

Configurar a autenticação da Web central (CWA) no Catalyst 9800 WLC e ISE

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração de AAA no 9800 WLC](#)

[Configuração de WLAN](#)

[Configuração de perfil de política](#)

[Configuração de marca de política](#)

[Atribuição de marca de política](#)

[Configuração de ACL de redirecionamento](#)

[Habilitar redirecionamento para HTTP ou HTTPS](#)

[Configuração do ISE](#)

[Adicionar o 9800 WLC ao ISE](#)

[Criar novo usuário no ISE](#)

[Criar perfil de autorização](#)

[Configurar regra de autenticação](#)

[Configurar regras de autorização](#)

[SOMENTE access points de switching local do FlexConnect](#)

[Certificados](#)

[Verificar](#)

[Troubleshooting](#)

[Lista de verificação](#)

[Suporte de porta de serviço para RADIUS](#)

[Coletar depurações](#)

[Examples](#)

Introdução

Este documento descreve como configurar uma LAN sem fio CWA em uma WLC Catalyst 9800 e ISE.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento da configuração de 9800 Wireless LAN Controllers (WLC).

Componentes Utilizados

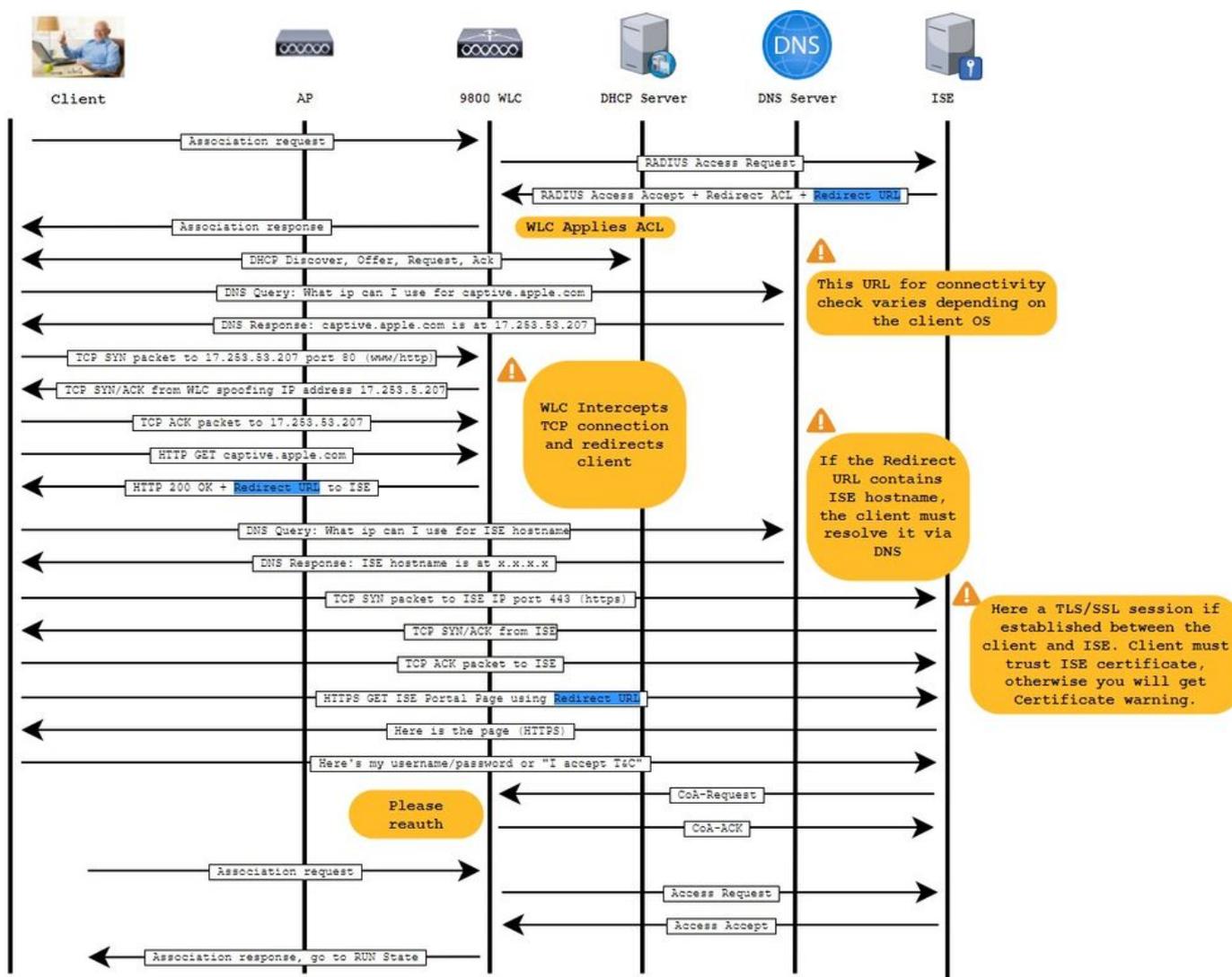
As informações neste documento são baseadas nestas versões de software e hardware:

- 9800 WLC Cisco IOS® XE Gibraltar v17.6.x
- Identity Service Engine (ISE) v3.0

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

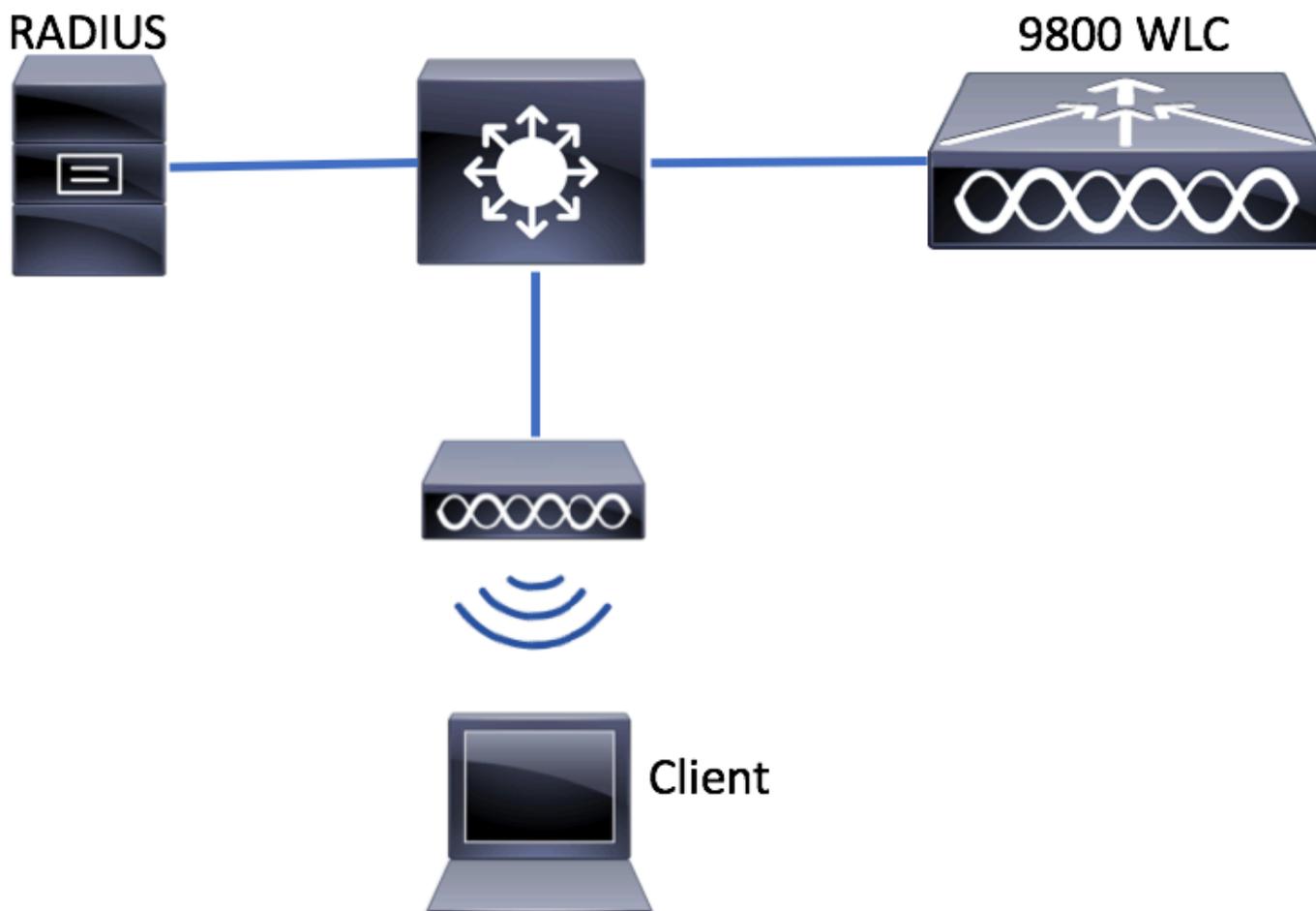
Informações de Apoio

O processo do CWA é mostrado aqui, onde você pode ver o processo do CWA de um dispositivo Apple como exemplo:



Configurar

Diagrama de Rede



Configuração de AAA no 9800 WLC

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

Navegue até `Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add` e insira as informações do servidor RADIUS conforme mostrado nas imagens.

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add × Delete

RADIUS

TACACS+

LDAP

Servers Server Groups

Name	Address
0	

10 items per page

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.

Create AAA Radius Server

Name*	ISE-server	Support for CoA	ENABLED
Server Address*	CoA Server Key Type	Clear Text
PAC Key	<input type="checkbox"/>	CoA Server Key
Key Type	Clear Text	Confirm CoA Server Key
Key* ⓘ	Automate Tester	<input type="checkbox"/>
Confirm Key*		
Auth Port	1812		
Acct Port	1813		
Server Timeout (seconds)	1-1000		
Retry Count	0-100		

Cancel Apply to Device



Observação: na versão 17.4.X e posterior, certifique-se de configurar também a chave do servidor CoA ao configurar o servidor RADIUS. Use a mesma chave que o segredo compartilhado (eles são os mesmos por padrão no ISE). A finalidade é, opcionalmente, configurar uma chave para CoA diferente do segredo compartilhado, se for isso que o servidor RADIUS configurou. No Cisco IOS XE 17.3, a interface do usuário da Web simplesmente usava o mesmo segredo compartilhado que a chave de CoA.

Etapa 2. Crie uma lista de métodos de autorização.

Navegue até Configuration > Security > AAA > AAA Method List > Authorization > + Add conforme mostrado na imagem.

Search Menu Items

- Dashboard
- Monitoring
- Configuration**
- Administration
- Troubleshooting

Authentication Authorization and Accounting

+ AAA Wizard

AAA Method List Servers / Groups AAA Advanced

General

Authentication

Authorization

Accounting

+ Add **x Delete**

Name	Type	Group Type	Group
<input type="checkbox"/> default	network	local	N/A

10 items per page

Quick Setup: AAA Authorization

Method List Name*

Type*

Group Type

Fallback to local

Authenticated

Available Server Groups **Assigned Server Groups**

ldap
tacacs+

radius

Etapa 3. (Opcional) Crie uma lista de métodos contábeis, conforme mostrado na imagem.

Dashboard
Monitoring
Configuration
Administration
Troubleshooting

+ AAA Wizard

AAA Method List

Servers / Groups

General
Authentication
Authorization
Accounting

+ Add

Name

0

Quick Setup: AAA Accounting

Method List Name*

Type*

Available Server Groups

- ldap
- tacacs+

Assigned Server Groups

- radius

Cancel Apply to Device

Observação: o CWA não funcionará se você decidir fazer o balanceamento de carga (a partir da configuração CLI do Cisco IOS XE) de seus servidores radius devido à ID de bug da Cisco [CSCvh03827](https://cisco.com/cisco/webbugtool/bugdetails?bug=CSCvh03827). O uso de balanceadores de carga externos é adequado. No entanto, certifique-se de que o balanceador de carga funcione por cliente usando o atributo RADIUS calling-station-id. Dependendo da porta de origem UDP não é um mecanismo suportado para equilibrar solicitações RADIUS do 9800.

Etapa 4. (Opcional) Você pode definir a política AAA para enviar o nome SSID como um atributo Called-station-id, que pode ser útil se você quiser aproveitar essa condição no ISE posteriormente no processo.

Navegue até Configuration > Security > Wireless AAA Policy e edite a política AAA padrão ou crie uma nova.

- Dashboard
- Monitoring >
- Configuration** >
- Administration >
- Troubleshooting

[Configuration](#) > [Security](#) > **Wireless AAA Policy**

+ Add
× Delete

Policy Name
<input type="checkbox"/> default-aaa-policy

⏪
⏩
1
⏪
⏩

10

items per page

Você pode escolher SSID como Opção 1. Lembre-se de que, mesmo quando você escolhe apenas o SSID, o ID da estação chamada ainda anexa o endereço MAC do AP ao nome do SSID.

Edit Wireless AAA Policy

Policy Name*

default-aaa-policy

Option 1

SSID ▼

Option 2

Not Configured ▼

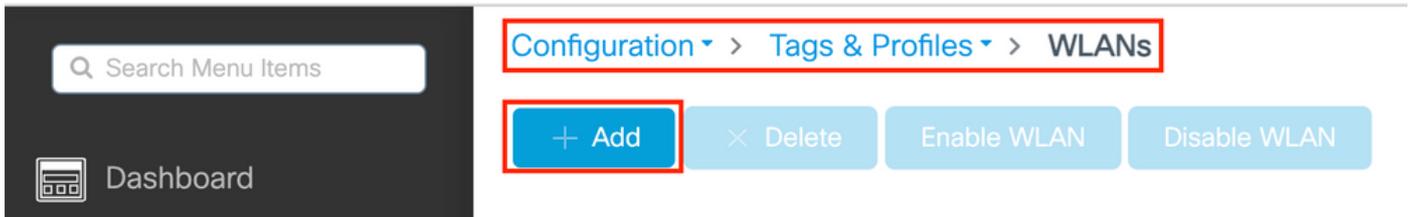
Option 3

Not Configured ▼

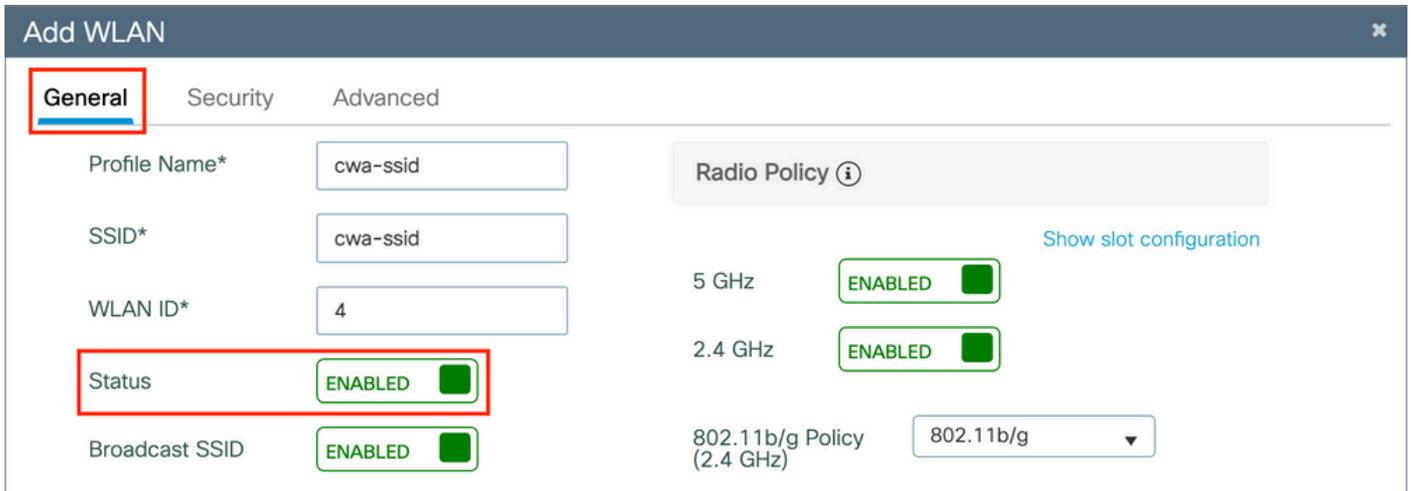
Configuração de WLAN

Etapa 1. Criar a WLAN.

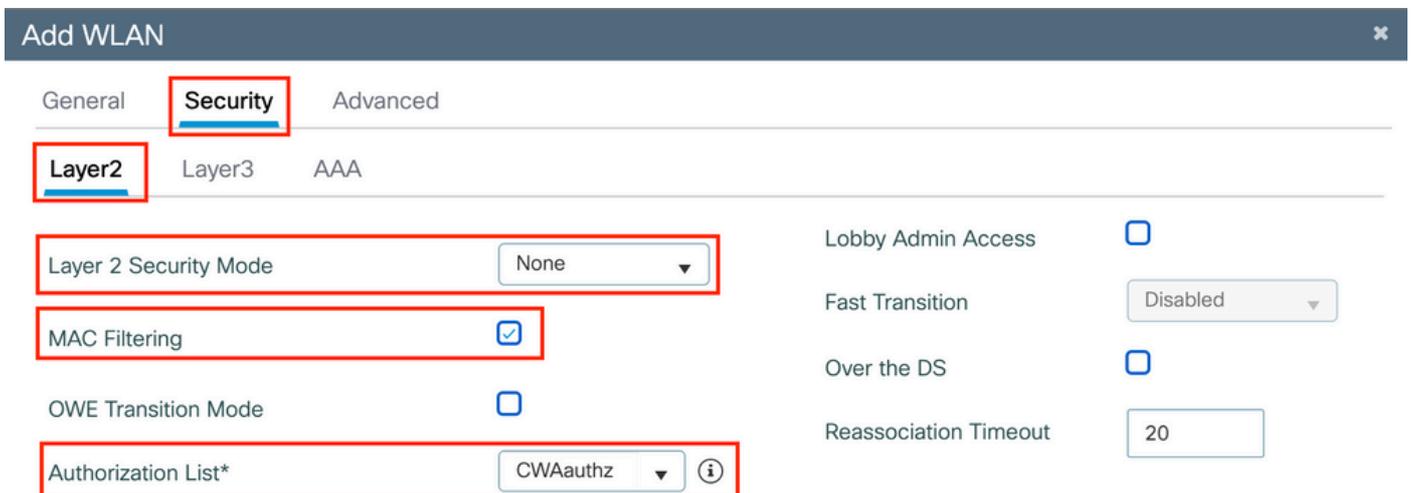
Navegue até a rede [Configuration](#) > [Tags & Profiles](#) > [WLANs](#) > [+ Add](#) e configure-a conforme necessário.



Etapa 2. Insira as informações gerais da WLAN.



Etapa 3. Navegue até a Security guia e escolha o método de segurança necessário. Nesse caso, somente 'MAC Filtering' e a lista de autorização AAA (que você criou na Etapa 2. na AAA Configuration seção) são necessários.



CLI:

```
#config t
(config)#wlan cwa-ssid 4 cwa-ssid
(config-wlan)#mac-filtering CWAauthz
(config-wlan)#no security ft adaptive
(config-wlan)#no security wpa
(config-wlan)#no security wpa wpa2
```

```
(config-wlan)#no security wpa wpa2 ciphers aes
(config-wlan)#no security wpa akm dot1x
(config-wlan)#no shutdown
```

Configuração de perfil de política

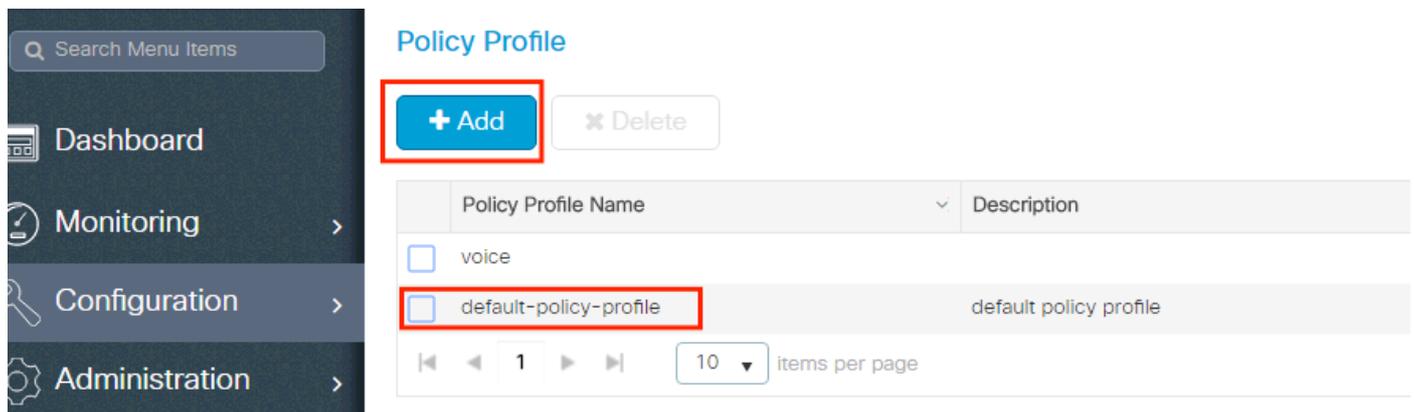
Dentro de um Perfil de política, você pode decidir atribuir os clientes a qual VLAN, entre outras configurações (como Lista de controles de acesso (ACLs), Qualidade de serviço (QoS), Âncora de mobilidade, Temporizadores, etc.).

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

GUI:

Etapa 1. Crie um novo Policy Profile.

Navegue até Configuration > Tags & Profiles > Policy e configure o default-policy-profile ou crie um novo.



The screenshot shows the 'Policy Profile' configuration page. On the left is a dark sidebar with a search bar and menu items: Dashboard, Monitoring, Configuration (selected), and Administration. The main content area has a title 'Policy Profile' and two buttons: '+ Add' (highlighted with a red box) and 'x Delete'. Below is a table with two columns: 'Policy Profile Name' and 'Description'. The table contains two rows: one for 'voice' and one for 'default-policy-profile' (highlighted with a red box). At the bottom of the table, there are navigation arrows, the number '1', and a dropdown menu set to '10 items per page'.

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

Verifique se o perfil está ativado.

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

Description

Status ENABLED

Passive Client DISABLED

Encrypted Traffic Analytics DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

WLAN Switching Policy

Central Switching ENABLED

Central Authentication ENABLED

Central DHCP ENABLED

Flex NAT/PAT DISABLED

Etapa 2. Escolha a VLAN.

Navegue até a Access Policies guia e escolha o nome da VLAN na lista suspensa ou digite manualmente a VLAN-ID. Não configure uma ACL no perfil de política.

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select ▼

VLAN

VLAN/VLAN Group

VLAN1416 ▼

Multicast VLAN

Enter Multicast VLAN

WLAN ACL

IPv4 ACL

Search or Select ▼

IPv6 ACL

Search or Select ▼

URL Filters

Pre Auth

Search or Select ▼

Post Auth

Search or Select ▼

Etapa 3. Configure o perfil de política para aceitar as substituições do ISE (Permitir substituição de AAA) e a alteração de autorização (CoA) (estado NAC). Como opção, você também pode especificar um método de auditoria.

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

DHCP

IPv4 DHCP Required

DHCP Server IP Address

[Show more >>>](#)

AAA Policy

Allow AAA Override

NAC State

NAC Type

Policy Name

Accounting List ⓘ ✕

WGB Parameters

Broadcast Tagging

WGB VLAN

Policy Proxy Settings

ARP Proxy DISABLED

IPv6 Proxy

Fabric Profile

Link-Local Bridging

mDNS Service Policy [Clear](#)

Hotspot Server

User Defined (Private) Network

Status

Drop Unicast

DNS Layer Security

DNS Layer Security Parameter Map [Clear](#)

Flex DHCP Option for DNS ENABLED

Flex DNS Traffic Redirect IGNORE

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Air Time Fairness Policies

2.4 GHz Policy

5 GHz Policy

EoGRE Tunnel Profiles

Tunnel Profile

CLI:

```
# config # wireless profile policy <policy-profile-name> # aaa-override
# nac
# vlan <vlan-id_or_vlan-name>
# accounting-list <acct-list>
# no shutdown
```

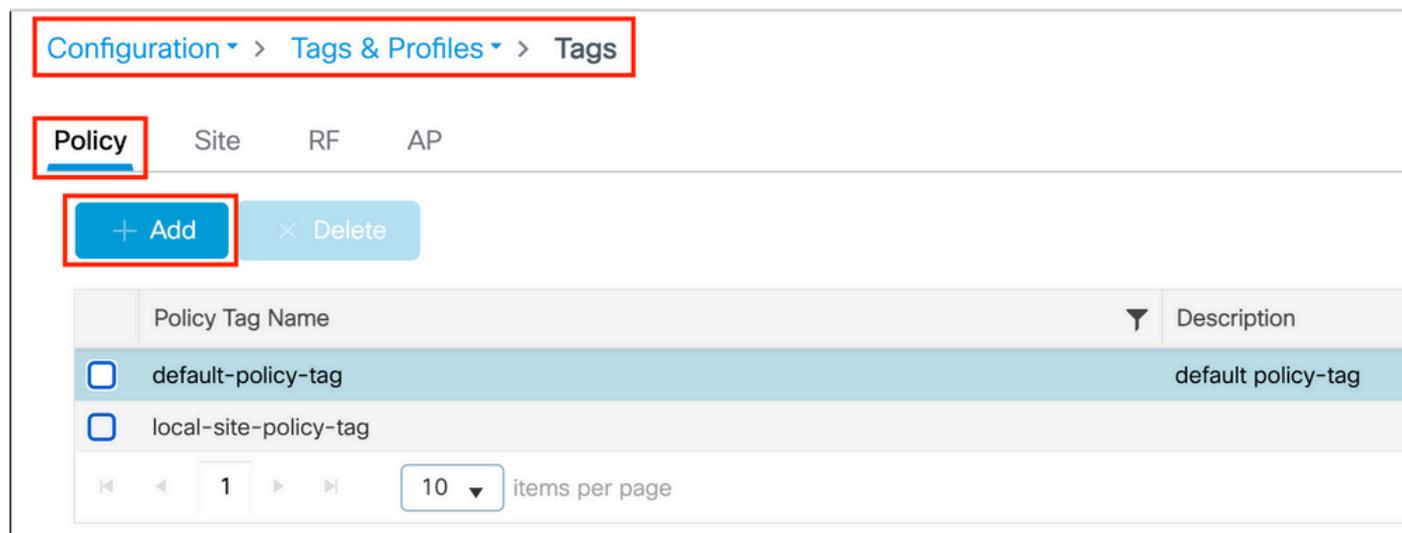
Configuração de marca de política

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.

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

GUI:

Navegue até Configuration > Tags & Profiles > Tags > Policy e adicione um novo, se necessário, como mostrado na imagem.



Configuration > Tags & Profiles > Tags

Policy Site RF AP

+ Add × Delete

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

1 10 items per page

Vincule o perfil de WLAN ao perfil de política desejado.

✕
Add Policy Tag

Name*

Description

▼ WLAN-POLICY Maps: 1

+ Add
✕ Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> cwa-ssid	default-policy-profile

◀ 1 ▶
10 items per page
1 - 1 of 1 items

➤ RLAN-POLICY Maps: 0

↶ Cancel

📄 Apply to Device

CLI:

```
# config t # wireless tag policy <policy-tag-name> # wlan <profile-name> policy <policy-profile-name>
```

Atribuição de marca de política

Atribua a marca de política aos APs necessários.

GUI:

Para atribuir a marca a um AP, navegue até Configuration > Wireless > Access Points > AP Name > General Tags, faça a atribuição necessária e clique em Update & Apply to Device.

Edit AP

- General**
- Interfaces
- High Availability
- Inventory
- ICap
- Advanced
- Support Bundle

General	Tags
AP Name*	<p>⚠ Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.</p>
Location*	
Base Radio MAC	Policy
Ethernet MAC	Site
Admin Status	RF
AP Mode	Write Tag Config to AP
Operation Status	

 **Observação:** lembre-se de que depois que você altera a tag de política em um AP, ele perde sua associação com a WLC 9800 e se junta novamente em cerca de 1 minuto.

Para atribuir a mesma etiqueta de política a vários APs, navegue até Configuration > Wireless > Wireless Setup > Advanced > Start Now.

Start

Tags & Profiles



WLAN Profile



Policy Profile



Policy Tag



AP Join Profile



Flex Profile



Site Tag



RF Profile



RF Tag



Apply

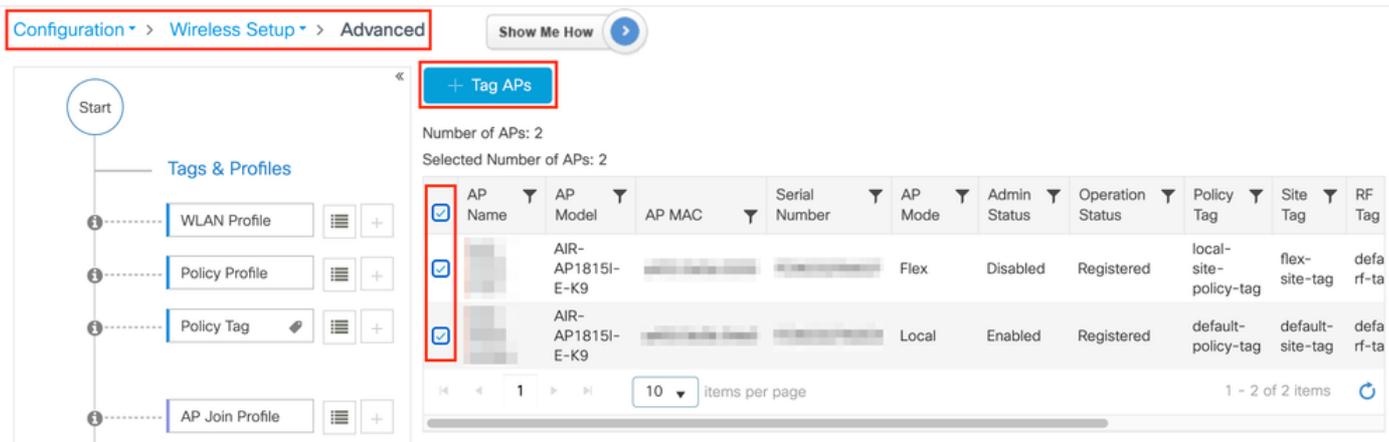


Tag APs

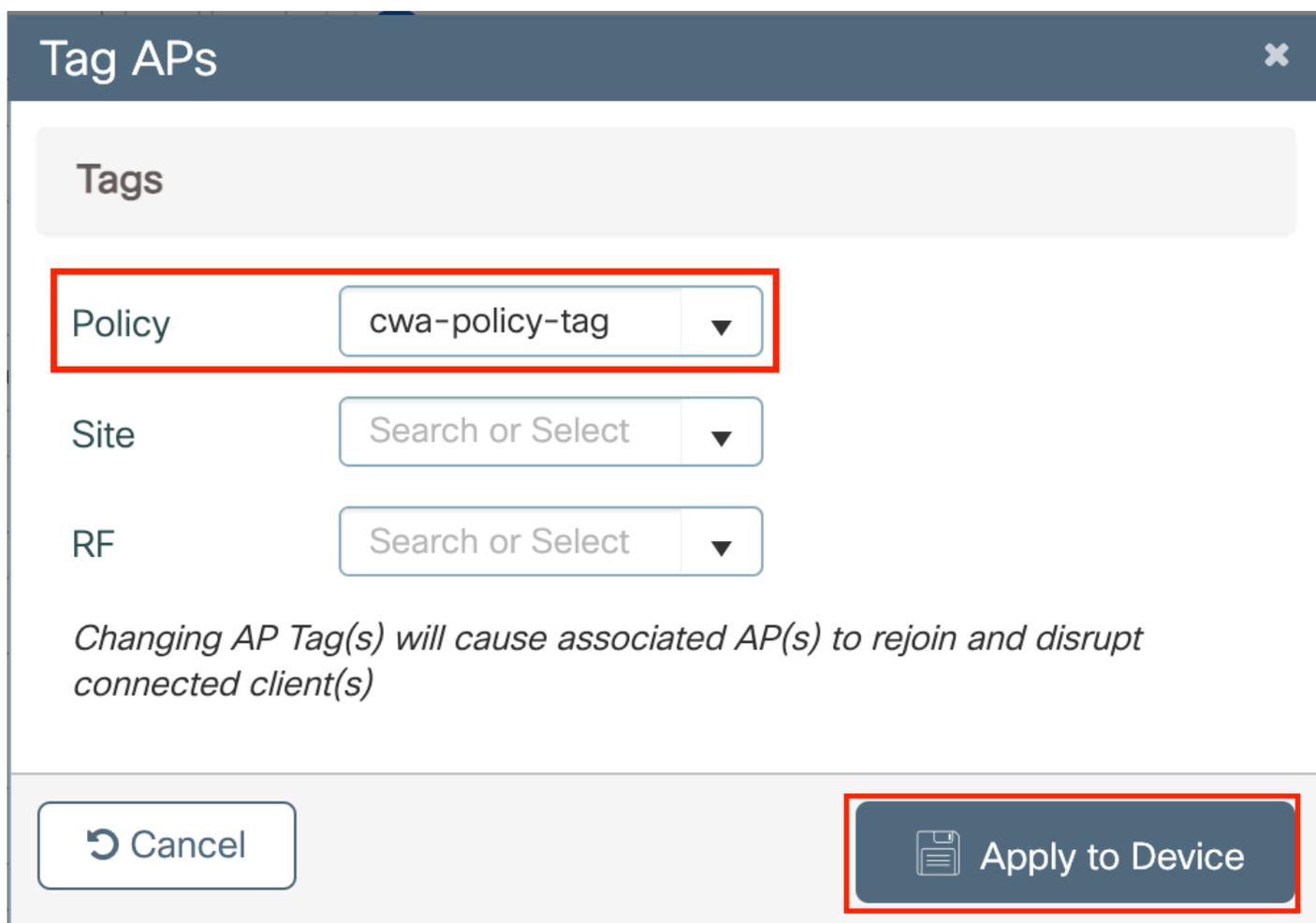


Start Now →

Done



Escolha a Tag desejada e clique Save & Apply to Device como mostrado na imagem.



CLI:

```
# config t # ap <ethernet-mac-addr> # policy-tag <policy-tag-name> # end
```

Configuração de ACL de redirecionamento

Etapa 1. Navegue até Configuration > Security > ACL > + Add a para criar uma nova ACL.

Escolha um nome para a ACL, faça-a IPv4 Extended digitar e adicione cada regra como uma sequência, como mostrado na imagem.

Add ACL Setup

ACL Name* ACL Type

Rules

Sequence* Action

Source Type

Destination Type Host Name* ! This field is mandatory

Protocol

Log DSCP

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
0										

10 items per page No items to display

Você precisa negar o tráfego para os nós de ISE PSNs, bem como negar o DNS e permitir todo o restante. Essa ACL de redirecionamento não é uma ACL de segurança, mas uma ACL de punt que define qual tráfego vai para a CPU (em permissões) para tratamento posterior (como redirecionamento) e qual tráfego permanece no plano de dados (em negação) e evita o redirecionamento.

A ACL deve ser semelhante a esta (substitua 10.48.39.28 pelo endereço IP do ISE neste exemplo):

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
<input type="checkbox"/> 10	deny	any		10.48.39.28		ip			None	Disabled
<input type="checkbox"/> 20	deny	10.48.39.28		any		ip			None	Disabled
<input type="checkbox"/> 30	deny	any		any		udp		eq domain	None	Disabled
<input type="checkbox"/> 40	deny	any		any		udp	eq domain		None	Disabled
<input type="checkbox"/> 50	permit	any		any		tcp		eq www	None	Disabled

1 items per page 10 items per page 1 - 5 of 5 items

Observação: para a ACL de redirecionamento, pense na ação deny como um redirecionamento de negação (e não como tráfego de negação) e na permit ação como redirecionamento de permissão. A WLC examina apenas o tráfego que pode redirecionar (portas 80 e 443 por padrão).

CLI:

```
ip access-list extended REDIRECT
deny ip any host <ISE-IP>
deny ip host<ISE-IP> any
deny udp any any eq domain
deny udp any eq domain any
permit tcp any any eq 80
```

 **Observação:** se você terminar a ACL com uma permit ip any any em vez de uma permissão focada na porta 80, a WLC também redirecionará o HTTPS, que geralmente é indesejável, pois tem que fornecer seu próprio certificado e sempre cria uma violação de certificado. Esta é a exceção à instrução anterior que diz que você não precisa de um certificado no WLC no caso do CWA: você precisa de um se tiver a interceptação HTTPS habilitada, mas nunca é considerado válido de qualquer maneira.

Você pode melhorar a ACL negando somente a porta de convidado 8443 ao servidor ISE.

Habilitar redirecionamento para HTTP ou HTTPS

A configuração do portal do administrador da Web está vinculada à configuração do portal de autenticação da Web e precisa escutar na porta 80 para ser redirecionada. Portanto, o HTTP precisa ser habilitado para que o redirecionamento funcione corretamente. Você pode optar por ativá-lo globalmente (com o uso do comando ip http server) ou pode ativar o HTTP somente para o módulo de autenticação da Web (com o uso do comando webauth-http-enable no mapa de parâmetros).



Observação: o redirecionamento do tráfego HTTP acontece dentro do CAPWAP, mesmo no caso do FlexConnect Local Switching. Como é a WLC que faz o trabalho de interceptação, o AP envia os pacotes HTTP(S) dentro do túnel CAPWAP e recebe o redirecionamento da WLC de volta no CAPWAP

Se você quiser ser redirecionado ao tentar acessar um URL HTTPS, adicione o comando `intercept-https-enable` sob o mapa de parâmetros, mas observe que essa não é uma configuração ideal, que tem um impacto na CPU da WLC e gera erros de certificado de qualquer forma:

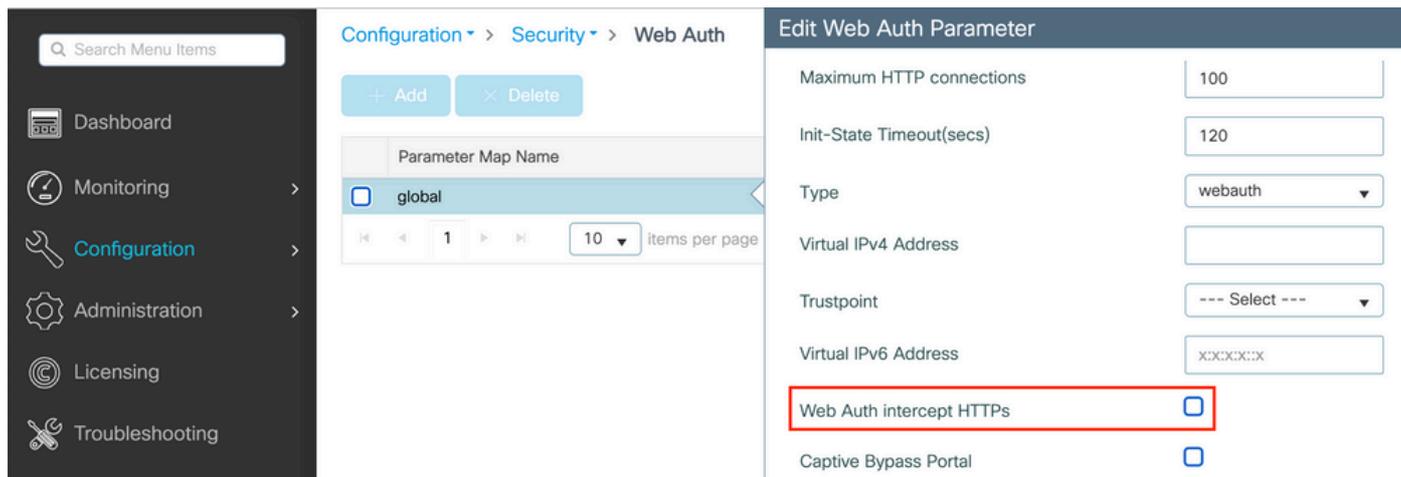
```
<#root>
```

```
parameter-map type webauth global  
type webauth
```

`intercept-https-enable`

`trustpoint xxxxx`

Você também pode fazê-lo através da GUI com a opção 'Web Auth intercept HTTPS' marcada no Mapa de Parâmetros (Configuration > Security > Web Auth).



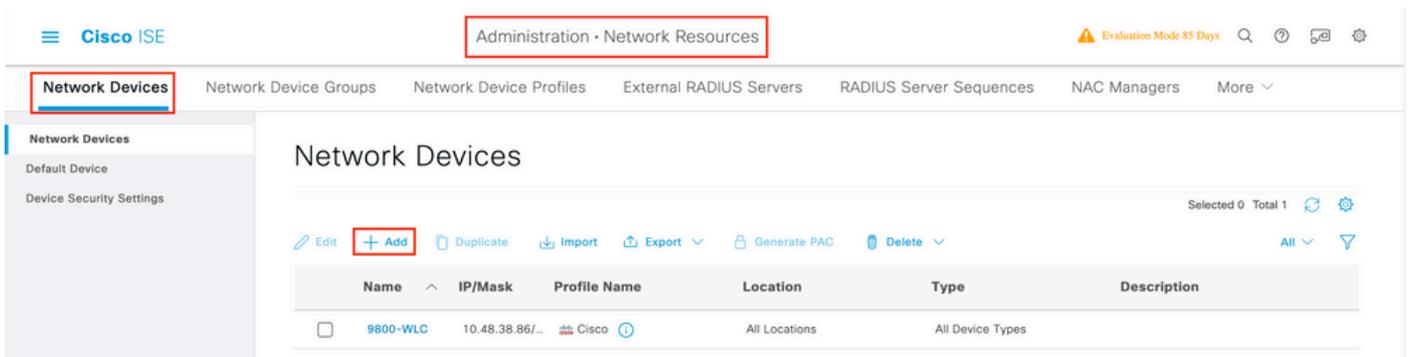


Observação: por padrão, os navegadores usam um site HTTP para iniciar o processo de redirecionamento. Se o redirecionamento de HTTPS for necessário, será necessário verificar o HTTPS de interceptação de Autenticação da Web; no entanto, essa configuração não é recomendada, pois aumenta o uso da CPU.

Configuração do ISE

Adicionar o 9800 WLC ao ISE

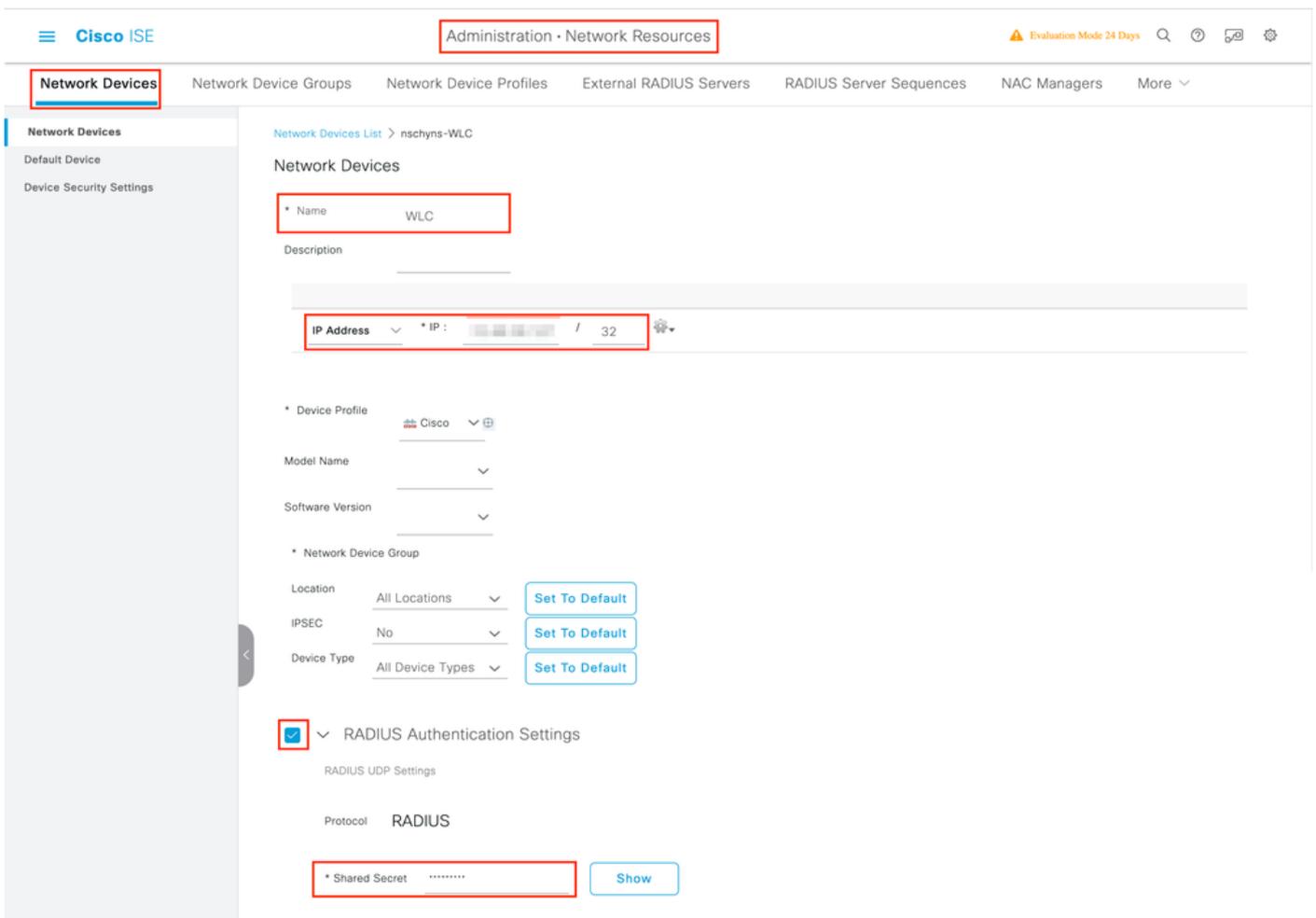
Etapa 1. Abra o console do ISE e navegue até `Administration > Network Resources > Network Devices > Add` como mostrado na imagem.



Etapa 2. Configure o dispositivo de rede.

Opcionalmente, pode ser um nome de Modelo, versão de software e descrição especificados e atribuir grupos de Dispositivos de Rede com base em tipos de dispositivo, localização ou WLCs.

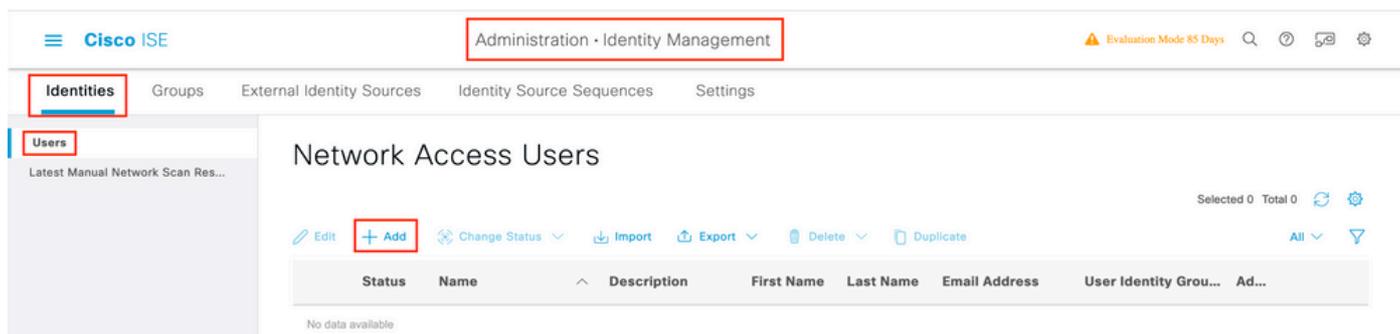
O endereço IP aqui corresponde à interface da WLC que envia as solicitações de autenticação. Por padrão, é a interface de gerenciamento, como mostrado na imagem:



Para obter mais informações sobre Grupos de dispositivos de rede, consulte o Capítulo do guia administrativo do ISE: Gerenciar dispositivos de rede: [ISE - Grupos de dispositivos de rede](#).

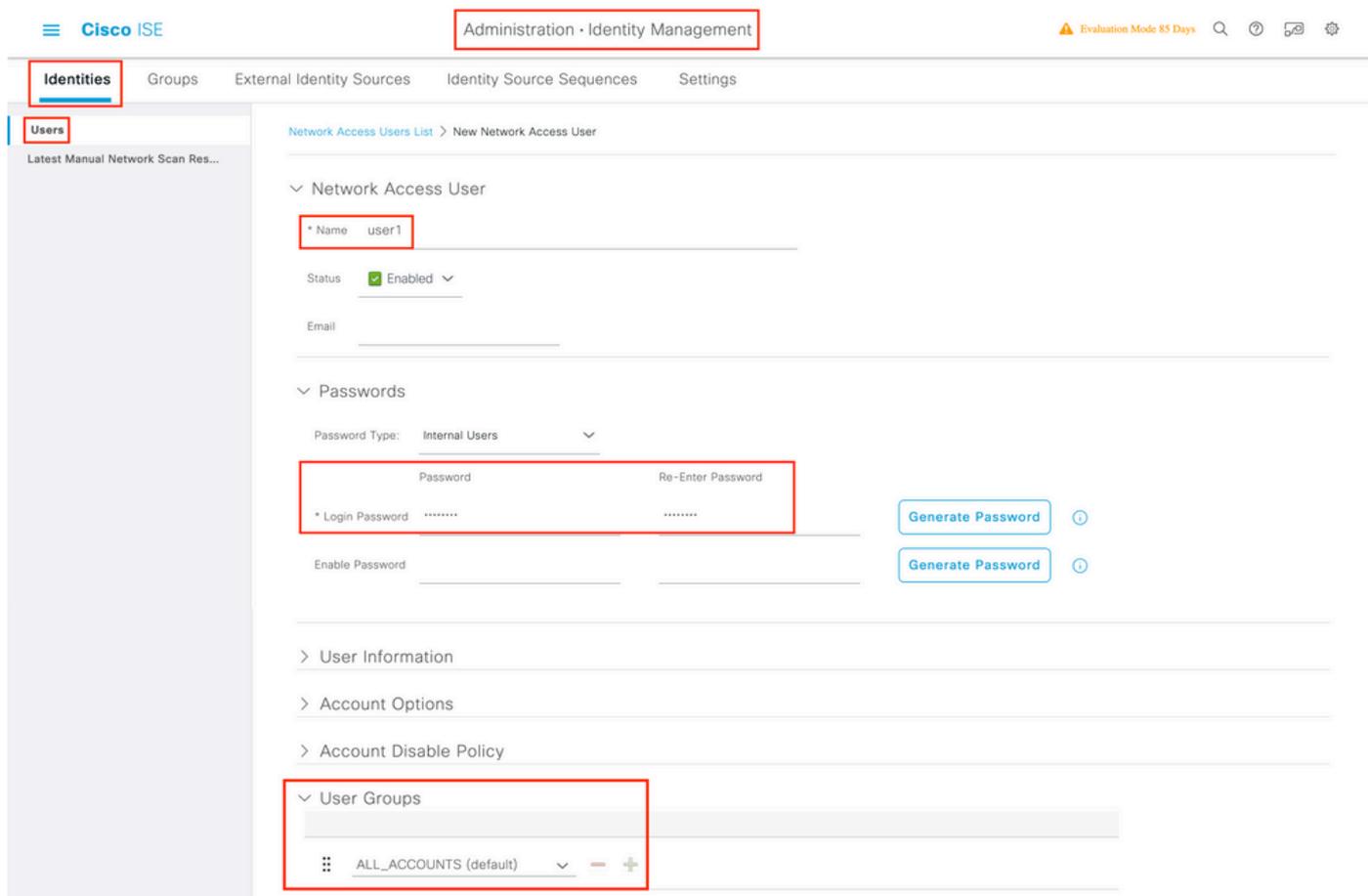
Criar novo usuário no ISE

Etapa 1. Navegue até Administration > Identity Management > Identities > Users > Add conforme mostrado na imagem.



Etapa 2. Inserir informações.

Neste exemplo, esse usuário pertence a um grupo chamado ALL_ACCOUNTS, mas pode ser ajustado conforme necessário, como mostrado na imagem.



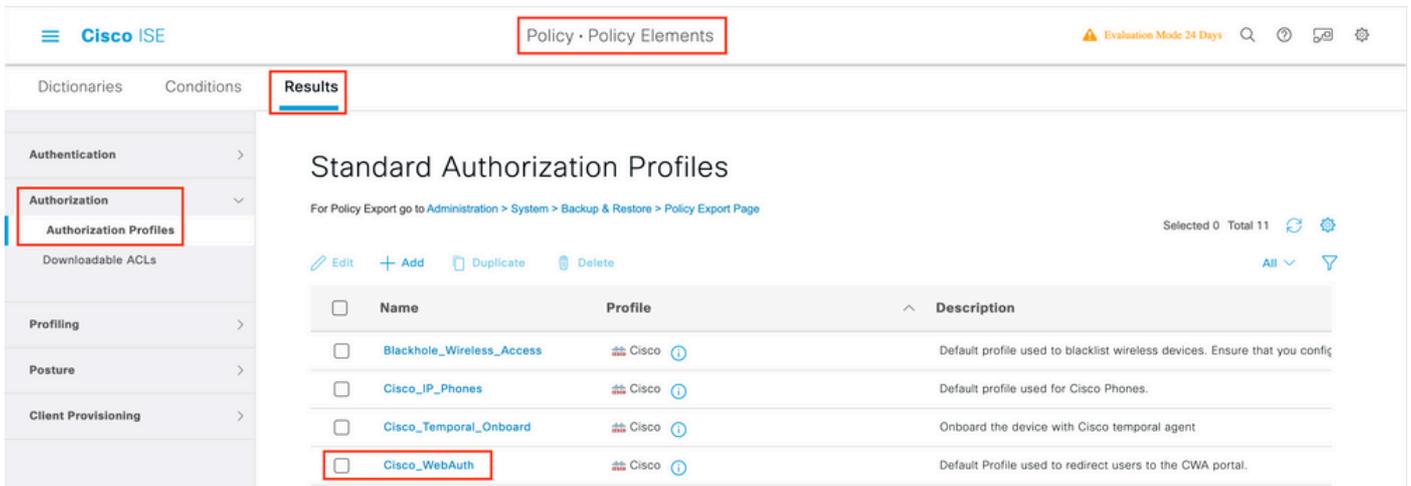
Criar perfil de autorização

O perfil de política é o resultado atribuído a um cliente com base em seus parâmetros (como endereço MAC, credenciais, WLAN usada etc.). Ele pode atribuir configurações específicas, como VLAN (Virtual Local Area Network, rede local virtual), ACLs (Access Control Lists, listas de controle de acesso), redirecionamentos de URL (Uniform Resource Locator, localizador uniforme de recursos) etc.

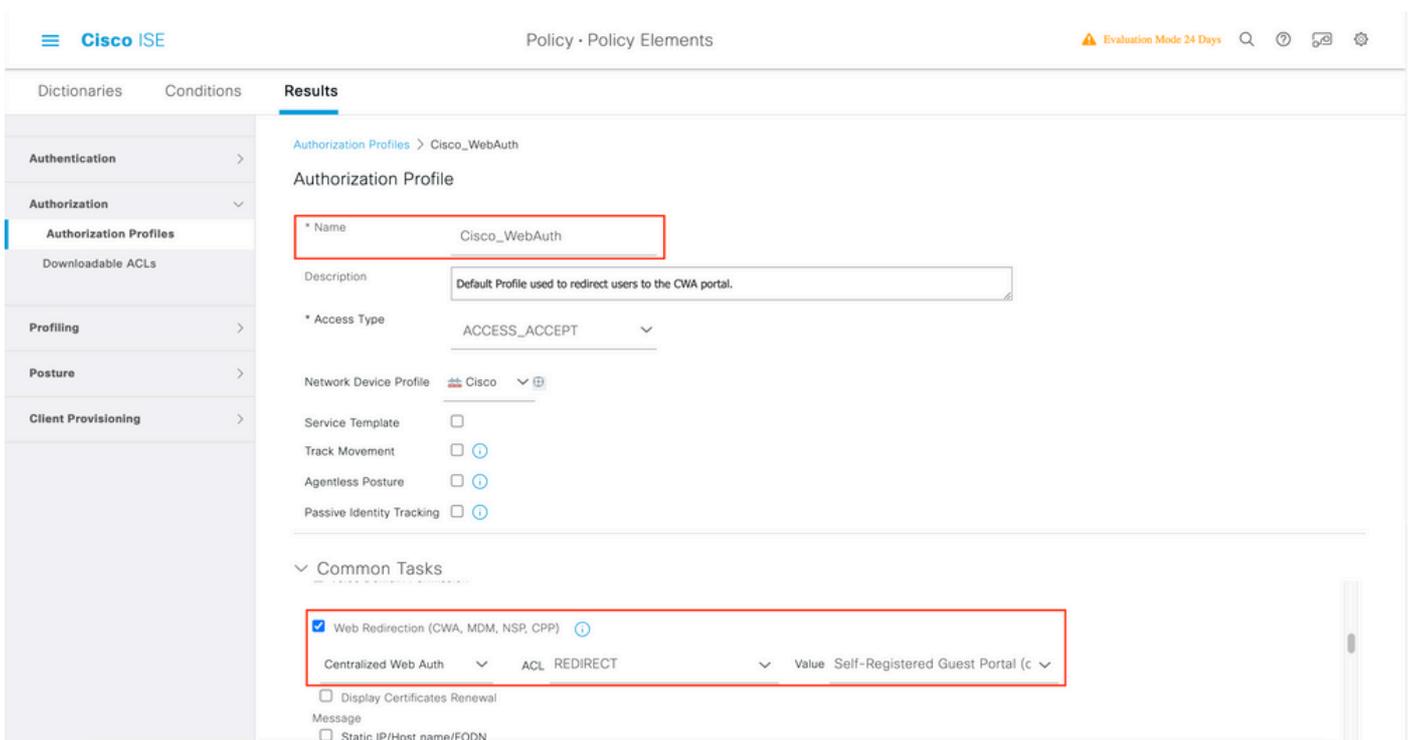
Observe que, nas versões recentes do ISE, já existe um resultado de autorização Cisco_Webauth. Aqui, você pode editá-lo para modificar o

nome da ACL de redirecionamento para corresponder à que você configurou no WLC.

Etapa 1. Navegue até Policy > Policy Elements > Results > Authorization > Authorization Profiles. Clique add para criar seu próprio resultado ou editar o resultado padrão Cisco_Webauth.

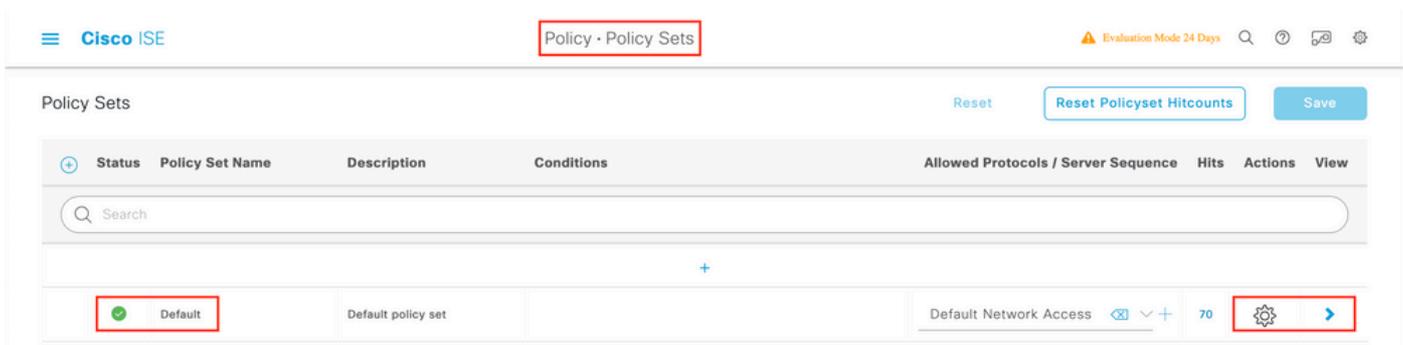


Etapa 2. Insira as informações de redirecionamento. Certifique-se de que o nome da ACL seja o mesmo que foi configurado na WLC 9800.



Configurar regra de autenticação

Etapa 1. Um conjunto de políticas define uma coleção de regras de Autenticação e Autorização. Para criar um, navegue até Policy > Policy Sets, clique na engrenagem do primeiro Conjunto de políticas na lista e Insert new row escolhou clique na seta azul à direita para escolher o Conjunto de políticas padrão.



Etapa 2. Expanda Authentication a política. Para a regra MAB (corresponder no MAB com ou sem fio), expanda Options e escolha a CONTINUE opção caso veja 'Se o usuário não for encontrado'.



Etapa 3. Clique Save para salvar as alterações.

Configurar regras de autorização

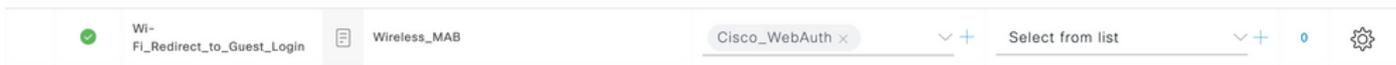
A regra de autorização é responsável por determinar qual resultado de permissões (qual perfil de autorização) é aplicado ao cliente.

Etapa 1. Na mesma página Conjunto de políticas, feche o Authentication Policy e expanda, Authorziation Policy conforme mostrado na imagem.

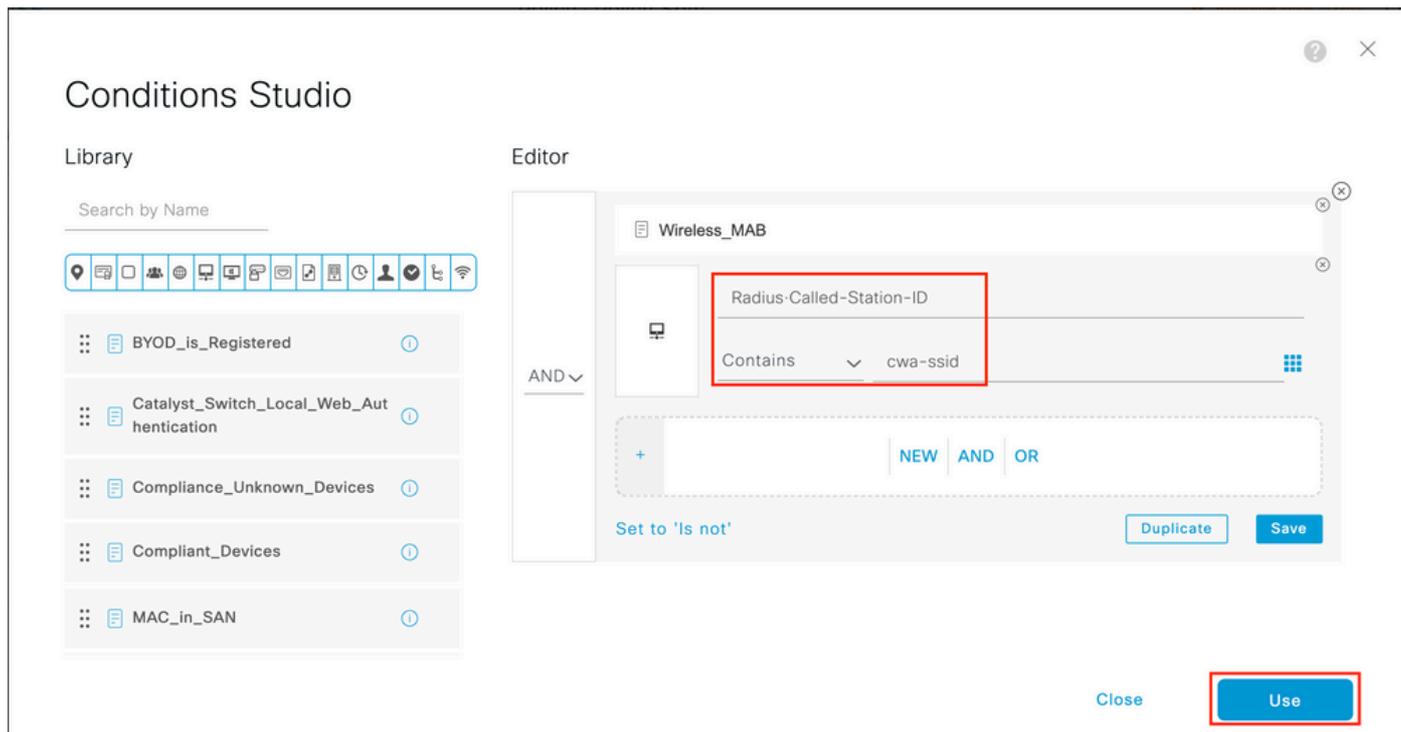


Etapa 2. As versões recentes do ISE começam com uma regra pré-criada chamada Wifi_Redirect_to_Guest_Login que atende principalmente às

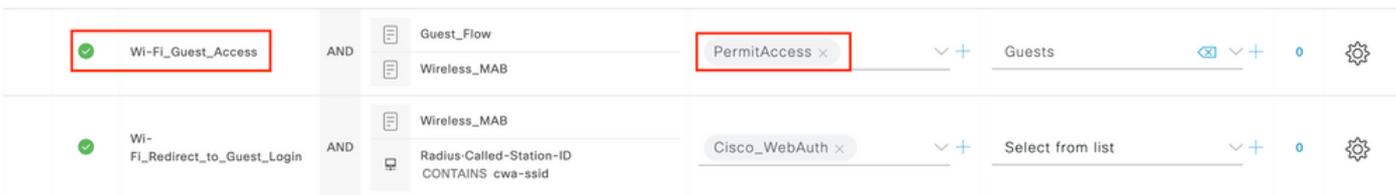
nossas necessidades. Vire o sinal cinza da esquerda para enable.



Etapa 3. Essa regra corresponde apenas a Wireless_MAB e retorna os atributos de redirecionamento do CWA. Agora, você pode, opcionalmente, adicionar uma pequena torção e fazê-la corresponder apenas ao SSID específico. Escolha a condição (Wireless_MAB a partir de agora) para fazer com que o Estúdio de Condições seja exibido. Adicione uma condição à direita e escolha o dicionárioRadius com o Called-Station-ID atributo. Faça com que ele corresponda ao nome da SSID. Valide com o Use na parte inferior da tela como mostrado na imagem.



Etapa 4. Agora você precisa de uma segunda regra, definida com uma prioridade mais alta, que corresponda à Guest Flow condição para retornar os detalhes de acesso à rede depois que o usuário tiver se autenticado no portal. Você pode usar a regra que Wifi Guest Access também é pré-criada por padrão em versões recentes do ISE. Basta ativar a regra com uma marca verde à esquerda. Você pode retornar o padrão PermitAccess ou configurar restrições de lista de acesso mais precisas.



Etapa 5. Salve as regras.

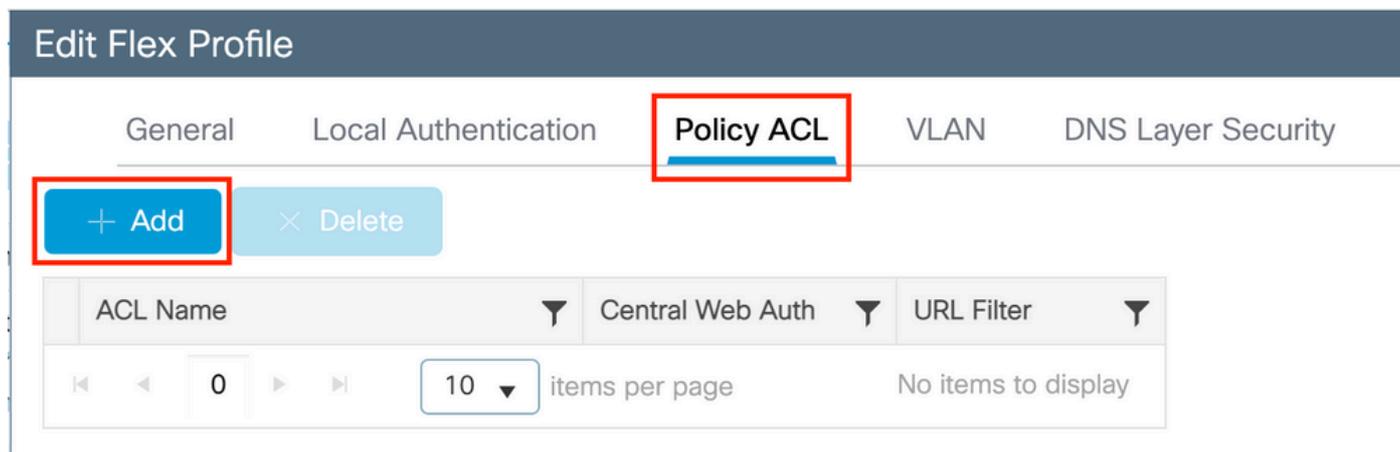
Clique Save na parte inferior das regras.

SOMENTE access points de switching local do FlexConnect

E se você tiver WLANs e access points de switching local do FlexConnect? As seções anteriores ainda serão válidas. No entanto, você precisa de uma etapa extra para enviar a ACL de redirecionamento aos APs com antecedência.

Navegue até Configuration > Tags & Profiles > Flex e escolha seu perfil do Flex. Em seguida, navegue até a Policy ACL guia.

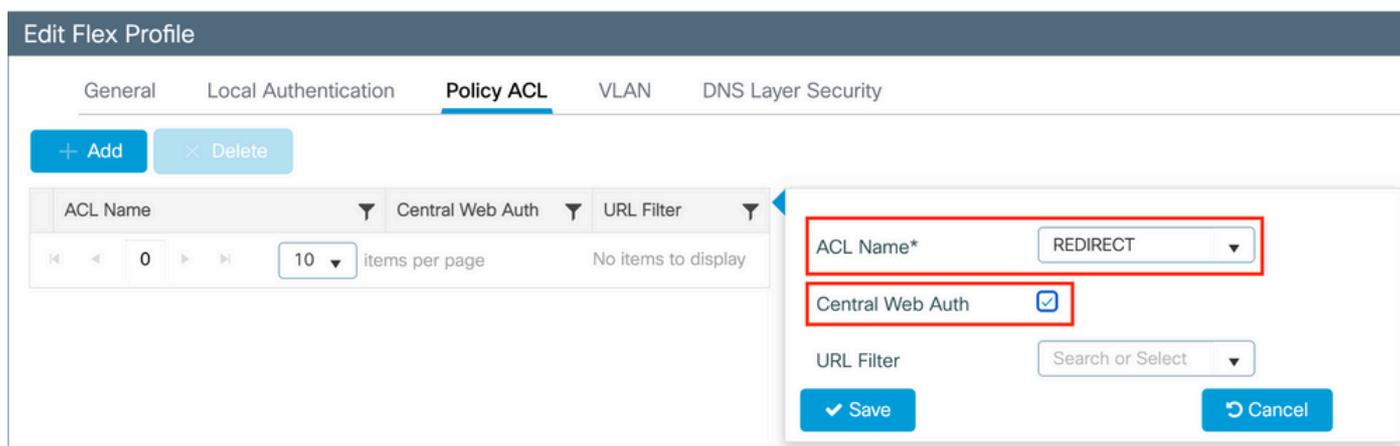
Clique Add conforme mostrado na imagem.



Escolha o nome da ACL de redirecionamento e habilite a autenticação da Web Central. Essa caixa de seleção inverte automaticamente a ACL no próprio AP (isso ocorre porque uma instrução 'deny' significa 'não redirecione para esse IP' na WLC no Cisco IOS XE. No entanto, no AP, a instrução 'deny' significa o oposto. Portanto, essa caixa de seleção troca automaticamente todas as permissões e as nega quando faz o envio para o AP. Você pode verificar isso com um show ip access list do AP (CLI).

Observação: no cenário de switching local do Flexconnect, a ACL deve mencionar especificamente instruções de retorno (que não são necessariamente necessárias no modo local), portanto, certifique-se de que todas as regras de ACL abranjam os dois modos de tráfego (de e para o ISE, por exemplo).

Não se esqueça de bater Save e depois Update and apply to the device.



Certificados

Para que o cliente confie no certificado de autenticação da Web, não é necessário instalar nenhum certificado na WLC, pois o único certificado apresentado é o certificado ISE (que deve ser confiável para o cliente).

Verificar

Você pode usar estes comandos para verificar a configuração atual.

```
<#root>
```

```
# show run wlan # show run aaa # show aaa servers # show ap config general # show ap name <ap-name> config general
# show ap tag summary
# show ap name <AP-name> tag detail
# show wlan { summary | id | nme | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
```

Aqui está a parte relevante da configuração da WLC que corresponde a este exemplo:

```
<#root>
```

```
aaa new-model !
aaa authorization network CWAauthz group radius aaa accounting identity CWAacct start-stop group radius ! aaa server radius dynamic-author client <ISE>
mac-filtering CWAauthz
no security ft adaptive
no security wpa
no security wpa wpa2
no security wpa wpa2 ciphers aes
no security wpa akm dot1x
no shutdown
ip http server (or "webauth-http-enable" under the parameter map)
ip http secure-server
```

Troubleshooting

Lista de verificação

- Verifique se o cliente se conecta e obtém um endereço IP válido.
- Se o redirecionamento não for automático, abra um navegador e tente um endereço IP aleatório. Por exemplo, 10.0.0.1. Se o redirecionamento funcionar, é possível que você tenha um problema de resolução DNS. Verifique se você tem um servidor DNS válido fornecido via DHCP e se ele pode resolver nomes de host.
- Certifique-se de que o comando `ip http server` esteja configurado para que o redirecionamento em HTTP funcione. A configuração do portal do administrador da Web está vinculada à configuração do portal de autenticação da Web e precisa ser listada na porta 80 para

ser redirecionada. Você pode optar por ativá-lo globalmente (com o uso do comando ip http server) ou pode ativar o HTTP somente para o módulo de autenticação da Web (com o uso do comando webauth-http-enable no mapa de parâmetros).

- Se você não for redirecionado ao tentar acessar um URL HTTPS e isso for necessário, verifique se você tem o comando intercept-https-enable no mapa de parâmetros:

<#root>

```
parameter-map type webauth global  
type webauth
```

intercept-https-enable

trustpoint xxxxx

Você também pode verificar, através da GUI, se a opção 'Web Auth intercept HTTPS' está marcada no Mapa de parâmetros:

The screenshot shows the Cisco GUI configuration page for 'Web Auth'. The breadcrumb path is 'Configuration > Security > Web Auth'. The 'Edit Web Auth Parameter' page is displayed for the 'global' parameter map. The 'Web Auth intercept HTTPS' checkbox is checked and highlighted with a red box. Other parameters include 'Maximum HTTP connections' (100), 'Init-State Timeout(secs)' (120), 'Type' (webauth), 'Virtual IPv4 Address', 'Trustpoint' (--- Select ---), 'Virtual IPv6 Address' (xxxx:xx:xx:xx), and 'Captive Bypass Portal' (unchecked).

Suporte de porta de serviço para RADIUS

O Cisco Catalyst 9800 Series Wireless Controller tem uma porta de serviço que é chamada de GigabitEthernet 0porta. A partir da versão 17.6.1, o RADIUS (que inclui CoA) é suportado por meio dessa porta.

Se quiser usar a Porta de serviço para RADIUS, você precisará desta configuração:

<#root>

```
aaa server radius dynamic-author  
client 10.48.39.28
```

vrf Mgmt-intf

```
server-key cisco123

interface GigabitEthernet0

vrf forwarding Mgmt-intf

ip address x.x.x.x x.x.x.x

!if using aaa group server:
aaa group server radius group-name
server name nicoISE

ip vrf forwarding Mgmt-intf

ip radius source-interface GigabitEthernet0
```

Coletar depurações

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



Observação: você pode retornar de algumas horas para vários dias nos logs, mas isso depende do volume de logs gerados.

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

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

```
<#root>
```

```
# show clock
```

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

```
<#root>
```

```
# show logging
```

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

```
<#root>
```

```
# show debugging Cisco IOS XE Conditional Debug Configs: Conditional Debug Global State: Stop Cisco IOS XE Packet Tracing Configs: Packet Infra d
```

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

Etapa 4. Com a suposição de que o endereço mac em teste não foi listado como uma condição na Etapa 3, colete os rastreamentos de nível de aviso sempre ativo para o endereço mac específico.

```
<#root>
```

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

Você pode exibir o conteúdo da sessão ou copiar o arquivo para um servidor TFTP externo.

```
<#root>
```

```
# more bootflash:always-on-<FILENAME.txt>
```

```
or
```

```
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

Depuração condicional e rastreamento radioativo

Se os rastreamentos sempre ativos não fornecerem informações suficientes para determinar o disparador do problema sob investigação, você poderá habilitar a depuração condicional e capturar o rastreamento de Radio Ativo (RA), que fornece rastreamentos em nível de depuração para todos os processos que interagem com a condição especificada (endereço mac do cliente, neste caso). Para habilitar a depuração condicional, continue com estas etapas.

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

```
<#root>
```

```
# clear platform condition all
```

Etapa 6. Ative a condição de depuração para o endereço MAC do cliente sem fio que você deseja monitorar.

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

```
<#root>
```

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

 **Observação:** para monitorar mais de um cliente por 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 do terminal, pois tudo é armazenado em buffer internamente para ser exibido posteriormente.

Etapa 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.

```
<#root>
```

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

Quando o tempo do monitor tiver decorrido ou a depuração sem fio tiver sido interrompida, a WLC 9800 gerará um arquivo local com o nome:

```
ra_trace_MAC_aaaabbbccccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

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

Verifique o nome do arquivo de rastreamentos de RA.

```
<#root>
```

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

Copie o arquivo para um servidor externo:

```
<#root>
```

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

Mostre o conteúdo:

```
<#root>
```

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

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

```
<#root>
```

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

 **Observação:** a saída desse comando retorna rastros para todos os níveis de log de todos os processos e é bastante volumosa. Envie o Cisco TAC para ajudar a analisar esses rastreamentos.

Você pode copiar o ra-internal-FILENAME.txt para um servidor externo ou exibir a saída diretamente na tela.

Copie o arquivo para um servidor externo:

```
<#root>
```

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

Mostre o conteúdo:

```
<#root>
```

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

Etapa 11. Remova as condições de depuração.

```
<#root>
```

```
# clear platform condition all
```



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

Examples

Se o resultado da autenticação não for o esperado, é importante navegar até a página do ISEOperations > Live logs e obter os detalhes do resultado da autenticação.

Você verá o motivo da falha (se houver uma falha) e todos os atributos RADIUS recebidos pelo ISE.

No próximo exemplo, o ISE rejeitou a autenticação porque nenhuma regra de autorização correspondeu. Isso ocorre porque você vê o atributo Called-station-ID enviado como o nome SSID anexado ao endereço MAC do AP, enquanto a autorização é uma correspondência exata ao nome SSID. Ele é corrigido com a alteração dessa regra para 'contém' em vez de 'igual'.

Event	5400 Authentication failed
Failure Reason	15039 Rejected per authorization profile
Resolution	Authorization Profile with ACCESS_REJECT attribute was selected as a result of the matching authorization rule. Check the appropriate Authorization policy rule-results.
Root cause	Selected Authorization Profile contains ACCESS_REJECT attribute
Username	E8:36:17:1F:A1:62

```
15048 Queried PIP - Radius.NAS-Port-1-type
15048 Queried PIP - Network Access.UserName
15048 Queried PIP - IdentityGroup.Name (2 times)
15048 Queried PIP - EndPoints.LogicalProfile
15048 Queried PIP - Radius.Called-Station-ID
15048 Queried PIP - Network Access.AuthenticationStatus
15016 Selected Authorization Profile - DenyAccess
15039 Rejected per authorization profile
11003 Returned RADIUS Access-Reject
```

Other Attributes

ConfigVersionId	140
Device Port	58209
DestinationPort	1812
RadiusPacketType	AccessRequest
Protocol	Radius
NAS-Port	71111
Framed-MTU	1485
OriginalUserName	e836171fa162
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	nicolse26/356963261/1
UseCase	Host Lookup
SelectedAuthenticationIdentityStores	Internal Endpoints
IdentityPolicyMatchedRule	MAB
AuthorizationPolicyMatchedRule	Default
EndPointMACAddress	E8-36-17-1F-A1-62
ISEPolicySetName	Default
IdentitySelectionMatchedRule	MAB
DTLSSupport	Unknown
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
RADIUS Username	E8:36:17:1F:A1:62
NAS-Identifler	cwa-ssid
Device IP Address	10.48.71.120
CPMSessionID	7847300A0000012DFC227BF1
Called-Station-ID	00-27-e3-8f-33-a0:cwa-ssid
CiscoAVPair	service-type=Call Check, audit-session-id=7847300A0000012DFC227BF1, method=mab, client-if-id=3003124185, vlan-id=1468, cisco-wlan-ssid=cwa-ssid

Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Troubleshooting

Troubleshooting > Radioactive Trace

Conditional Debug Global State: **Stopped**

+ Add Delete Start Stop

MAC/IP Address	Trace file
<input type="checkbox"/> e836.171f.a162	debugTrace_e836.171f.a162.txt Generate

10 items per page 1 - 1 of 1 items

Nesse caso, o problema está no fato de que você cometeu um erro de digitação quando criou o nome da ACL e ele não corresponde ao nome da ACL retornado pelos ISEs ou a WLC reclama que não há nenhuma ACL como a solicitada pelo ISE:

<#root>

2019/09/04 12:00:06.507 {wncd_x_R0-0}{1}: [client-auth] [24264]: (ERR): MAC: e836.171f.a162 client authz result: FAILURE 2019/09/04 12:00:06.51

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.