Configurar autenticação local no modo FlexConnect

Contents

- Introdução
  - Informações de Apoio
    - Visão geral e requisitos do FlexConnect
    - Modos de operação
    - Roaming rápido e seguro
    - Modo de alta escala FlexConnect
    - Suporte a Wi-Fi 7 FlexConnect
    - Cenários de resiliência do FlexConnect
- Pré-requisitos
  - Requisitos
  - Componentes Utilizados
- Configurar
  - Diagrama de Rede
  - Configurar servidores AAA
  - Configurar o modo FlexConnect no site remoto
  - Configurar a WLAN 802.1x com autenticação local usando um servidor RADIUS externo
  - Configurar o ISE
  - Configurar a WLAN PSK com autenticação local
- Verificar
- Troubleshooting
  - Cenário autônomo
- Informações Relacionadas

Introdução

Este documento descreve como a autenticação local do FlexConnect funciona e como configurá-la usando o Cisco Catalyst 9800 Series Wireless Controller (WLC)

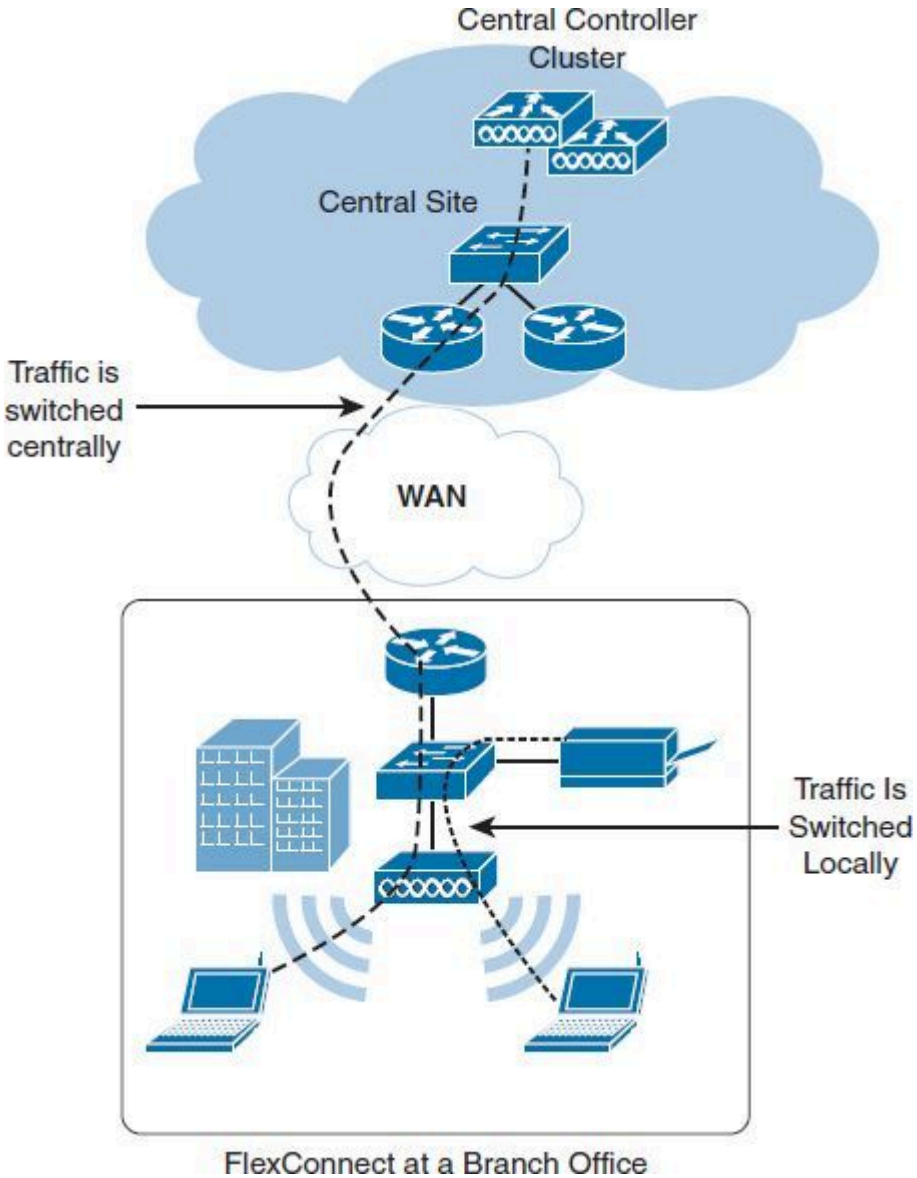
Informações de Apoio

Visão geral e requisitos do FlexConnect

O FlexConnect permite que o ponto de acesso (AP) em escritórios remotos ou filiais se conecte a

um controlador centralizado, ao mesmo tempo em que permite o processamento local do tráfego sem fio. Diferentemente das implantações sem fio centralizadas tradicionais, em que todo o tráfego sem fio é encapsulado no controlador usando CAPWAP (Control and Provisioning of Wireless Access Points, Controle e provisionamento de access points sem fio) — o FlexConnect permite que o tráfego seja comutado localmente e tratado diretamente pelo AP da filial. Essa comutação local fornece ao AP um grau de autonomia, permitindo que serviços-chave como segurança, roaming e Qualidade de Serviço (QoS) funcionem independentemente do controlador.

Embora o FlexConnect seja projetado principalmente para switching de tráfego local, ele também oferece a flexibilidade de alternar centralmente SSIDs (Service Set Identifier) específicos quando necessário. Por exemplo, se determinado tráfego deve passar por um firewall central, esses SSIDs podem ser enviados de volta ao controlador via CAPWAP para switching centralizado. Esse recurso duplo permite que um único AP FlexConnect suporte simultaneamente WLANs (Wireless Local Area Network, Rede local sem fio) com comutação local e central.



Um AP FlexConnect implantado em uma filial comuta localmente um SSID enquanto outro é comutado centralmente

Modos de operação

Os APs FlexConnect operam em dois modos: modo conectado e modo autônomo.

- Modo conectado, o AP mantém uma conexão ativa com o controlador através do canal de controle CAPWAP.
- O modo autônomo é um estado de fallback que ocorre quando o AP perde a conectividade com o controlador.

Em condições normais, os APs FlexConnect funcionam no modo conectado, em que o controlador gerencia serviços essenciais, como autenticação centralizada, criação de perfis de clientes e RRM (Radio Resource Management, gerenciamento de recursos de rádio). Embora o AP deva permanecer nesse modo a maior parte do tempo, ele automaticamente alterna para o modo autônomo se a comunicação com o controlador for perdida. No modo autônomo, o AP continua a operar, comutando localmente o tráfego e permitindo que os clientes permaneçam conectados. Os APs autenticam os clientes de forma independente, sem encaminhar solicitações de autenticação a um controlador central. No entanto, determinados serviços dependentes de controlador, como RRM e autenticação centralizada de cliente, tornam-se temporariamente indisponíveis.

Por exemplo, se uma interrupção de WAN (Wide Area Network) interromper a conexão entre o AP e o controlador, mas o acesso à Internet permanecer ativo, o AP faz a transição para o modo autônomo e continua a processar o tráfego comutado localmente sem interrupção. Os clientes existentes permanecem conectados, mas os novos clientes que requerem autenticação central não conseguem se associar à rede, a menos que a autenticação local esteja configurada. Os APs FlexConnect podem ser configurados para executar autenticação local durante falhas de WAN, garantindo serviço contínuo mesmo quando o controlador estiver inacessível.

No modo autônomo, estes recursos não estão disponíveis para o AP:

- Autenticação da Web do cliente
- Autenticação de convidado (redirecionamento do portal)
- Qualquer SSID comutado centralmente
- RRM
- Mobilidade de Camada 3 IPv6
- Criação de perfil nativa
- Classificação da política

- Gateway de Descoberta de Serviços
- Atualizações de configuração

Para obter uma lista completa de recursos e configurações de WLAN suportados no modo autônomo (autenticação local), consulte a matriz de recursos: Matriz de recursos para pontos de acesso sem fio Cisco

Um cenário de falha comum do FlexConnect envolve uma perda completa ou degradação significativa da WAN, o que interrompe o canal de controle do CAPWAP. Quando o AP perde a conectividade com o controlador devido a problemas de WAN, ele imediatamente muda para o modo autônomo.

O objetivo principal durante uma falha de WAN é restaurar a comunicação com o controlador o mais rápido possível para retomar a funcionalidade completa.

Quando um AP FlexConnect entra no modo autônomo devido a uma falha na WAN, os clientes ativos permanecem conectados e podem fazer roaming perfeitamente entre APs dentro da tag de domínio/site do FlexConnect, mas o roaming entre diferentes tags de site do FlexConnect pode exigir uma reautenticação completa. No entanto, os novos clientes que tentam se unir à WLAN comutada localmente não conseguem se autenticar porque o servidor AAA (Authentication, Authorization, and Accounting Server) no local central está inacessível.

Roaming rápido e seguro

A autenticação EAP (Extensible Authentication Protocol) introduz uma latência mais alta em comparação à autenticação PSK (Pre-Shared Key) devido à troca de quadros EAP com o servidor AAA. No entanto, com o roaming rápido e seguro, um cliente passa por uma autenticação 802.1X/EAP completa apenas durante sua associação inicial com a rede. Em roams subsequentes para APs vizinhos, a troca de EAP é ignorada, deixando apenas o handshake de quatro vias, que é significativamente mais rápido, já que não envolve o servidor AAA. Esta tabela descreve os vários métodos de roaming rápido e seguro suportados pela WLC 9800 no modo local e nas implantações FlexConnect.

Recurso	Modo local	FlexConnect (modo conectado; Autenticação Central)	FlexConnect (Modo conectado—Autenticação local)	FlexConnect (independente)
Cache de chave	Not Supported	Not Supported	Not Supported	Not Supported

sticky (SKC)				
Cache de chave oportunista (OKC)	Supported	Supported	Supported	Suportado (até a sessão do cliente expirar)
Gerenciamento centralizado de chaves (CCKM) da Cisco	Supported	Supported	Supported	Not Supported
FT-802.11r/ Adaptive 11r (Transição rápida) (Over the Air)	Supported	Supported	Supported	Suportado (até a sessão do cliente expirar)
FT-802.11r/ Adaptive 11r (Transição rápida) (Sobre o DS)	Supported	Supported	Not Supported	Not Supported

No modo autônomo, o roaming rápido depende do material da chave armazenada em cache permanecer válido. Quando a sessão/PMK (Pairwise Master Key) em cache expira, o AP não pode obter novas informações de chave derivadas do controlador até que a conectividade do controlador seja restaurada.

Modo de alta escala FlexConnect

A partir do Cisco IOS XE 17.8.1, a capacidade do local flexível foi escalada para acomodar 300 APs e 3000 clientes 802.1x.

A propagação de PMK permite que os APs no mesmo site do FlexConnect compartilhem informações de PMK, reduzindo a necessidade de uma troca de EAP completa durante o roaming. A propagação de PMK não está ativada por padrão.

Use estes comandos para verificar a propagação da PMK e para ativar a PMK:

- show wireless stats pmk-propagation
- pmk propagate

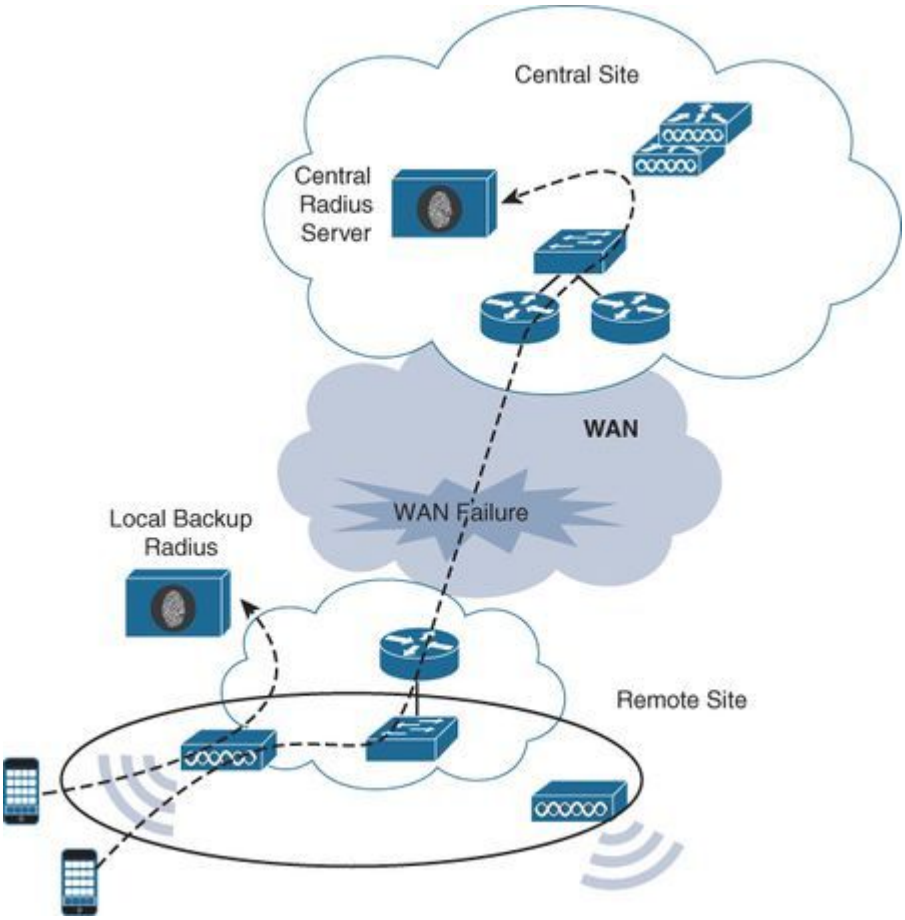
Suporte a Wi-Fi 7 FlexConnect

Esta tabela resume os recursos do FlexConnect suportados pela família AP CW917x Wi-Fi 7.

Recurso	Support
Switching local	Supported
Switching central	Supported
Mapeamento de WLAN-VLAN	Supported
Autenticação local com RADIUS externo	Supported
WPA3-Empresa	Supported
Roaming rápido FT-802.11r	Supported
Operação de vários links (MLO)	Supported
Autenticação local com RADIUS interno	Not Supported
WPA3-Empresa-192	Not Supported

Cenários de resiliência do FlexConnect

1. Em uma configuração de resiliência N+1, vários controladores ativos compartilham um controlador de backup comum que assume se qualquer controlador ativo falhar. Quando um controlador principal fica off-line, os APs FlexConnect mudam imediatamente para o modo autônomo e começam a procurar o controlador de backup. Durante esse período de desconexão, os clientes comutados centralmente são desconectados dos APs. Depois que os APs localizam e sincronizam com o controlador de backup, os clientes que precisam de acesso a SSIDs comutados centralmente são reconectados. Enquanto isso, os clientes comutados localmente permanecem inalterados e continuam a operar sem perceber a interrupção do serviço.
2. Forneça um servidor AAA de backup no local remoto, acessível pelo grupo FlexConnect. Com a autenticação local habilitada, esse servidor RADIUS de backup é usado somente quando os APs entram no modo autônomo — ele permanece inativo enquanto os APs estão no modo conectado. Quando os APs FlexConnect usam o servidor AAA de backup local para autenticação, as chaves de autenticação são distribuídas por todos os APs no grupo FlexConnect, da mesma forma que seriam com um servidor AAA centralizado. Isso garante que novos clientes ainda possam fazer roaming perfeitamente entre APs sem precisar reautenticar, mesmo quando o servidor RADIUS de backup estiver em uso.
3. Qualquer método presente na Matriz de Recursos para Pontos de Acesso Sem Fio Cisco que permita a Autenticação Local.



Os clientes autenticam em um servidor AAA de backup local quando o servidor AAA central se torna indisponível devido a uma falha de WAN

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Controlador sem fio Catalyst C9800-CL para nuvem com Cisco IOS® XE Dublin 17.18.3
- Ponto de acesso Catalyst CW9164I-ROW v17.18.3.18
- Access point Aironet® AIR-AP2802I-E-K9 v17.18.3.18
- 2 x Identity Services Engine v3.2.0.542

As informações neste documento foram criadas a partir de dispositivos em um ambiente de

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

Configurar

Diagrama de Rede

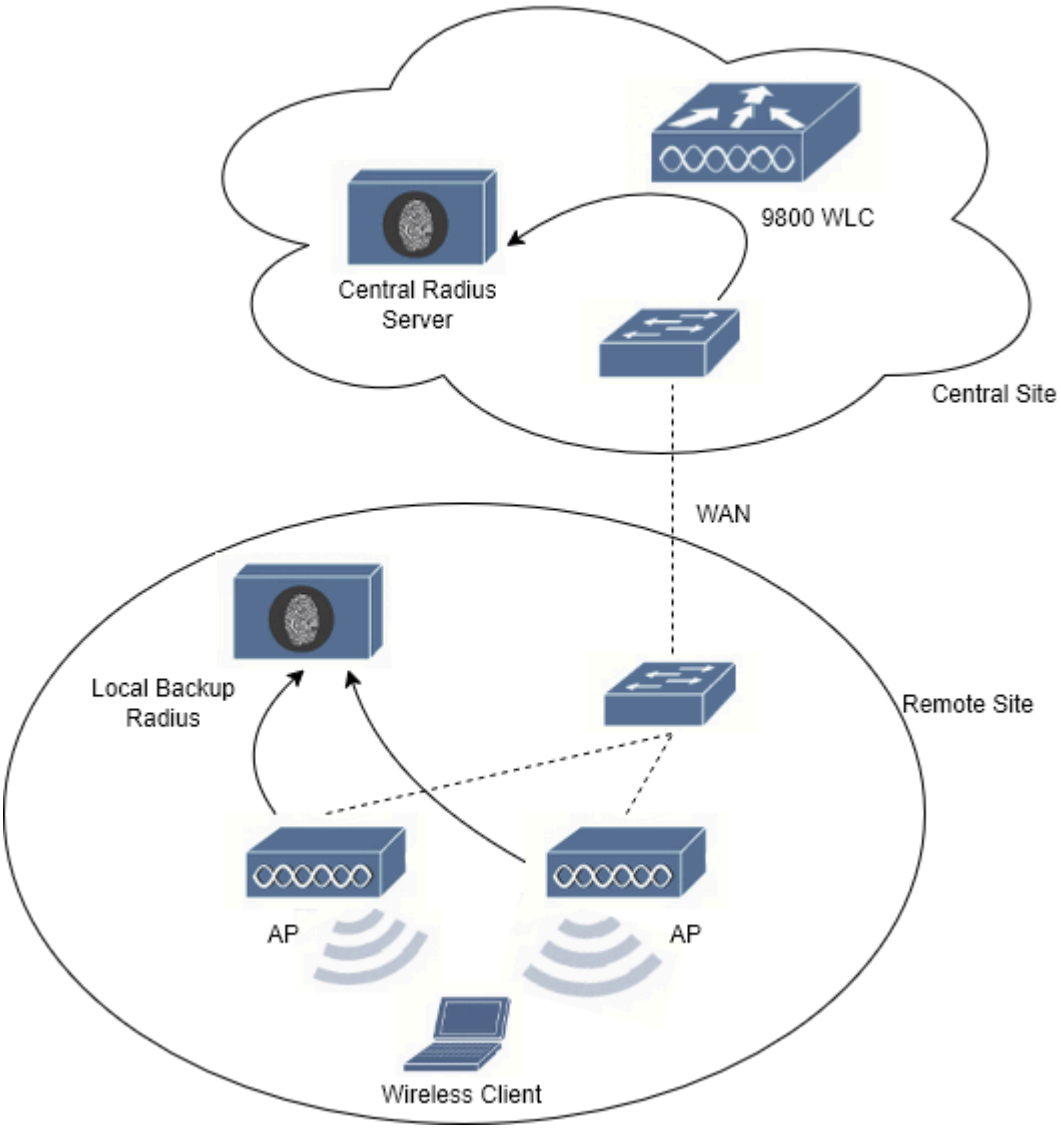


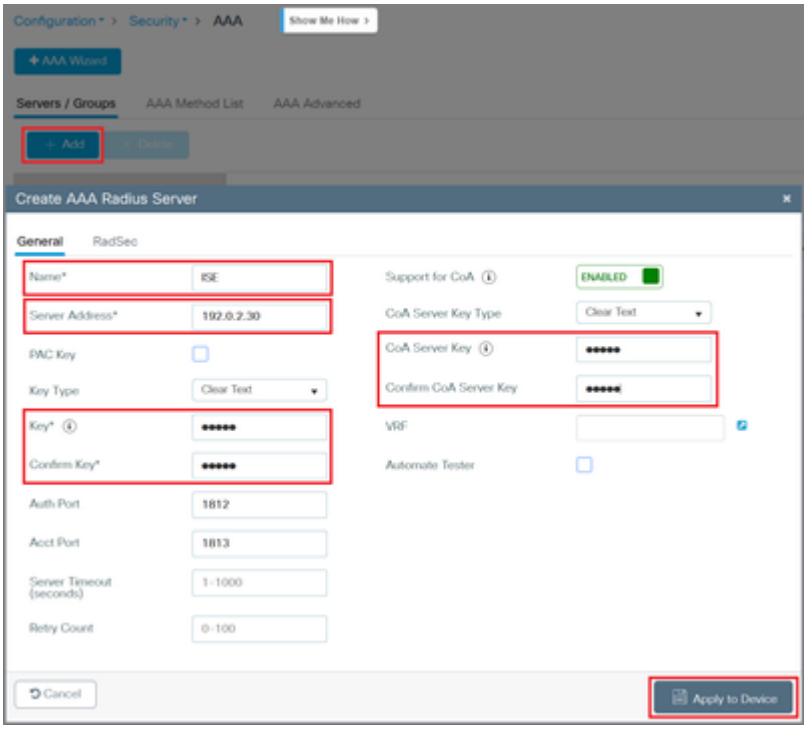
Diagrama de Rede

Configurar servidores AAA

Etapa 1. Para configurar uma WLAN 802.1x é necessário criar o grupo de servidores AAA na WLC 9800.

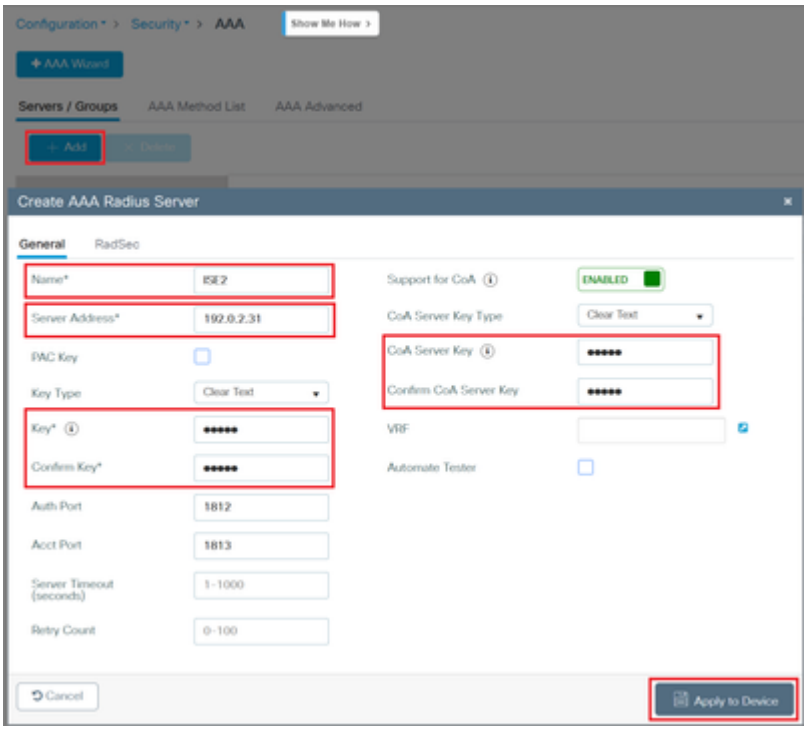
Crie um servidor AAA para cada site - o do site central e o outro do site remoto.

Navegue para Configuration > Security > AAA > Server/Groups > Servers e selecione +Add. Dê um nome ao servidor, seu endereço IP, a chave (e confirme a chave), habilite o suporte de CoA (Alteração de autorização) e insira a chave do servidor de CoA (e confirme a chave do servidor de CoA). As chaves devem ser as mesmas.



Clique em Apply to Device.

Etapa 2. Crie o outro servidor AAA:



Clique em Apply to Device.

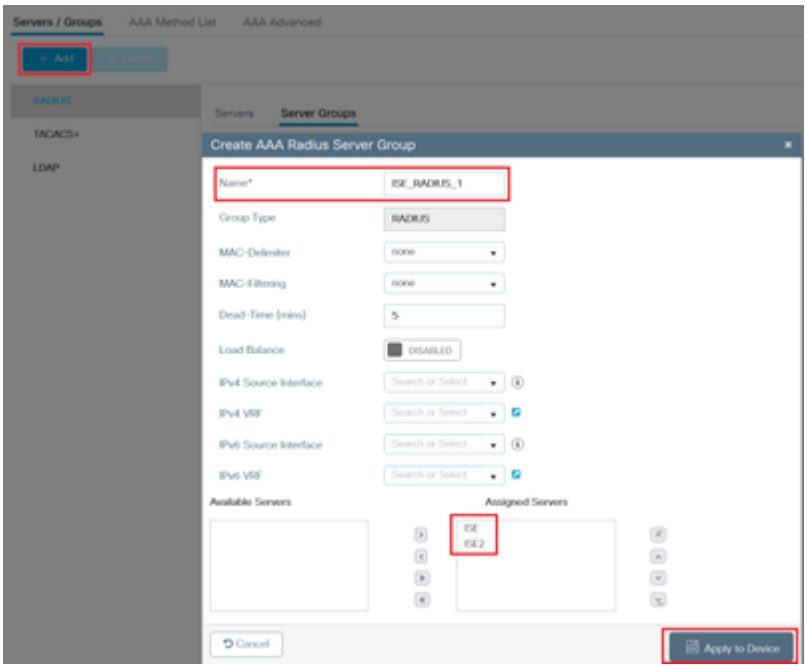
Agora você verá seus servidores AAA configurados:

Servers | Server Groups

	Name	Address	Auth Port	Acct Port
☐	ISE	192.0.2.30	1812	1813
☐	ISE2	192.0.2.31	1812	1813

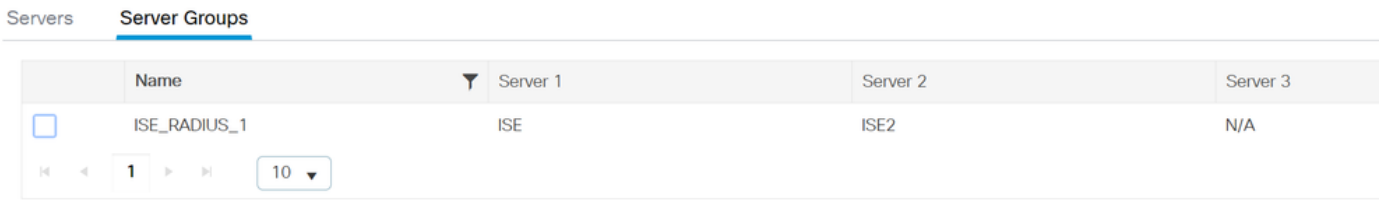
1 | 10 | 1 - 2 of 2 items

Etapa 3. Navegue até Configuration > Security > AAA > Server/Groups > Server Groups e selecione +Add. Dê um nome ao servidor do grupo e selecione os servidores AAA criados anteriormente para a coluna Assigned Servers:



Clique em Apply to Device.

Em seguida, você verá o grupo de servidores AAA configurado:



CLI:

```
aaa new-model
!
radius server ISE
address ipv4 192.0.2.30 auth-port 1812 acct-port 1813
key keystring
!
radius server ISE2
address ipv4 192.0.2.31 auth-port 1812 acct-port 1813
key keystring
!
aaa server radius dynamic-author
client 192.0.2.30 server-key keystring
client 192.0.2.31 server-key keystring
!
aaa group server radius ISE_RADIUS_1
server name ISE
server name ISE2
deadtime 5
```

Configurar o modo FlexConnect no site remoto

Etapa 1. A primeira etapa é configurar o FlexConnect no local remoto.

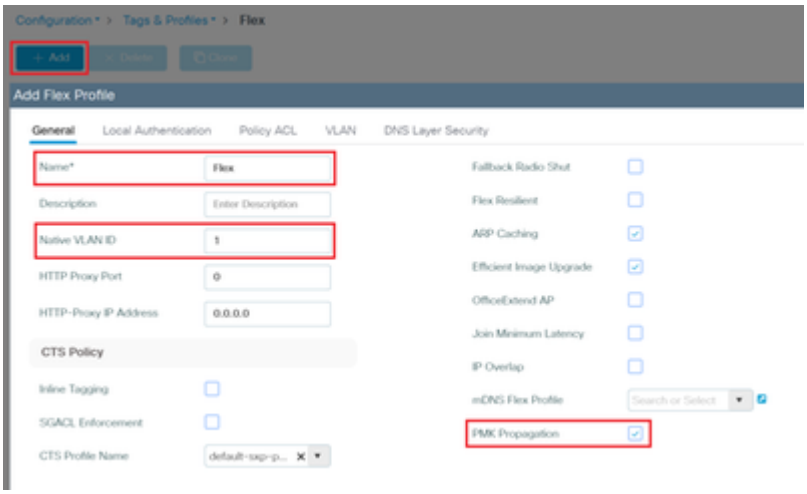
Use este guia para alterar o modo de seus APs para Flex: Compreenda o FlexConnect no Catalyst 9800 Wireless Controller.

Os APs neste guia/laboratório usam o mesmo perfil Flex.

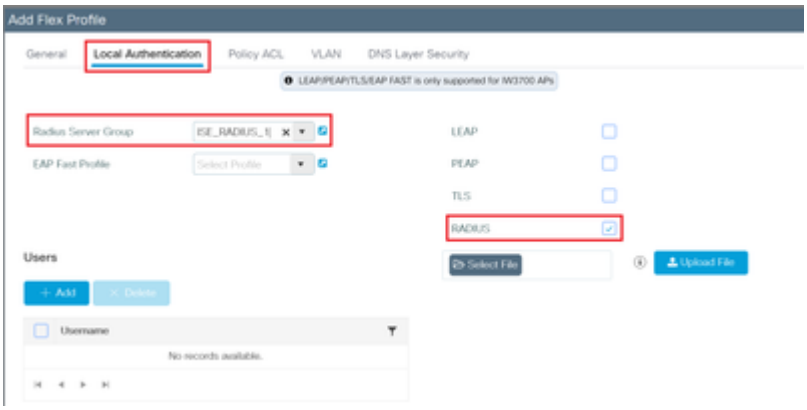
Etapa 2. Navegue até Configuration > Tags & Profiles > Flex.

Crie um novo Nome de Perfil Flex com +Adicionar. Na guia General (Geral) dê um nome ao perfil, insira a ID da VLAN nativa (Virtual Local Area Network) e ative a Propagação PMK.

Habilite a propagação de PMK para facilitar o roaming de cliente sem fio transparente, compartilhando informações de PMK entre AP em um único site.

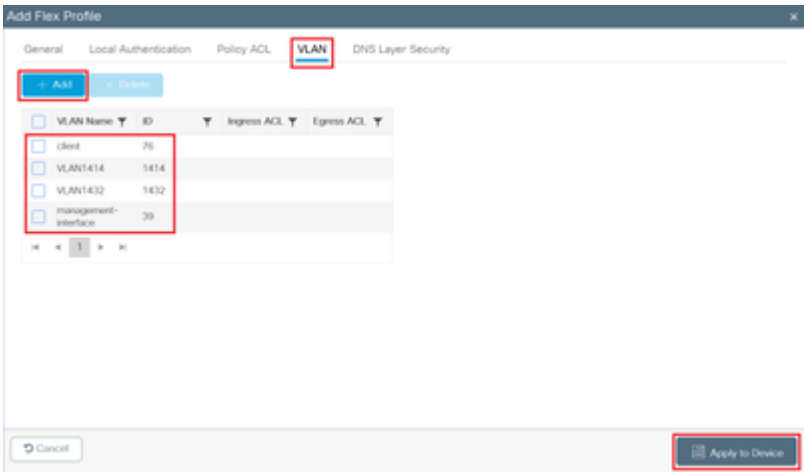


Etapa 3. Para a WLAN 802.1x, na guia Autenticação Local, selecione o Grupo de Servidores Radius e ative o RADIUS:



Tip: Para uma PSK WLAN, não é necessário adicionar nada a essa guia.

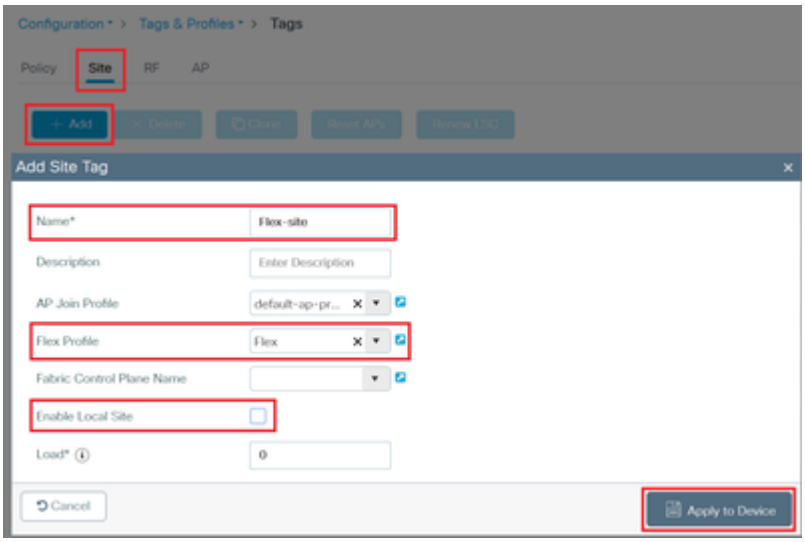
Etapa 4. Na guia VLAN, adicione todas as VLANs que são usadas por clientes, APs e servidor RADIUS. Certifique-se de fazer a correspondência correta de cada nome de VLAN com o ID de VLAN correto:



No final, clique em Update & Apply to Device.

Etapa 5. Navegue até Configuration > Tags & Profiles > Tags > Site e selecione +Add.

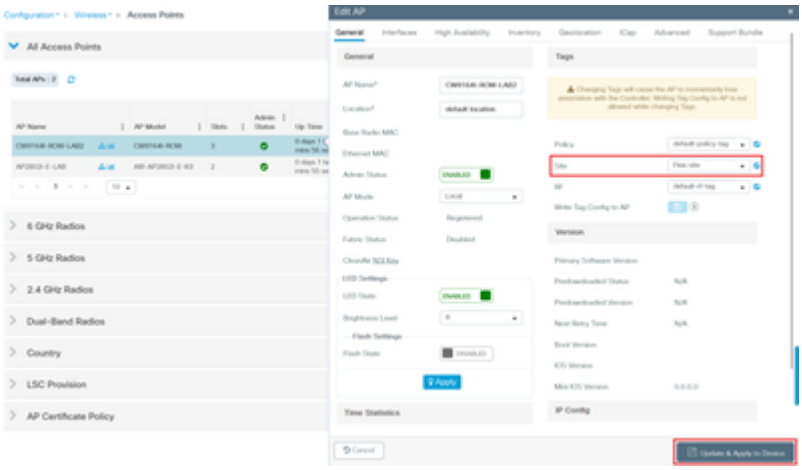
Crie a marca de site com o Perfil Flex criado anteriormente. Dê um nome a ele, selecione o Perfil Flex correto e desabilite Habilitar Site Local. Certifique-se de que o perfil de junção AP seja o correto.



Clique em Aplicar ao dispositivo.

Etapa 6. Navegue até Configuration > Wireless > Access Points.

Selecione seu AP, em Geral > Tags, altere a tag Site para a tag configurada anteriormente:



Clique em Update & Apply to Device.

O AP se desconecta da WLC e se une novamente com o modo Flex AP.

Na mesma página, quando o AP se reune, você pode verificar o modo do AP na coluna Modo do AP.

Se você selecionar o AP, ele exibirá a nova marca Site:



CLI:

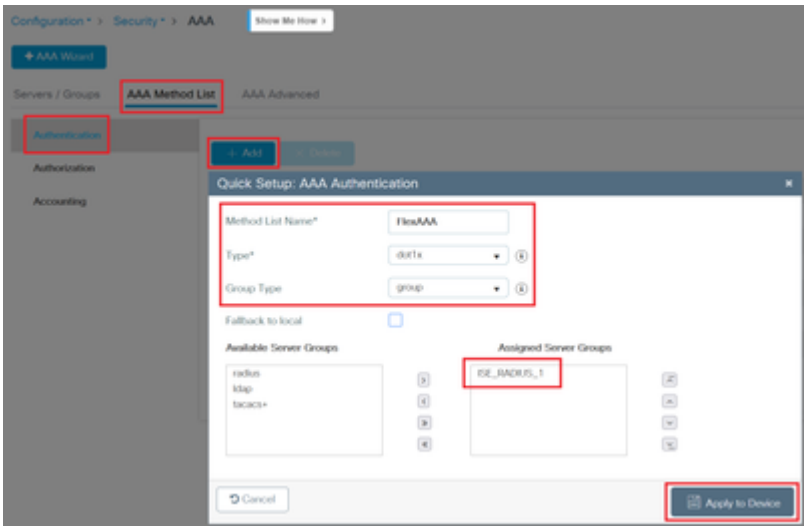
```
wireless profile flex Flex
ip http client proxy 0.0.0.0 0
local-auth radius-server-group ISE_RADIUS_1
vlan-name client
vlan-id 76
vlan-name VLAN1414
vlan-id 1414
vlan-name VLAN1432
vlan-id 1432
vlan-name management-interface
vlan-id 39
pmk propagate
!
wireless tag site Flex-site
ap-profile default-ap-profile
no local-site
flex-profile Flex
!
ap h.h.h (AP Radio MAC address)
policy-tag default-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

Configurar a WLAN 802.1x com autenticação local usando um servidor RADIUS externo

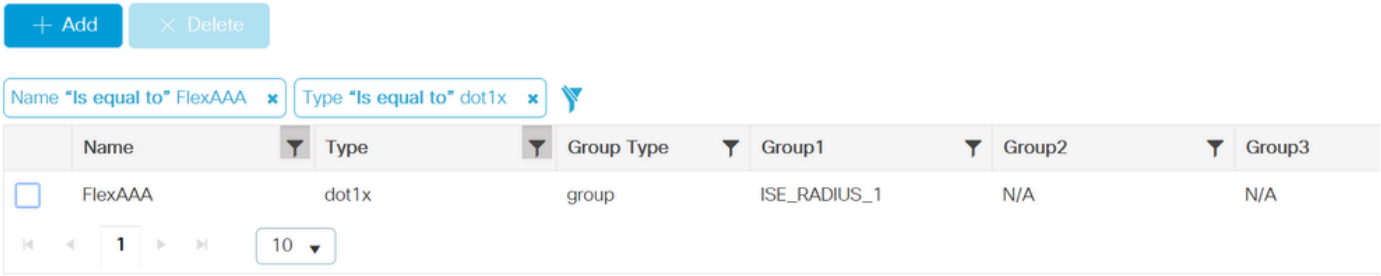
Etapa 1. Criar a lista de métodos de autenticação.

Navegue para Configuration > Security > AAA, na guia AAA Method List > Authentication.

Selecione +Add, dê um nome ao nome da lista de métodos, selecione dot1x como tipo, selecione group como tipo de grupo e atribua o grupo de servidores AAA na coluna Assigned Server Groups:



Agora você verá a lista de métodos AAA criada:



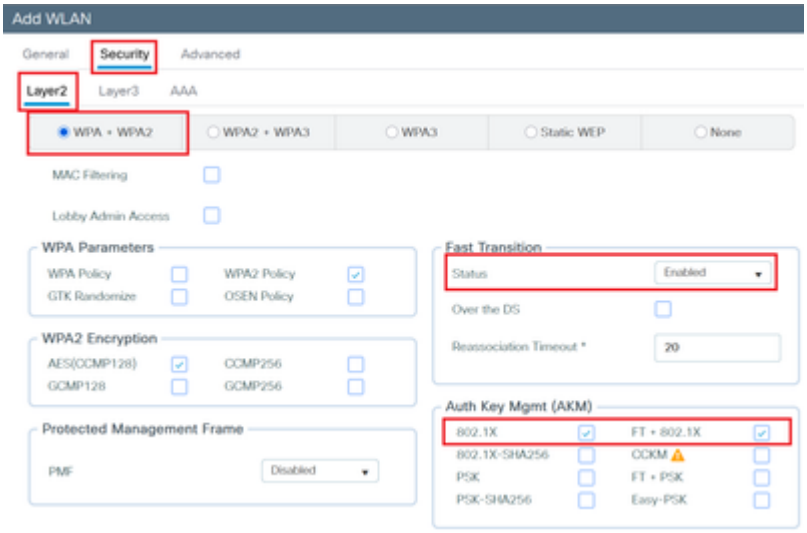
Etapa 2. Criar a WLAN.

Navegue até Configuration > Tags & Profiles > WLANs, selecione +Add.

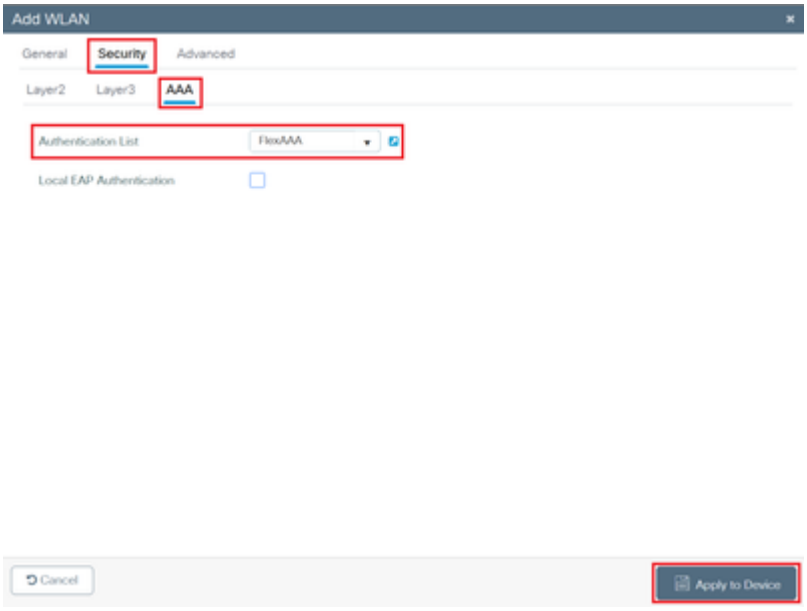
Na marca General, crie um nome para o Profile Name, SSID e habilite Status:



Etapa 3. Navegue até a guia Security > Layer 2, selecione WPA+WPA2 (Wi-Fi Protected Access), Fast Transition as Enabled, Auth Key Mgmt 802.1X and FT+802.1X:



Etapa 4. Navegue até a guia Security > AAA, no menu suspenso Authentication List, selecione a lista criada anteriormente:



Clique em Update & Apply to Device.

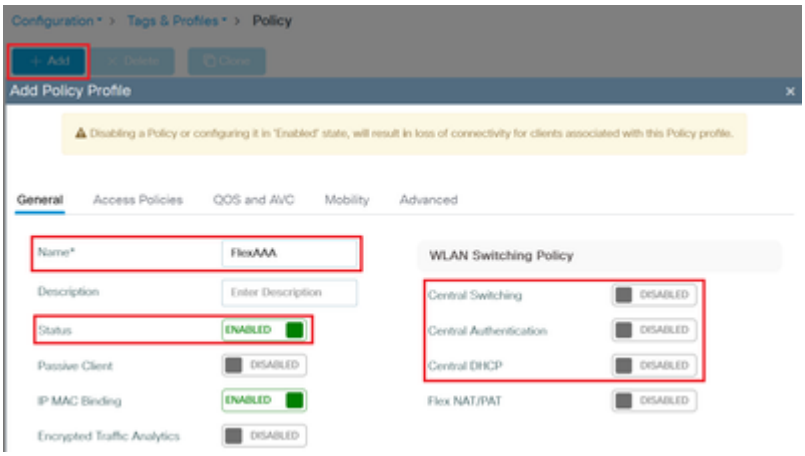
Em seguida, você verá a WLAN criada:



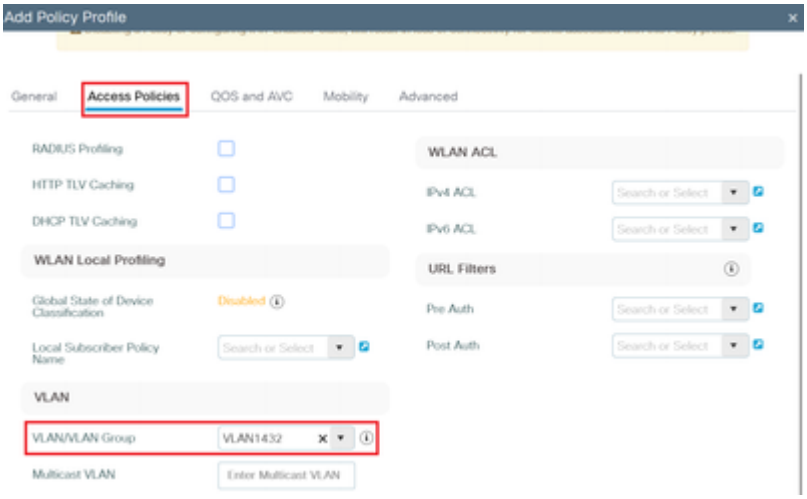
Etapa 5. Criar o Perfil de Política.

Navegue até Configuration > Tags & Profiles > Policy.

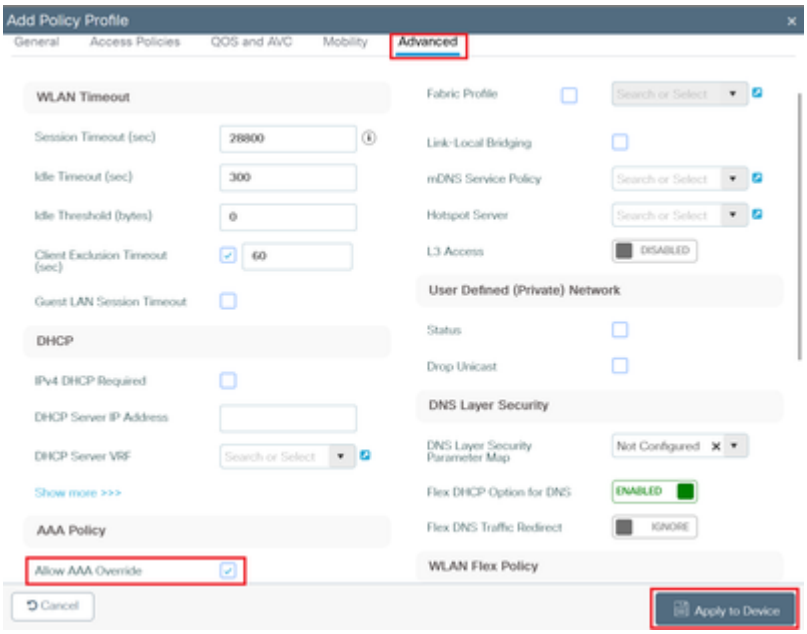
Selecione +Add e, na guia General, atribua um nome ao perfil de política, habilite o status e desabilite a comutação central, a autenticação central e o DHCP central (Dynamic Host Configuration Protocol):



Etapa 6. Navegue até a guia Access Policies, selecione a VLAN:

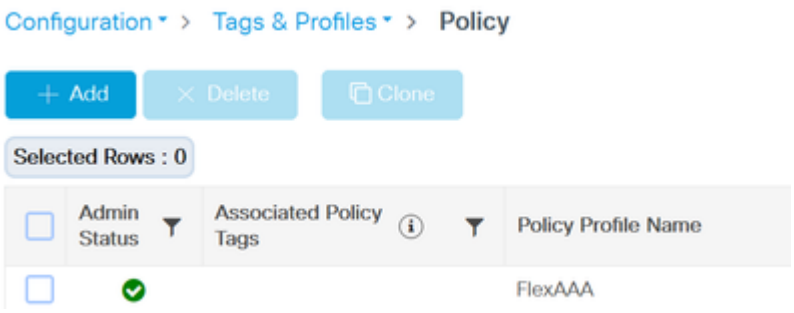


Etapa 7. Navegue até a guia Advanced, habilite Allow AAA Override.:



Clique em Update & Apply to Device.

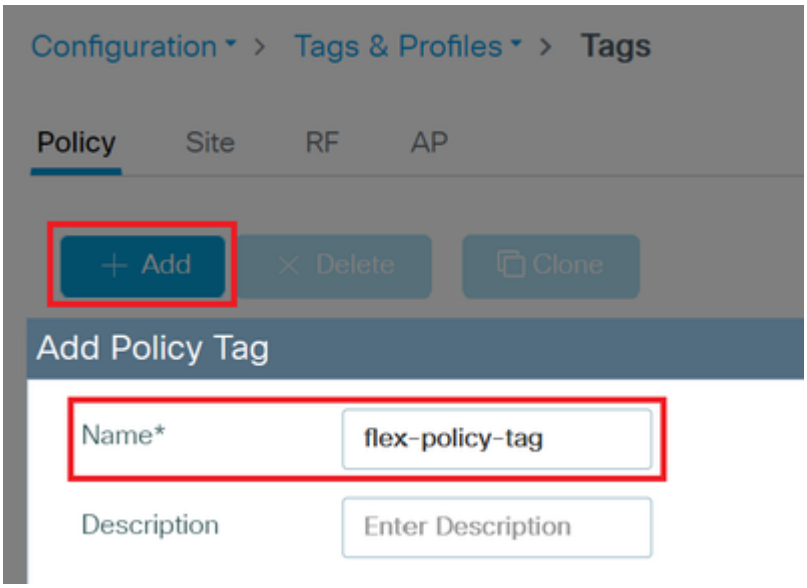
Você pode ver o perfil da regra na lista:



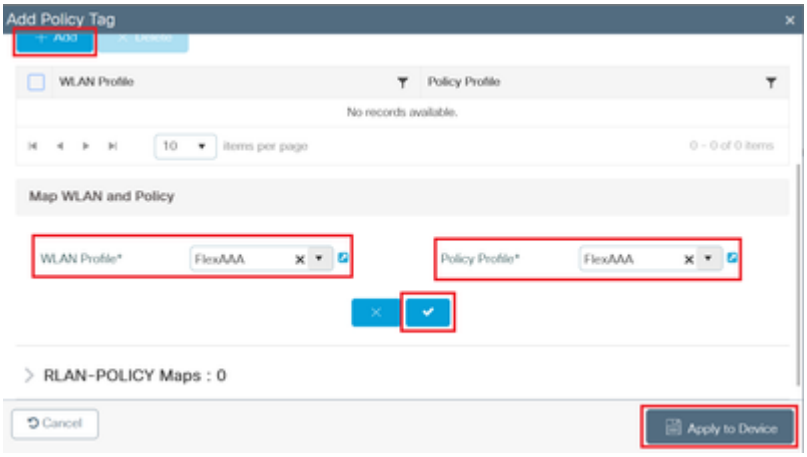
Etapa 8. Criar Tag de Política.

Navegue até Configuração > Marcas e perfis > Marcas

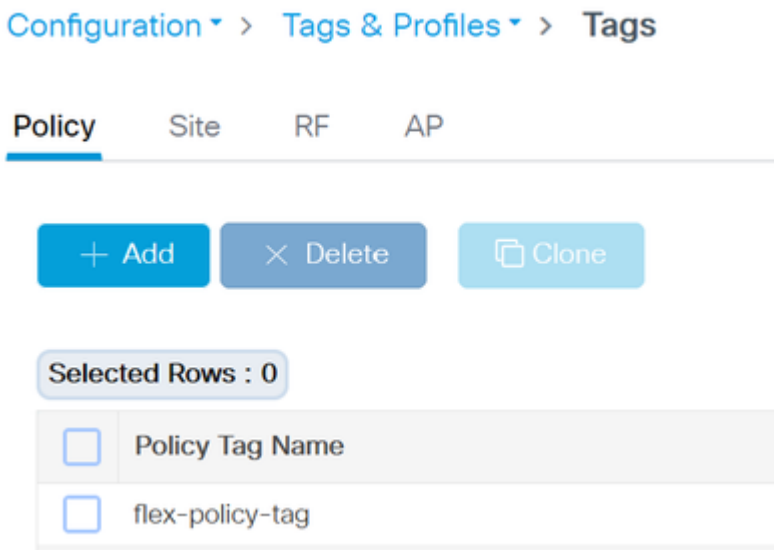
Na guia Política, selecione +Adicionar. Dê um nome à Marca de Diretiva:



Role para baixo e selecione +Add em WLAN-POLICY Maps. Em Perfil de WLAN, selecione a WLAN criada anteriormente no menu suspenso. Em Perfil de diretiva, selecione o Perfil de diretiva criado anteriormente no menu suspenso. Clique no botão de seleção e, em seguida, em Aplicar ao dispositivo:

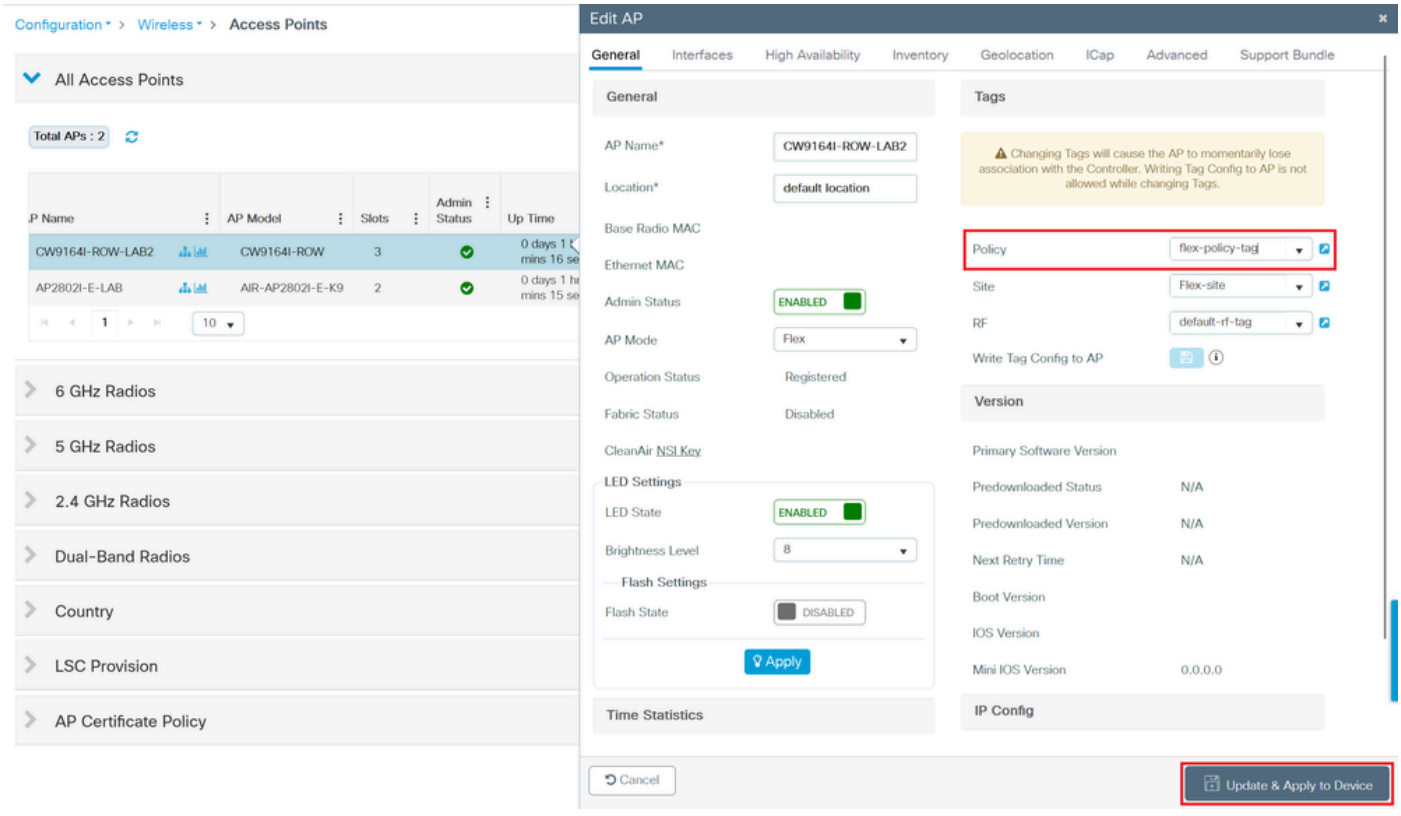


Você pode ver a tag policy na lista:



Etapa 9. Atribua a tag policy na tag APs.

Navegue até Configuration > Wireless > Access Points. Selecione o AP para alterar a marca.

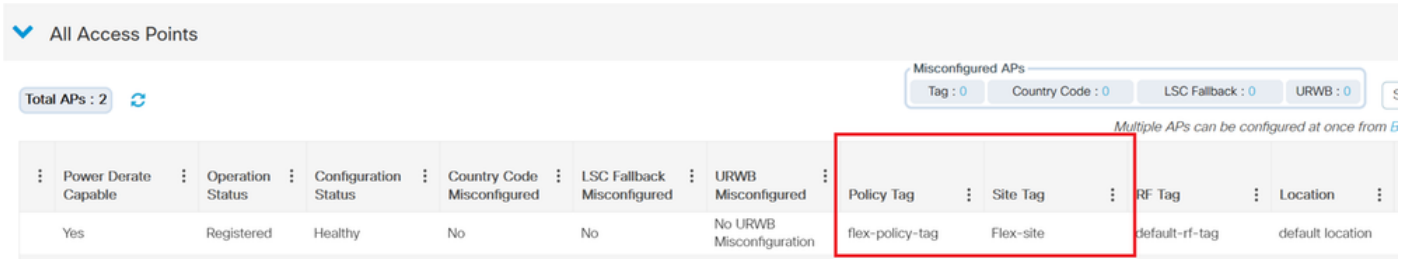


Clique em Update & Apply to Device.

O AP se desjunta e se junta novamente com a nova marca de política.

Quando o AP se une novamente, você pode verificar a lista de Pontos de acesso, confirmar se o

AP está no modo Flex e as tags atribuídas:



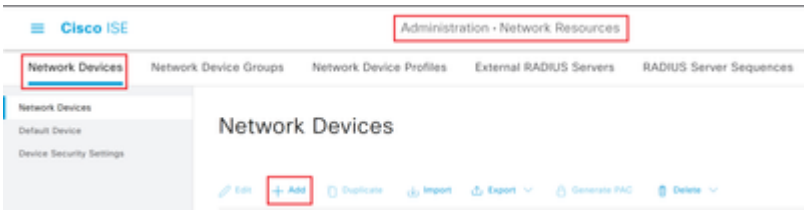
CLI:

```
aaa authentication dot1x FlexAAA group ISE_RADIUS_1
!
wlan FlexAAA 4 FlexAAA
radio policy dot11 24ghz
radio policy dot11 5ghz
security ft
security wpa akm ft dot1x
security dot1x authentication-list FlexAAA
no shutdown
!
wireless profile policy FlexAAA
aaa-override
no central authentication
no central dhcp
no central switching
vlan VLAN1432
no shutdown
!
wireless tag policy flex-policy-tag
wlan FlexAAA policy FlexAAA
!
ap h.h.h (AP Radio MAC address)
policy-tag flex-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

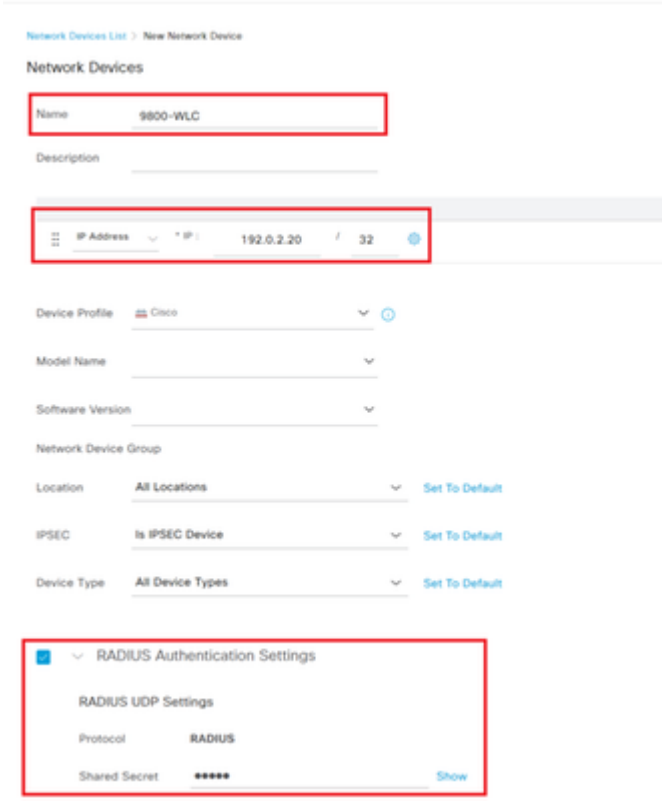
Configurar o ISE

Agora você precisa configurar o ISE para poder autenticar clientes quando eles estiverem na autenticação local.

Etapa 1.Navegue até Administração > Recursos de rede > Dispositivos de rede. Selecione +Adicionar.



Etapa 2. Adicionar a WLC 9800. Dê um nome a ele, adicione seu endereço IP, habilite as Configurações de Autenticação RADIUS e adicione a Chave Secreta Compartilhada. Essa chave deve ser a mesma que você configurou anteriormente quando criou os servidores AAA na WLC 9800.



No canto inferior direito, clique em Save.

Etapa 3. Precisamos adicionar os APs na lista de dispositivos de rede, para que eles possam agir como autenticadores/encaminhadores AAA quando o local remoto perder o link da WAN (e quando os APs moverem para o modo independente).

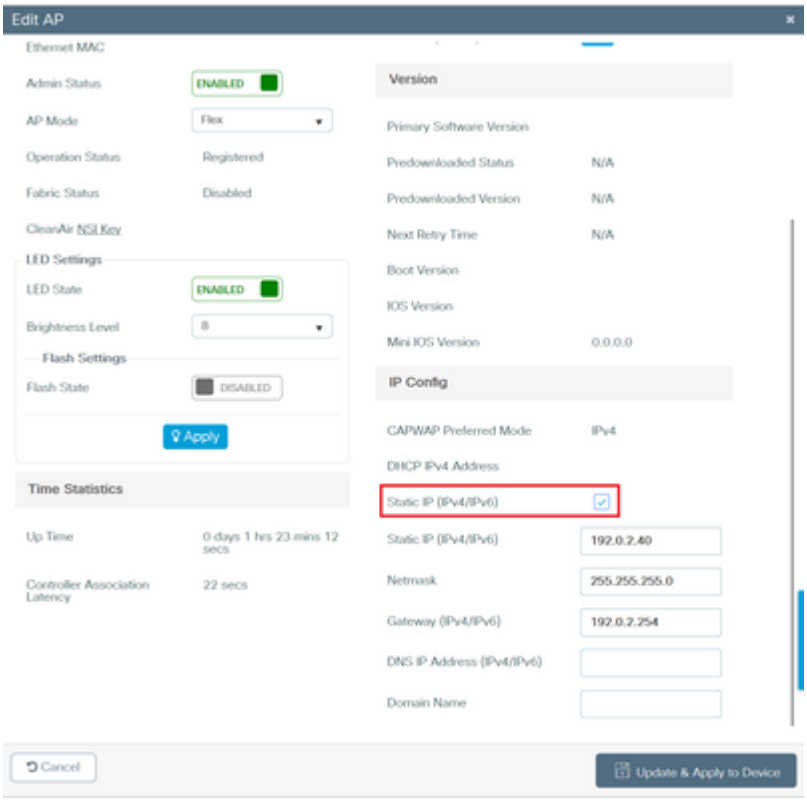
Navegue para Configuration > Wireless > Access Points na GUI da WLC 9800 e anote os endereços IP de cada AP.

Note: Configure o endereço IP de cada AP Flex como Static. Quando os APs perdem e

---

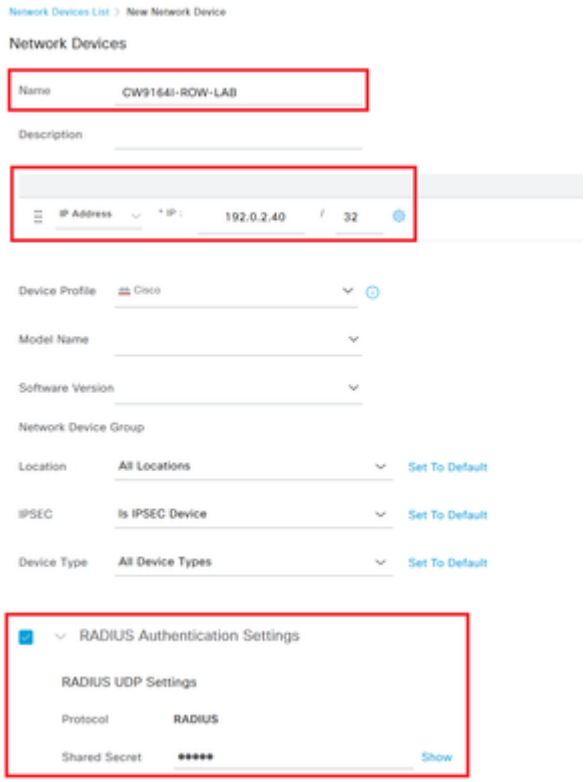
recuperam a conexão com a WLC 9800, eles podem voltar com um endereço IP diferente do DHCP e, portanto, perder a comunicação com o ISE.

Habilite o IP estático (IPv4/IPv6). Clique em Update & Apply to Device:



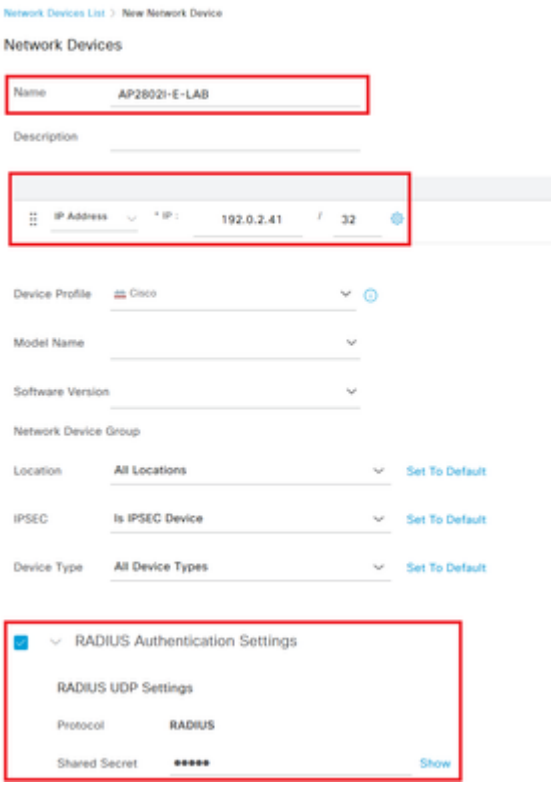
Etapa 4. Voltar no ISE, navegue até Administração > Recursos de rede > Dispositivos de rede. Selecione +Adicionar.

Adicione seus APs como dispositivos de rede, a mesma configuração que a WLC 9800:



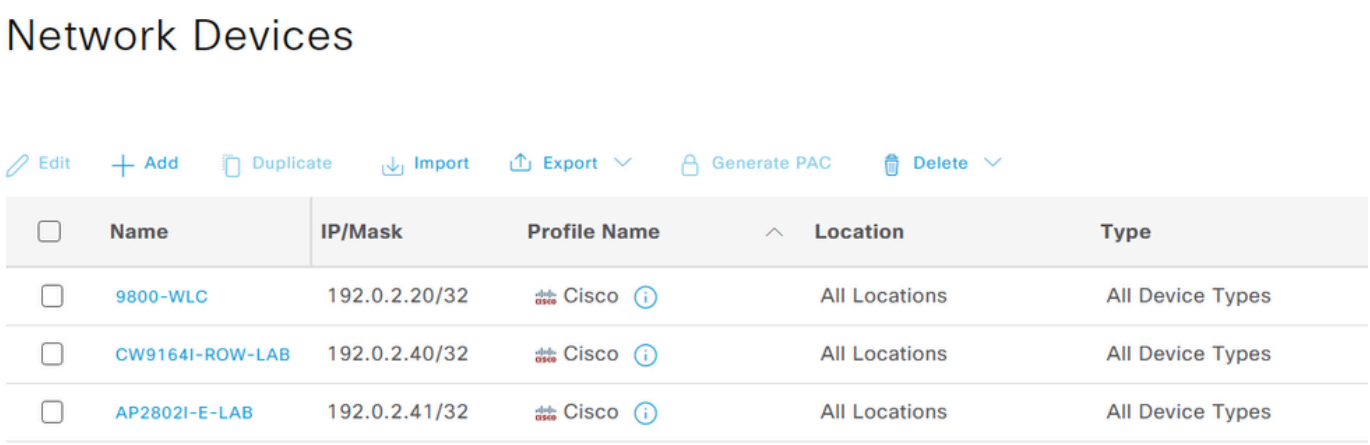
No canto inferior direito, clique em Save.

Para o segundo AP:



No canto inferior direito, clique em Save.

Você pode ver esta lista de dispositivos de rede:

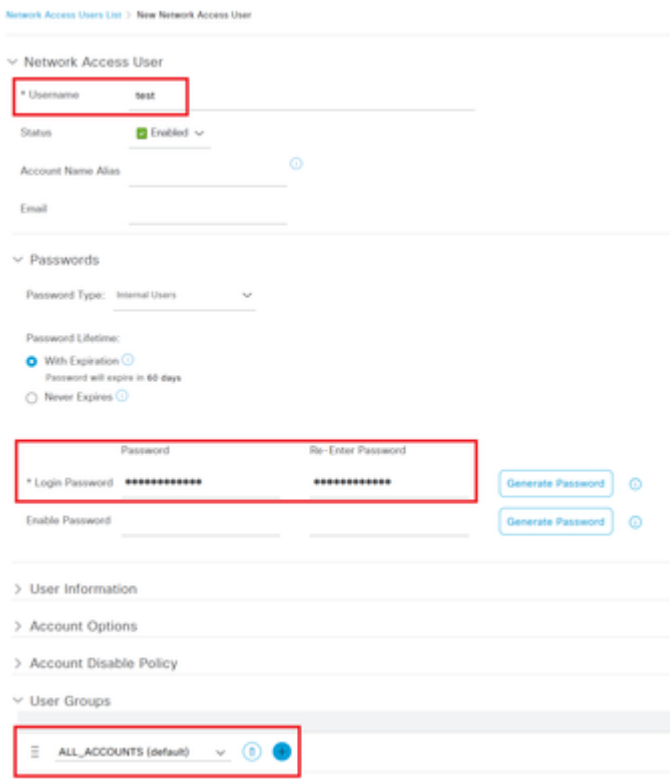


Se seus APs estiverem em intervalos de IP contíguos, você poderá usar o recurso de máscara para configurar uma única entrada que defina o segredo compartilhado para um grupo inteiro (se não todos) de APs. Não há necessidade real de configurar um dispositivo de rede por AP no ISE. Observe, no entanto, que usando curingas e máscaras, você deixa algum espaço para um dispositivo invasor tentar atuar como encaminhador para o ISE.

Etapa 5. Navegue até Administration > Identity Management > Identities, na guia Users, e crie um usuário para a autenticação 802.1x. Selecione +Adicionar:

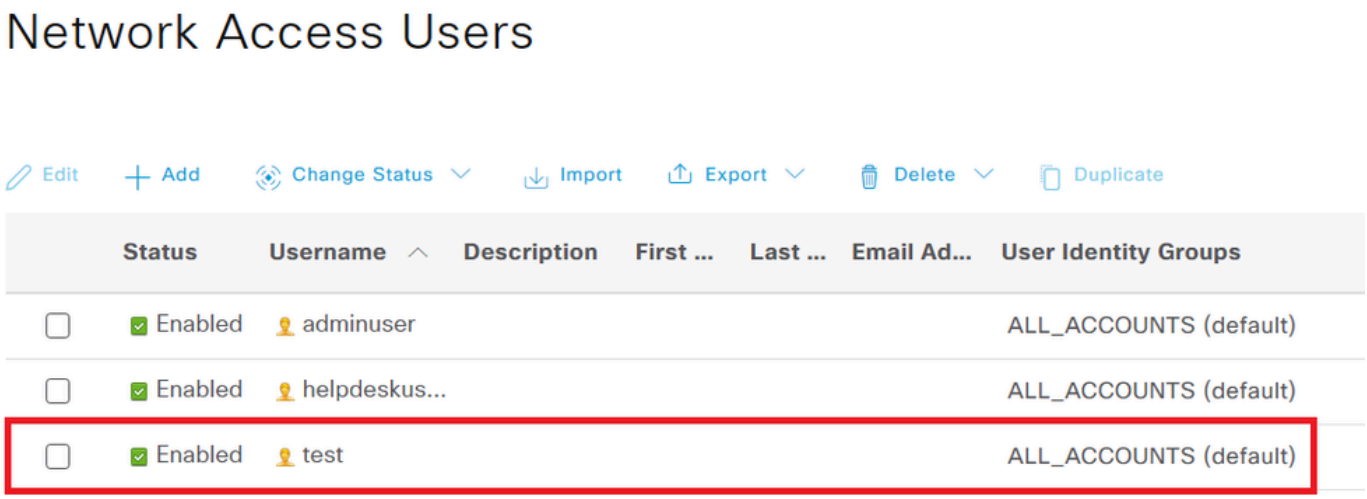


Crie um nome de usuário, a senha (e digite a mesma senha em Insira a senha novamente) e selecione ALL_ACCOUNTS (padrão) no menu suspenso Grupos de usuários:

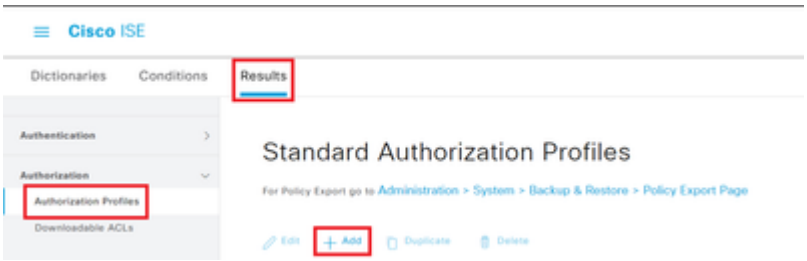


No canto inferior direito, clique em Enviar.

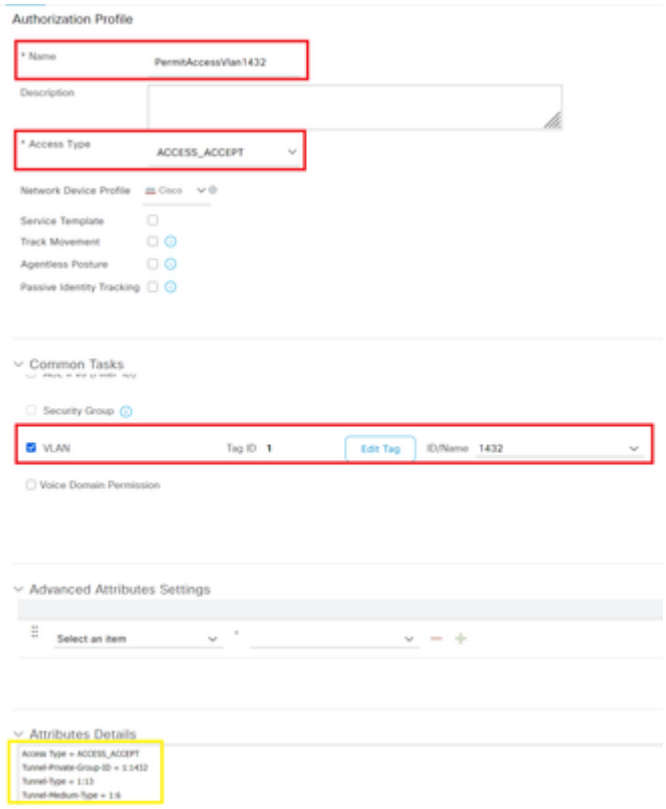
Você pode ver o usuário na lista Usuários com acesso à rede:



Etapa 6. Navegue até Política > Elementos de Política > Resultados. Na guia Authorization > Authorization Profiles, selecione +Add.



Crie o perfil de autorização para a VLAN à qual os clientes de autenticação local estão atribuídos:

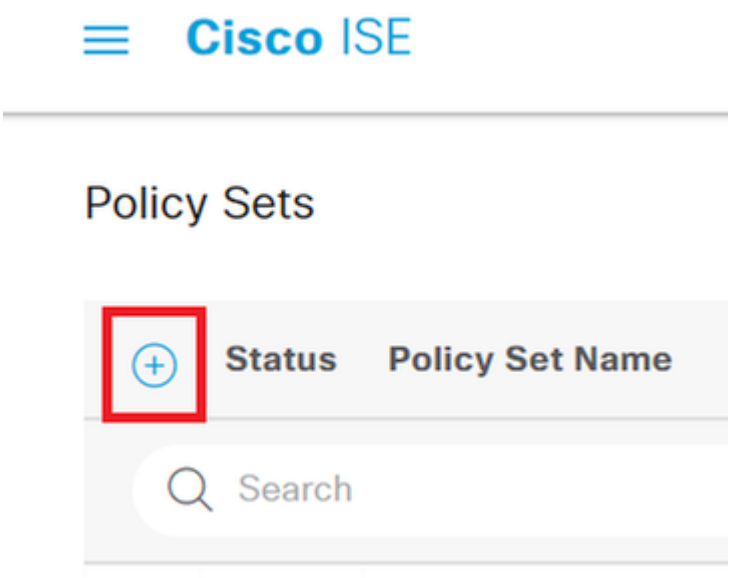


No canto inferior direito, clique em Enviar.

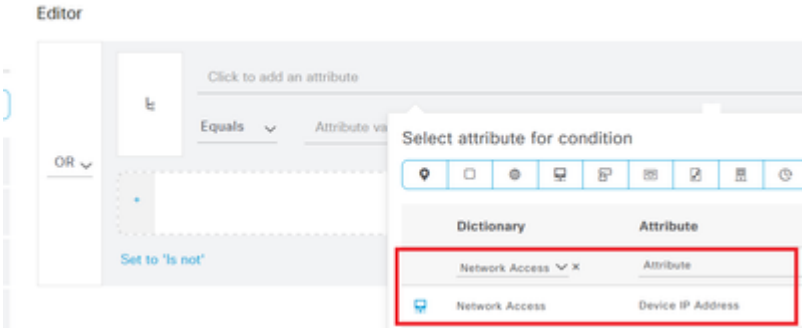
Você vê os detalhes dos atributos que o ISE envia para os WLC/APs em um cenário de sucesso.

Etapa 7. Navegue até Política > Conjuntos de Políticas. Crie um novo conjunto de políticas.

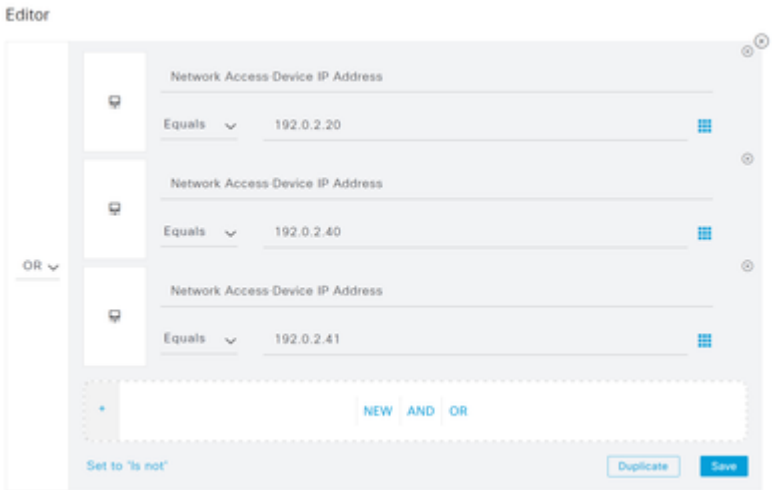
Clique no sinal +:



Dê um nome ao conjunto de políticas. Na coluna Condições, adicione a regra OU e adicione o dicionário Acesso à rede, com o Atributo Endereço IP do dispositivo, selecione Iguais a:

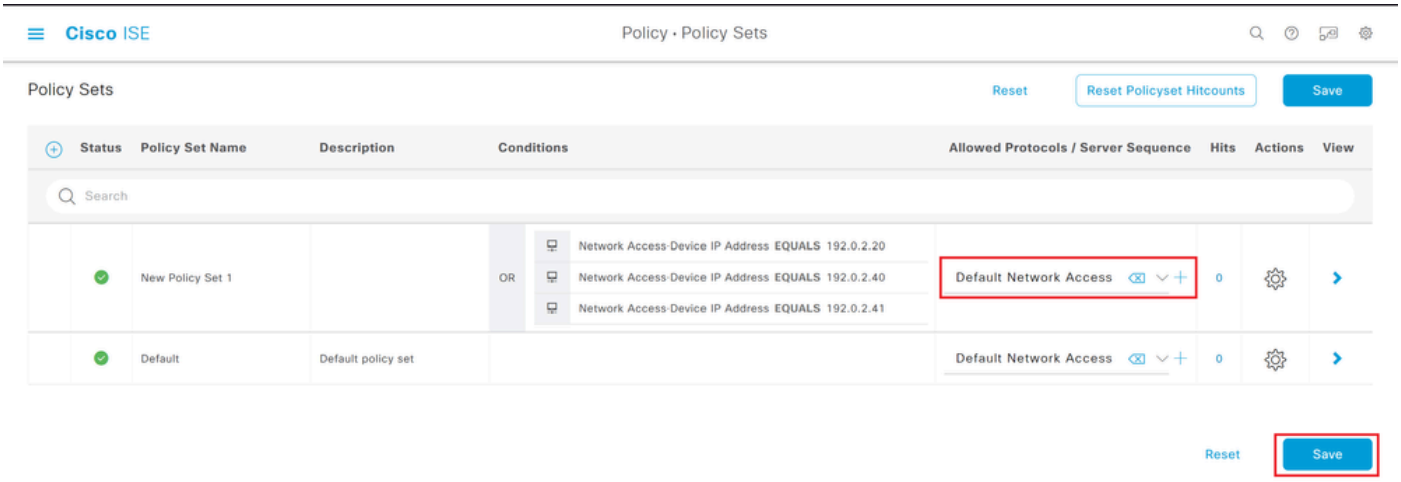


Adicione os endereços IP da WLC 9800 e dos APs:

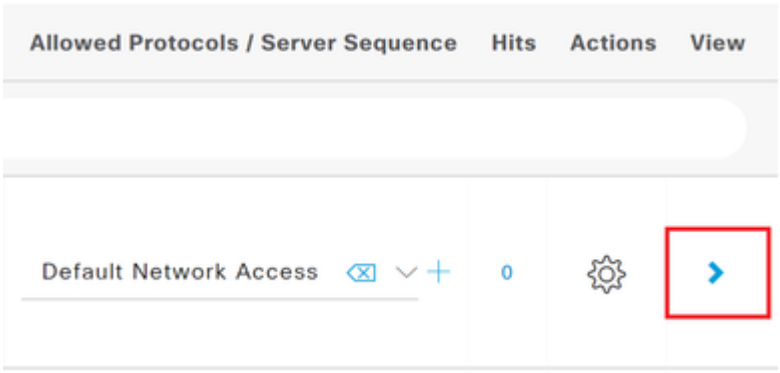


No canto inferior direito, clique em Usar.

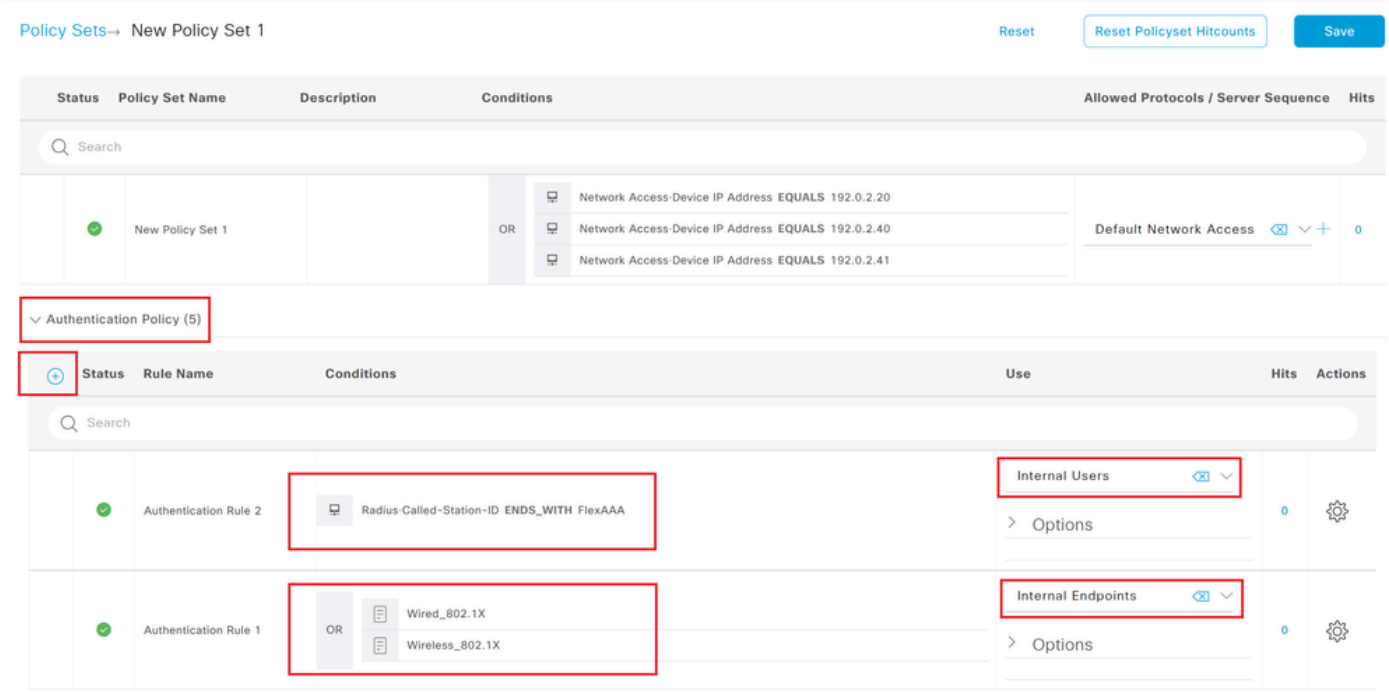
Etapa 8. Na coluna Allowed Protocols, selecione Default Network Access. No final, clique em Salvar:



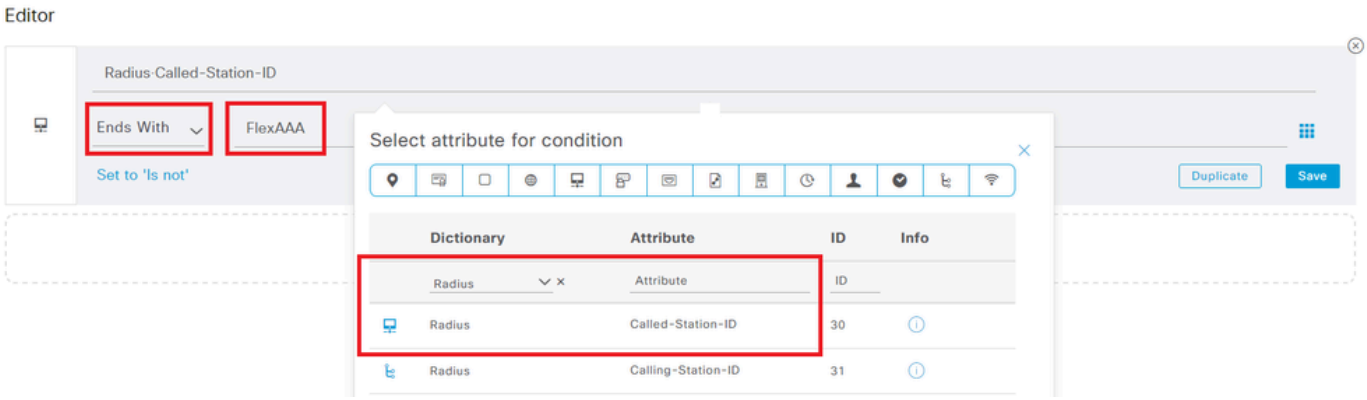
Etapa 9. Na coluna View, clique no sinal de seta:



Etapa 10. Expanda Authentication Policy, crie duas novas políticas: uma para o nome da WLAN e a outra para a configuração 802.1X:

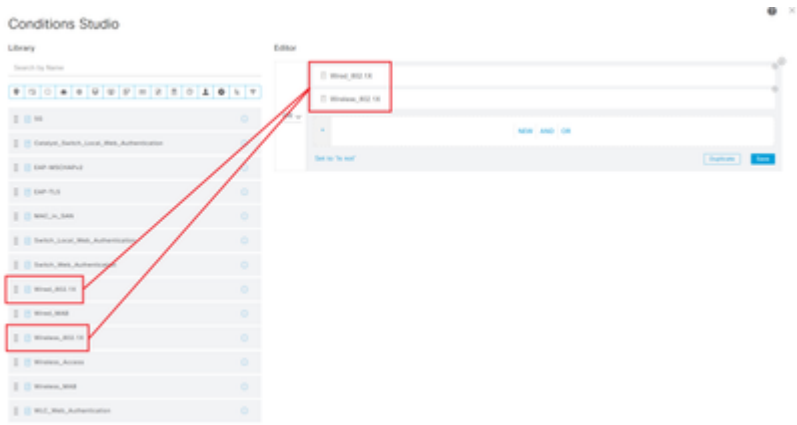


Para o nome da WLAN, crie a condição com o dicionário Radius e o atributo Called-Station-ID. Selecione Termina com e digite o nome da WLAN:



No canto inferior direito, clique em Usar. Para esta política, na coluna Uso, selecione Usuários internos.

Etapa 11. Para a política 802.1X, crie a condição com a biblioteca Wired_802.1X e Wireless_802.1X disponível no ISE. Você pode arrastar e soltar esses itens e selecionar a condição OU:



No canto inferior direito, clique em Usar. Para esta política, na coluna Use, selecione Internal Endpoints.

Etapa 12. Role para baixo até Authorization Policy e crie uma nova política. Dê um nome a ele e crie a mesma Condição criada para o nome da WLAN na Política de autenticação.

Na coluna Profiles, selecione no menu suspenso o perfil PermitAccessVlan1432:



No canto inferior direito, clique em Save.

Configurar a WLAN PSK com autenticação local

Etapa 1. Primeiro configure os APs no modo Flex, conforme descrito na seção Configurar o modo FlexConnect no site remoto.

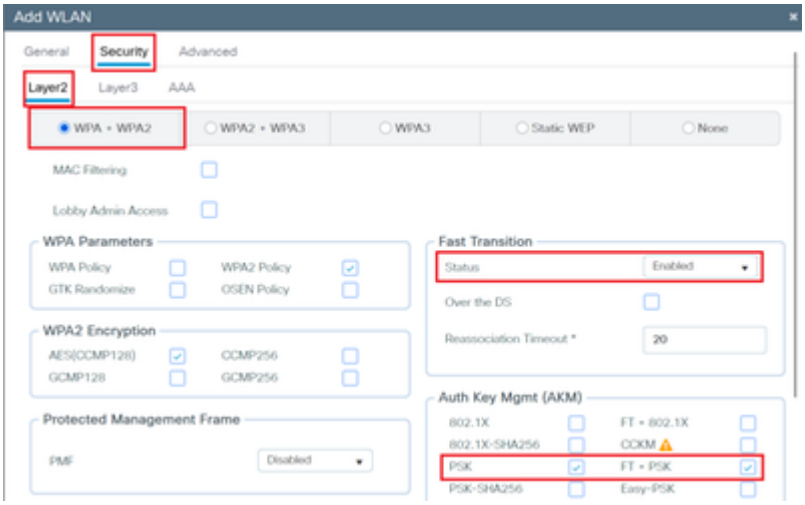
Etapa 2. Criar a WLAN.

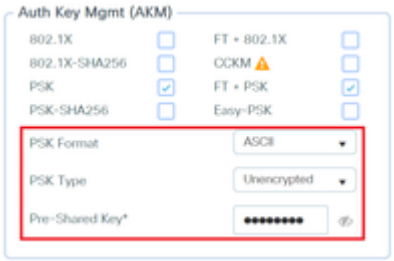
Navegue até Configuration > Tags & Profiles > WLANs, selecione +Add.

Na marca General, crie um nome para o Profile Name, SSID e habilite Status:



Etapa 3. Navegue até a guia Security > Layer 2 e selecione WPA+WPA2, Fast Transition as Enabled, Auth Key Mgmt PSK e FT+PSK, escolha o formato PSK e o tipo PSK desejados e digite a chave pré-compartilhada que seus clientes devem usar:





Clique em Update & Apply to Device.

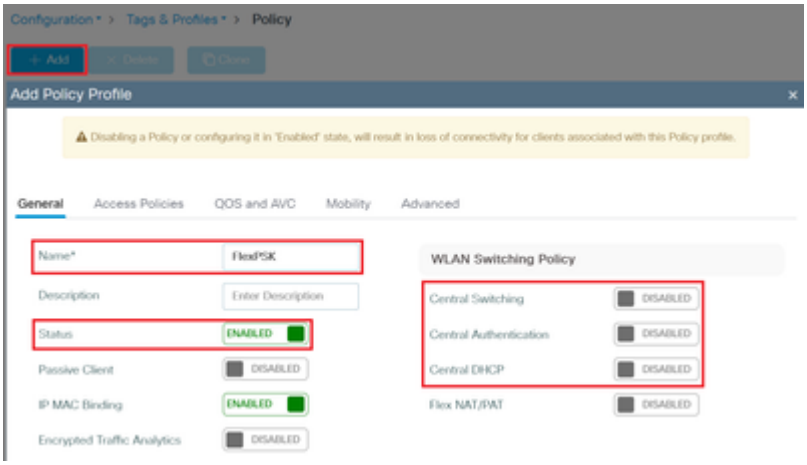
Você pode ver a WLAN criada:



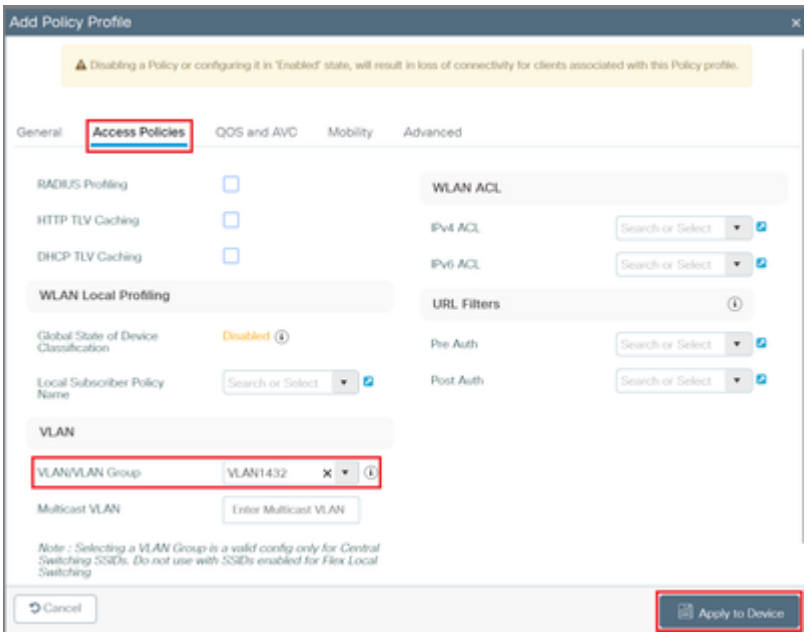
Etapa 4. Criar o Perfil de Política.

Navegue até Configuration > Tags & Profiles > Policy.

Selecione +Add e, na guia General, atribua um nome ao perfil de diretiva, habilite o status e desabilite a comutação central, a autenticação central e o DHCP central:

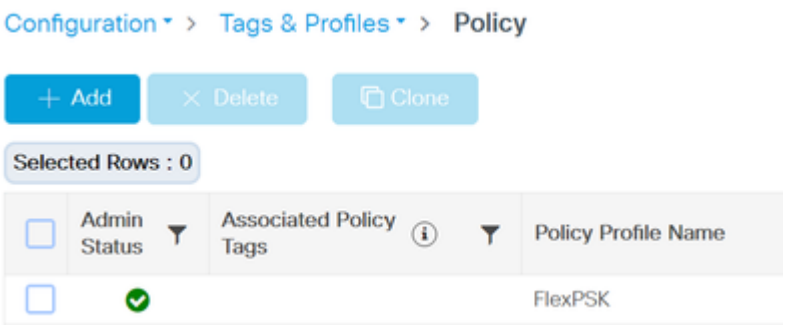


Etapa 5. Navegue até a guia Access Policies, selecione a VLAN:



Clique em Update & Apply to Device.

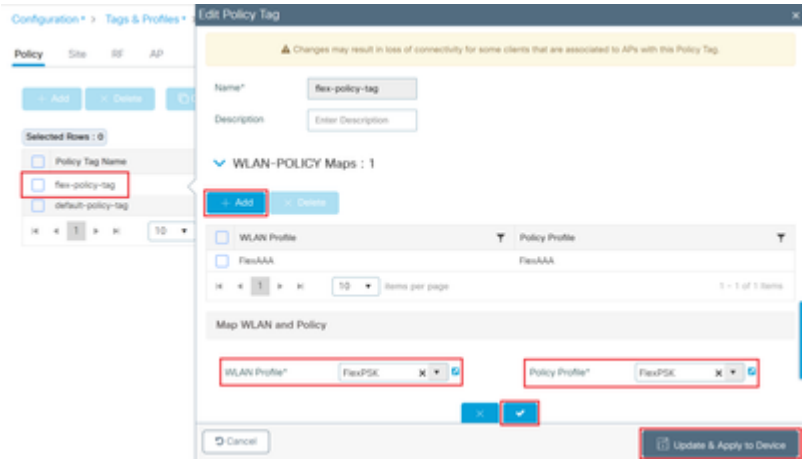
Você pode ver o perfil da regra na lista:



Etapa 6. Você pode criar uma nova tag Policy ou editar a existente.

Navegue até Configuration > Tags & Profiles > Tags para editar a tag policy existente. Selecione a tag a ser editada.

Selecione +Add em WLAN-POLICY Maps. Em Perfil de WLAN, selecione a WLAN criada anteriormente no menu suspenso. Em Perfil de diretiva, selecione o Perfil de diretiva criado anteriormente no menu suspenso. Clique no botão de seleção e, em seguida, em Aplicar ao dispositivo:



Se a etiqueta de política já estiver atribuída no AP, você não precisa fazer mais nada.

Caso contrário, atribua a tag policy na tag APs. Navegue até Configuration > Wireless > Access Points. Selecione o AP para alterar a tag de política e clique em "Atualizar e aplicar ao dispositivo".

O AP se desjunta e se junta novamente com a nova tag policy.

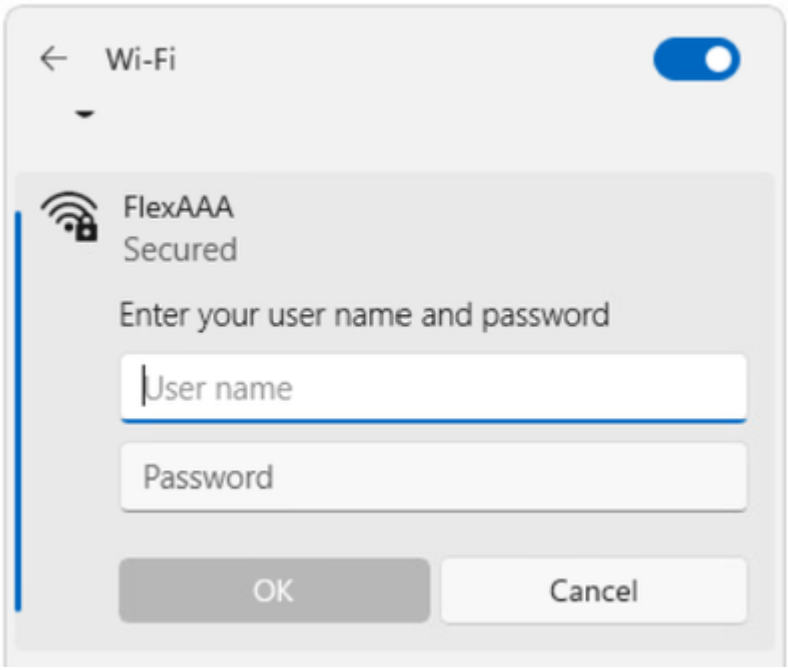
Quando o AP se une novamente, você pode verificar a lista de Pontos de acesso, confirmar se o AP está no modo Flex e se ele tem as tags atribuídas corretas.

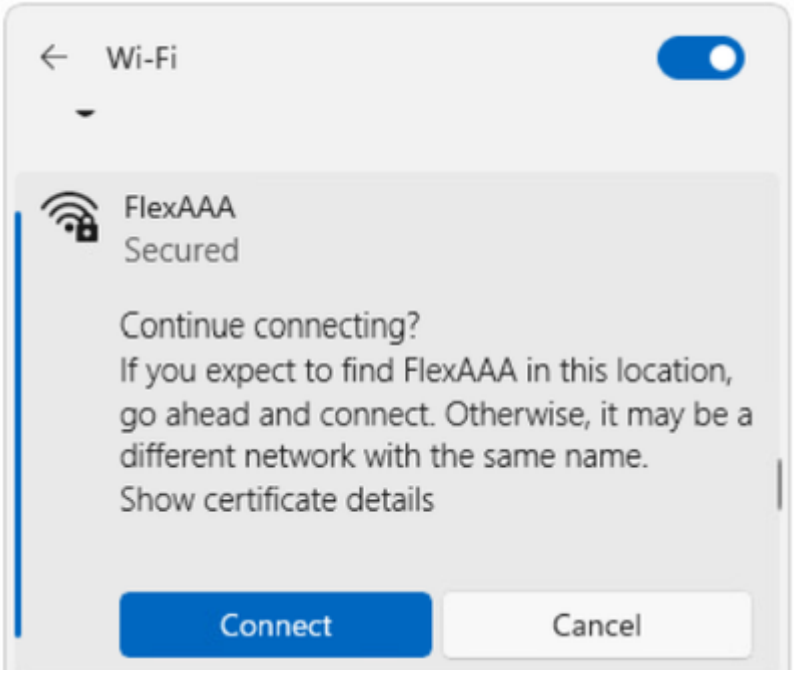
CLI:

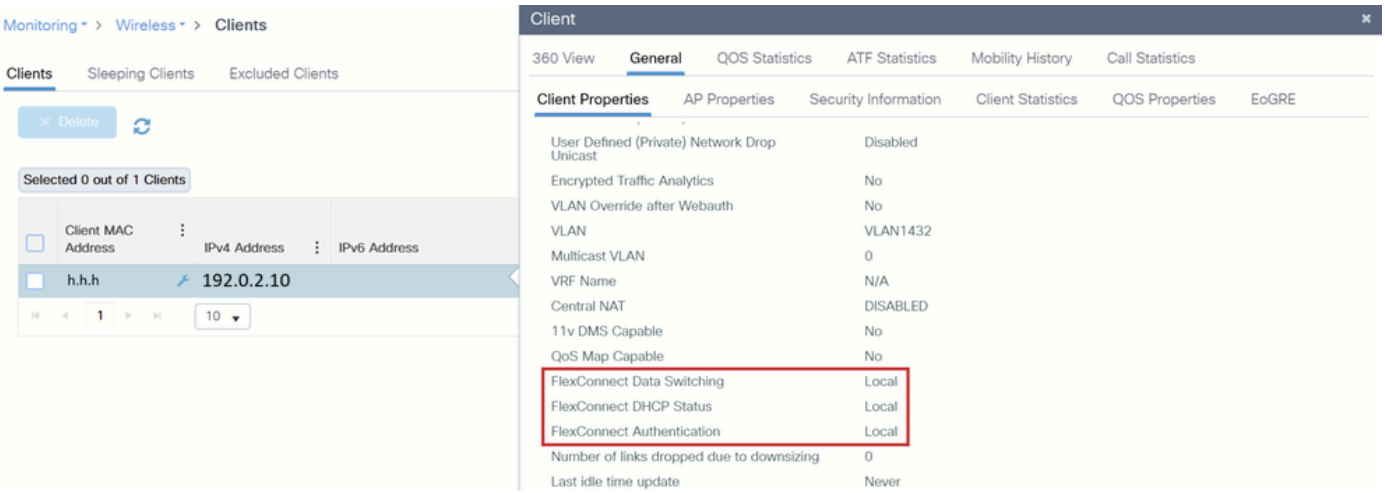
```
wlan FlexPSK 5 FlexPSK
radio policy dot11 24ghz
radio policy dot11 5ghz
security ft
security wpa psk set-key ascii 0 Password123
no security wpa akm dot1x
security wpa akm ft psk
security wpa akm psk
no shutdown
!
wireless profile policy FlexPSK
no central authentication
no central dhcp
no central switching
vlan VLAN1432
no shutdown
!
wireless tag policy flex-policy-tag
wlan FlexAAA policy FlexAAA
wlan FlexPSK policy FlexPSK
!
ap h.h.h (AP Radio MAC address)
policy-tag flex-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

Verificar

Para WLAN 802.1x:


Wi-Fi
FlexAAA
Secured
Enter your user name and password
User name
Password
OK
Cancel


Wi-Fi
FlexAAA
Secured
Continue connecting?
If you expect to find FlexAAA in this location, go ahead and connect. Otherwise, it may be a different network with the same name.
Show certificate details
Connect
Cancel


Monitoring > Wireless > Clients
Clients
Sleeping Clients
Excluded Clients
Delete
Selected 0 out of 1 Clients
Client MAC Address
IPv4 Address
IPv6 Address
h.h.h
192.0.2.10
1
10
Client
360 View
General
QOS Statistics
ATF Statistics
Mobility History
Call Statistics
Client Properties
AP Properties
Security Information
Client Statistics
QOS Properties
EoGRE
User Defined (Private) Network Drop Unicast
Disabled
Encrypted Traffic Analytics
No
VLAN Override after Webauth
No
VLAN
VLAN1432
Multicast VLAN
0
VRF Name
N/A
Central NAT
DISABLED
11v DMS Capable
No
QoS Map Capable
No
FlexConnect Data Switching
Local
FlexConnect DHCP Status
Local
FlexConnect Authentication
Local
Number of links dropped due to downsizing
0
Last idle time update
Never

CLI:

```
C9800-1#show wireless client mac-address      h.h.h        detail

Client MAC Address : h.h.h
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address :192.0.2.10
Client IPv6 Addresses :
Client Username : test
AP MAC Address :
AP Name: CW9164I-ROW-LAB2
AP slot : 1
Client State : Associated
Policy Profile : FlexAAA
Flex Profile : Flex
Wireless LAN Id: 4
WLAN Profile Name: FlexAAA
Wireless LAN Network Name (SSID): FlexAAA
BSSID :
Connected For : 134 seconds
Protocol : 802.11ac
Channel : 48
Client IIF-ID : 0xa0000001
Association Id : 33
```

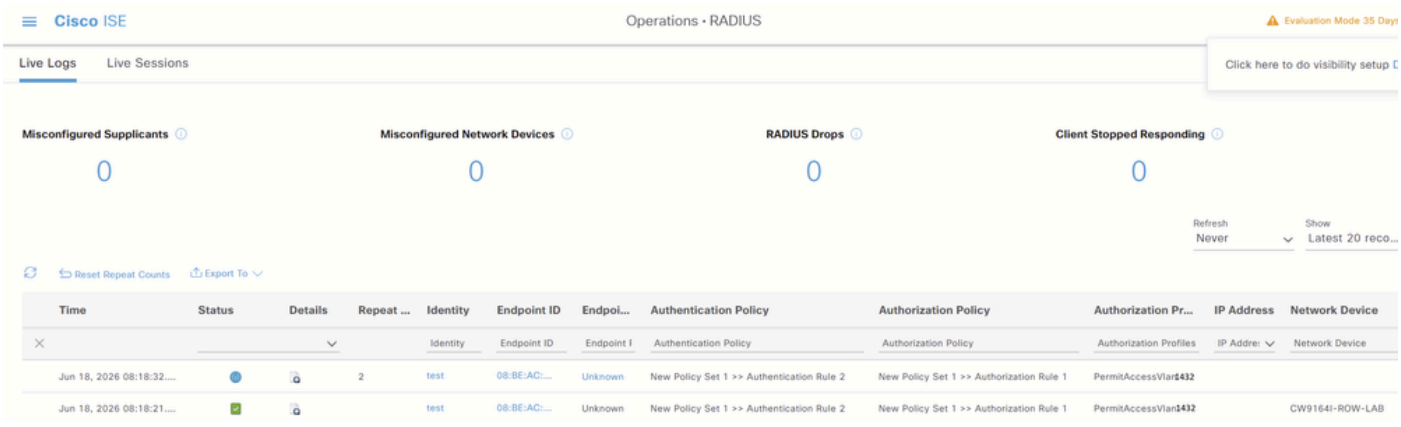
```
QoS Map Capable : No
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Local
Client Statistics:
```

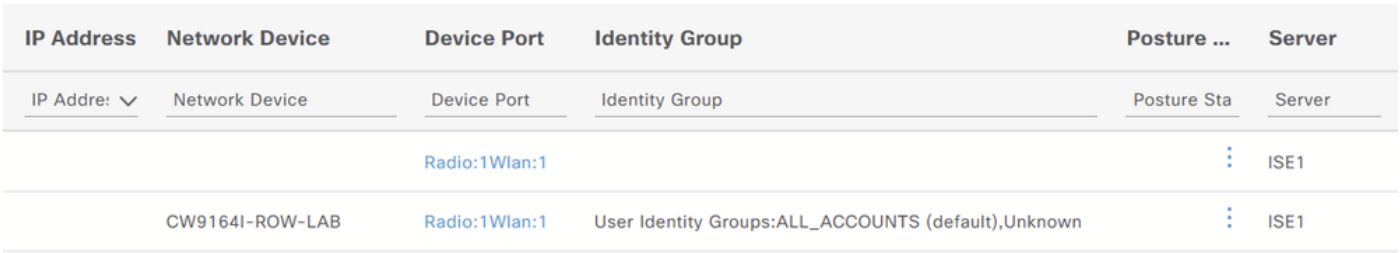
Na CLI do AP:

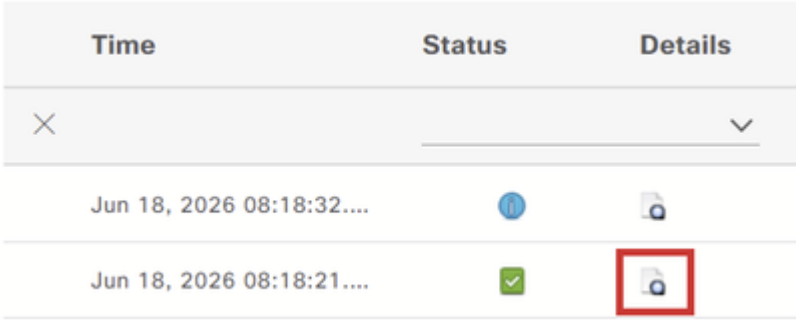
```
CW9164I-ROW-LAB#show dot11 clients

Total dot11 clients: 1
      Client MAC    Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH          1       1  33   FlexAAA  -45 MCS9ISS           No         No
```

No ISE







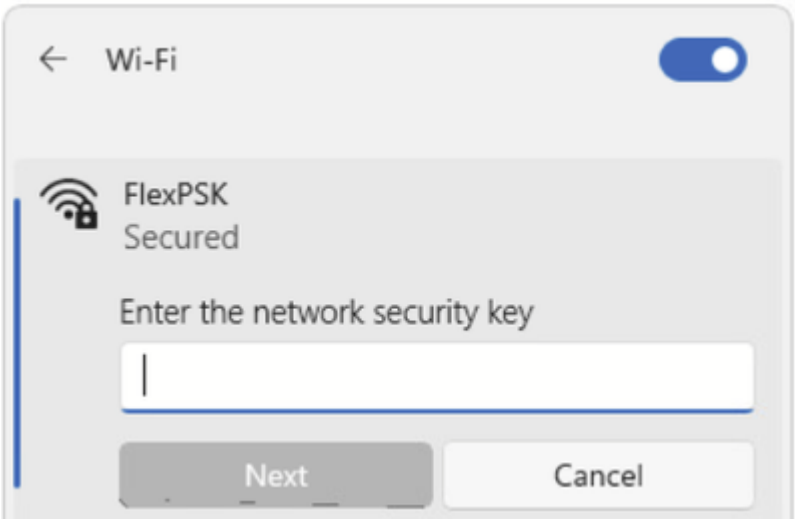
Cisco ISE

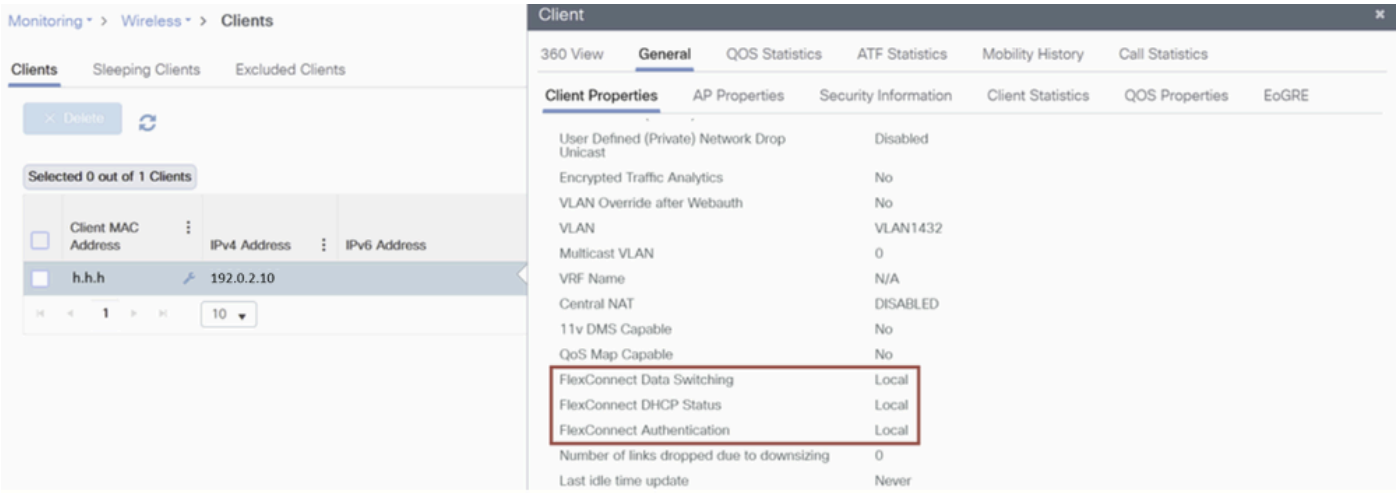
Overview

Event	5200 Authentication succeeded
Username	test
Endpoint Id	HH:HH:HH:HH:HH:HH
Endpoint Profile	Unknown
Authentication Policy	New Policy Set 1 >> Authentication Rule 2
Authorization Policy	New Policy Set 1 >> Authorization Rule 1
Authorization Result	PermitAccessVlan1432

Authentication Identity Store	Internal Users
Identity Group	User Identity Groups:ALL_ACCOUNTS (default),Unknown
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	CW9164I-ROW-LAB
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	192.0.2.40
NAS Port Id	Radio:1Wlan:1
NAS Port Type	Wireless - IEEE 802.11
Authorization Profile	PermitAccessVlan1432
Response Time	64 milliseconds

Para WLAN PSK:





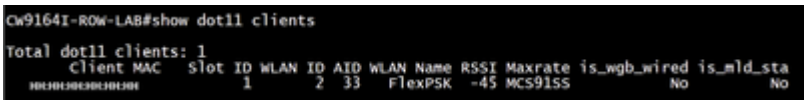
CLI:

```
C9800-1#show wireless client mac-address h.h.h detail

Client MAC Address : h.h.h
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address : 192.0.2.10
Client IPv6 Addresses :
Client Username: N/A
AP MAC Address :
AP Name: CW9164I-ROW-LAB2
AP slot : 1
Client State : Associated
Policy Profile : FlexPSK
Flex Profile : Flex
Wireless LAN Id: 5
WLAN Profile Name: FlexPSK
Wireless LAN Network Name (SSID): FlexPSK
BSSID :
Connected For : 116 seconds
Protocol : 802.11ac
Channel : 48
Client IIF-ID : 0xa0000001
Association Id : 33
```

```
QoS Map Capable : No
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Local
Client Statistics:
```

No AP CLI:



Troubleshooting

Ative as depurações de AP e o rastreamento de RA com o endereço MAC do cliente, em sincronia.

No AP, habilite estas depurações:

debug flexconnect event
debug flexconnect pmk
debug flexconnect dot11r
debug dot11 client management information
debug dot11 client management critical
debug dot11 client management errors
debug dot11 client management events

Para WLAN 802.1x:

Logs de depuração de AP com autenticação bem-sucedida:

O AP lida com a máquina de estado 802.11 e o gerenciamento de chave local.
O AP processa a associação e prepara o cliente para a autenticação.

```
[*06/19/2026 06:49:00.1836] CLSM[HH:HH:HH:HH:HH:HH]: client moved from UNASSOC to AUTH
[*06/19/2026 06:49:00.1890] wcp/flex_roam_st :: Flexconnect 11r enabled for client HH:HH:HH:HH:HH:HH
[*06/19/2026 06:49:00.1908] CLSM[HH:HH:HH:HH:HH:HH]: client moved from AUTH to ASSOC
[*06/19/2026 06:49:00.1909] Sending ADD MOBILE to client SM for local auth client mac HH:HH:HH:HH:HH:HH
[*06/19/2026 06:49:00.1931] CLSM[HH:HH:HH:HH:HH:HH]: client moved from ASSOC to 8021X
```

O AP processa a autorização, aplica a substituição de VLAN e move o cliente para o estado FWD (Encaminhamento).

```
[*06/19/2026 06:49:20.3601] received WCP_EVENT_CLIENT_AUTHORIZE (non) roaming case clearing roam flags
[*06/19/2026 06:49:20.3601] CLSM[HH:HH:HH:HH:HH:HH]: WCP_EVENT_CLIENT_AUTHORIZE : Plumbing key info to
```

```
[*06/19/2026 06:49:20.3612] wcp/flex_roam_st :: Flexconnect AAA Override Vlan with WLAN mapping: 1432 f
[*06/19/2026 06:49:20.3625] CLSM[HH:HH:HH:HH:HH:HH]: client moved from 8021X to IPLEARN_PENDING
[*06/19/2026 06:49:20.3627] wcp/flex_roam_st :: Flexconnect Sending HREAP_APAUTH_CLIENT_ADD
[*06/19/2026 06:49:20.3627] CLSM[HH:HH:HH:HH:HH:HH]: Retrieved key for FT+FT_DOT1X algono: 8, vlanId: 1
[*06/19/2026 06:49:20.3627] CLSM[HH:HH:HH:HH:HH:HH]: Local auth (Add) on radio 1 Vap 0 reported to WLC
[*06/19/2026 06:49:20.3701] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*06/19/2026 06:49:20.4313] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr1v0
[*06/19/2026 06:49:20.4317] CLSM[HH:HH:HH:HH:HH:HH]: Local auth on radio 1 Vap 0 IP 192.0.2.10 updatere
[*06/19/2026 06:49:20.4318] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD
```

Logs de rastreamento de RA para a mesma autenticação bem-sucedida:

O rastreamento do RA registra a orquestração da sessão pela WLC. A WLC valida a identidade e a política do cliente.
A WLC reconhece a associação FlexConnect.

```
2026/06/19 06:49:20.934325580 {wncd_x_R0-1}{1}: [client-orch-sm] [18318]: (note): MAC: hhhh.hhhh.hhhh H
2026/06/19 06:49:20.936543415 {wncd_x_R0-1}{1}: [dot1x] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040000
2026/06/19 06:49:20.936579730 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.936600851 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.936654791 {wncd_x_R0-1}{1}: [ewlc-infra-evq] [18318]: (note): Authentication Succes
2026/06/19 06:49:20.936769433 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
```

A WLC envia a política para o AP.

```
2026/06/19 06:49:20.937447786 {wncd_x_R0-1}{1}: [svm] [18318]: (info): [hhhh.hhhh.hhhh] Applied User Pr
2026/06/19 06:49:20.937451734 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: c
2026/06/19 06:49:20.937452534 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937455590 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: v
2026/06/19 06:49:20.937456177 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: m
2026/06/19 06:49:20.937458436 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: u
2026/06/19 06:49:20.937462127 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile:tu
2026/06/19 06:49:20.937462755 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937463426 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937464035 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
```

Êxito na autorização.

```
2026/06/19 06:49:20.937594042 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.937597878 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
```

Parâmetros do cliente.

06/2026/19 06:49:20.939394217 {wncd_x_R0-1}{1}: [ponto11] [18318]: (nota): MAC: hhhh.hhhh.hhhh Parâmetros de entrada de caminho de dados do cliente - ssid:FlexAAA,slot_id:1 bssid ifid: 0x0, radio_if: 0x90400008, wlan_ifid: 0xf0400004

A WLC aprende o IP através do DHCP/ARP local.
06/2026/19 06:49:21.001000218 {wncd_x_R0-1}{1}: [cliente-aluno] [18318]: (nota): MAC: hhhh.hhhh.hhhh IP do cliente aprendido com êxito. Método: IP de rastreamento de IP: 192.0.2.10

O cliente está totalmente conectado.
06/2026/19 06:49:21.002363496 {wncd_x_R0-1}{1}: [errmsg] [18318]: (informações): %CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: R0/1: wcd: Entrada de nome de usuário (teste) unida com ssid (FlexAAA) para dispositivo com MAC: hhhh.hhhh.hhh no canal (48)
06/2026/19 06:49:21.002795009 {wncd_x_R0-1}{1}: [client-orch-state] [18318]: (nota): MAC: transição de estado do cliente hhhh.hhh.hhh: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN

Cenário autônomo

Comportamento durante a perda de conectividade do AP-WLC e a recuperação subsequente.

O AP está unido à WLC. O cliente executa com êxito a autenticação 802.1X e o AP faz a transição do cliente para o estado FWD (Encaminhamento).

Nos registros ao vivo do ISE RADIUS, vemos a sessão do cliente.

```
[*07/06/2026 20:26:05.8590] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr0v0
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: Local auth on radio 0 Vap 0 IP 192.0.2.10 updatere
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD
```

```
CW9164I-ROW-LAB2#show dot11 clients

Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7 No No
```

O AP não consegue alcançar a WLC, esgota sua contagem de retransmissão e muda para o modo autônomo. Os clientes existentes permanecem conectados localmente.

```
[*07/06/2026 20:28:47.0840] Re-Tx Count=1, Max Re-Tx Value=5, SendSeqNum=33, NumofPendingMsgs=4
[*07/06/2026 20:28:50.0860] Re-Tx Count=2, Max Re-Tx Value=5, SendSeqNum=34, NumofPendingMsgs=5
```

```
[*07/06/2026 20:28:53.0870] Re-Tx Count=3, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:28:56.0990] Re-Tx Count=4, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:28:59.1000] Re-Tx Count=5, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:29:02.1010] Max retransmission count exceeded, going back to DISCOVER mode.
[*07/06/2026 20:29:02.1020] Flexconnect Switching to Standalone Mode!
[*07/06/2026 20:29:02.2170] CAPWAP State: DTLS Teardown
```

Mas o cliente ainda está conectado:

CW9164I-ROW-LAB2#show dot11 clients

Total de clientes dot1: 1
ID do slot MAC do cliente ID da WLAN ID da WLAN Nome da WLAN RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7 Não Não

Quando o cliente faz roaming para outro AP no modo independente, o handshake EAP falha devido à incapacidade de acessar o servidor RADIUS. O cliente é desautorizado e removido do AP.

```
[*07/06/2026 20:34:44.7240] CLSM[HH:HH:HH:HH:HH:HH]: Session timeout
[*07/06/2026 20:36:15.2670] hostapd:apr0v0: CTRL-EVENT-EAP-RETRANSMIT hh:hh:hh:hh:hh:hh
[*07/06/2026 20:36:15.2670] hostapd:apr0v0: CTRL-EVENT-EAP-TIMEOUT-FAILURE hh:hh:hh:hh:hh:hh
[*07/06/2026 20:36:15.2680] wcp/flex_roam_st :: Flexconnect hapdev: Received UNAUTHORIZE for hh:hh:hh:h
[*07/06/2026 20:36:15.2680] wcp/flex_roam_st :: Flexconnect hapdev: recv'd UNAUTH with DISCONNECT REQUE
[*07/06/2026 20:36:15.2680] CLSM[HH:HH:HH:HH:HH:HH]: Client delete initiated with timeout of 10 seconds
[*07/06/2026 20:36:15.2770] CLSM[HH:HH:HH:HH:HH:HH]: Remove success from ClientIPTable on apr0v0
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: Not sending DELETE to cont, reason CLIENT_DEL_EAP_
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: Deauthorize succeeded to radio intf apr0v0
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: client moved from FWD to DELETE_PENDING
[*07/06/2026 20:36:15.2880] CLSM[HH:HH:HH:HH:HH:HH]: Send Deauth with reason 2 force 1 - Radio 0 Vap 0
[*07/06/2026 20:36:25.0830] CLSM[HH:HH:HH:HH:HH:HH]: Delete timeout
[*07/06/2026 20:36:25.0830] CLSM[HH:HH:HH:HH:HH:HH]: Delete client reassoc 0 succeeded to radio intf ap
```

O AP envia a sessão do cliente para o servidor RADIUS de backup.

O AP recupera a conectividade com a WLC. O AP volta para o modo conectado e sincroniza as informações da sessão do cliente local com o WLC.

A sessão do cliente faz a transição entre os nós ISE principal e de backup com base no status de conectividade do AP.

O AP e o cliente são exibidos como conectados na WLC, e o cliente não observou nenhuma

desconexão ou oscilação quando a conectividade entre o AP e a WLC estava inoperante.

```
CW9164I-ROW-LAB2#show dot11 clients

Total dot11 clients: 0


Upon roaming back, the client undergoes local authentication. The AP processes the association and move

[*07/06/2026 20:48:49.2830] CLSM[HH:HH:HH:HH:HH:HH]: US Auth(b0) seq 2653 IF 23 slot 0 vap 0 len 30 sta
[*07/06/2026 20:48:49.2840] CLSM[HH:HH:HH:HH:HH:HH]: DS Auth len 30 slot 0 vap 0
[*07/06/2026 20:48:49.2850] CLSM[HH:HH:HH:HH:HH:HH]: Driver send mgmt frame success Radio 0 Vap 0
[*07/06/2026 20:48:49.2850] CLSM[HH:HH:HH:HH:HH:HH]: client moved from UNASSOC to AUTH
[*07/06/2026 20:48:49.2920] CLSM[HH:HH:HH:HH:HH:HH]: US Reassoc Req(20) seq 2654 IF 23 slot 0 vap 0 len
[*07/06/2026 20:48:49.2930] CLSM[HH:HH:HH:HH:HH:HH]: AUTH TYPE RSNIE DOT1X
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: Populate client capability: cap_from_click=true, ma
[*07/06/2026 20:48:49.2940] Flexconnect local_auth 1 local_assoc 1 frame subtype 32
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: radio id: 0, vap id: 0, max clients for this wlan:
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: radio state: 1, client state: 1, max_client_per_ra
[*07/06/2026 20:48:49.2940] Adding RM Capable IE - Len = 5, RRM[0] = 73, RRM[1] = c0
[*07/06/2026 20:48:49.2940] DS [re]Assoc 1 req_len=201 resp_len=146 11r_len=0 cckm 0 qos_flag 1 status
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: DS Reassoc Resp(30) IF 0 slot 0 vap 0 state AUTH,
[*07/06/2026 20:48:49.2950] CLSM[HH:HH:HH:HH:HH:HH]: Driver send mgmt frame success Radio 0 Vap 0
[*07/06/2026 20:48:49.2950] CLSM[HH:HH:HH:HH:HH:HH]: client moved from AUTH to ASSOC
[*07/06/2026 20:48:49.2950] Sending ADD MOBILE to client SM for local auth client mac HH:HH:HH:HH:HH:HH
[*07/06/2026 20:48:49.2960] wcp/flex_roam_st :: Flexconnect Sending ADD_MOBILE_PAYLOAD (v4-client-acl-na
[*07/06/2026 20:48:49.2960] wcp/flex_roam_st :: Flexconnect encode_and_send_add_mobile_to_dott11_client_
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: ADD_MOBILE AID 1
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: Driver Add Client success AID 1 Radio 0 Vap 0 Enc
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: Added to ClientIPTable on apr0v0
[*07/06/2026 20:48:49.2970] CLSM[HH:HH:HH:HH:HH:HH]: client moved from ASSOC to 8021X
[*07/06/2026 20:48:49.2970] CLSM[HH:HH:HH:HH:HH:HH]: Added to WCP client table AID 1 Radio 0 Vap 0 Enc
[*07/06/2026 20:48:49.2980] wcp/flex_roam_st :: Flexconnect hapdev: client WCP_EVENT_CLIENT_ASSOC/REASSO
[*07/06/2026 20:48:49.6360] received WCP_EVENT_CLIENT_AUTHORIZE (non) roaming case clearing roam flags
[*07/06/2026 20:48:49.6360] wcp/flex_roam_st :: Flexconnect (AUTHORIZE) received PTK thru wcp_event
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect HH:HH:HH:HH:HH:HH client ACL , Qos Profile:
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect AAA Override Vlan with WLAN mapping: 1432 f
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect Sending ADD_MOBILE_PAYLOAD (v4-client-acl-na
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect encode_and_send_add_mobile_to_dott11_client_
[*07/06/2026 20:48:49.6370] CLSM[HH:HH:HH:HH:HH:HH]: ADD_MOBILE AID 1
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: check vlan override vlan 1432
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: Client ADD Encrypt Key success AID 1 Radio 0 Enc 4
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: client moved from 8021X to IPLEARN_PENDING
[*07/06/2026 20:48:49.6390] wcp/flex_roam_st :: Flexconnect Sending HREAP_APAUTH_CLIENT_ADD
[*07/06/2026 20:48:49.6900] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr0v0
[*07/06/2026 20:48:49.6910] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD


CW9164I-ROW-LAB2#show dot11 clients

Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -39 M7 No No

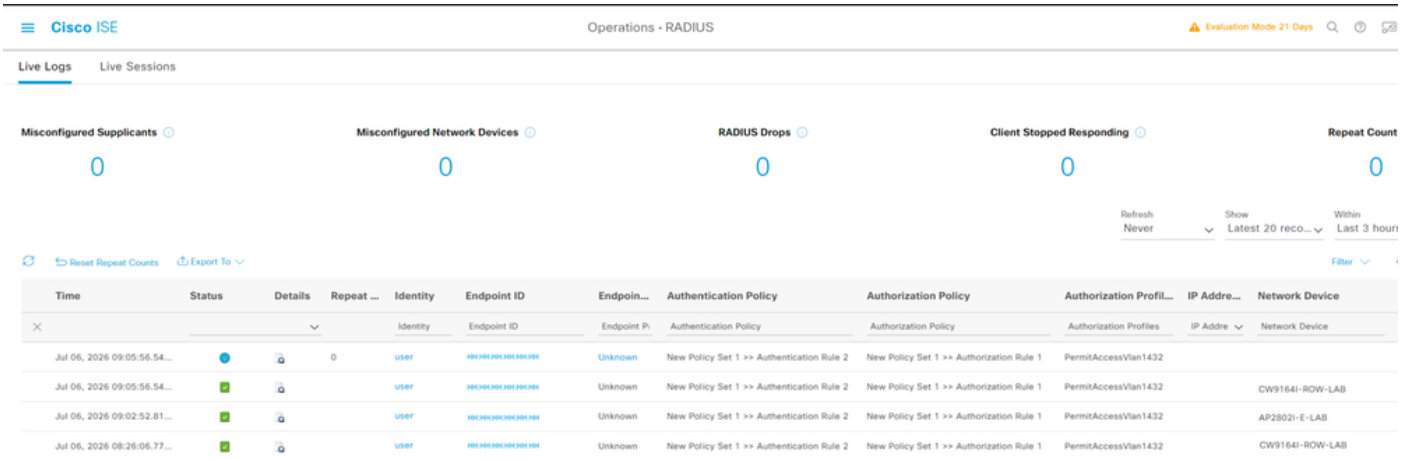



*07/06/2026 20:59:57.7690] Discovery Response from 192.0.2.20
[*07/06/2026 21:00:08.0080] CAPWAP State: DTLS Setup
```

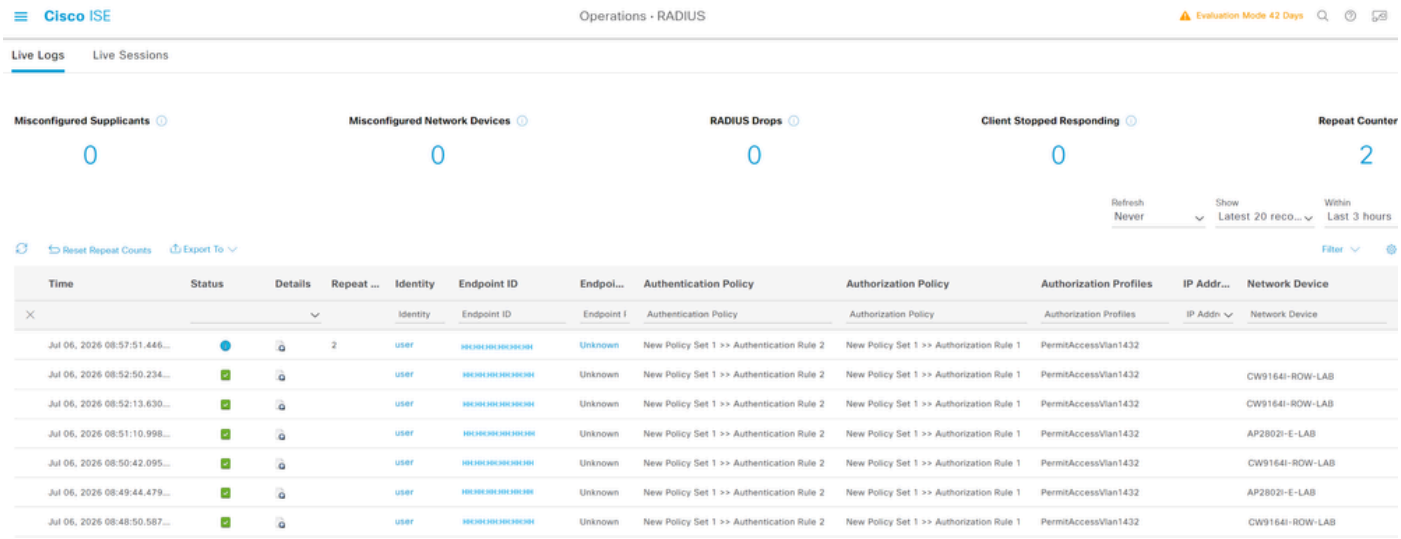
```
[*07/06/2026 21:00:08.4820] CAPWAP State: Join
[*07/06/2026 21:00:09.3740] Sending Join request to 192.0.2.20 through port 5253, packet size 1376
[*07/06/2026 21:00:09.3780] Join Response from 192.0.2.20, packet size 1397
[*07/06/2026 21:00:09.4040] CAPWAP State: Image Data
[*07/06/2026 21:00:09.5020] CAPWAP State: Configure
[*07/06/2026 21:00:12.5510] CAPWAP State: Run
[*07/06/2026 21:00:12.6480] AP has joined controller C9800-1
[*07/06/2026 21:00:12.6490] Flexconnect Switching to Connected Mode!
[*07/06/2026 21:00:12.6520] CLSM[HH:HH:HH:HH:HH:HH]: AP_REAP_CLIENT_INFO_PAYLOAD Client MAC HH:HH:HH:HH
[*07/06/2026 21:00:12.6520] AssocTimeAtAP 1783371169 clientBitmap=0x13
[*07/06/2026 21:00:12.6520] CLSM[00:00:00:00:00:00]: Numbers of Local Switching clients to report : 1
[*07/06/2026 21:00:14.8270] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 21:00:14.8270] chatter: bssid BB:BB:BB:BB:BB:BB, life_time 1783371774, created_at 17833716
[*07/06/2026 21:00:14.8280] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 21:00:14.8280] chatter: bssid BB:BB:BB:BB:BB:BB, life_time 1783371774, created_at 17833716
```

```
CW9164I-ROW-LAB2# show dot11 clients

Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7 No No
```



ISE principal: Registra a sessão inicial (08:26:06) e a sessão retomada após a restauração da conectividade da WLC (09:02:52).



ISE de backup: Captura a atividade da sessão (08:48:50 - 08:57:51) enquanto o AP estava operando no Modo Independente.

A primeira sessão foi às 08:26:06, depois disso o AP perdeu a conectividade com a WLC e mudou-se para o modo independente.

A sessão 09:02:52 é a primeira sessão após o AP restabelecer a conectividade com a WLC.

Informações Relacionadas

- CCNP Enterprise Wireless Design ENWLSD 300-425 e implementação ENWLSI 300-430 Official Cert Guide, 2ª Edição
- Guia de Configuração de Software do Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE 17.8.x - Capítulo: FlexConnect
- Notas de versão do Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Cupertino versão 17.8.x
- Matriz de recursos para pontos de acesso sem fio Cisco
- 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.