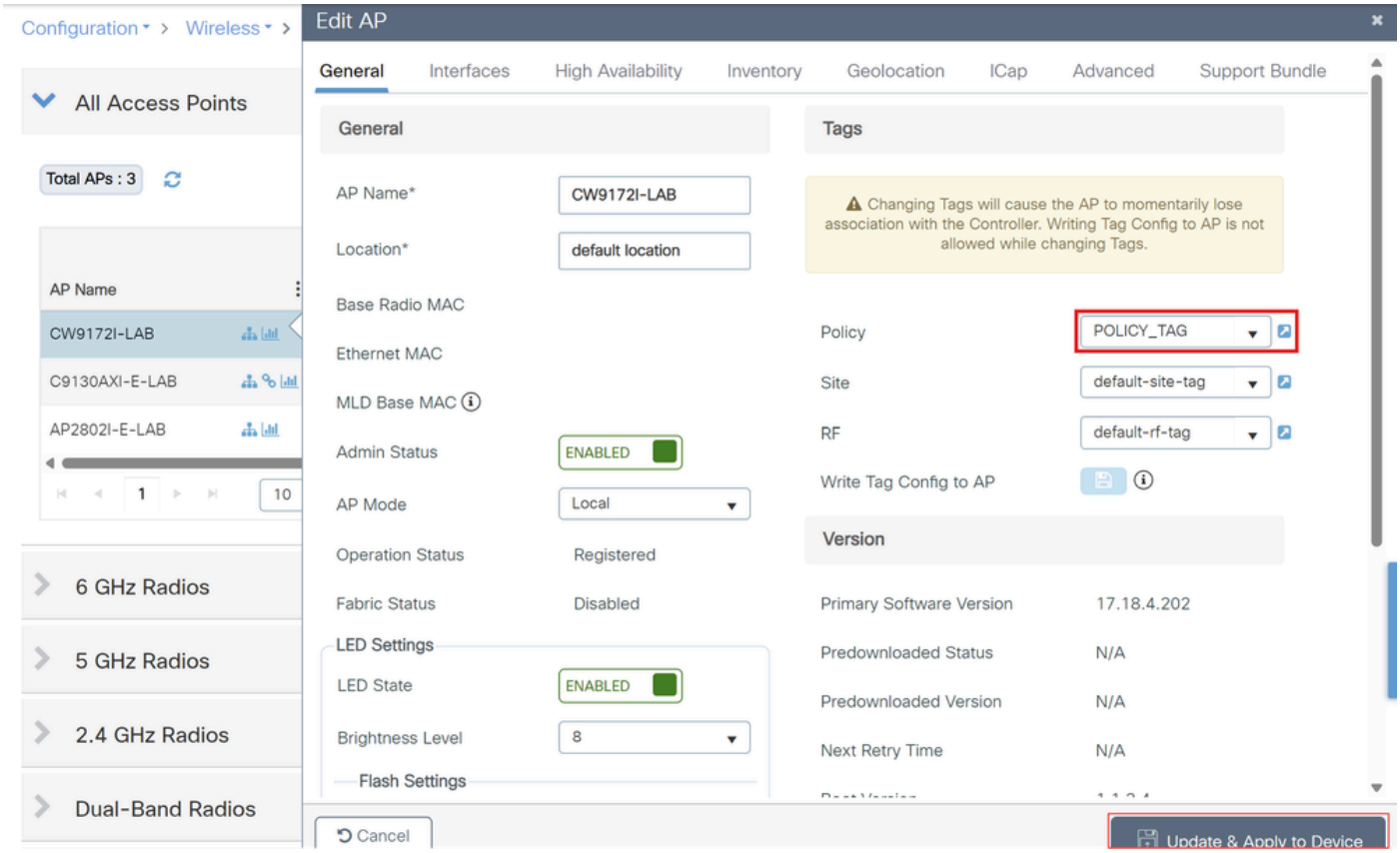


Configuração de marca de política

Atribuição de marca de política

Atribua a marca de política aos APs necessários.

Para atribuir a marca a um AP, navegue até Configuração > Conexão sem fio > Access points > Nome do AP > Marcas gerais , faça a atribuição necessária e clique em Atualizar e aplicar ao dispositivo.

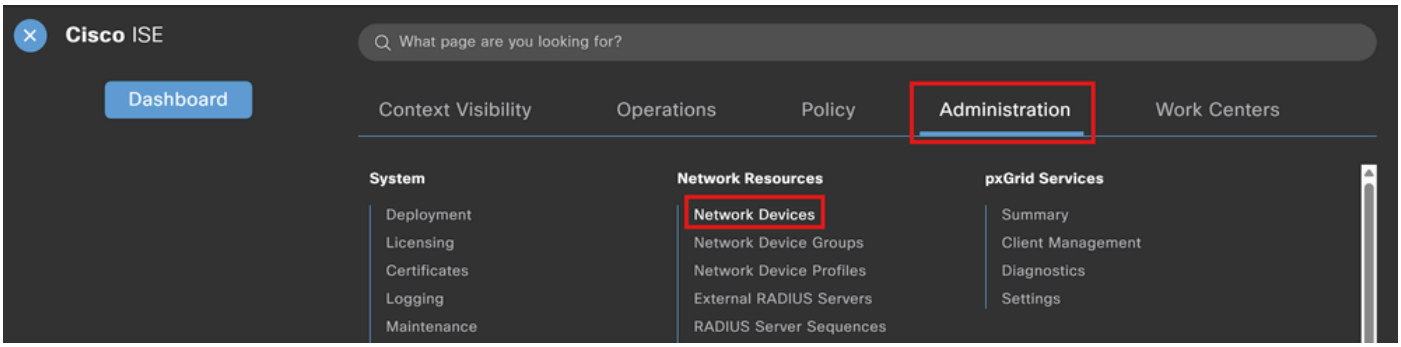


Atribuição de marca de política

Configuração do ISE

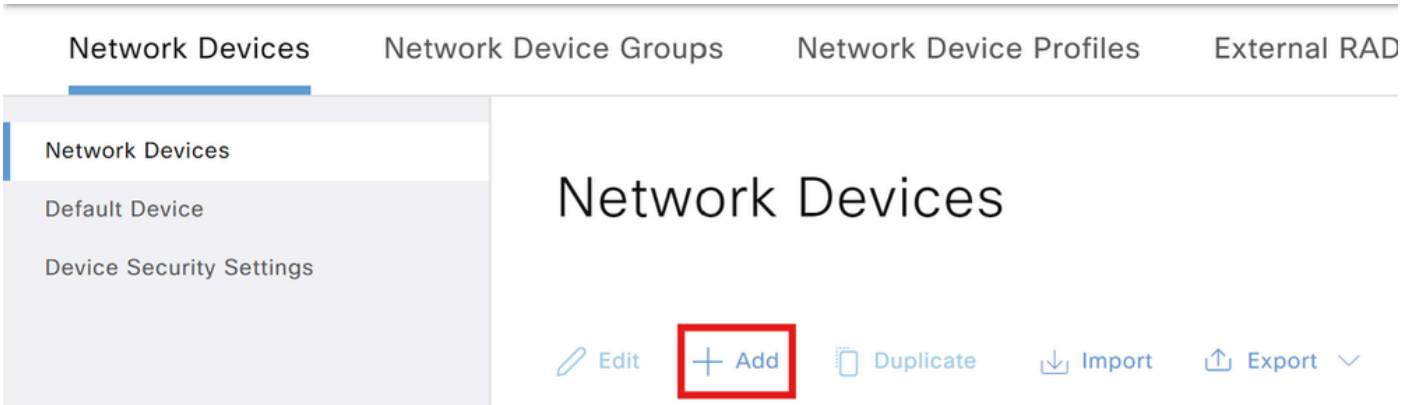
Adicionar o 9800 WLC ao ISE

Etapa 1. Navegue até Administration > Network Resources > Network Devices conforme mostrado na imagem.



Adicionar o 9800 WLC ao ISE

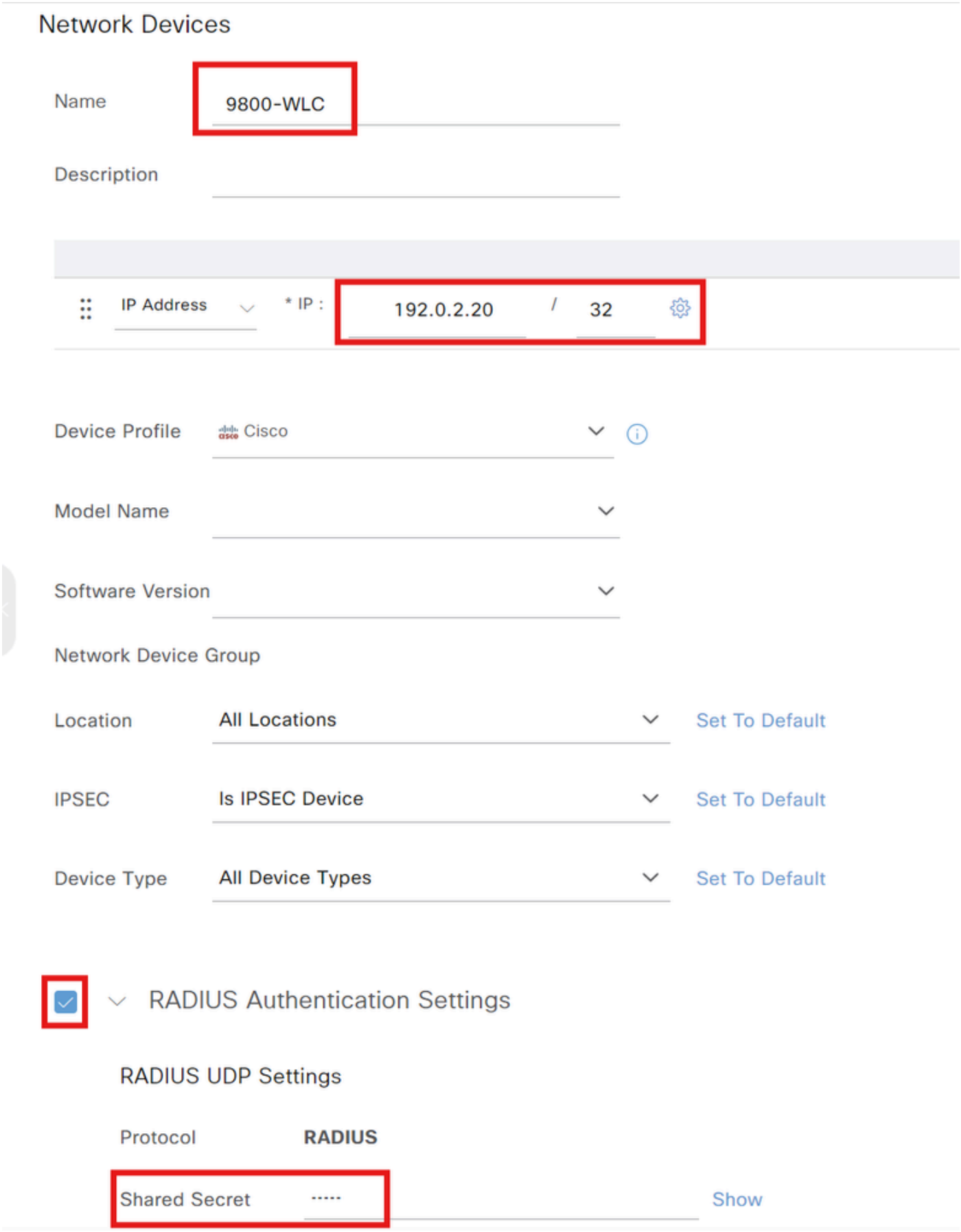
Etapa 2. Clique em +Adicionar.



Adicionar dispositivos de rede

Opcionalmente, pode ser um nome de modelo especificado, uma versão de software, uma descrição e atribuir grupos de dispositivos de rede de acordo com os tipos de dispositivos, localização ou WLCs.

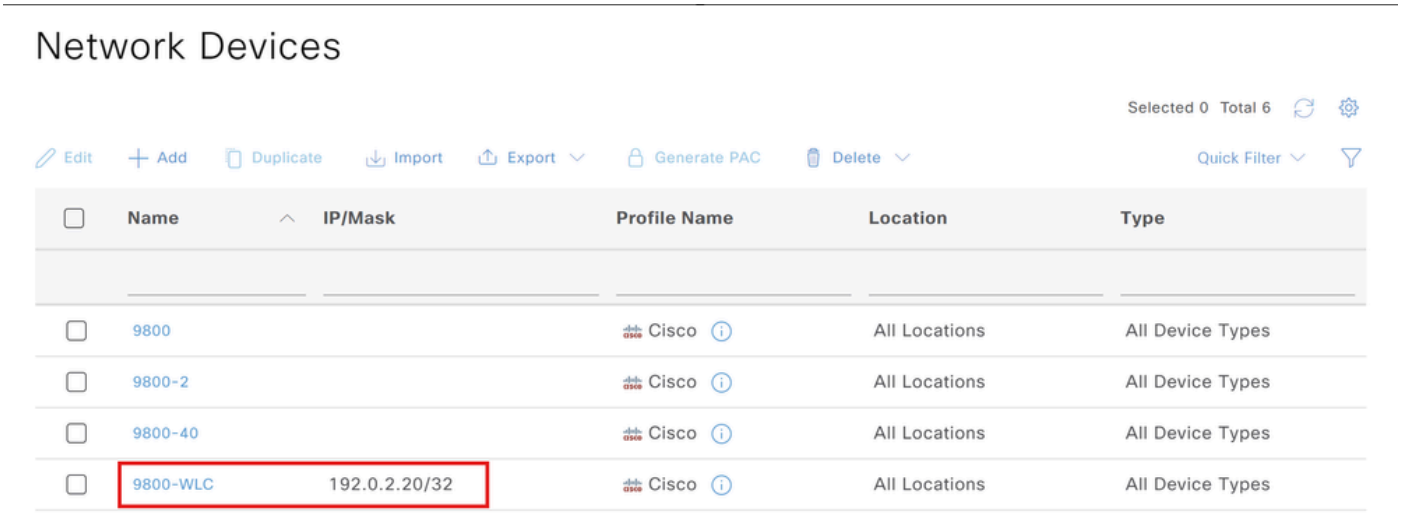
Etapa 3. Insira as configurações da WLC 9800 conforme mostrado na imagem. Insira a mesma chave RADIUS definida na criação do servidor no lado da WLC. Em seguida, clique em Enviar.



Configurações da WLC 9800

Etapa 4. Navegue até Administration > Network Resources > Network Devices, você pode ver a

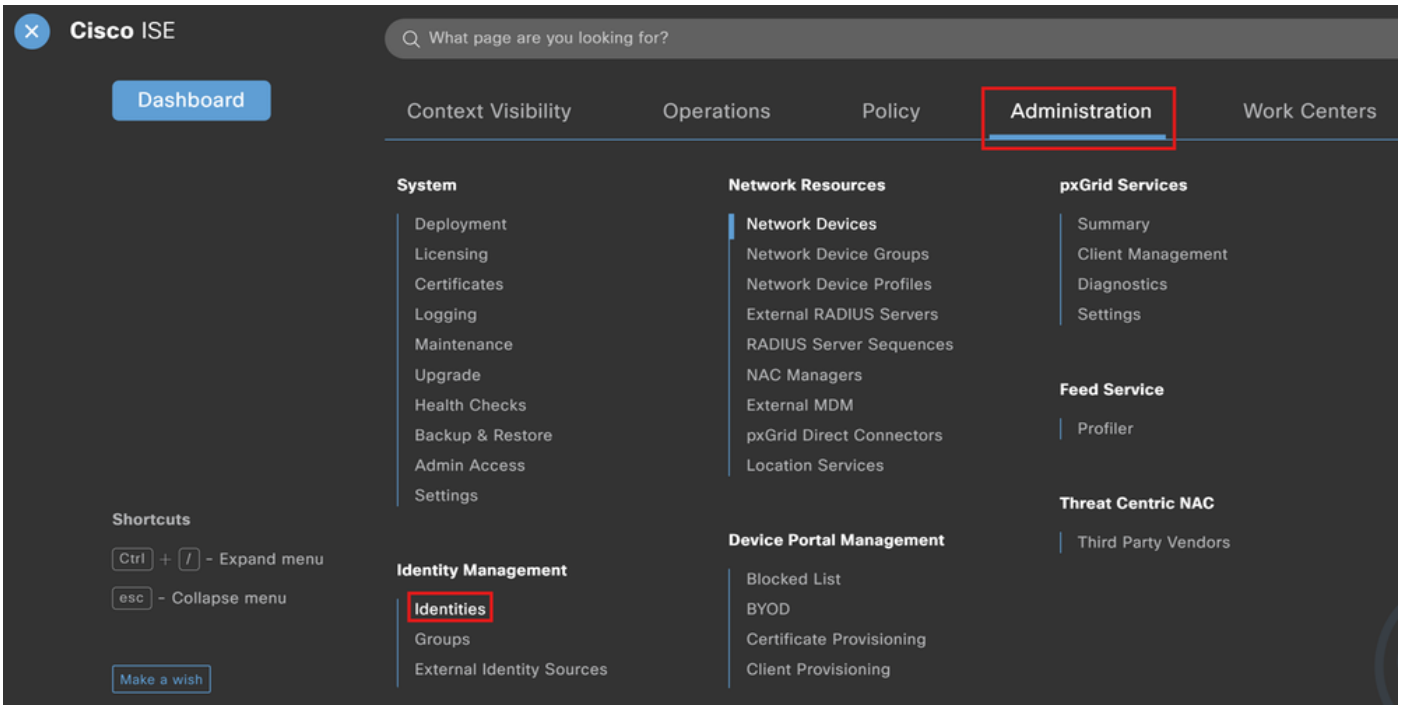
lista de dispositivos de rede.



Lista de dispositivos de rede

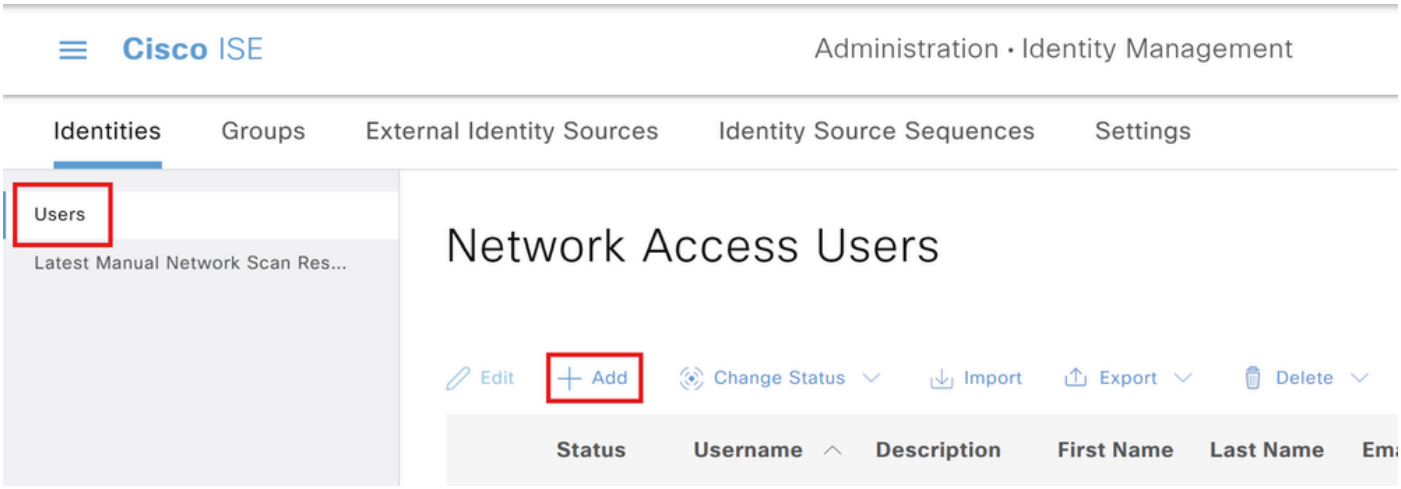
Criar novo usuário no ISE

Etapa 1. Navegue até Administração > Gerenciamento de identidades > Identidades:



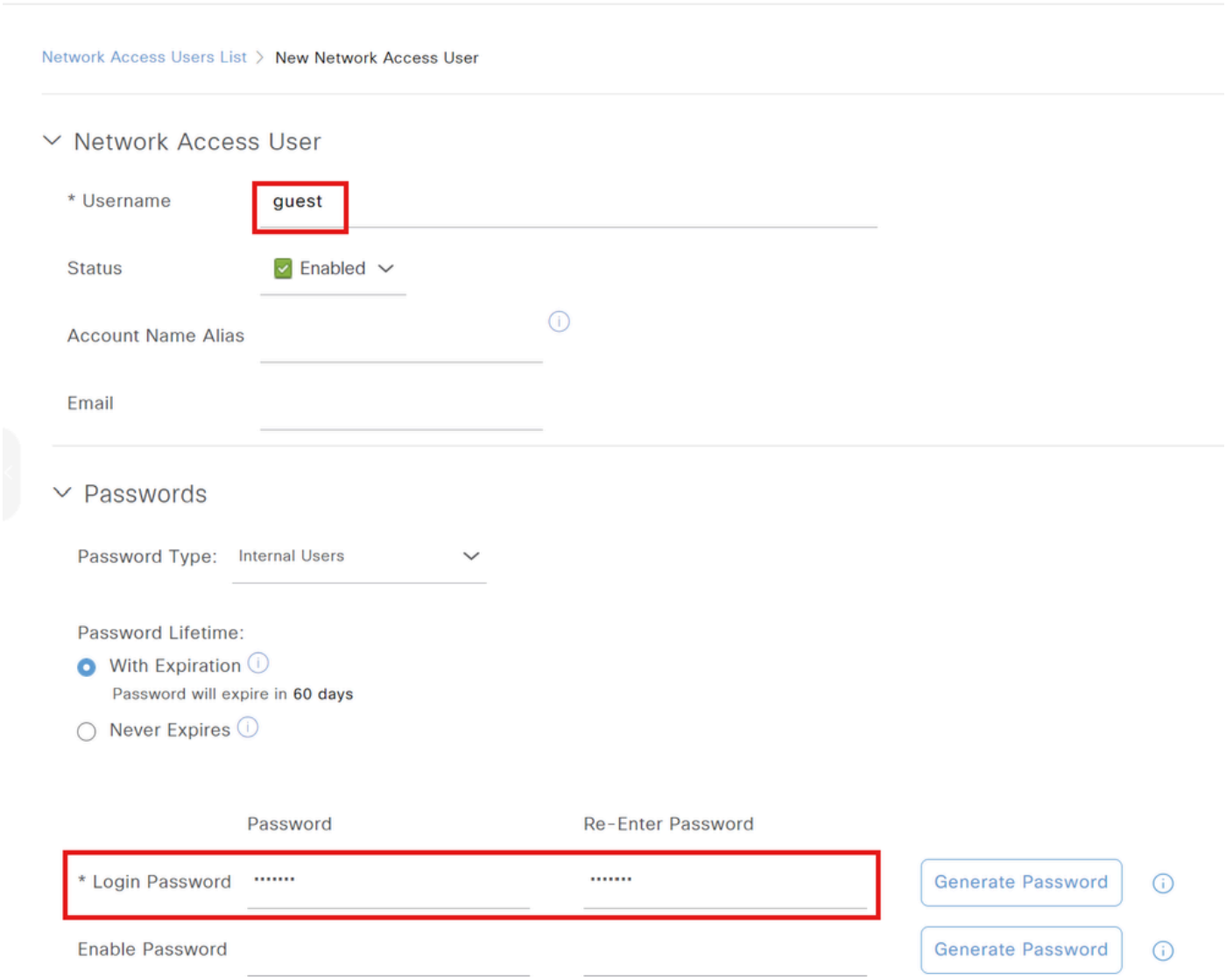
Administração do ISE - Identidades

Etapa 2. Navegue até Usuários, clique em +Adicionar.



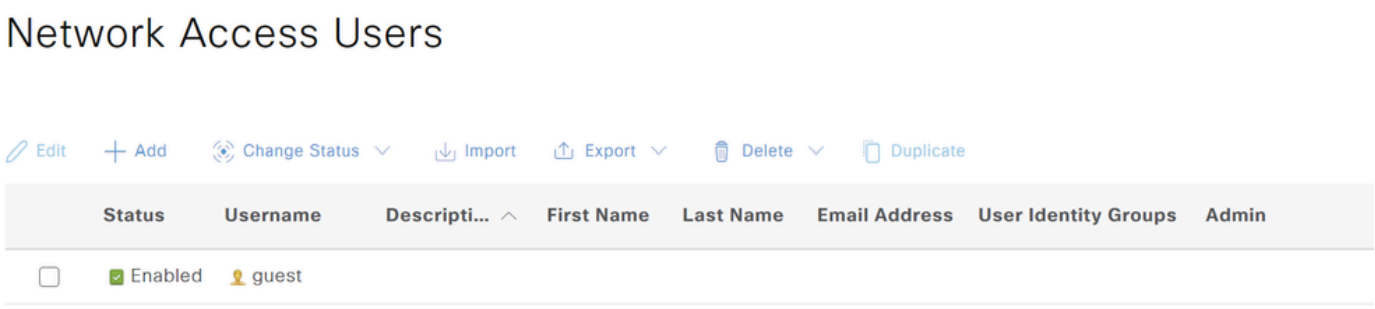
Adicionar usuário

Etapa 3. Insira o nome de usuário e a senha do usuário convidado e clique em Submit.



Criar novo usuário no ISE

Etapa 4. Navegue até Administration > Identity Management > Identities > Users, você pode ver a lista de usuários.



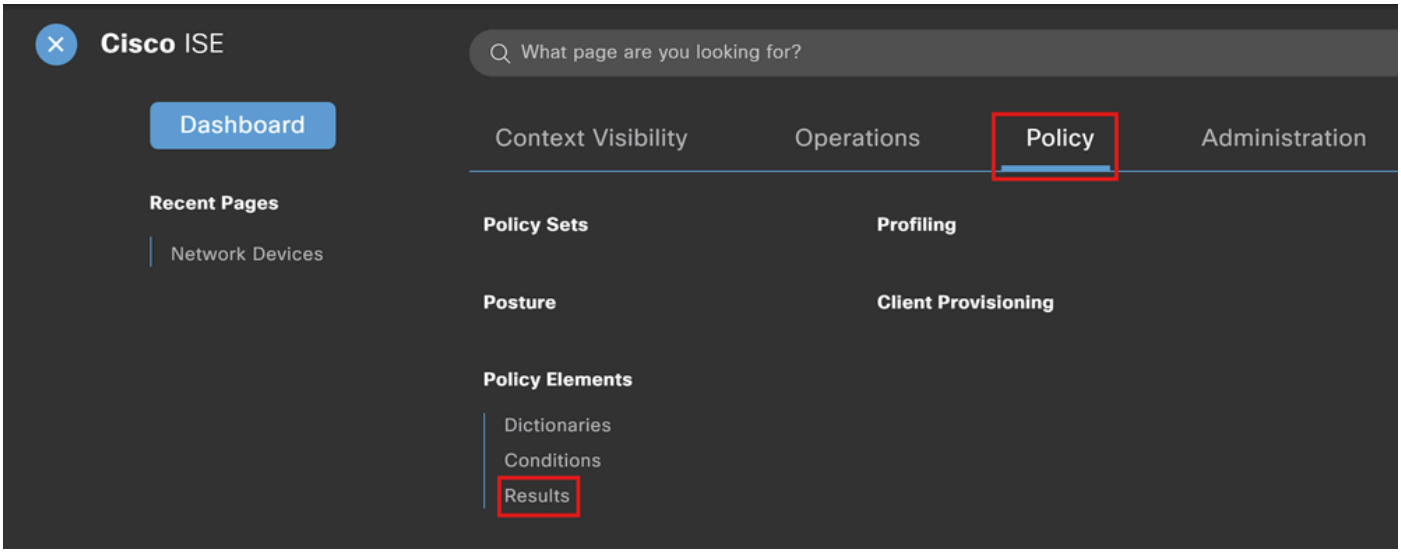
Lista de usuários de acesso à rede

Criar perfil de autorização

O perfil de política é o resultado atribuído a um cliente com base nos parâmetros (como endereço MAC, credenciais, WLAN usada e assim por diante). Pode atribuir configurações específicas, como rede de área local virtual (VLAN), listas de controle de acesso (ACLs), redirecionamentos de Uniform Resource Locator (URL) e assim por diante.

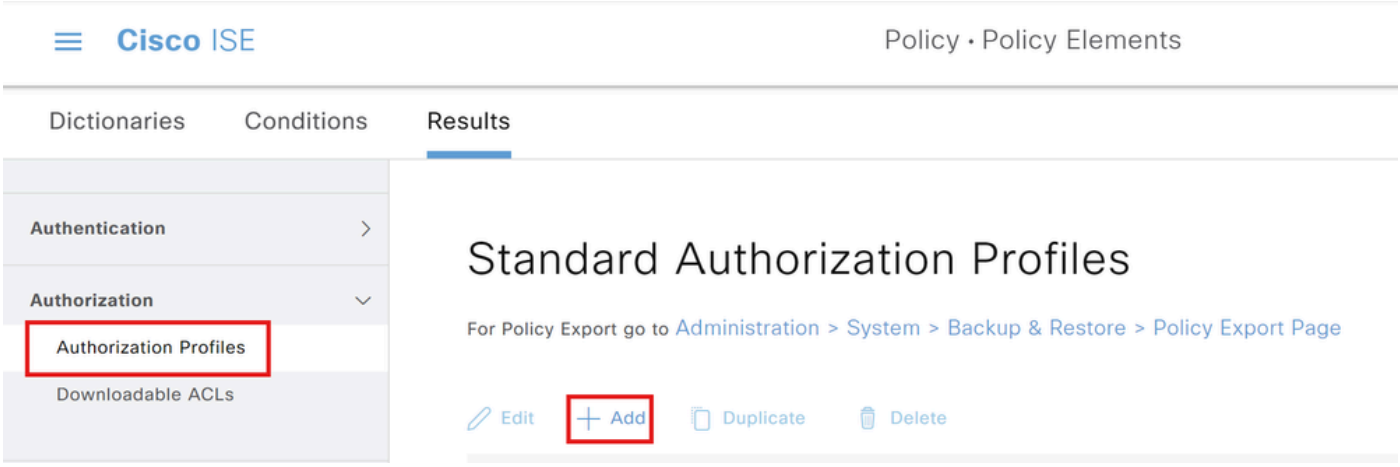
Estas etapas mostram como criar o perfil de autorização necessário para redirecionar o cliente para o portal de autenticação. Observe que, nas versões recentes do ISE, já existe um resultado de autorização Cisco_Webauth. Aqui, você pode editá-lo para modificar o nome da ACL de redirecionamento para corresponder à que você configurou no WLC.

Etapa 1. Navegue até Política > Elementos de Política > Resultados.



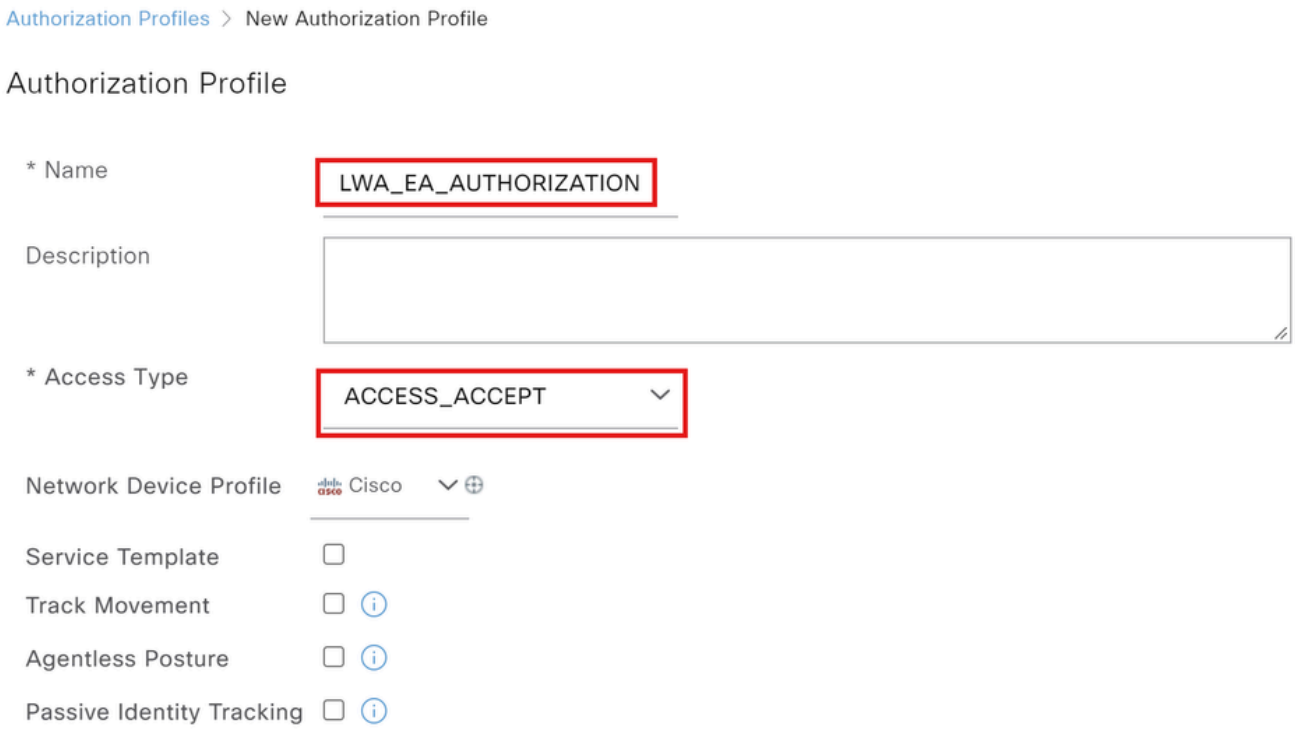
Política do ISE - Resultados

Etapa 2. Navegue até Autorização > Perfis de autorização. Clique em +Add para criar o perfil de autorização.



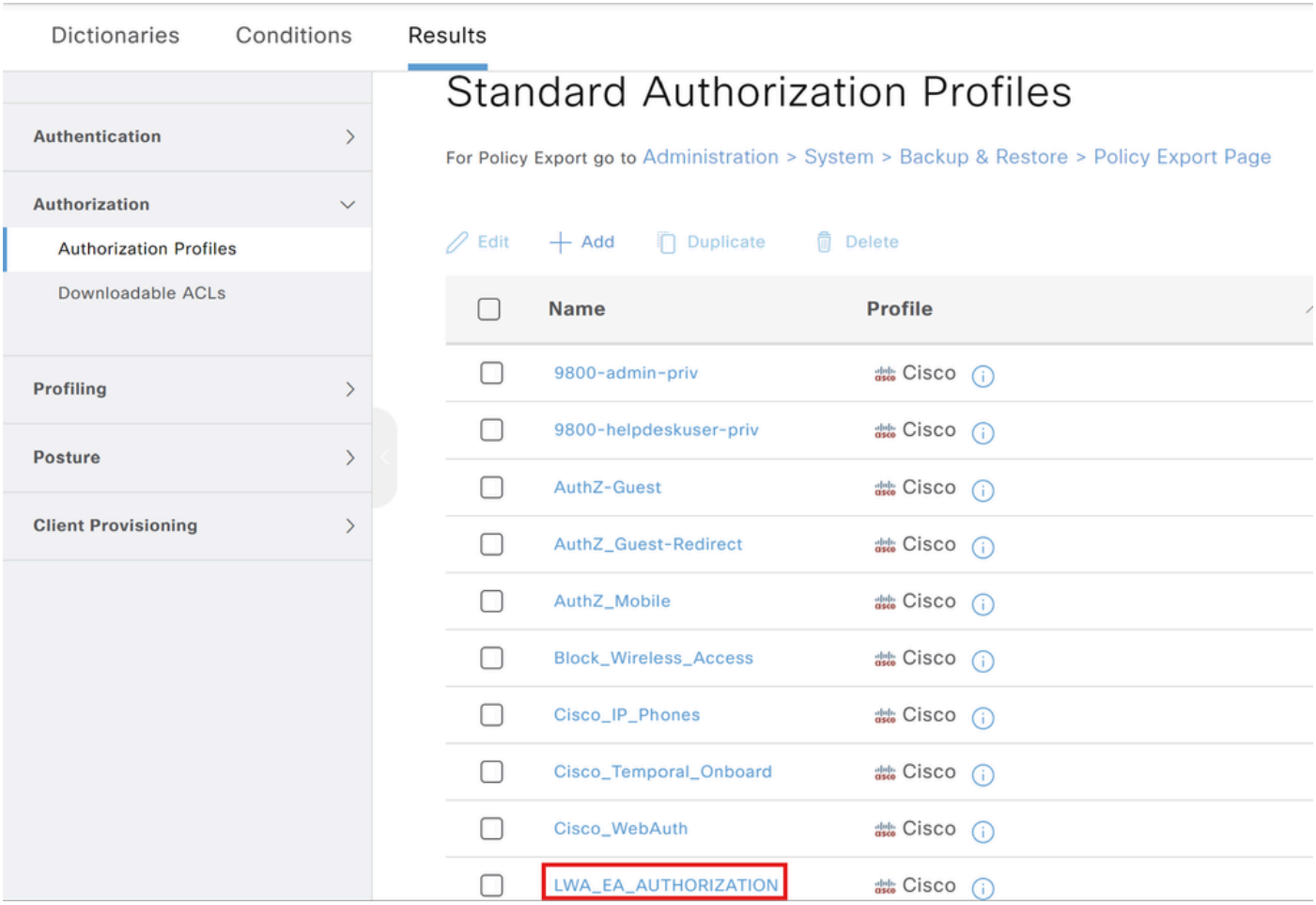
Adicionar perfil de autorização

Etapa 3. Crie o perfil de autorização LWA_EA_AUTHORIZATION. Os detalhes dos atributos devem ser do tipo de acesso=ACCESS_ACCEPT. Clique em Submit.



Criar perfil de autorização

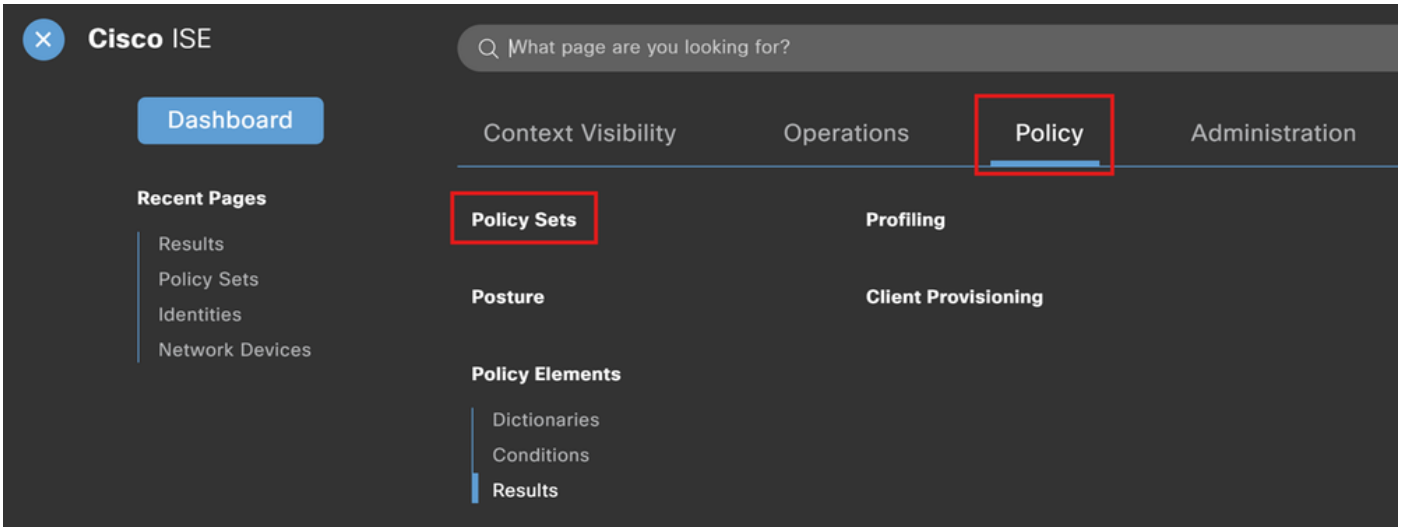
Etapa 4. Navegue até Policy > Policy Elements > Results > Authorization > Authorization Profiles, você pode ver os perfis de autorização.



Lista de perfis de autorização

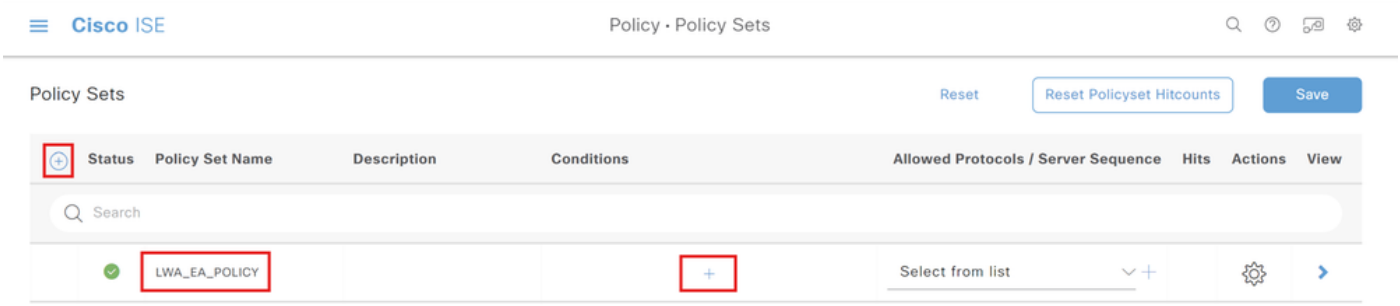
Configurar regra de autenticação

Etapa 1. Navegue até Política > Conjuntos de Políticas.



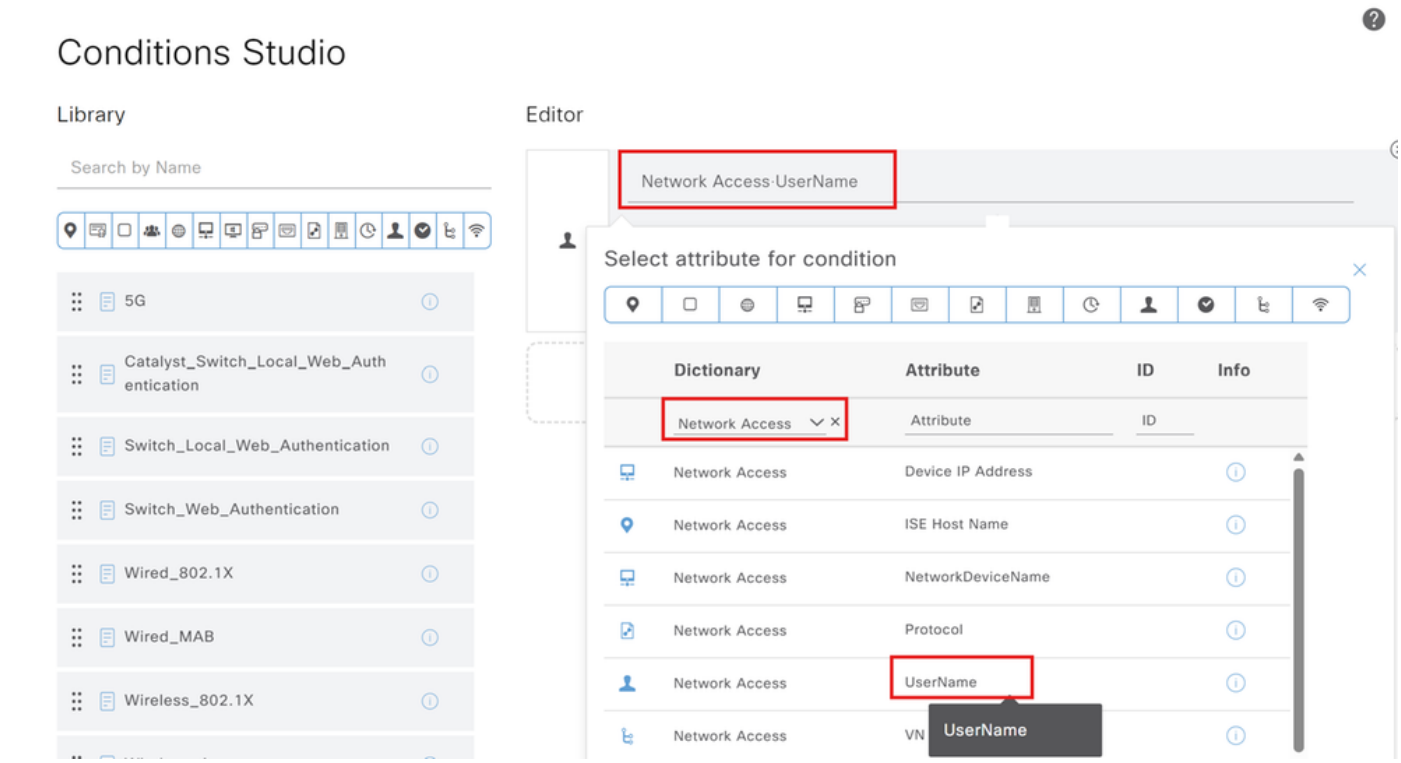
Política do ISE - Conjuntos de políticas

Etapa 2. Selecione o sinal +, digite o nome do conjunto de políticas LWA_EA_POLICY. Clique na coluna Condições.



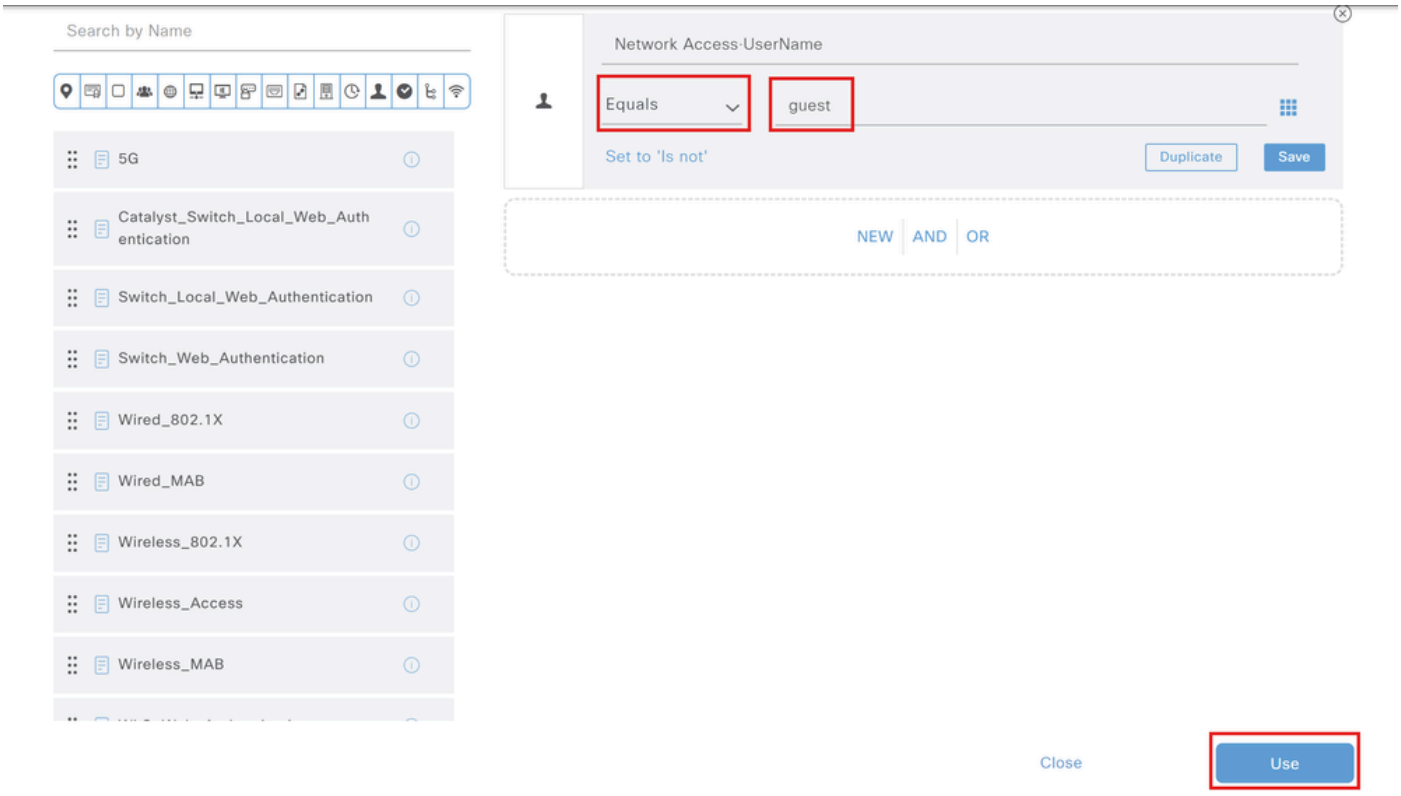
Configurar regra de autenticação

Etapa 3. No Dicionário, selecione Acesso à Rede. Em Atributo, selecione Nome de Usuário.



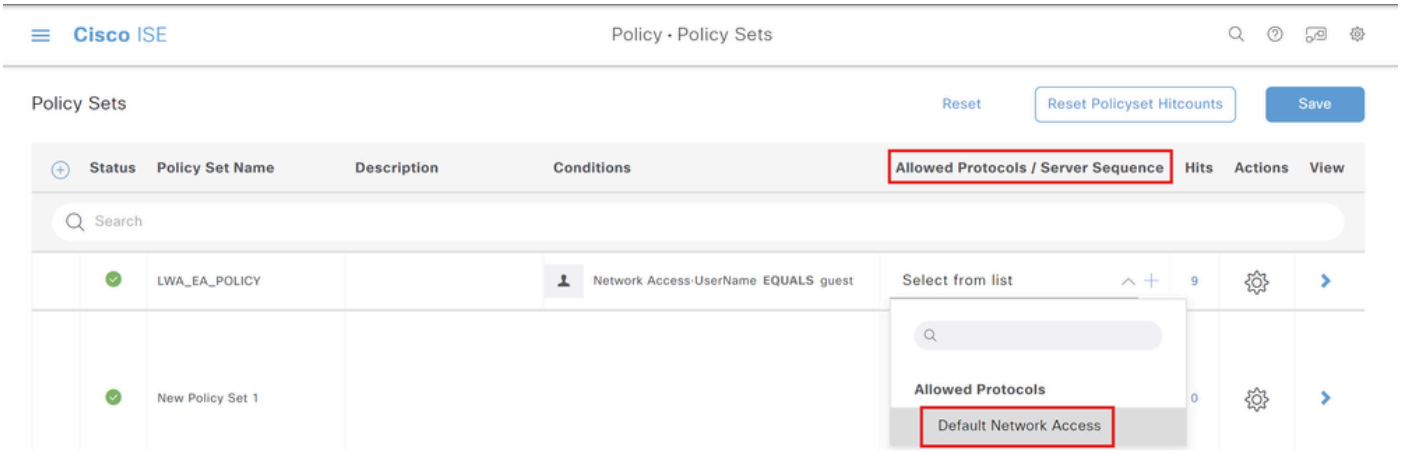
Acesso à rede de dicionários

Etapa 4. Defina Igual a e digite guest na caixa de texto (o nome de usuário definido em Administração > Gerenciamento de Identidades > Identidades > Usuários). Clique em Salvar para salvar as alterações.



Nome de usuário convidado

Etapa 5. Navegue até Política > Conjuntos de Políticas. No conjunto de políticas criado, na coluna Allowed Protocols/Server Sequence, selecione Default Network Access.



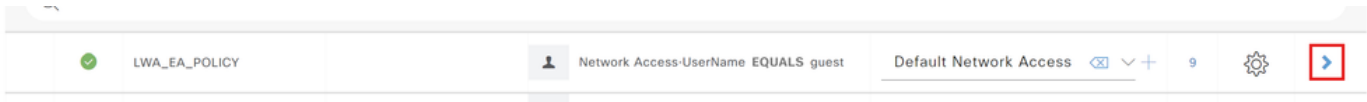
Conjuntos de políticas

Etapa 6. Clique em Save para salvar as alterações.

Configurar regras de autorização

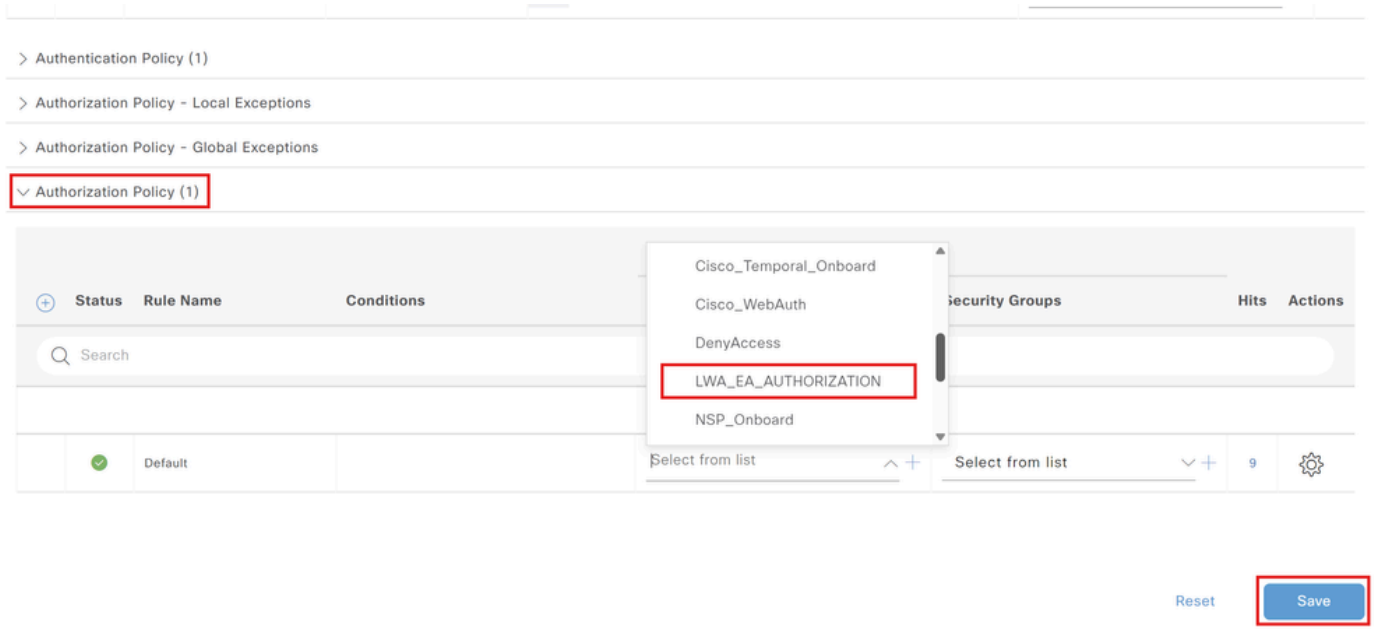
A regra de autorização é responsável por determinar qual resultado de permissões (qual perfil de autorização) é aplicado ao cliente.

Etapa 1. Navegue até Política > Conjuntos de Políticas. Clique no ícone de seta no conjunto de políticas criado.



Seta de Definição de Política

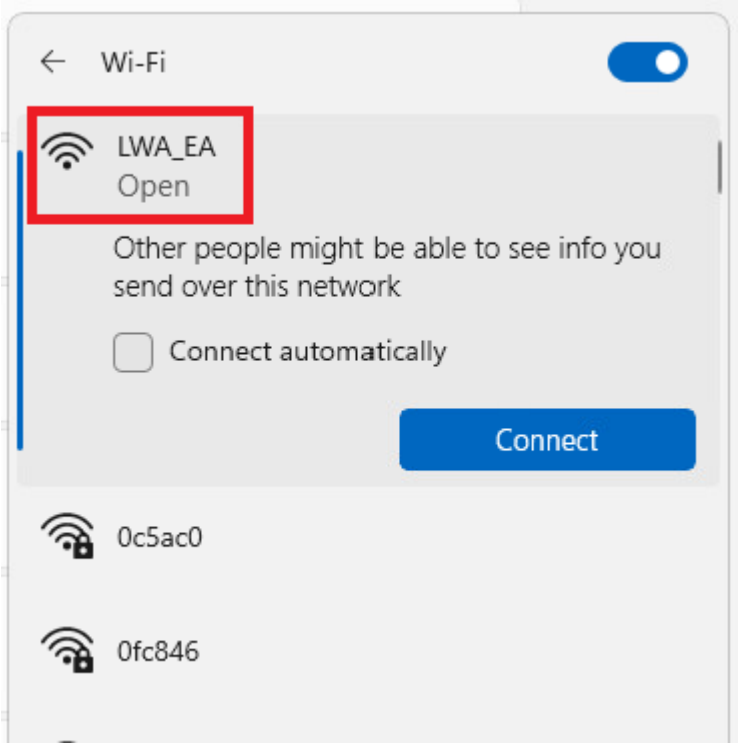
Etapa 2. Na mesma página Conjunto de políticas, expanda Política de autorização conforme mostrado na imagem. Na coluna Profiles, exclua DenyAccess e adicione LWA_EA_AUTHORIZATION. Clique em Save para salvar as alterações.



Política de Autorização

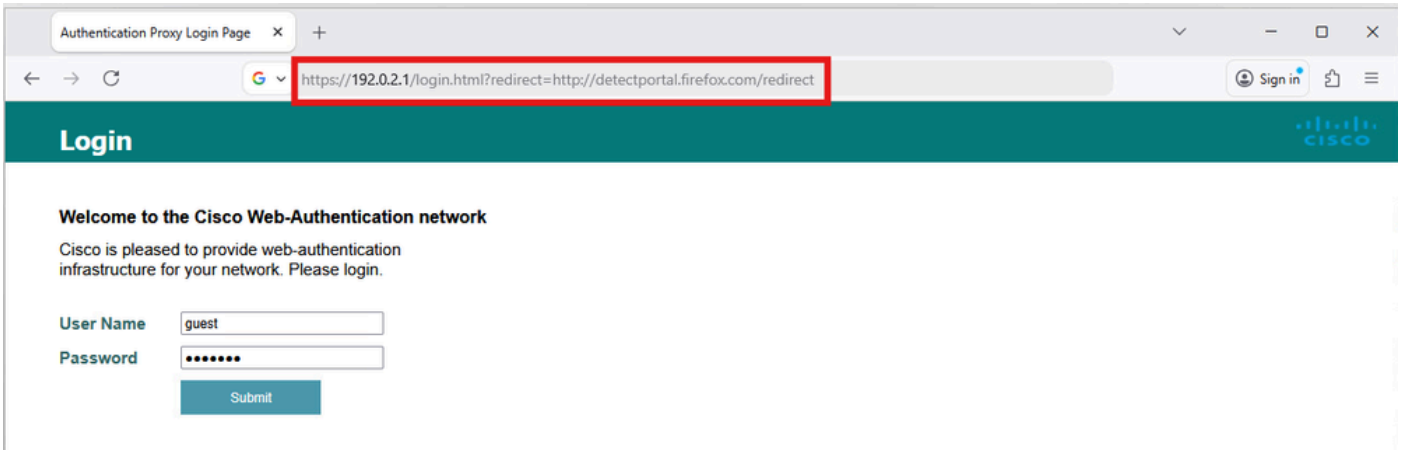
Conectar cliente convidado

Etapa 1. No computador ou telefone, navegue até as redes Wi-Fi, localize o SSID LWA_EA e selecione Connect.



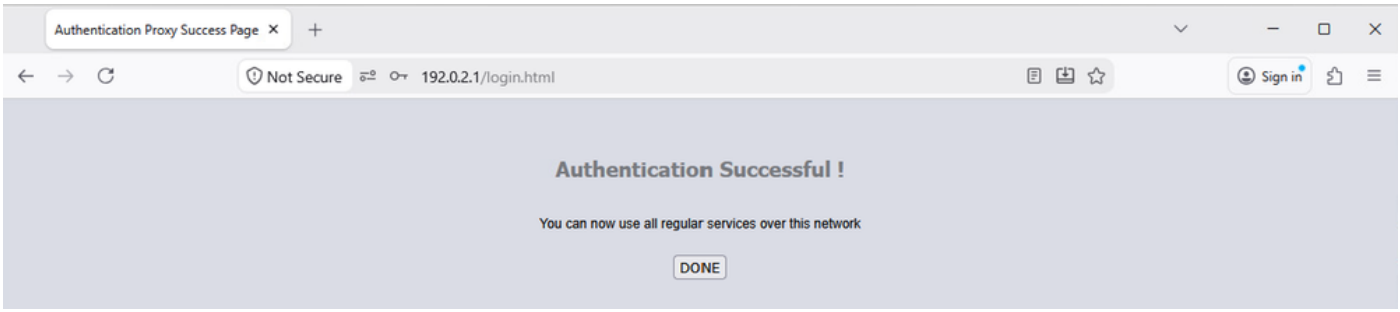
Conectar cliente convidado

Etapa 2. Uma janela do navegador é exibida, com a página de login. A URL de redirecionamento está na caixa de URL e você precisa digitar o Nome de usuário e a Senha para obter acesso à rede. Em seguida, selecione Enviar.



Página de login com URL de redirecionamento

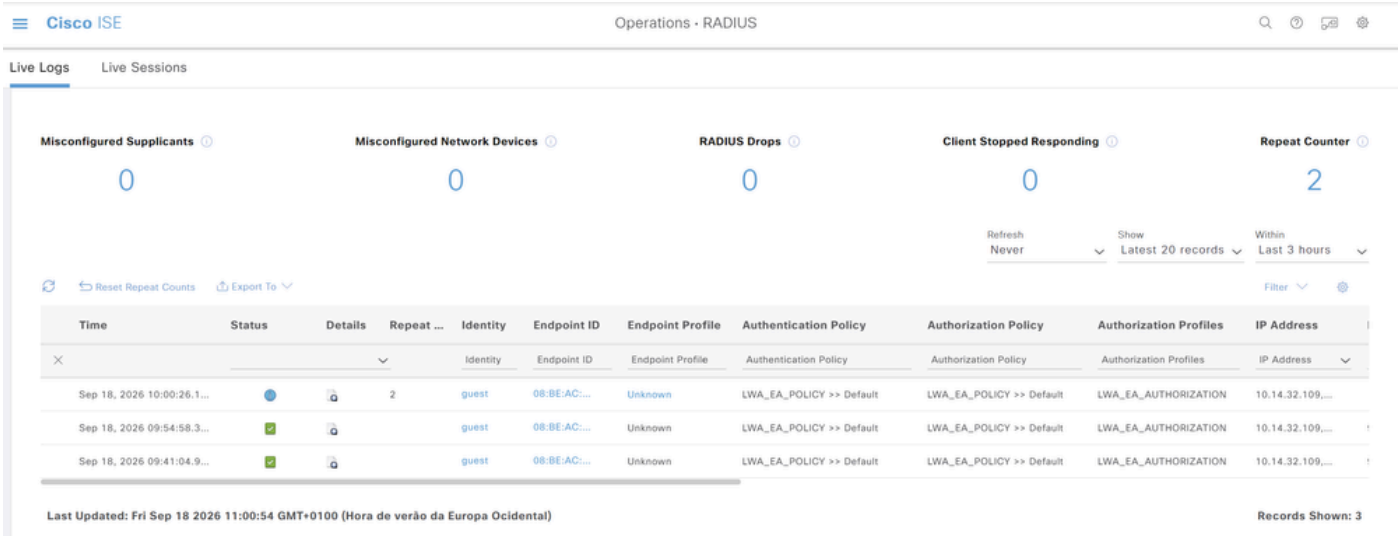
Se as credenciais estiverem corretas, uma página de autenticação bem-sucedida será exibida:



Página de login de autenticação bem-sucedida

Note: O URL apresentado foi fornecido pela WLC. Ele contém o IP virtual da WLC e o redirecionamento para o URL de teste de conexão do Windows.

Etapa 3. Navegue até Operations > RADIUS > Live Logs. Você pode ver o dispositivo cliente autenticado, juntamente com suas políticas de autenticação e autorização.



Logs ao vivo do Radius

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Show WLAN Summary

<#root>

9800WLC#show wlan summary

```
Number of WLANs: 1
```

```
ID Profile Name SSID Status 2.4GHz/5GHz Security
-----------------------------------------------
```

1 LWA_EA LWA_EA UP [open],[Web Auth]

```
9800WLC#
```

show wlan name LWA_EA

```
WLAN Profile Name : LWA_EA
==========================================
Identifier : 1
Description :
Network Name (SSID) : LWA_EA
Status : Enabled
Broadcast SSID : Enabled
Advertise-Apname : Disabled
Universal AP Admin : Disabled
(...)
Accounting list name :
802.1x authentication list name : Disabled
802.1x authorization list name : Disabled
Security
```

Web Based Authentication : Enabled

```
OWE Transition Mode : Disabled
Conditional Web Redirect : Disabled
Splash-Page Web Redirect : Disabled
Webauth On-mac-filter Failure : Disabled
```

Webauth Authentication List Name : LWA_AUTHENTICATION

Webauth Authorization List Name : Disabled

Webauth Parameter Map : global

```
(...)
Security-2.4GHz/5GHz
```

802.11 Authentication : Open System

```
Static WEP Keys : Disabled
```

Wi-Fi Protected Access (WPA/WPA2/WPA3) : Disabled

```
OSEN : Disabled
PMF Support : Disabled
(...)
Band Select : Disabled
Load Balancing : Disabled
(...)
```

Show Parameter Map Configuration

9800WLC#show running-config | section parameter-map type webauth global

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
trustpoint TP-self-signed-123456
```

Show AAA Information

<#root>

9800WLC#show aaa method-lists authentication

```
authen queue=AAA_ML_AUTHEN_LOGIN
```

name=LWA_AUTHENTICATION valid=TRUE id=BD000005 :state=ALIVE : SERVER_GROUP RADIUSGROUP

```
authen queue=AAA_ML_AUTHEN_ENABLE
authen queue=AAA_ML_AUTHEN_PPP
authen queue=AAA_ML_AUTHEN_SGBP
(...)
```

9800WLC#show aaa method-lists authorization

```
author queue=AAA_ML_AUTHOR_SHELL
author queue=AAA_ML_AUTHOR_NET
```

name=LWA_AUTHORIZATION valid=TRUE id=90000006 :state=ALIVE : SERVER_GROUP RADIUSGROUP

```
author queue=AAA_ML_AUTHOR_CONN
author queue=AAA_ML_AUTHOR_IPMOBILE
author queue=AAA_ML_AUTHOR_RM
(...)
```

9800WLC#show aaa servers

```
RADIUS: id 2, priority 1, host 192.0.2.30, auth-port 1812, acct-port 1813, hostname RADIUS


State: current UP, duration 8421s, previous duration 0s
Dead: total time 0s, count 0
Platform State from SMD: current UP, duration 8421s, previous duration 0s
SMD Platform Dead: total time 0s, count 0
Platform State from WNCD (0) : current UP
(...)
```

Troubleshooting

Problemas comuns

Estes são vários guias sobre como solucionar problemas de autenticação da Web, como:

- Os usuários não podem se autenticar.
- Problemas de certificado.
- A URL de redirecionamento não funciona.
- Os usuários convidados não podem se conectar à WLAN de convidados.
- Os usuários não obtêm um endereço IP.
- O redirecionamento para a Página de Login da Autenticação da Web falhou.
- Após a autenticação bem-sucedida, os usuários convidados não conseguem acessar a Internet.

Estes guias descrevem as etapas da solução de problemas em detalhes:

- Solucionar problemas comuns de autenticação da Web
- Outras situações para solucionar problemas

Depuração condicional e rastreamento ativo de rádio e captura de pacotes incorporada

Você pode 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). Para habilitar a depuração condicional, use as etapas no guia, Depuração condicional e rastreamento RadioActive.

Você também pode coletar EPC (Embedded Packet capture, captura de pacote incorporado). O EPC é um recurso de captura de pacotes que permite a visualização de pacotes destinados,

originados e transmitidos pelas WLCs do Catalyst 9800, ou seja, pacotes DHCP, DNS, HTTP GET no LWA. Essas capturas podem ser exportadas para análise offline com o Wireshark. Para obter etapas detalhadas sobre como fazer isso, consulte Captura de pacotes incorporada.

Exemplo de uma tentativa bem-sucedida

Esta é a saída de RA_traces de uma tentativa bem-sucedida de identificar cada uma das fases no processo de associação/autenticação, enquanto está em conexão com um SSID convidado com o servidor RADIUS.

Associação/autenticação 802.11:

[client-orch-sm] [17062]: (nota): MAC: Associação 08be.ac3f recebida. BSSID cc70.edcf.552f, WLAN LWA_EA, Slot 1 AP 2ce3.8eb4, CW9172I-LAB
[client-orch-sm] [17062]: (depurar): MAC: 08be.ac3f Solicitação de associação Dot11 recebida. Processamento iniciado,SSID: LWA_EA, Perfil de diretiva: POLICY_PROFILE, Nome do AP: CW9172I-LAB, Endereço Mac Do Ap: 2ce3.8eb4BSSID MAC0000.0000.0000wlan ID: 1RSSI: -49, SNR: 46
[client-orch-state] [17062]: (nota): MAC: 08be.ac3f Transição de estado do cliente: S_CO_INIT -> S_CO_ASSOCIATING
[dot11-validate] [17062]: (informações): MAC: 08be.ac3f Dot11 ie validar taxas de ext/supp. Validação Aprovada para taxas com suporte radio_type 2
[dot11-validate] [17062]: (informações): MAC: 08be.ac3f WiFi direto: Dot11 valida IE P2P. IE P2P ausente.
[ponto11] [17062]: (depurar): MAC: 08be.ac3f dot11 envia resposta de associação. Resposta de associação de enquadramento com resp_status_code: 0
[ponto11] [17062]: (depurar): MAC: 08be.ac3f Dot11 Informações de capacidade byte1 1, byte2: 11
[quadro dot11] [17062]: (informações): MAC: 08be.ac3f WiFi direto: ignorar compilação de Assoc Resp com IE P2P: Política de WiFi Direct desabilitada
[ponto11] [17062]: (informações): MAC: 08be.ac3f dot11 envia resposta de associação. Enviando resposta assoc de comprimento: 130 com resp_status_code: 0, STATUS_DOT11: DOT11_STATUS_SUCCESS
[ponto11] [17062]: (nota): MAC: Sucesso da associação 08be.ac3f. AID 1, Roaming = Falso, WGB = Falso, 11r = Falso, 11w = Falso Roam rápido = Falso
[ponto11] [17062]: (informações): MAC: 08be.ac3f transição de estado DOT11: S_DOT11_INIT -> S_DOT11_ASSOCIATED
[client-orch-sm] [17062]: (depurar): MAC: Associação 08be.ac3f Station Dot11 bem-sucedida.

Processo de aprendizado de IP:

[client-orch-state] [17062]: (nota): MAC: 08be.ac3f Transição de estado do cliente: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS
[cliente-aluno] [17062]: (informações): MAC: 08be.ac3f Transição de estado de aprendizagem IP: S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS
[client-auth] [17062]: (informações): MAC: 08be.ac3f Transição de estado de interface de autenticação de cliente: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_L2_WEBAUTH_DONE
[cliente-aluno] [17062]: (nota): MAC: 08be.ac3f Aprendizado do IP do cliente bem-sucedido. Método: IP DHCP: 10.14.32.109
[cliente-aluno] [17062]: (informações): MAC: 08be.ac3f Transição de estado de aprendizagem IP: S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE
[client-orch-sm] [17062]: (depurar): MAC: 08be.ac3f Resposta de aprendizagem de ip recebida. método: IPLEARN_METHOD_DHCP

Autenticação da camada 3:

[client-orch-sm] [17062]: (depurar): MAC: 08be.ac3f Autenticação L3 disparada. status = 0x0, Êxito
[client-orch-state] [17062]: (nota): MAC: 08be.ac3f Transição de estado do cliente:

S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS
[client-auth] [17062]: (nota): MAC: 08be.ac3f Autenticação L3 iniciada. LWA
[client-auth] [17062]: (informações): MAC: 08be.ac3f Transição de estado de interface de autenticação de cliente: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING

[webauth-httpd] [17062] (informações): capwap_90000004[08be.ac3f][10.14.32.109]GET rcvd quando no estado LOGIN
[webauth-httpd] [17062] (informações): capwap_90000004[08be.ac3f][10.14.32.109]HTTP GET request
[webauth-httpd] [17062] (informações): capwap_90000004[08be.ac3f][10.14.32.109]Analisar GET, src [10.14.32.109] dst [10.107.221.82] url [http://firefox detect portal/]
[webauth-httpd] [17062] (informações): capwap_90000004[08be.ac3f][10.14.32.109]Leitura completa: parse_request return 8
[webauth-io] [17062]: (informações): capwap_90000004[08be.ac3f][10.14.32.109]56538/219 LEITURA de estado de E/S -> GRAVAÇÃO
[webauth-io] [17062]: (informações): capwap_90000004[08be.ac3f][10.14.32.109]56538/219 GRAVAÇÃO de estado de E/S -> LEITURA
[webauth-io] [17062]: (informações): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 Estado de E/S NOVO -> LEITURA
[webauth-io] [17062]: (informações): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 Evento de leitura, Pronto para mensagem
[webauth-httpd] [17062] (informações): capwap_90000004[08be.ac3f][10.14.32.109]POST rcvd quando em estado LOGIN

Autenticação da camada 3 bem-sucedida, mova o cliente para o estado RUN:

[auth-mgr] [17062]: (informações): [08be.ac3f:capwap_90000004] Nome de usuário convidado recebido para o cliente 08be.ac3f
[auth-mgr] [17062]: (informações): [08be.ac3f:capwap_90000004] notificação de adição/alteração de attr de auth mgr recebida para attr auth-domain(954)
[auth-mgr] [17062]: (informações): [08be.ac3f:capwap_90000004] Método webauth alterando estado de 'Em Execução' para 'Êxito da Autenticação'
[auth-mgr] [17062]: (informações): [08be.ac3f:capwap_90000004] Estado de alteração de contexto de 'Em Execução' para 'Êxito na Autenticação'
[auth-mgr] [17062]: (informações): [08be.ac3f:capwap_90000004] a notificação de adição/alteração de attr do auth mgr foi recebida para o método attr(757)
[auth-mgr] [17062]: (informações): [08be.ac3f:capwap_90000004] Evento gerado AUTHZ_SUCCESS (11)
[auth-mgr] [17062]: (informações): [08be.ac3f:capwap_90000004] Contexto alterando estado de 'Êxito da Autenticação' para 'Êxito da Autenticação'
[webauth-acl] [17062]: (informações): capwap_90000004[08be.ac3f][10.14.32.109]Aplicando ACL de logout IPv4 via SVM, nome: IP-Adm-V4-LOGOUT-ACL, prioridade: 51, IIF-ID: 0
[webauth-sess] [17062]: (informações): capwap_90000004[08be.ac3f][10.14.32.109]Mapa de parâmetros usado: global
[webauth-state] [17062]: (informações): capwap_90000004[08be.ac3f][10.14.32.109]Mapa de parâmetros usado: global
[webauth-state] [17062]: (informações): capwap_90000004[08be.ac3f][10.14.32.109]State AUTHC_SUCCESS -> AUTHZ
[webauth-page] [17062]: (informações): capwap_90000004[08be.ac3f][10.14.32.109]Enviando página de sucesso de Webauth
[webauth-io] [17062]: (informações): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 IO state AUTHENTICATING -> WRITING
[webauth-io] [17062]: (informações): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 GRAVAÇÃO de estado de E/S -> END
[webauth-httpd] [17062] (informações): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 Remova o ctx de E/S e feche o soquete, id [99000029]
[client-auth] [17062]: (nota): MAC: 08be.ac3f Autenticação L3 Bem-sucedida. ACL:[]

[client-auth] [17062]: (informações): MAC: 08be.ac3f Transição de estado de interface de autenticação de cliente: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH_DONE
[webauth-httpd] [17062] (informações): capwap_90000004[08be.ac3f][10.48.39.243]56538/219 Remova o ctx de E/S e feche o soquete, id [D7000028]
[errmsg] [17062]: (informações): %CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: R0/0: wcd: Entrada de nome de usuário (convidado) unida com ssid (LWA_EA) para dispositivo com MAC: 08be.ac3f
[aaa-attr-inf] [17062]: (informações): [Atributo aplicado :bsn-vlan-interface-name 0 "VLAN0039"]
[aaa-attr-inf] [17062]: (informações): [Atributo aplicado: timeout 0 1800 (0x708)]
[aaa-attr-inf] [17062]: (informações): [Atributo aplicado: url-redirect-acl 0 "IP-Adm-V4-LOGOUT-ACL"]
[ewlc-qos-client] [17062]: (informações): MAC: 08be.ac3f Manipulador de estado de execução de QoS de Cliente
[rog-proxy-capwap] [17062]: (depurar): Notificação de estado de execução de cliente gerenciado: 08be.ac3f
[client-orch-state] [17062]: (nota): MAC: 08be.ac3f Transição de estado do cliente: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RUN

Informações Relacionadas

- Suporte técnico e downloads da Cisco

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.