Configurar EAP-TLS no 9800 WLC com CA interna do ISE

Contents

Introdução

Este documento descreve a autenticação EAP-TLS usando a Certificate Authority of Identity

Services Engine para autenticar usuários.

Pré-requisitos

Componentes Utilizados

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

- Controlador sem fio: C9800-40-K9 executando 17.09.04a
- Cisco ISE: Executando o Patch 4 da Versão 3
- Modelo do AP: C9130AXI-D
- Switch: 9200-L-24P

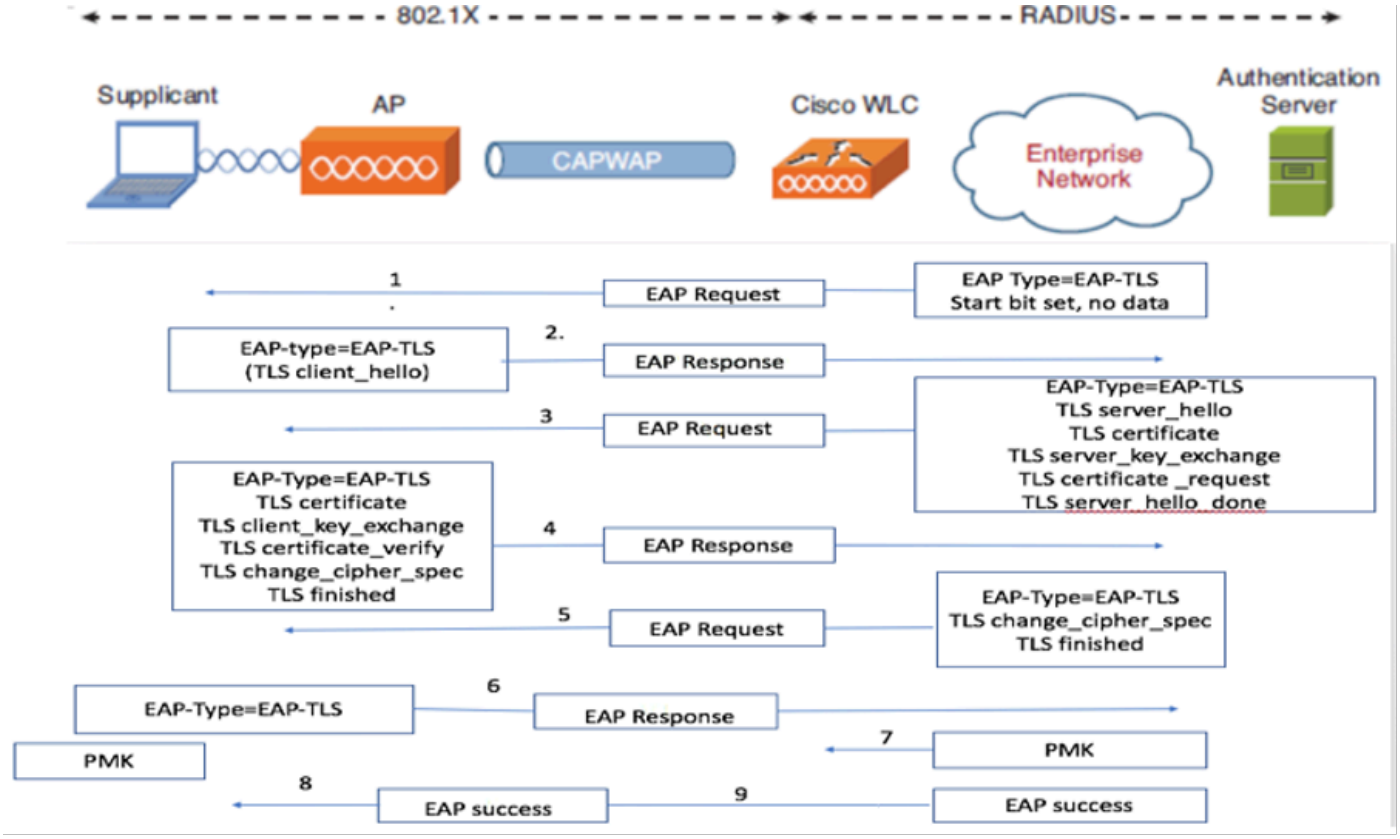
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer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

Informações de Apoio

A maioria das organizações tem sua própria CA que emite certificados para usuários finais para autenticação EAP-TLS. O ISE inclui uma autoridade de certificação incorporada que pode ser usada para gerar certificados para usuários a serem usados na autenticação EAP-TLS. Em cenários onde o uso de uma CA completa não é viável, o uso da CA do ISE para autenticação de usuário se torna vantajoso.

Este documento descreve as etapas de configuração necessárias para usar efetivamente a CA do ISE para autenticar usuários sem fio. Fluxo de autenticação EAP-TLS

Fluxo de autenticação EAP-TLS



Fluxo de autenticação EAP-TLS

Etapas do fluxo EAP-TLS

1. O cliente sem fio se associa ao Ponto de Acesso (AP).
2. Nesse estágio, o AP não permite a transmissão de dados e envia uma solicitação de autenticação.
3. O cliente, atuando como o requerente, responde com uma Identidade de Resposta EAP.
4. A controladora Wireless LAN (WLC) encaminha as informações de ID do usuário ao Servidor de autenticação.
5. O servidor RADIUS responde ao cliente com um pacote de inicialização EAP-TLS.
6. A conversação EAP-TLS começa a partir desse ponto.
7. O cliente envia uma EAP-Response de volta ao servidor de autenticação, incluindo uma mensagem de handshake client_hello com uma cifra definida como NULL.
8. O servidor de autenticação responde com um pacote Access-Challenge contendo:

```
TLS server_hello
Handshake message
Certificate
Server_key_exchange
Certificate request
Server_hello_done
```

9. O cliente responde com uma mensagem EAP-Resposta que inclui:

```
Certificate (for server validation)
Client_key_exchange
Certificate_verify (to verify server trust)
Change_cipher_spec
TLS finished
```

10. Após a autenticação bem-sucedida do cliente, o servidor RADIUS envia um Desafio de Acesso contendo:

```
Change_cipher_spec
Handshake finished message
```

11. O cliente verifica o hash para autenticar o servidor RADIUS.

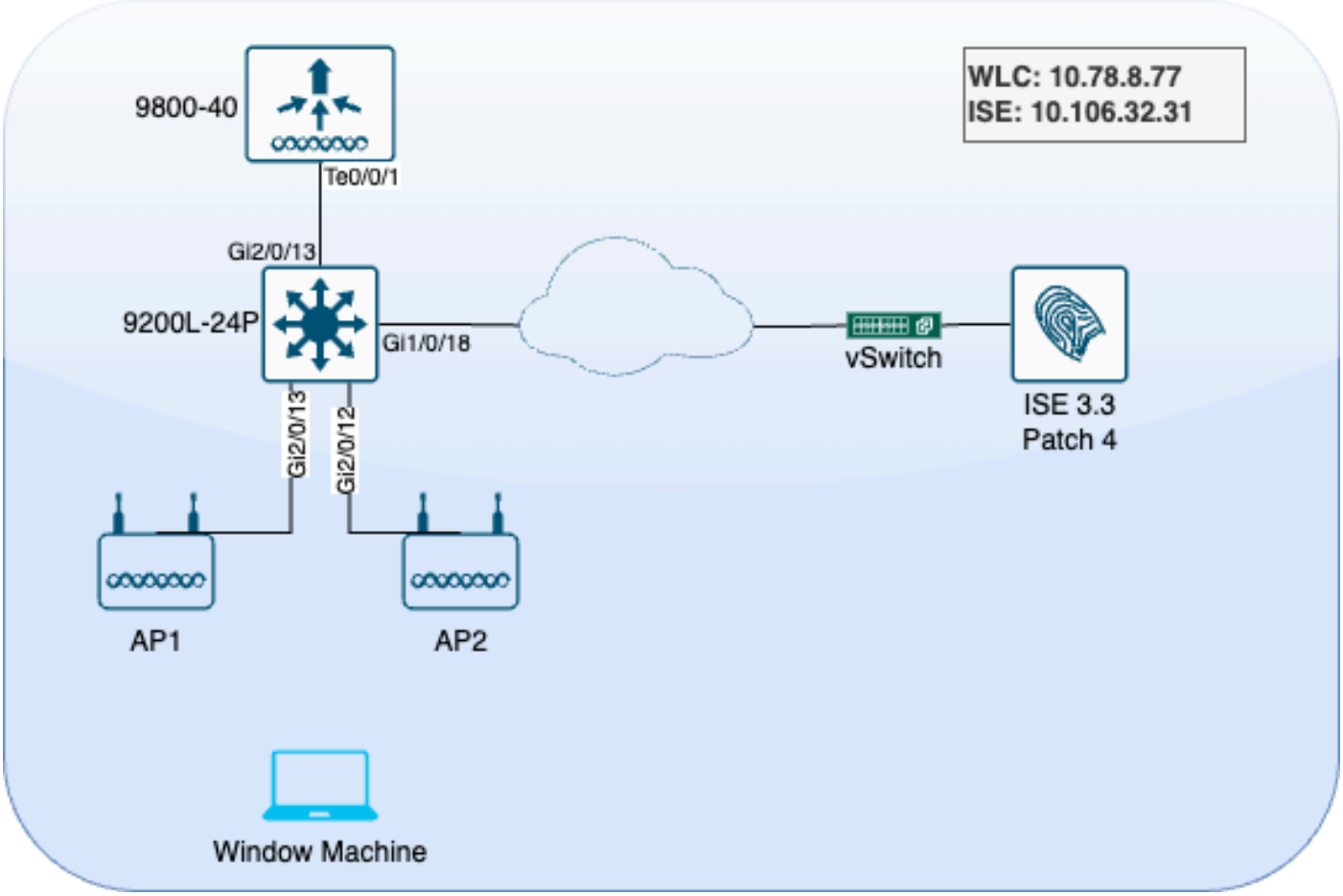
12. Uma nova chave de criptografia é derivada dinamicamente do segredo durante o handshake TLS.

13. Uma mensagem EAP-Sucesso é enviada do servidor para o autenticador e, em seguida, para o requerente.

14. O cliente sem fio habilitado para EAP-TLS agora pode acessar a rede sem fio.

Configurar

Diagrama de Rede



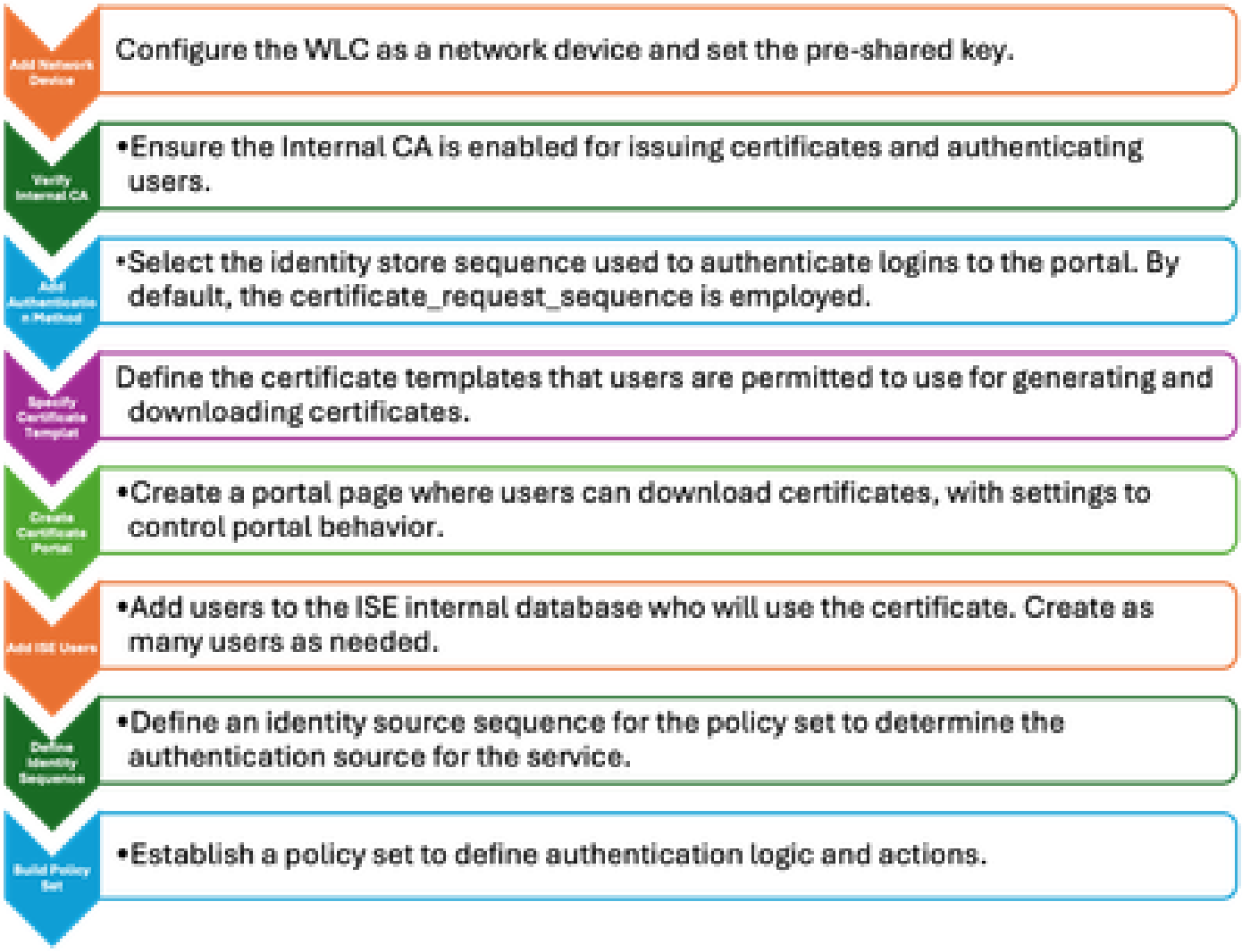
Topologia de laboratório

Configurações

Nesta seção, configuramos dois componentes: ISE e 9800 WLC.

Configuração do ISE

Estas são as etapas de configuração do servidor ISE. Cada etapa é acompanhada por capturas de tela nesta seção para fornecer orientação visual.

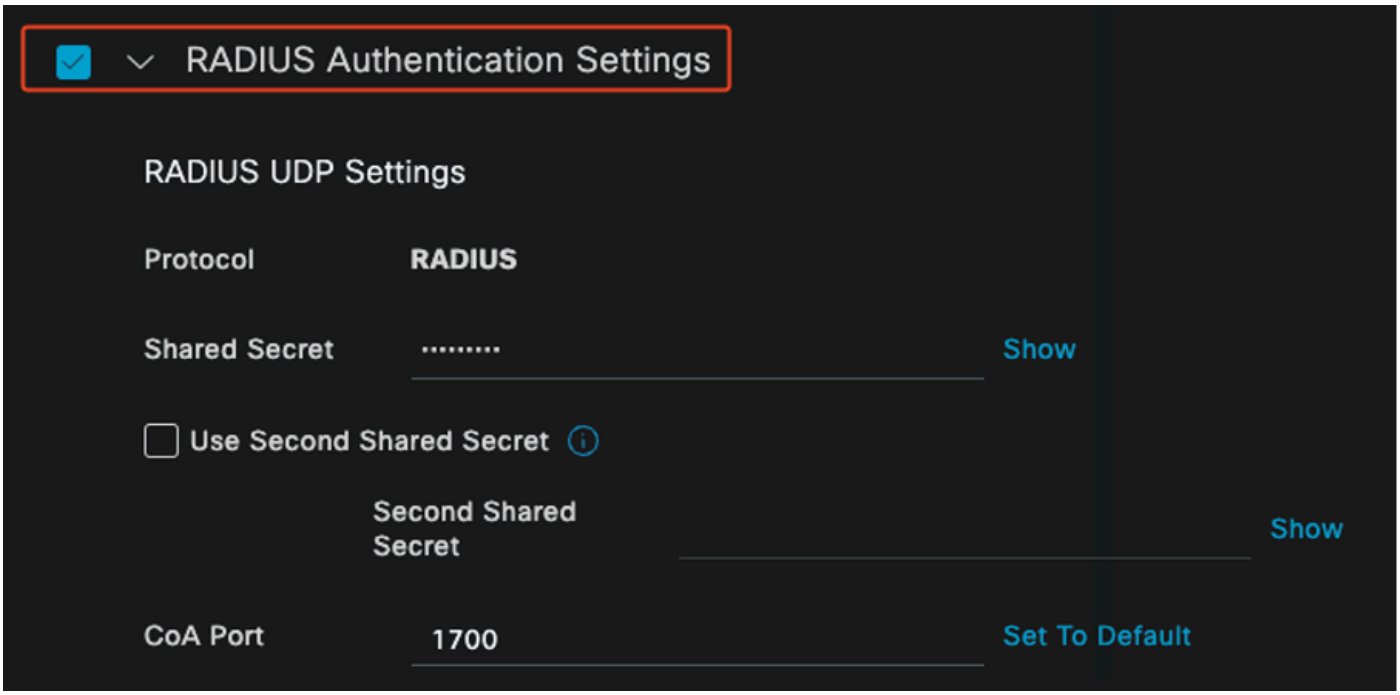


Etapas de configuração do servidor ISE

Adicionando um dispositivo de rede

Para adicionar a controladora Wireless LAN (WLC) como um dispositivo de rede, use estas instruções:

1. Navegue até Administração > Recursos de rede > Dispositivos de rede.
2. Clique no ícone +Add para iniciar o processo de adição da WLC.
3. Certifique-se de que a chave pré-compartilhada corresponda ao servidor WLC e ISE para permitir a comunicação apropriada.
4. Depois que todos os detalhes forem inseridos corretamente, clique em Submit no canto inferior esquerdo para salvar a configuração

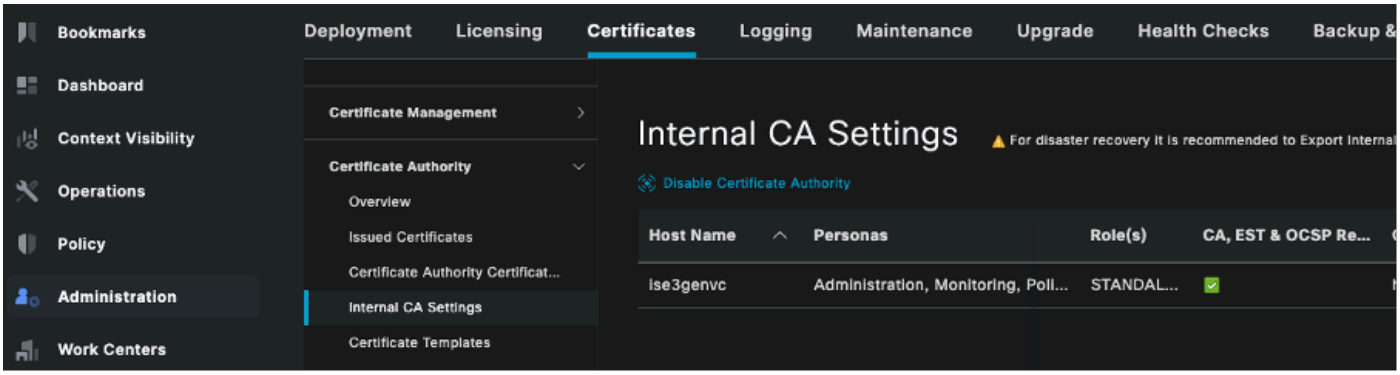


Adicionando um dispositivo de rede

Verificar CA interna

Para verificar as configurações de Autoridade de Certificação Interna (CA), siga estas etapas:

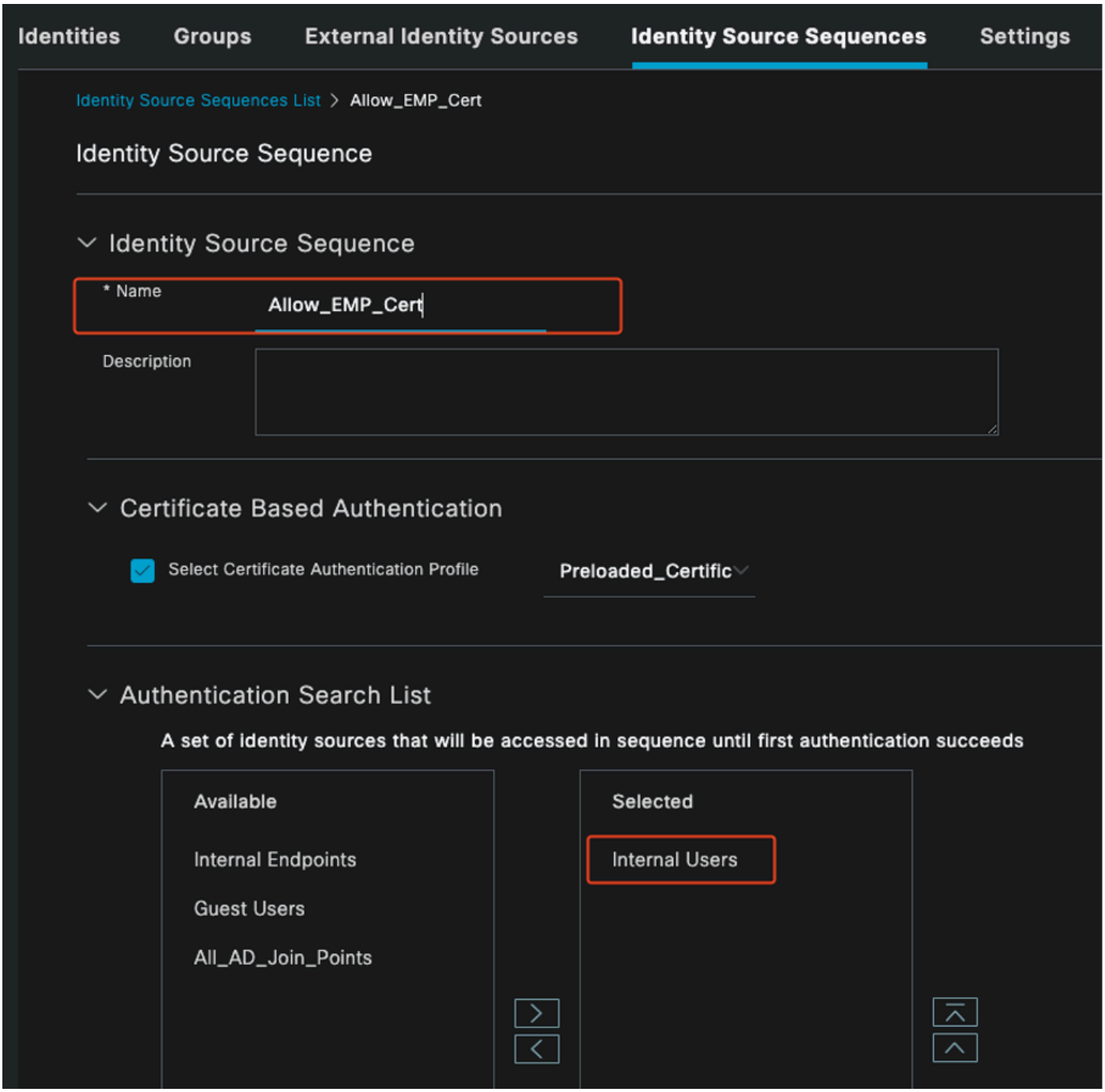
1. Vá para Administration > System > Certificates > Certificate Authority > Internal CA Settings.
2. Certifique-se de que a coluna CA esteja habilitada para confirmar se a CA interna está ativa.



Verificar CA interna

Adicionar método de autenticação

Navegue até Administração > Gerenciamento de identidades > Sequências de origem de identidade. Adicione uma sequência de identidade personalizada para controlar a fonte de logon do portal.



método de autenticação

Especificar Modelo de Certificado

Para especificar um modelo de certificado, siga estas etapas:

Etapa 1. Navegue até Administration > System > Certificates > Certificate Authority > Certificate Templates.

Etapa 2. Clique no ícone +Add para criar um novo modelo de certificado:

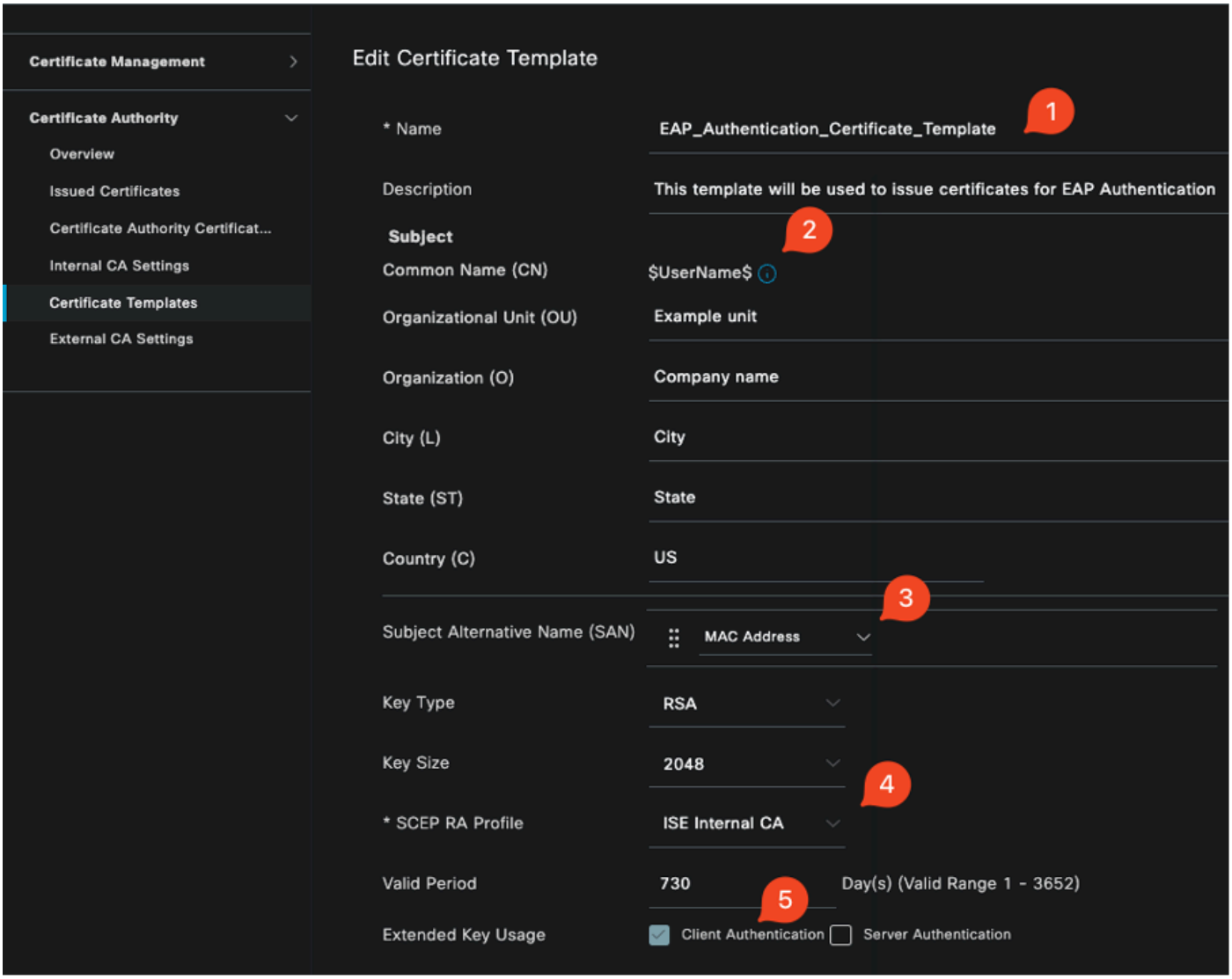
2.1 Forneça um nome exclusivo que seja local para o servidor ISE do modelo.

2.2 Verifique se o CN (Common Name, Nome comum) está definido como $UserName$.

2.3 Verifique se o SAN (Nome alternativo do assunto) está mapeado para o endereço MAC.

2.4 Defina o perfil SCEP RA como CA interna do ISE.

2.5 Na seção utilização de chave estendida, ative a autenticação do cliente.



Modelo de certificado

Criar Portal de Certificados

Para criar um portal de certificados para a geração de certificados de cliente, siga estas etapas:

Etapa 1. Navegue até Administration > Device Portal Management > Certificate Provisioning.

Etapa 2. Clique em Criar para configurar uma nova página do portal.

Etapa 3. Forneça um nome exclusivo para o portal para identificá-lo facilmente.

3.1. Escolha o número da porta em que o portal deverá operar; defina como 8443.

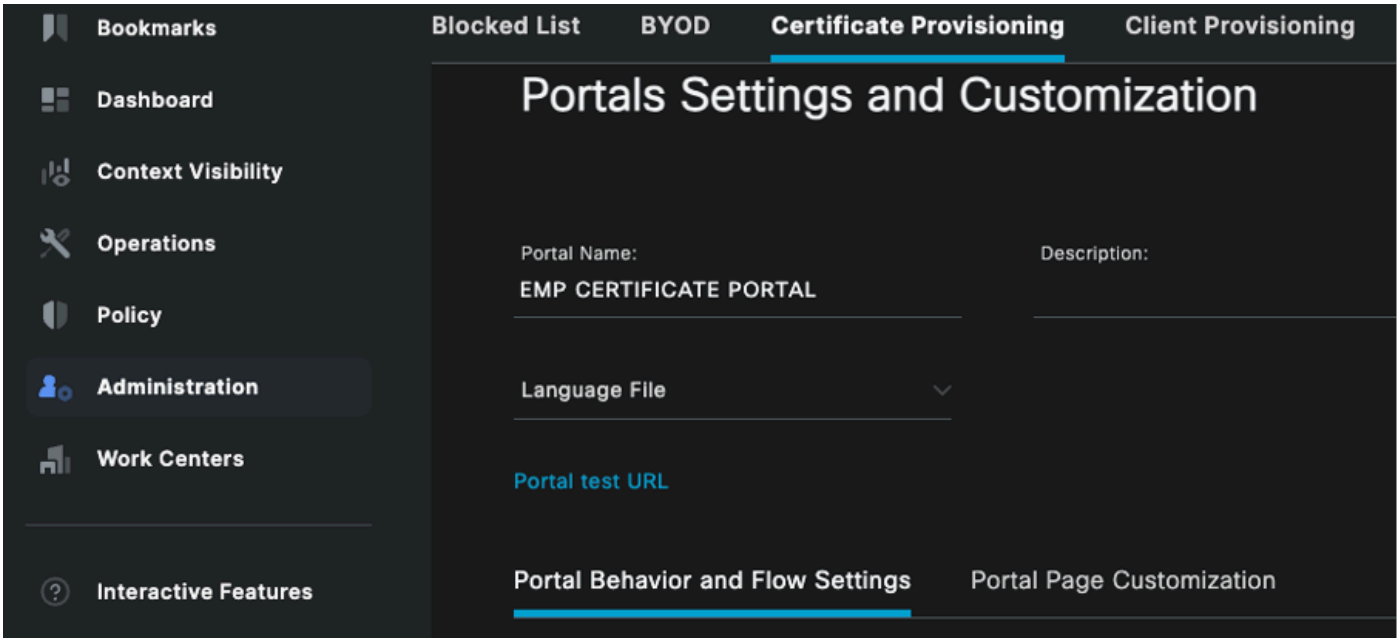
3.2. Especifique as interfaces nas quais o ISE escuta esse portal.

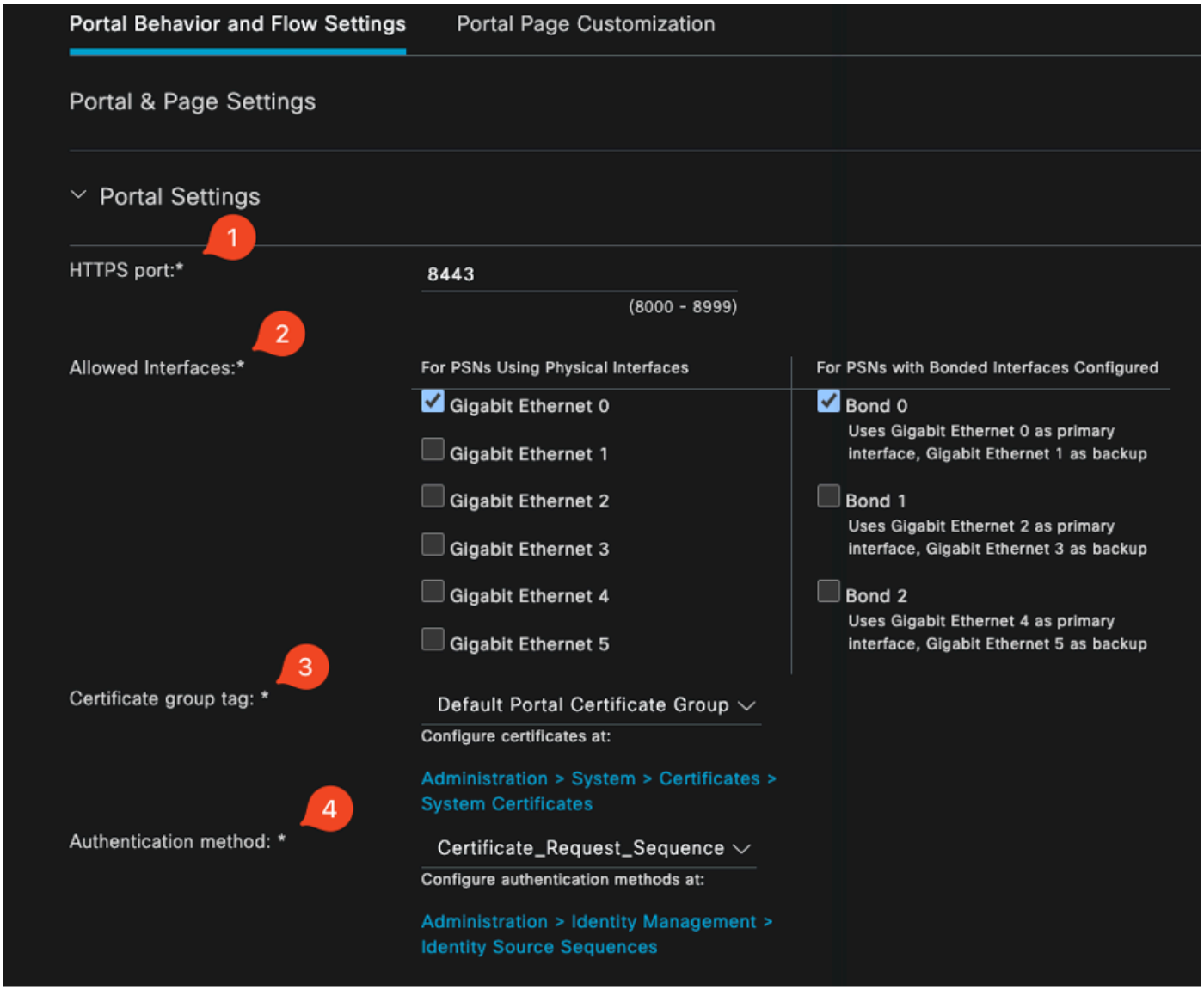
3.3. Selecione a Tag do grupo de certificados como o grupo de certificados do portal padrão.

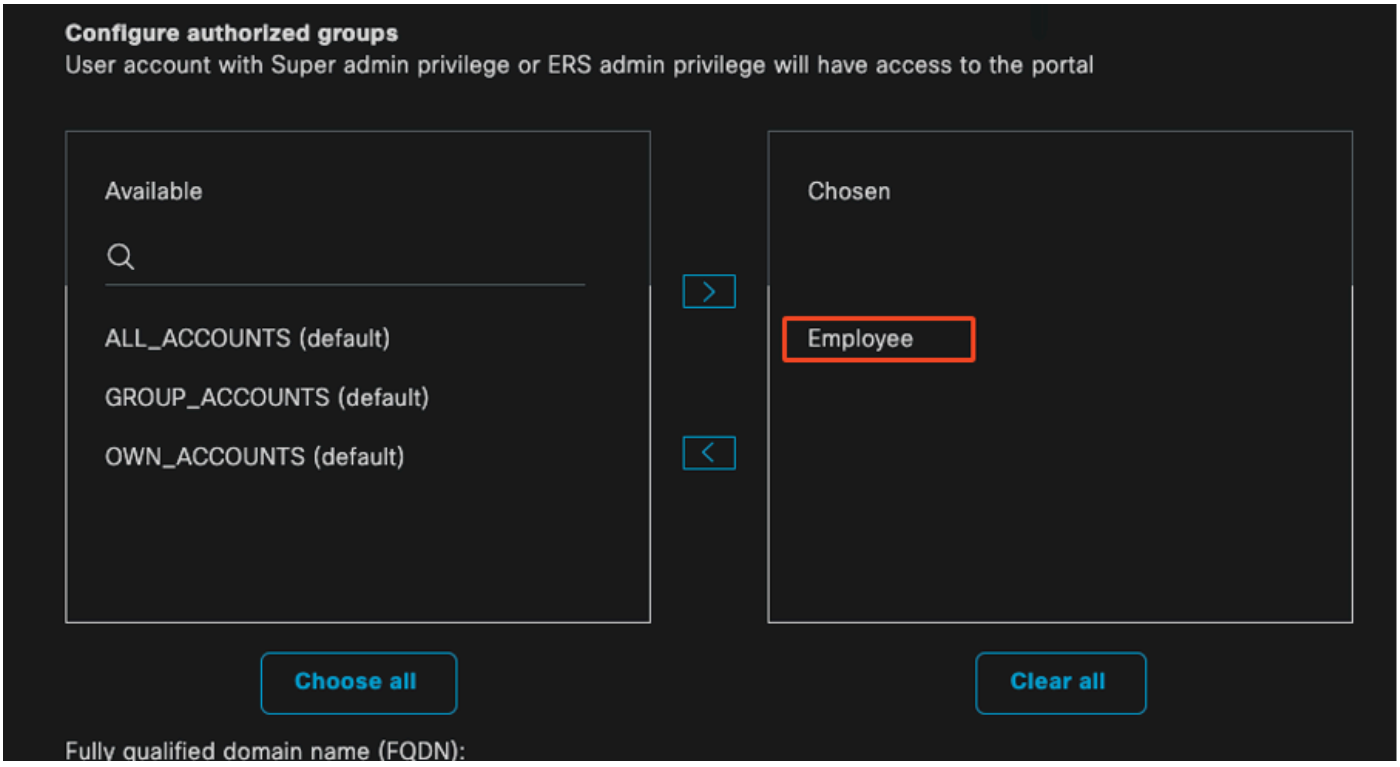
3.4. Selecione o método de autenticação, que indica a sequência de armazenamento de identidade usada para autenticar o logon neste portal.

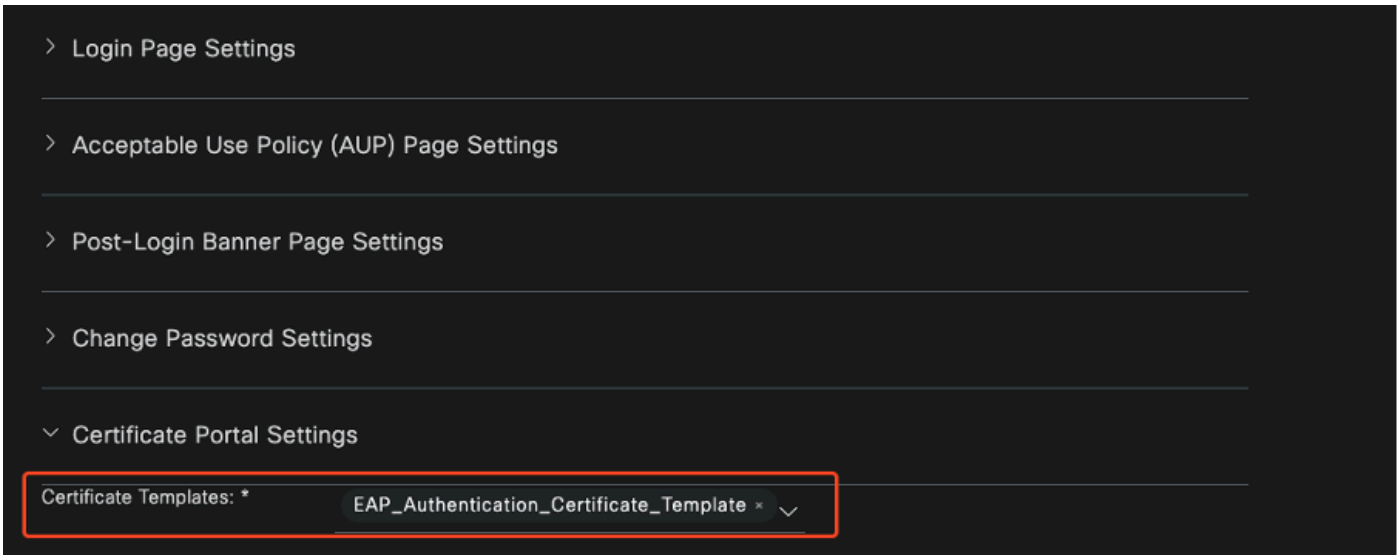
3.5. Inclua os grupos autorizados cujos membros podem acessar o portal. Por exemplo, selecione o grupo de usuários Funcionário se os usuários pertencerem a esse grupo.

3.6. Defina os modelos de certificado permitidos nas configurações de Provisionamento de Certificado.



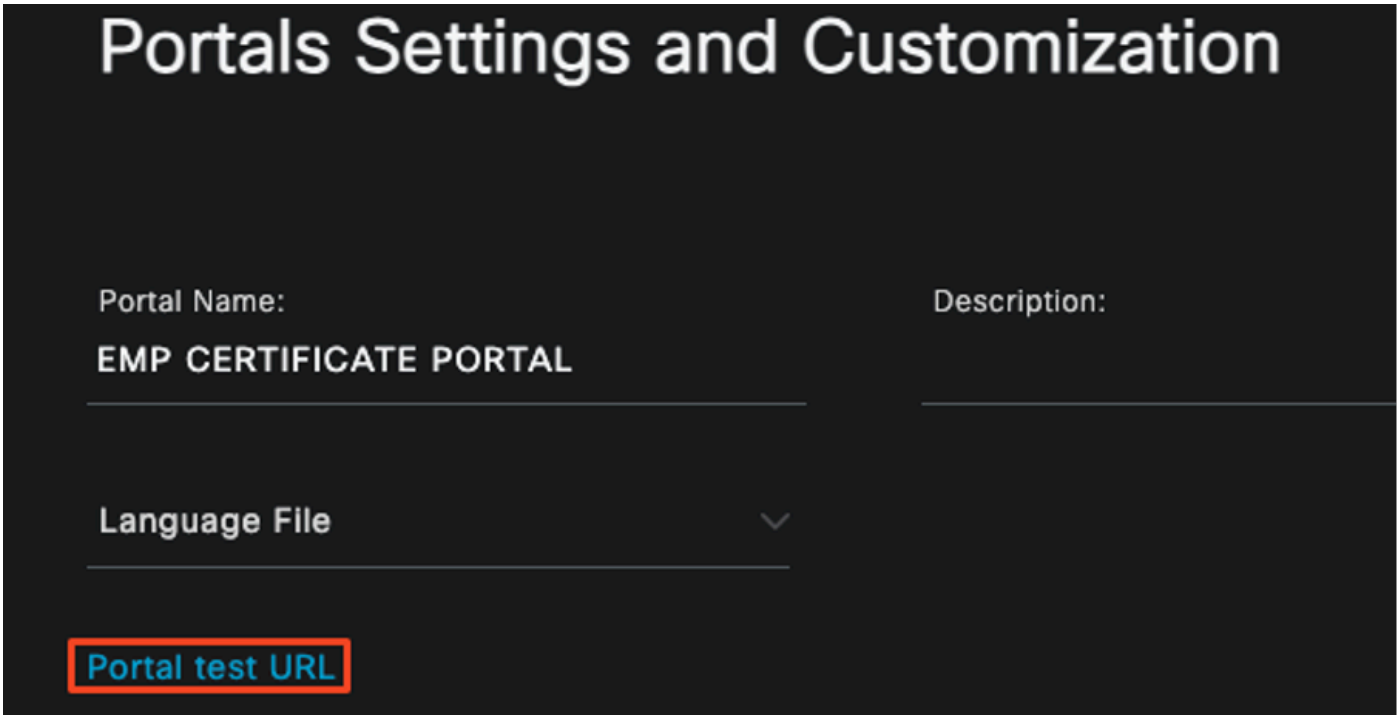

Portal Behavior and Flow Settings
Portal Page Customization
Portal & Page Settings
Portal Settings
1
HTTPS port:*
8443
(8000 - 8999)
2
Allowed Interfaces:*
For PSNs Using Physical Interfaces
Gigabit Ethernet 0
Gigabit Ethernet 1
Gigabit Ethernet 2
Gigabit Ethernet 3
Gigabit Ethernet 4
Gigabit Ethernet 5
For PSNs with Bonded Interfaces Configured
Bond 0
Uses Gigabit Ethernet 0 as primary interface, Gigabit Ethernet 1 as backup
Bond 1
Uses Gigabit Ethernet 2 as primary interface, Gigabit Ethernet 3 as backup
Bond 2
Uses Gigabit Ethernet 4 as primary interface, Gigabit Ethernet 5 as backup
3
Certificate group tag: *
Default Portal Certificate Group
Configure certificates at:
Administration > System > Certificates > System Certificates
4
Authentication method: *
Certificate_Request_Sequence
Configure authentication methods at:
Administration > Identity Management > Identity Source Sequences


Configure authorized groups
User account with Super admin privilege or ERS admin privilege will have access to the portal
Available
ALL_ACCOUNTS (default)
GROUP_ACCOUNTS (default)
OWN_ACCOUNTS (default)
Chosen
Employee
Choose all
Clear all
Fully qualified domain name (FQDN):

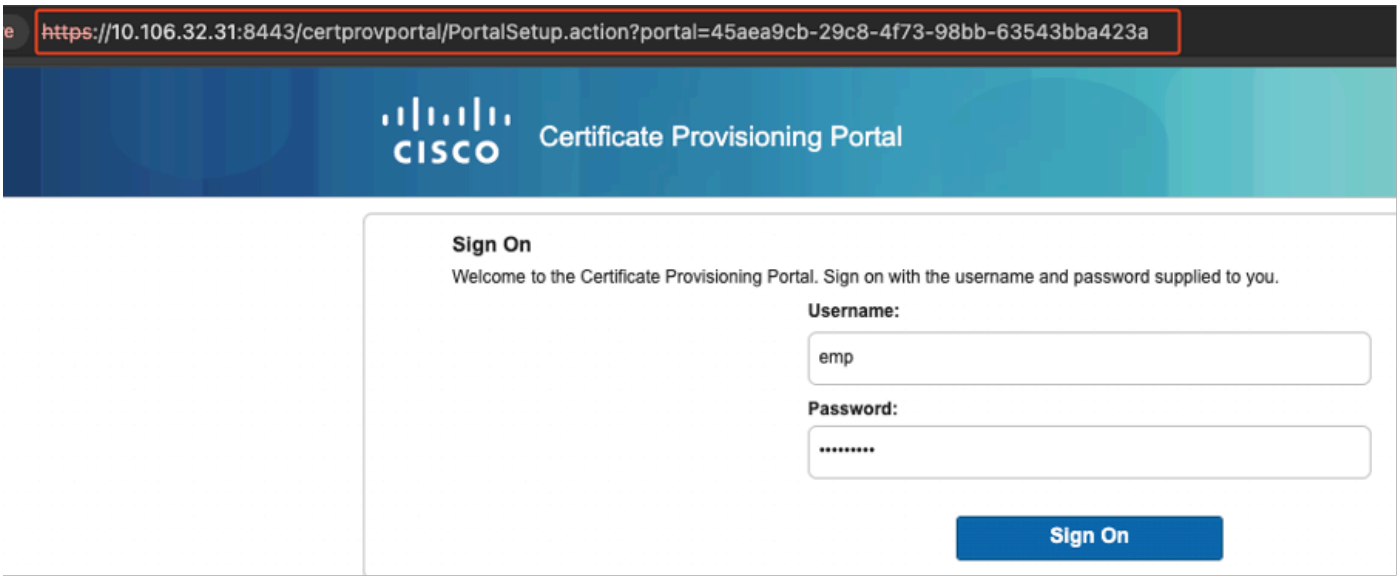


Configuração do Portal de Certificados

Quando essa configuração estiver concluída, você poderá testar o portal clicando no URL de teste do portal. Esta ação abre a página do portal.



URL da página do portal de teste

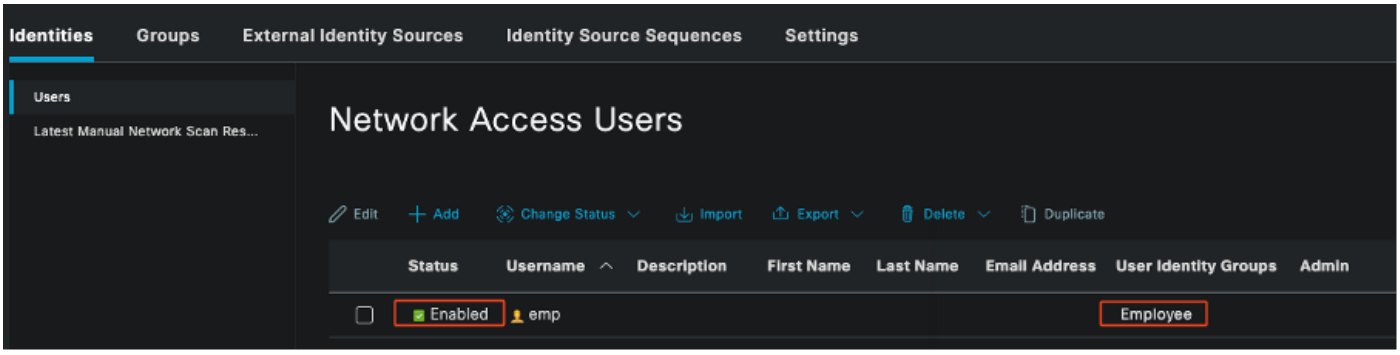


Página do portal

Adicionar usuário interno

Para criar um usuário para autenticação por meio do portal de certificados, siga estas etapas:

1. Vá para Administração > Gerenciamento de identidades > Identidades > Usuários.
2. Clique na opção para adicionar um usuário ao sistema.
3. Selecione os grupos de identidade do usuário aos quais o usuário pertence. Para este exemplo, atribua o usuário ao grupo Funcionário.



Adicionando usuário interno

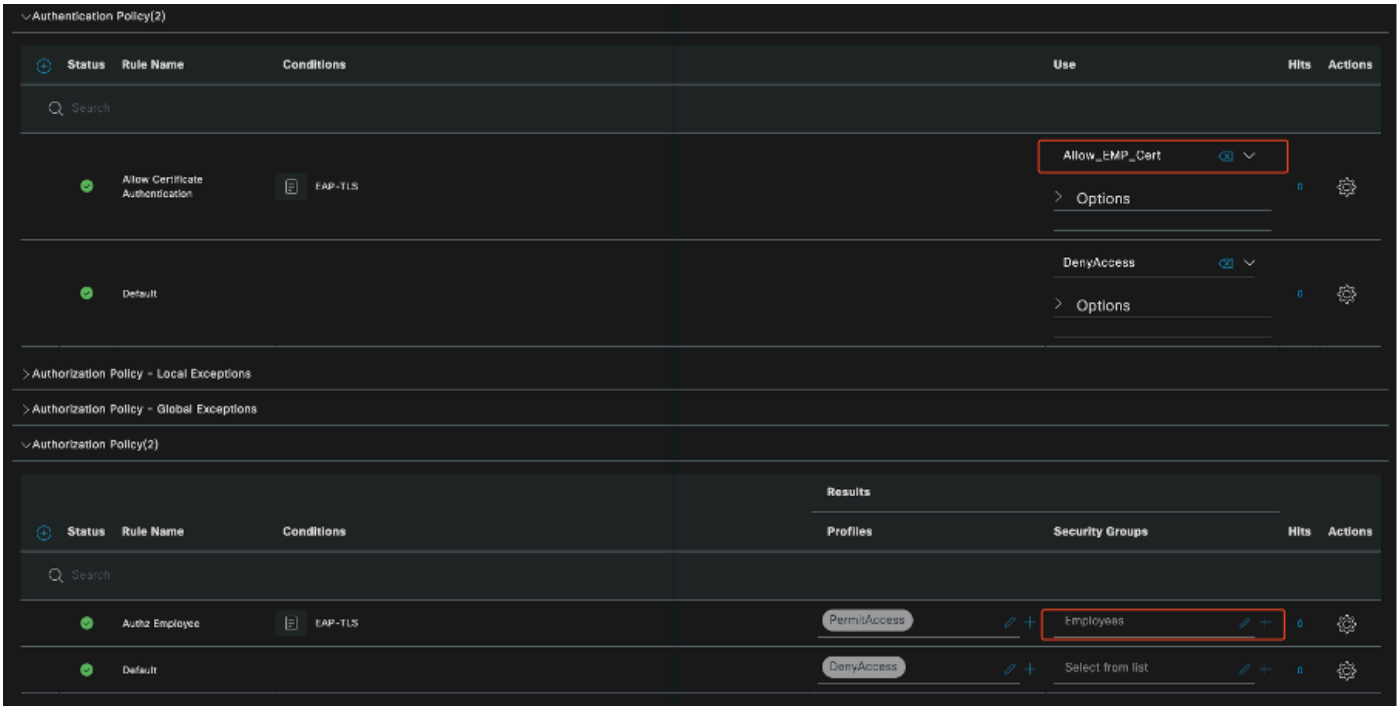
Portal de Provisionamento de Certificado ISE e Configuração de Política RADIUS

A seção anterior cobria a configuração do portal de provisionamento de certificados do ISE. Agora, configuramos os conjuntos de políticas do ISE RADIUS para permitir a autenticação do usuário.

1. Configurar conjuntos de políticas ISE RADIUS
2. Navegue até Política > Conjuntos de política.
3. Clique no sinal de mais (+) para criar um novo conjunto de políticas.

Neste exemplo, configure um conjunto de políticas simples projetado para autenticar usuários usando seus certificados.

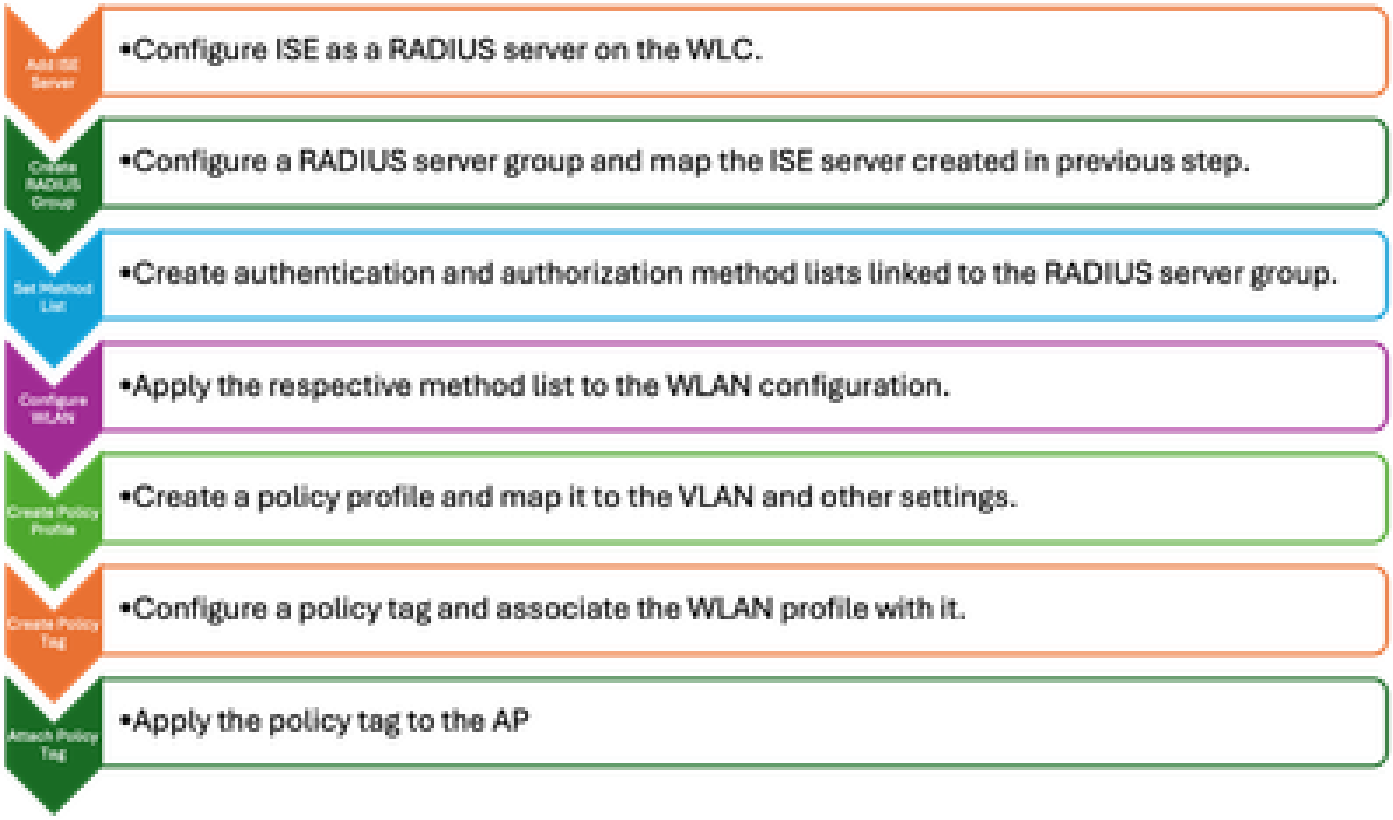
Conjunto de políticas



Conjunto de políticas exibindo políticas de autenticação e autorização

Configuração da WLC 9800

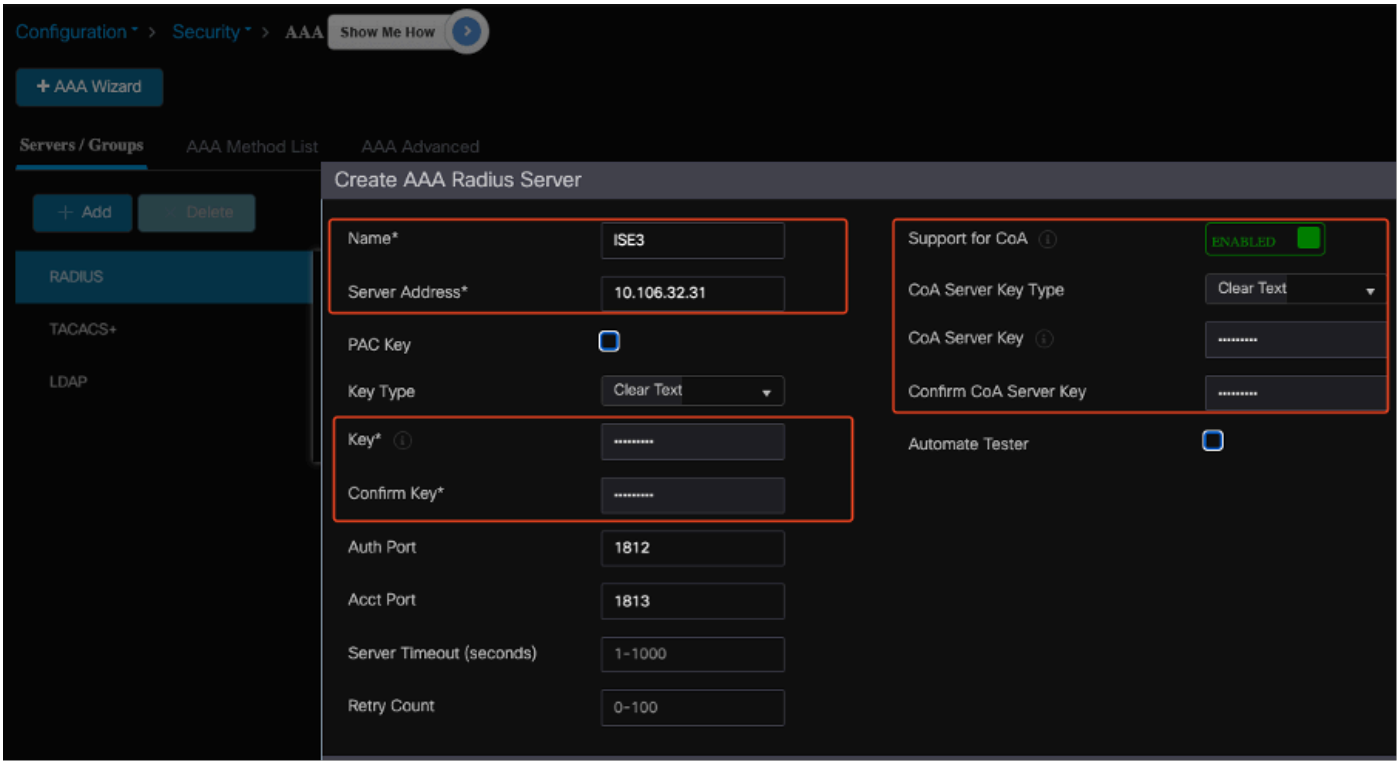
Estas são as etapas de configuração para a WLC 9800. Cada etapa é acompanhada por capturas de tela nesta seção para fornecer orientação visual.



Etapas de configuração da WLC

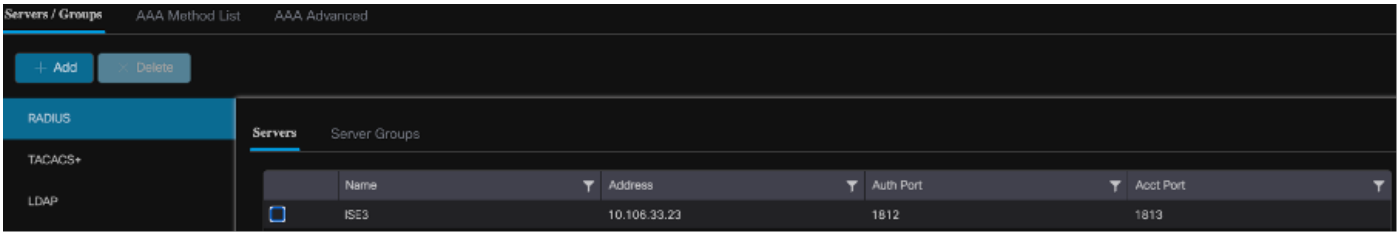
Adicionar o servidor ISE ao WLC 9800

1. Para integrar o servidor ISE com a controladora Wireless LAN (WLC) 9800, siga estas etapas:
2. Vá para Configuration > Security > AAA.
3. Clique no botão Add para incluir o servidor ISE na configuração da WLC.



Adicionando o servidor ISE na WLC

Quando o servidor for adicionado, ele aparecerá na lista de servidores.

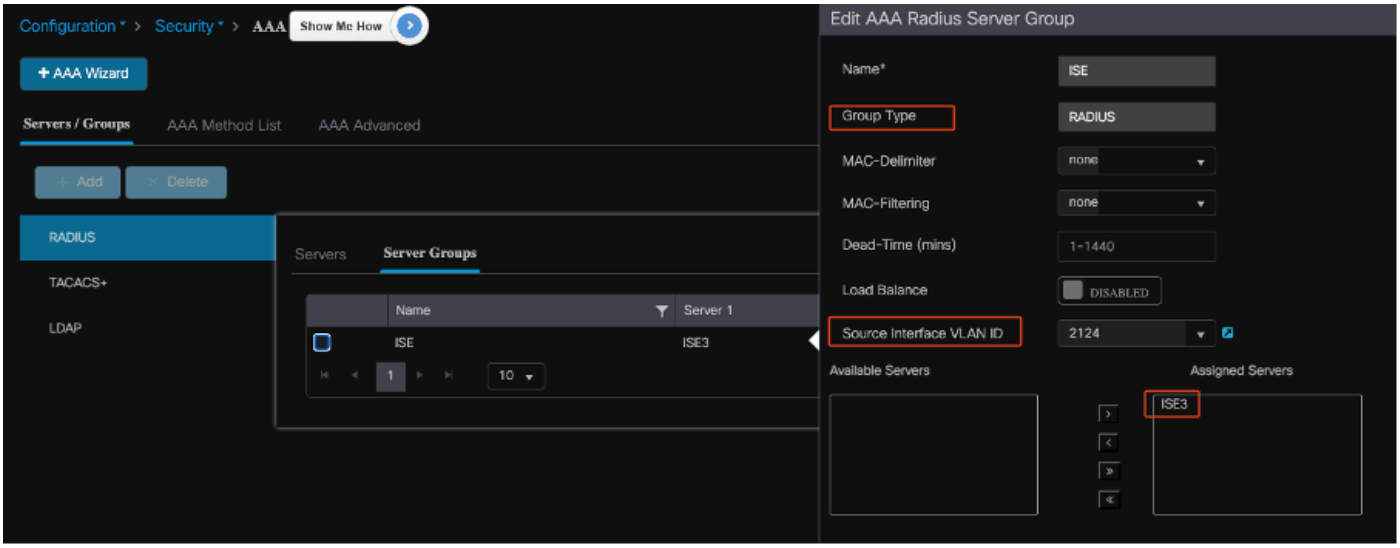


Mostrando servidores Radius

Adicionar grupo de servidores na WLC 9800

Para adicionar um grupo de servidores à controladora Wireless LAN 9800, siga estas etapas:

1. Navegue até Configuration > Security > AAA.
2. Clique na guia Server Group e, em seguida, clique em Add para criar um novo grupo de servidores.

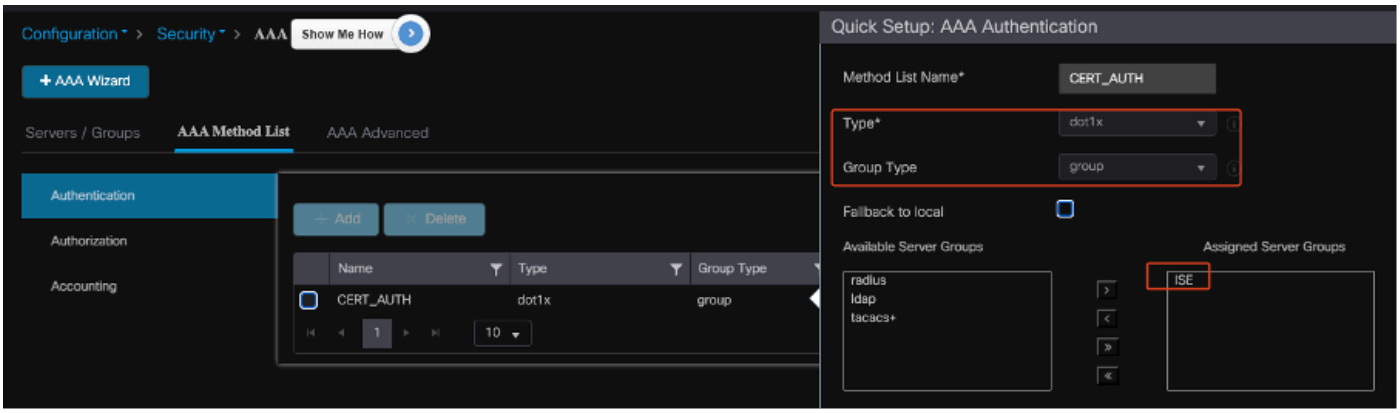


Mapeamento de servidores ISE para um grupo de servidores Radius

Configure a lista de métodos AAA no 9800 WLC

Depois de criar o grupo de servidores, configure a lista de métodos de autenticação usando estas etapas:

1. Navegue até Configuration > Security > AAA > AAA Method List.
2. Na guia Autenticação, adicione uma nova lista de métodos de autenticação.
3. Defina o tipo como dot1x.
4. Selecione group como o tipo de grupo.
5. Inclua os grupos de servidores do ISE criados anteriormente como os grupos de servidores.

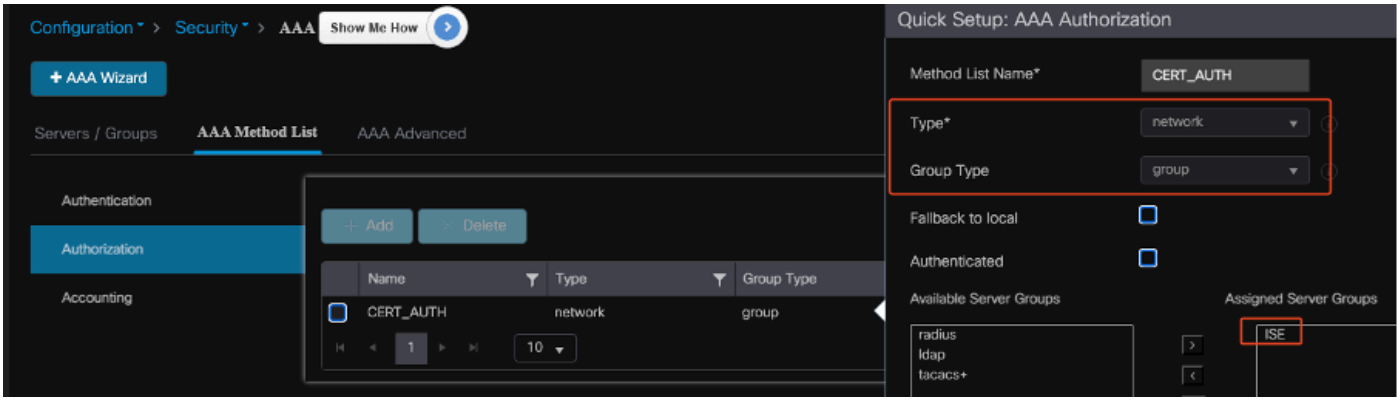


Criando listas de métodos de autenticação

Configurar a lista de métodos de autorização no 9800 WLC

Para configurar a lista de métodos de autorização, siga estas etapas:

1. Navegue até a guia Authorization na seção AAA Method List.
2. Clique em Adicionar para criar uma nova lista de métodos de autorização.
3. Escolha network como o tipo.
4. Selecione group como o tipo de grupo.
5. Inclua o grupo de servidores do ISE como o grupo de servidores.

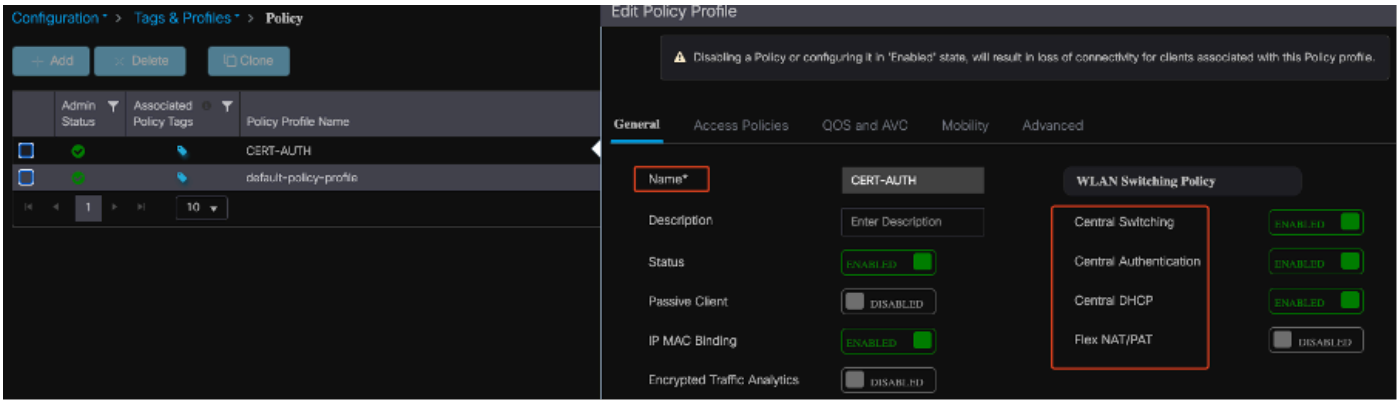


Adicionando lista de métodos de autorização

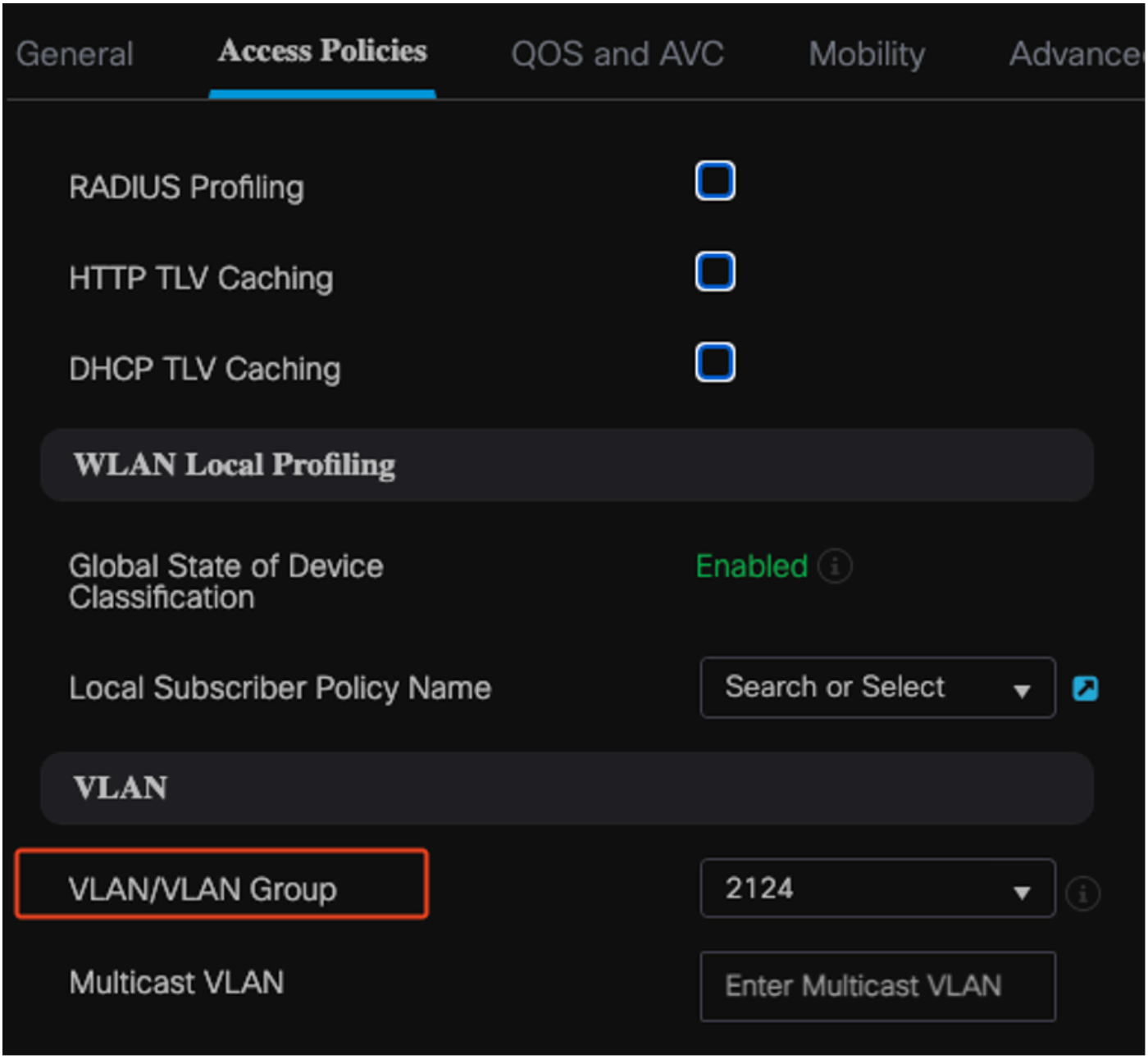
Crie um perfil de política no 9800 WLC

Com a configuração do grupo RADIUS concluída, prossiga para criar um perfil de política:

1. Navegue até Configuração > Marcas e perfis > Política.
2. Clique em Add para criar um novo perfil de diretiva.
3. Escolha os parâmetros apropriados para o seu perfil de política. Neste exemplo, tudo é central e a VLAN do LAB é usada como a VLAN cliente.



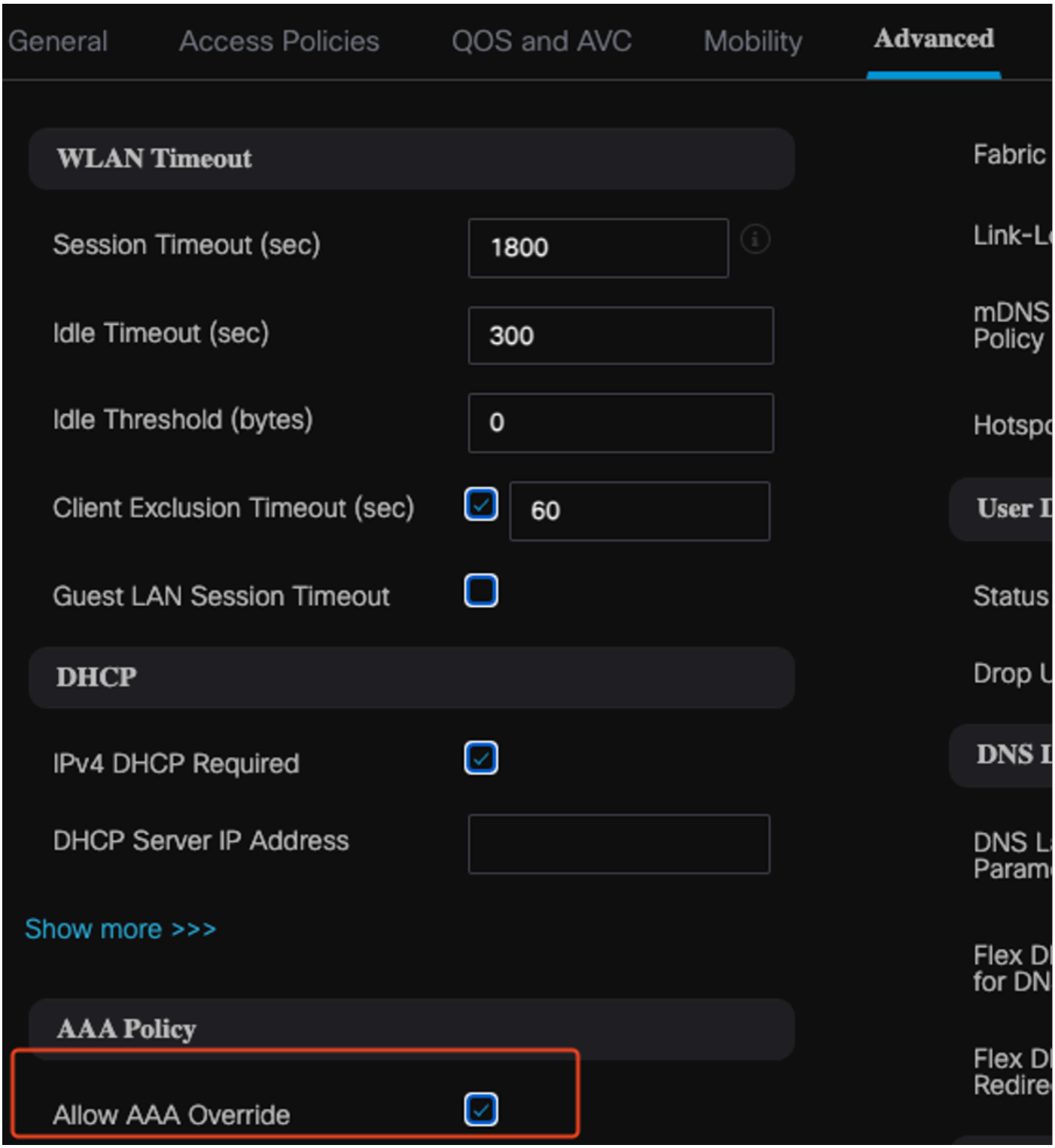
Configurando o perfil de política



VLAN para mapeamento de política

Ao configurar a autorização RADIUS, certifique-se de que a opção AAA Override esteja habilitada na guia advanced das configurações de perfil de regra. Esta configuração permite que o

Controlador de LAN Sem Fio aplique políticas de autorização baseadas em RADIUS a usuários e dispositivos.



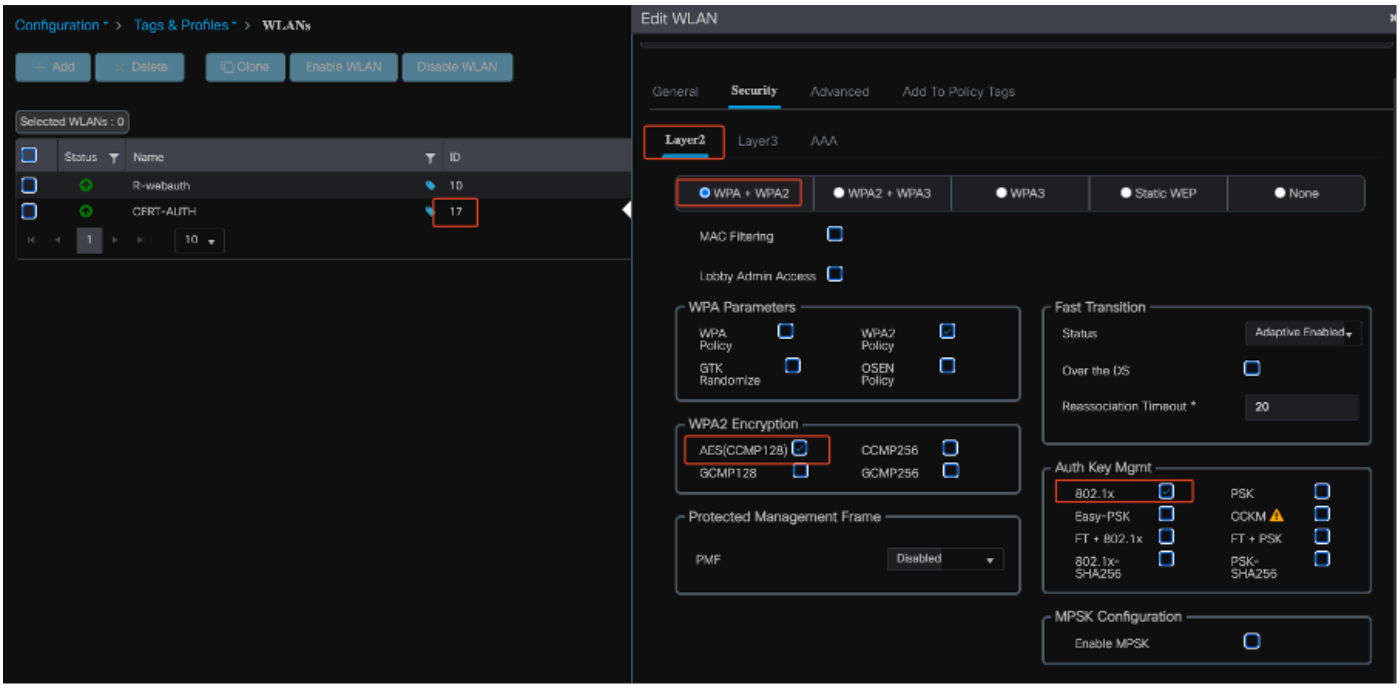
Substituição de AAA

Crie uma WLAN no 9800 WLC

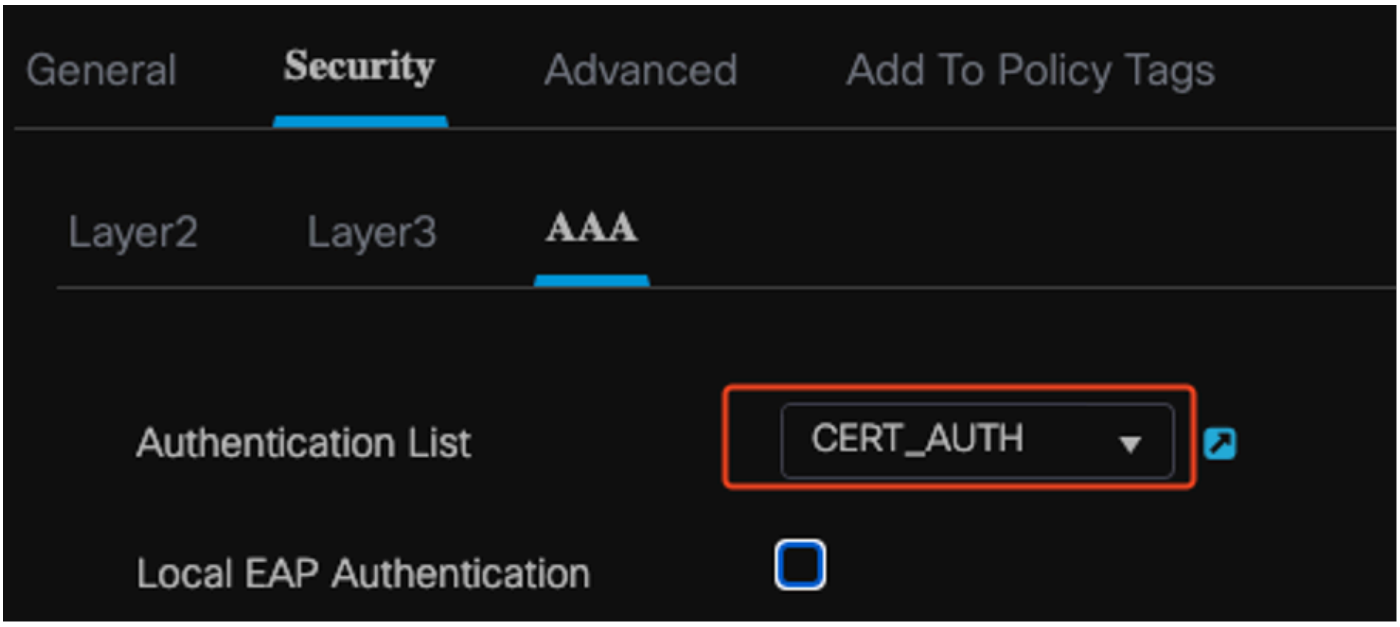
Para configurar uma nova WLAN com autenticação 802.1x, use estes passos:

1. Navegue até Configuration > Tags & Profiles > WLANs.
2. Clique em Add para criar uma nova WLAN.

3. Selecione as configurações de autenticação da Camada 2 e habilite a autenticação 802.1x.



Configuração do perfil da WLAN

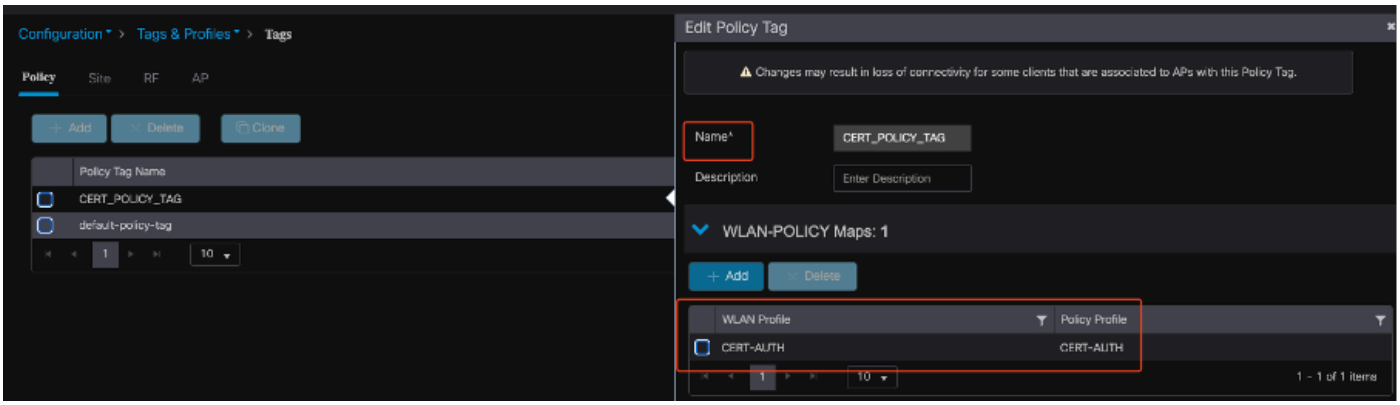


Perfil da WLAN para Mapa da Lista de Métodos

Mapear WLAN com Perfil de Política no 9800 WLC

Para associar sua WLAN a um perfil de política, siga estas etapas:

1. Navegue até Configuração > Marcas e perfis > Marcas.
2. Clique em Adicionar para adicionar uma nova marca.
3. Na seção WLAN-POLICY, mapeie a WLAN recém-criada para o perfil de política apropriado.

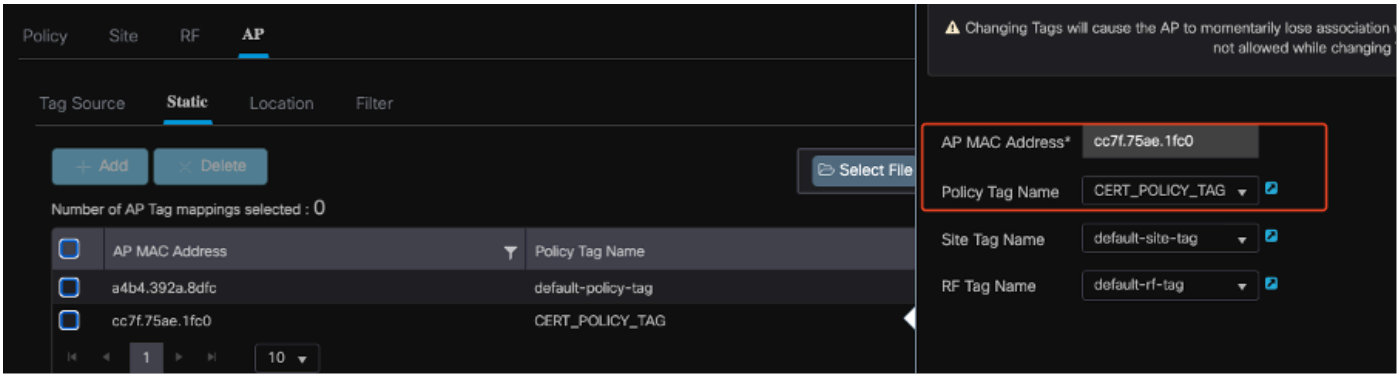


Configuração de marca de política

Mapeie a marca de política para o ponto de acesso na WLC 9800

Para atribuir a etiqueta de política a um ponto de acesso (AP), siga estas etapas:

1. Navegue até Configuration > Tags & Profiles > Tags > AP.
2. Vá para a seção Static (Estático) na configuração do AP.
3. Clique no AP específico que deseja configurar.
4. Atribua a tag policy que você criou ao AP selecionado.



Atribuição de TAG AP

Executando a configuração da WLC após a conclusão da instalação

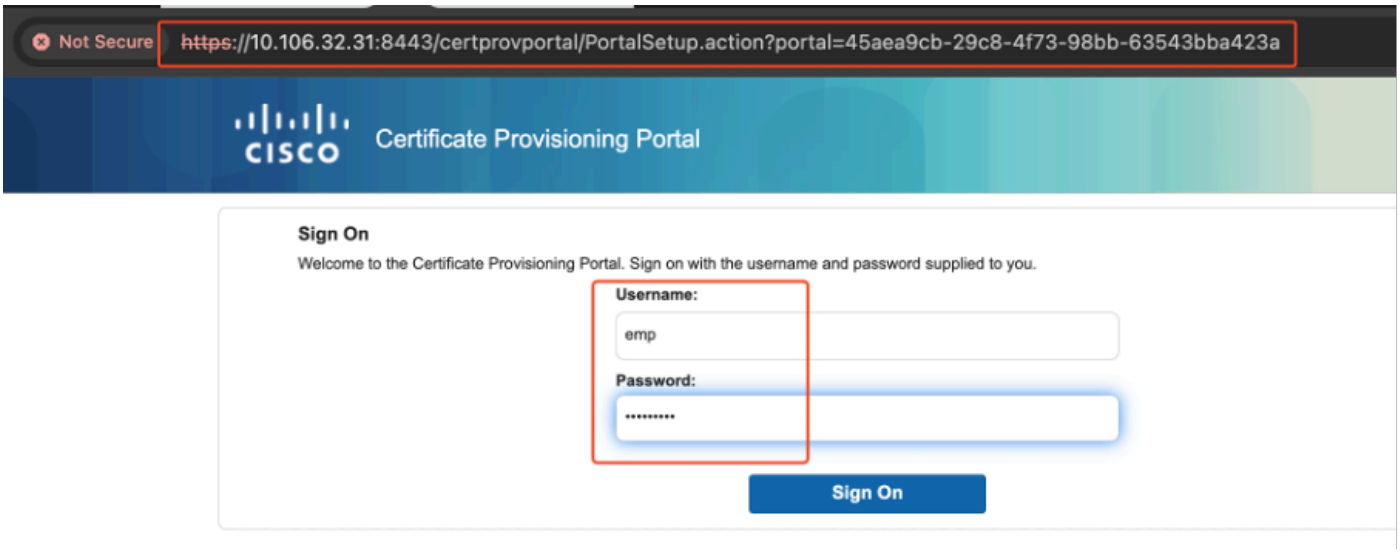
```
aaa group server radius ISE
 server name ISE3
 ip radius source-interface Vlan2124
aaa authentication dot1x CERT_AUTH group ISE
aaa authorization network CERT_AUTH group ISE
aaa server radius dynamic-author
 client 10.106.32.31 server-key Cisco!123
!

wireless profile policy CERT-AUTH
 aaa-override
 ipv4 dhcp required
 vlan 2124
 no shutdown
 wlan CERT-AUTH policy CERT-AUTH
wlan CERT-AUTH 17 CERT-AUTH
```

```
 security dot1x authentication-list CERT_AUTH
 no shutdown
!
wireless tag policy CERT_POLICY_TAG
 wlan CERT-AUTH policy CERT-AUTH
```

Criar e fazer download de certificado para o usuário

Para criar e baixar um certificado para um usuário, siga estas etapas:

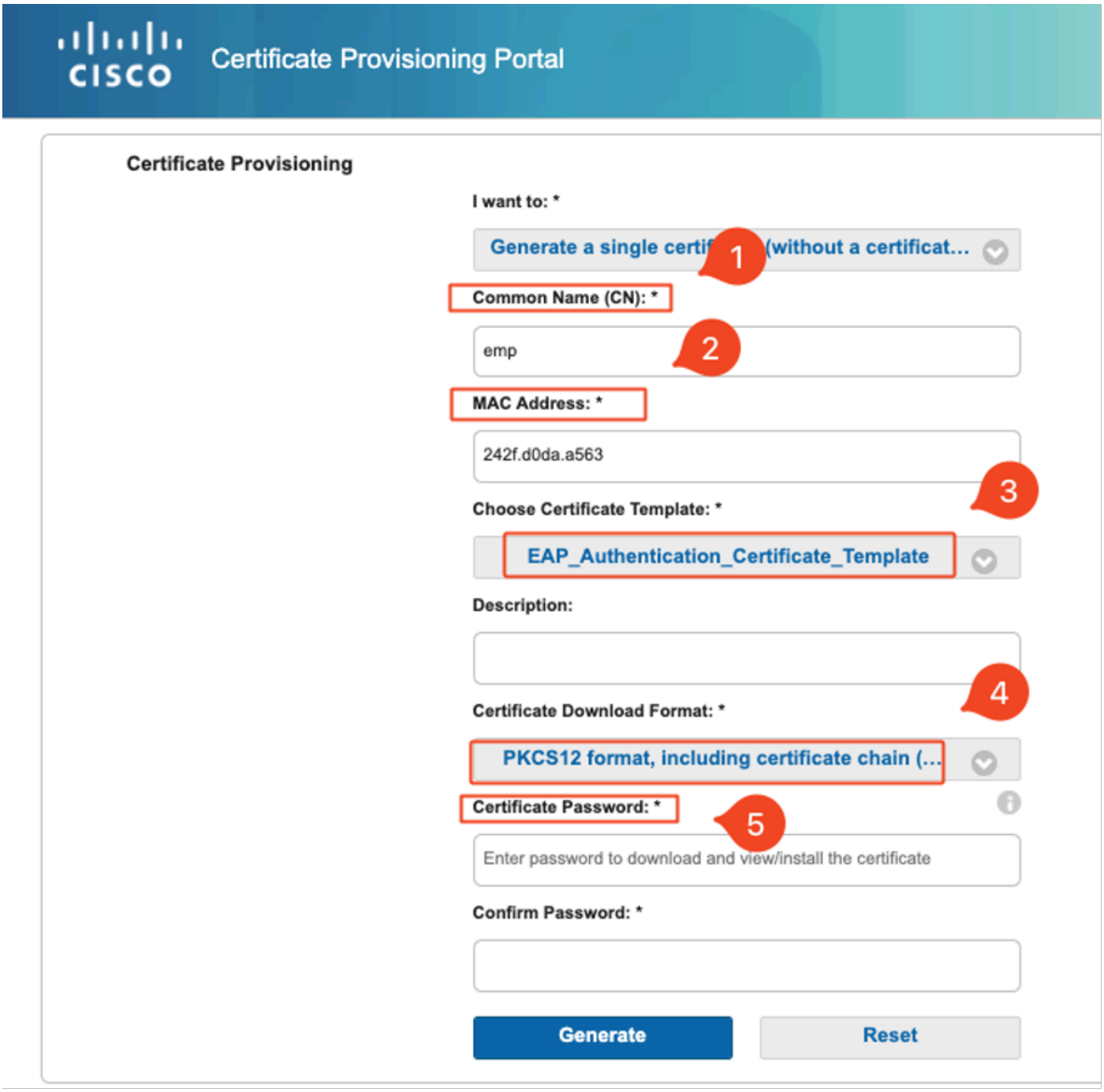
1. Faça com que o usuário faça login no portal de certificados que foi configurado anteriormente.



Acessando o Portal de Certificados

2. Aceite a Política de Uso Aceitável (AUP). Em seguida, o ISE apresenta uma página para geração de certificado.

3. Selecione Gerar um único certificado (sem uma solicitação de assinatura de certificado).



Gerando certificado

Para gerar um certificado por meio do Portal de Provisionamento de Certificado, verifique se estes campos obrigatórios estão preenchidos:

- CN: O servidor de autenticação usa o valor apresentado no campo Nome comum no certificado do cliente para autenticar um usuário. No campo Nome comum, insira o nome de usuário (que você usou para fazer login no Portal de provisionamento de certificado).
- Endereço MAC: A SAN (Subject Alternative Names, nomes alternativos da entidade) é uma extensão X.509 que permite que vários valores sejam associados a um certificado de segurança. O Cisco ISE, versão 2.0, suporta apenas endereços MAC. Portanto, no campo de endereço SAN/MAC.
    - Modelo de certificado: O modelo de certificado define um conjunto de campos que a CA usa ao validar uma solicitação e emitir um certificado. Campos como CN (Common

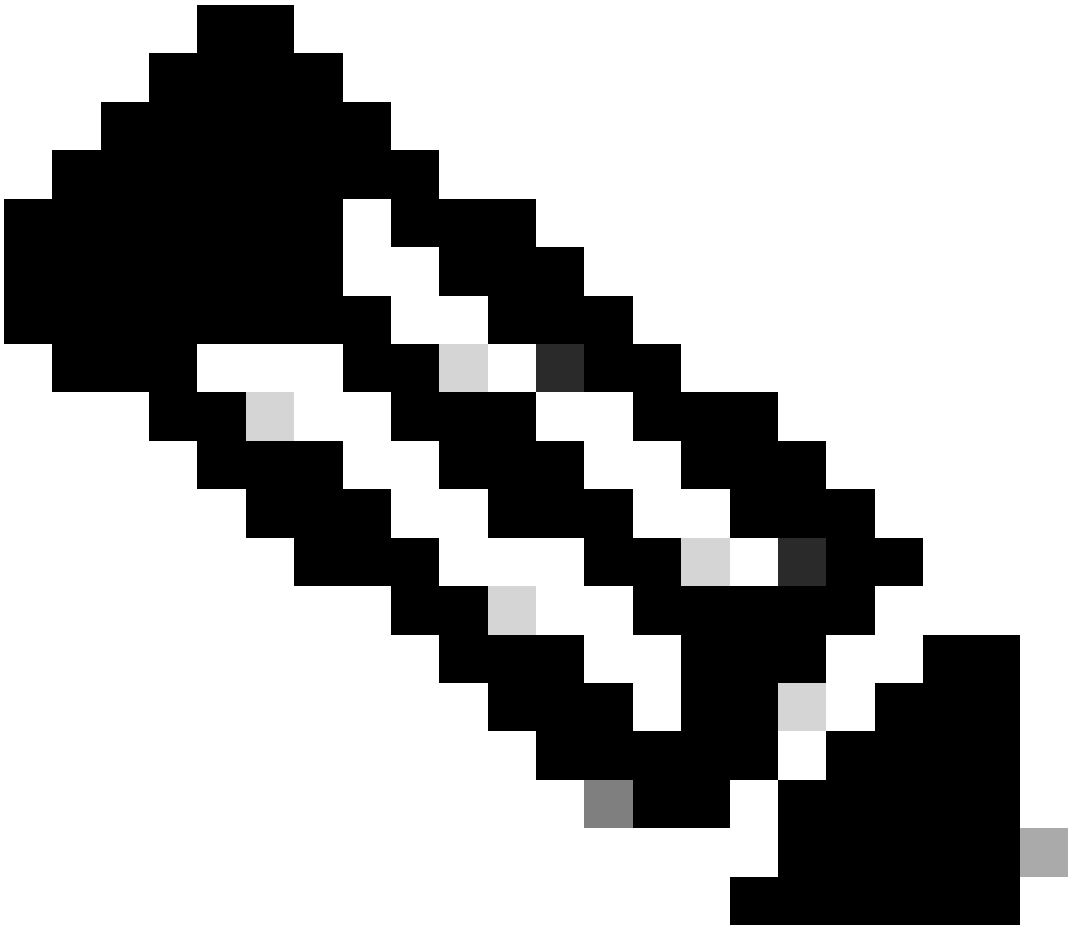
Name, Nome comum) são usados para validar a solicitação (CN deve corresponder ao nome de usuário). Outros campos são usados pela CA ao emitir o certificado.

- Senha do certificado: Você precisa de uma senha de certificado para proteger seu certificado. Você deve fornecer a senha do certificado para exibir o conteúdo do certificado e importar o certificado em um dispositivo.
- Sua senha deve estar de acordo com estas regras:
- A senha deve conter pelo menos 1 letra maiúscula, 1 letra minúscula e 1 dígito
    - A senha deve ter entre 8 e 15 caracteres
    - Os caracteres permitidos incluem A-Z, a-z, 0-9, _, #

Quando todos os campos estiverem preenchidos, selecione Gerar para criar e baixar o certificado.

Instalação do certificado em um computador com Windows 10

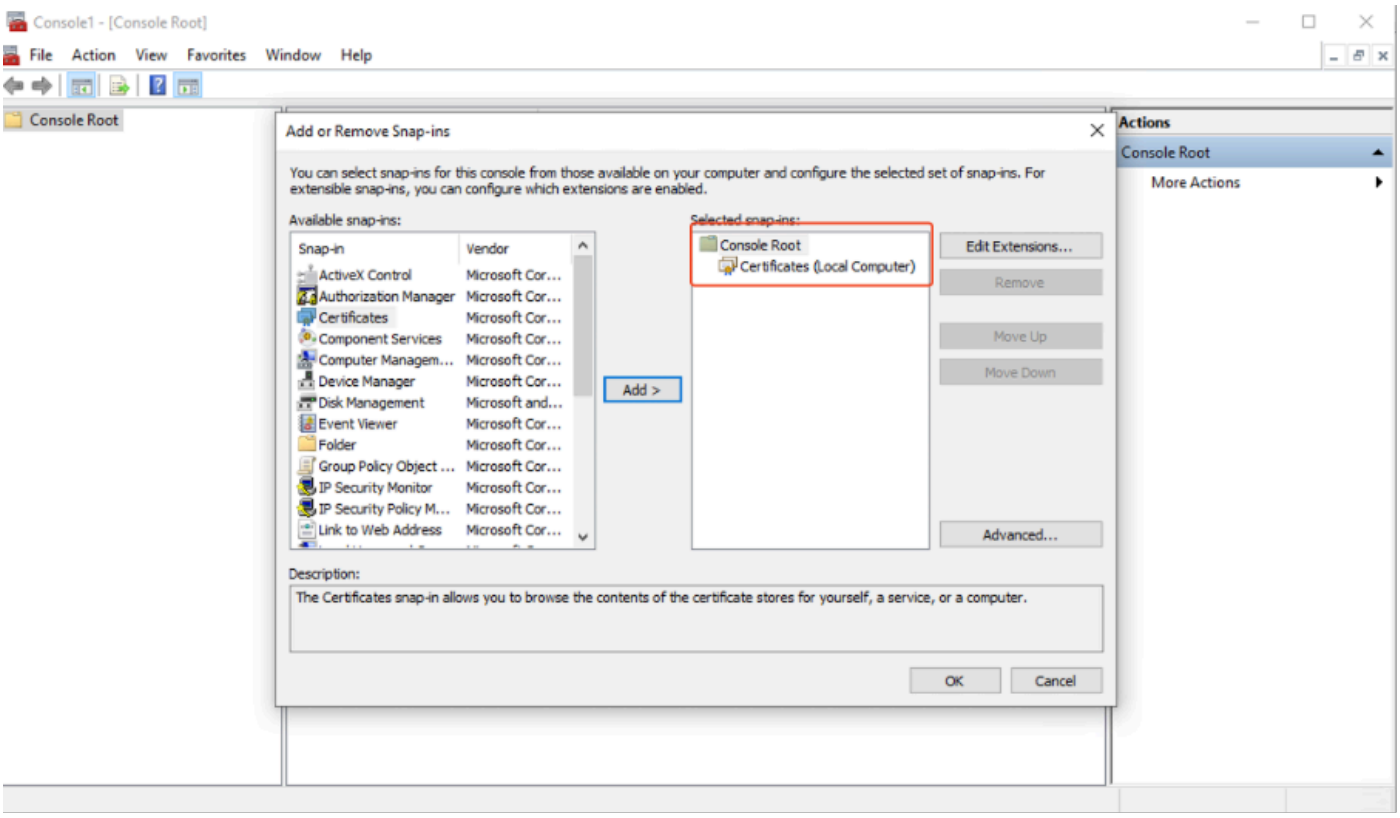
Para instalar um certificado em uma máquina com Windows 10, abra o Console de Gerenciamento Microsoft (MMC) usando estas etapas:



Note: Essas instruções podem variar de acordo com a configuração do Windows, portanto, é recomendável consultar a documentação da Microsoft para obter detalhes específicos.

1. Clique em Iniciar e em Executar.
2. Digite mmc na caixa Executar e pressione Enter. O Console de Gerenciamento Microsoft é aberto.
3. Adicionar Snap-In de Certificado:
4. Vá para Arquivo > Adicionar/Remover snap-in.
5. Selecione Add, escolha Certificates e clique em Add.
6. Selecione Conta do Computador, depois Computador Local e clique em Concluir.

Estas etapas permitem que você gerencie certificados em seu computador local.



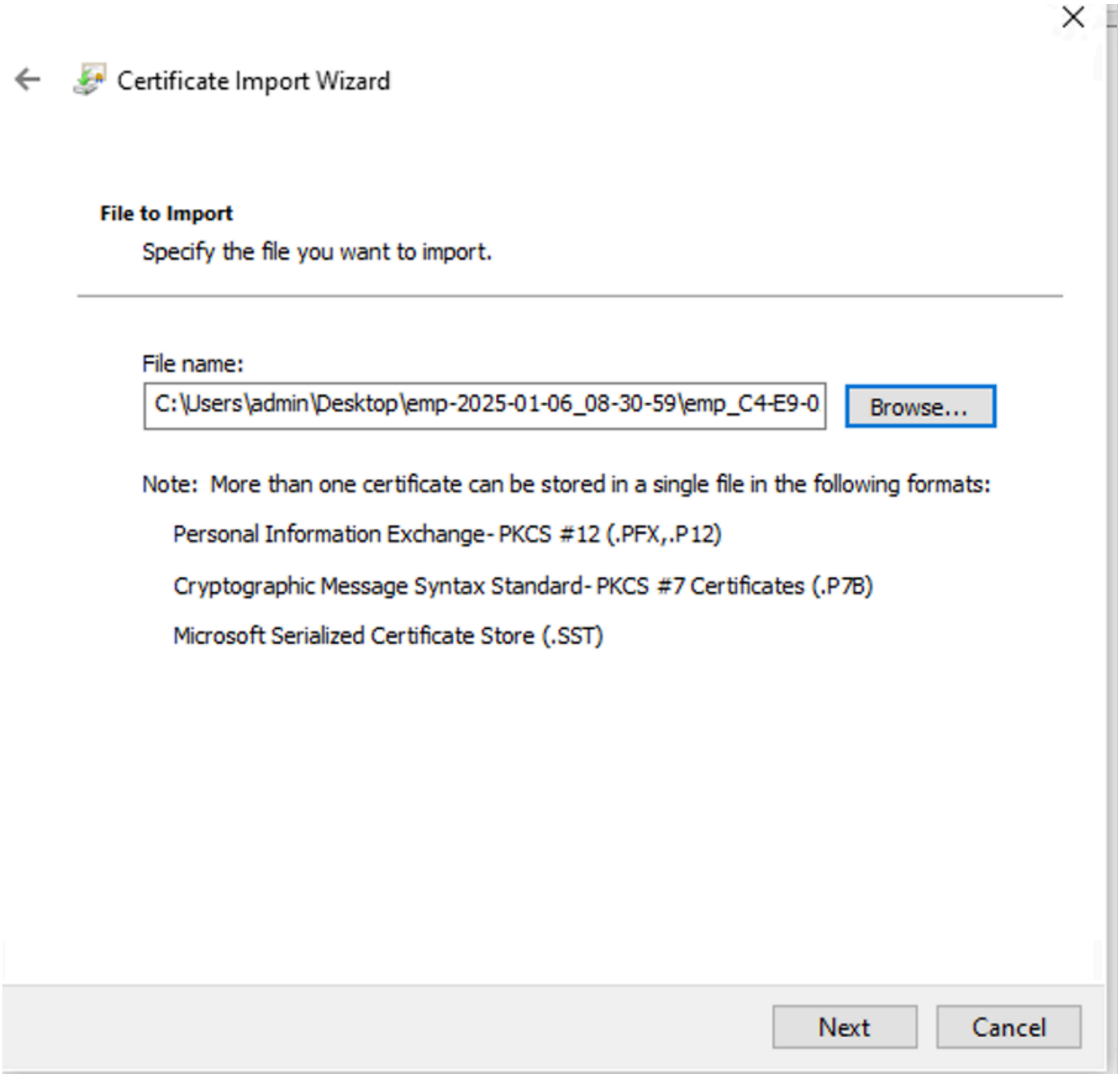
Console MMC do Windows

Etapa 1. Importar o certificado:

1.1. Clique em Action no menu.

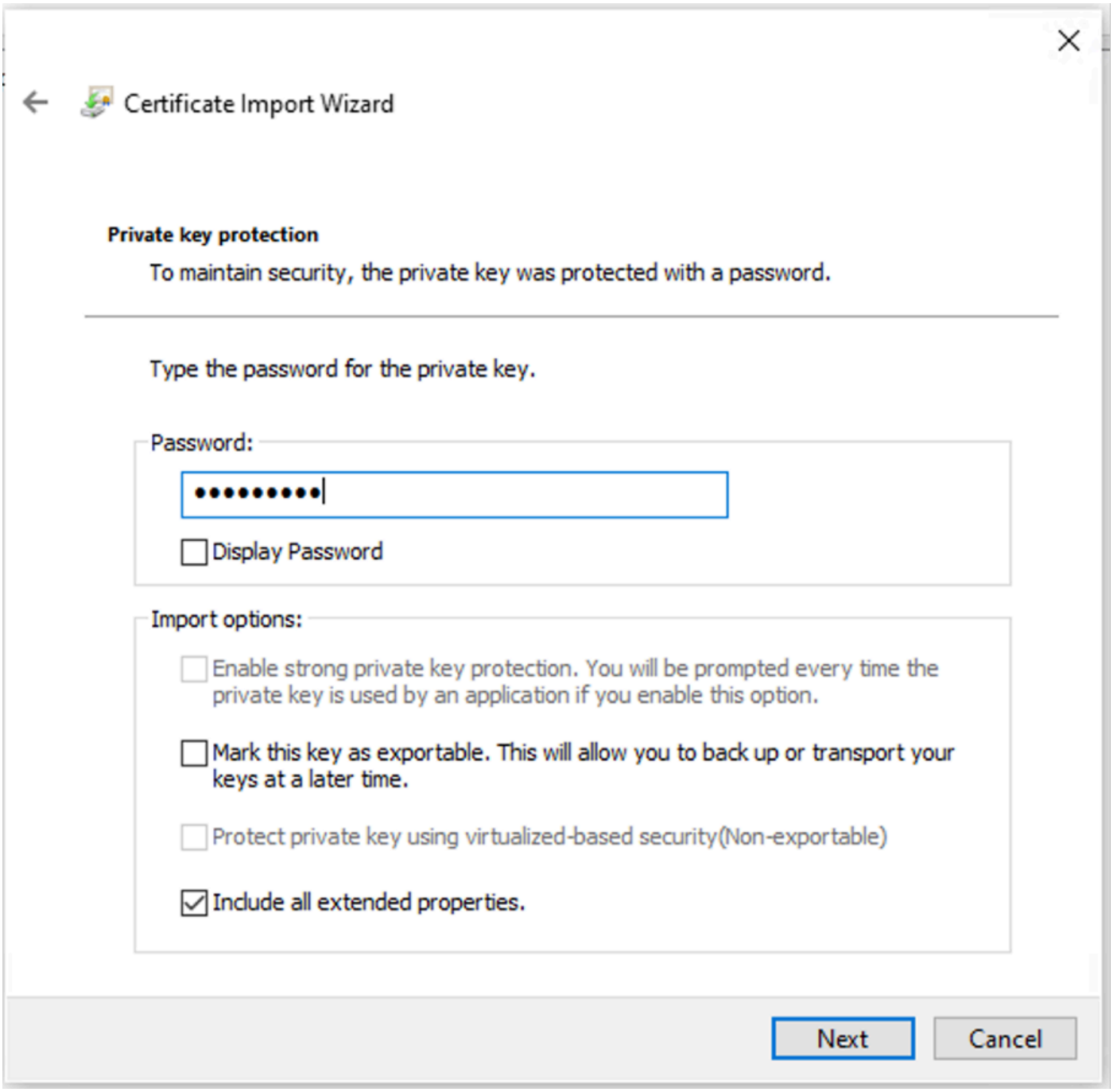
1.2. Vá para All Tasks e selecione Import.

1.3. Continue com os avisos para localizar e selecionar o arquivo de certificado armazenado na sua máquina.



Importando certificado

Durante o processo de importação de certificado, você será solicitado a inserir a senha que criou ao gerar o certificado no portal. Certifique-se de inserir essa senha com precisão para importar e instalar o certificado no seu computador.



Digitando a senha do certificado

Etapa 2. Mover Certificados para as Pastas Apropriadas:

2.1. Abra o Console de Gerenciamento Microsoft (MMC) e navegue até a pasta Certificados (Computador Local) > Pessoal.

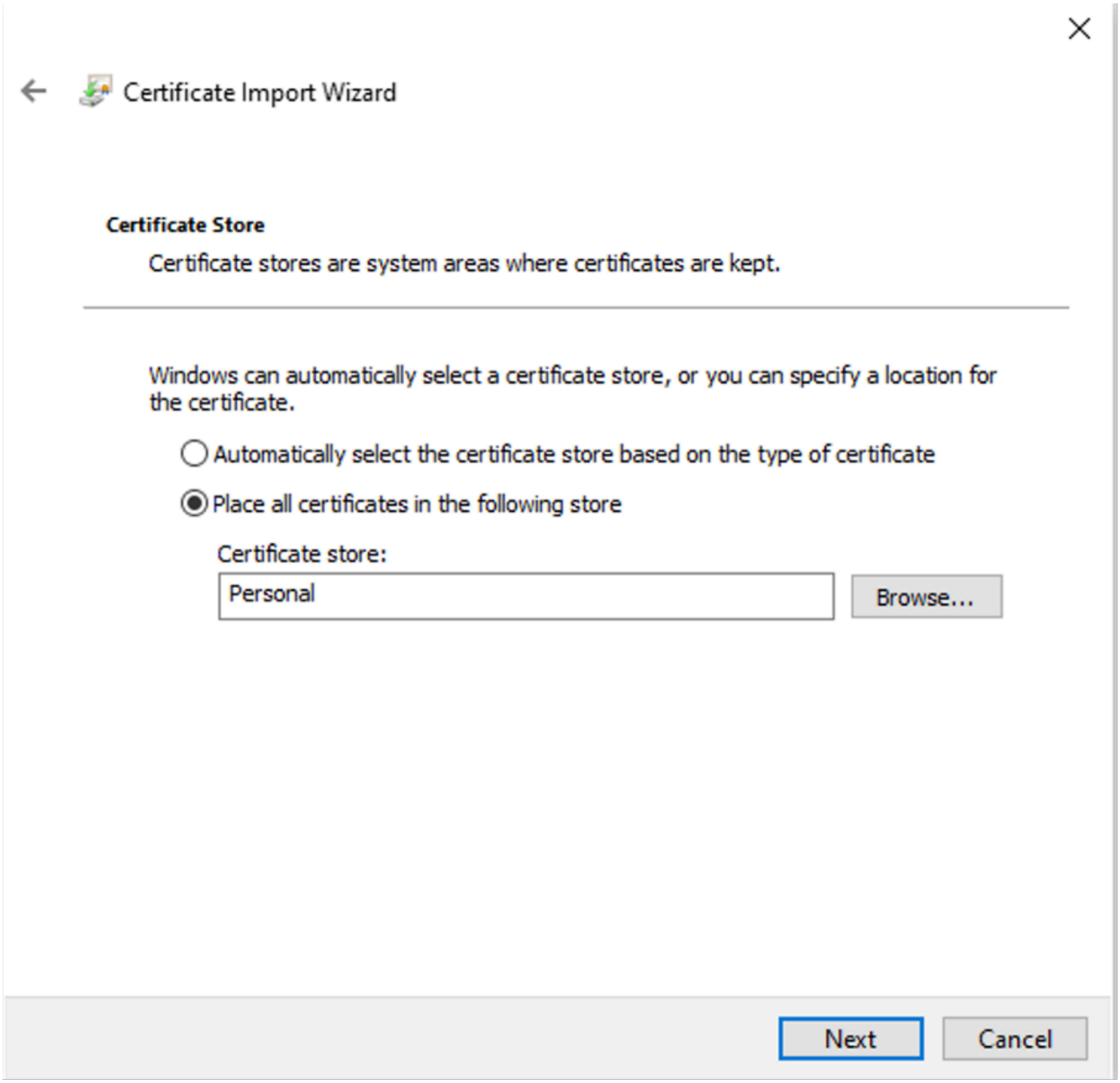
2.2. Revise os certificados e determine seus tipos (por exemplo, CA raiz, CA intermediária ou Pessoal).

2.3. Transferir cada certificado para o armazém adequado:

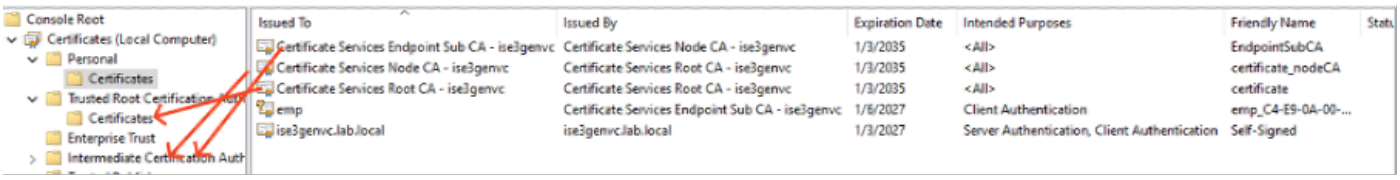
2.4. Certificados de AC de raiz: Mover para Autoridades de Certificação Raiz Confiáveis.

2.5. Certificados CA intermédios: Mude para Autoridades de certificação intermediárias.

2.6. Certificados pessoais: Deixe na pasta Pessoal.



Armazenando certificados na pasta pessoal

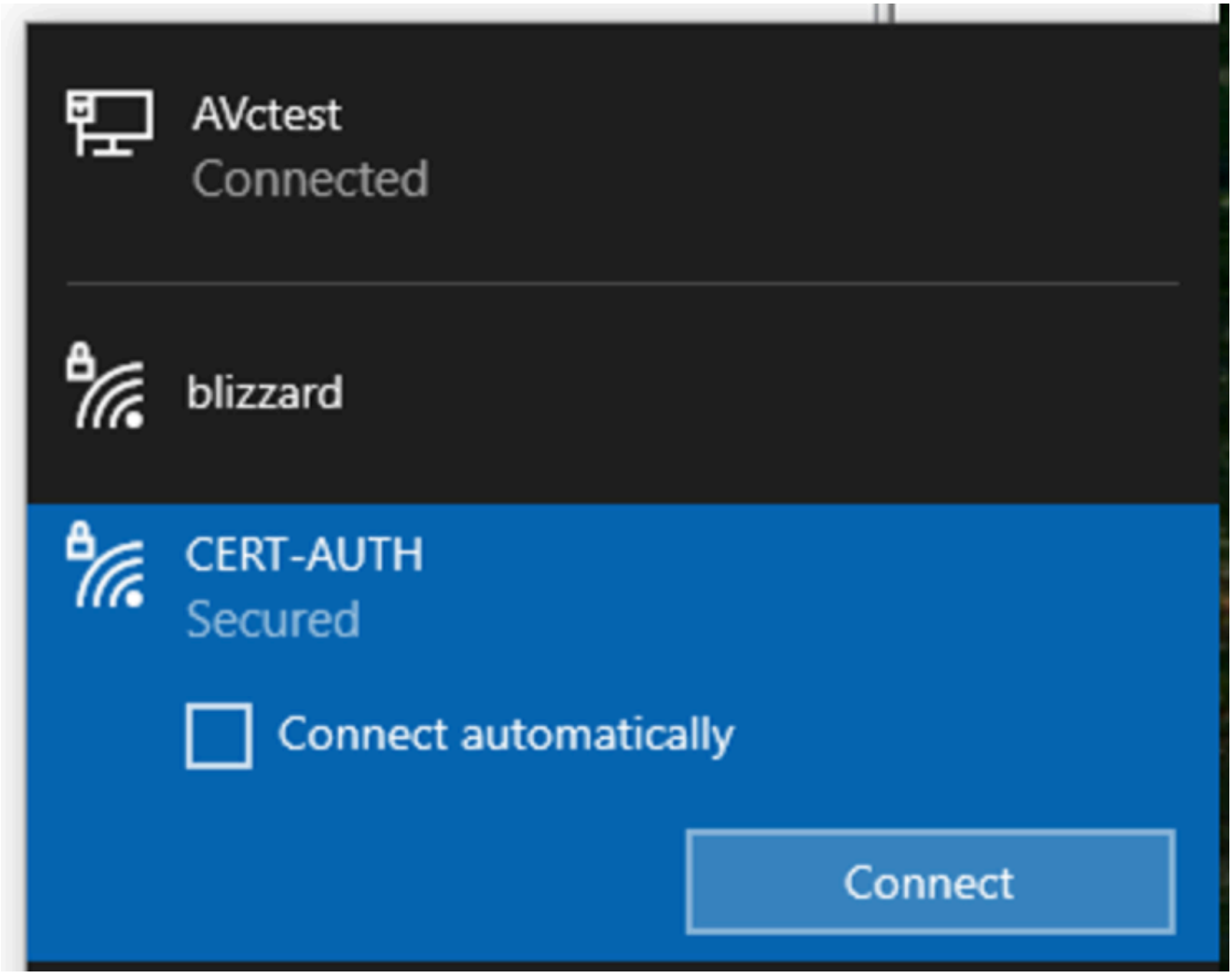


Movendo Certificados em suas Lojas

Conectando a Máquina Windows

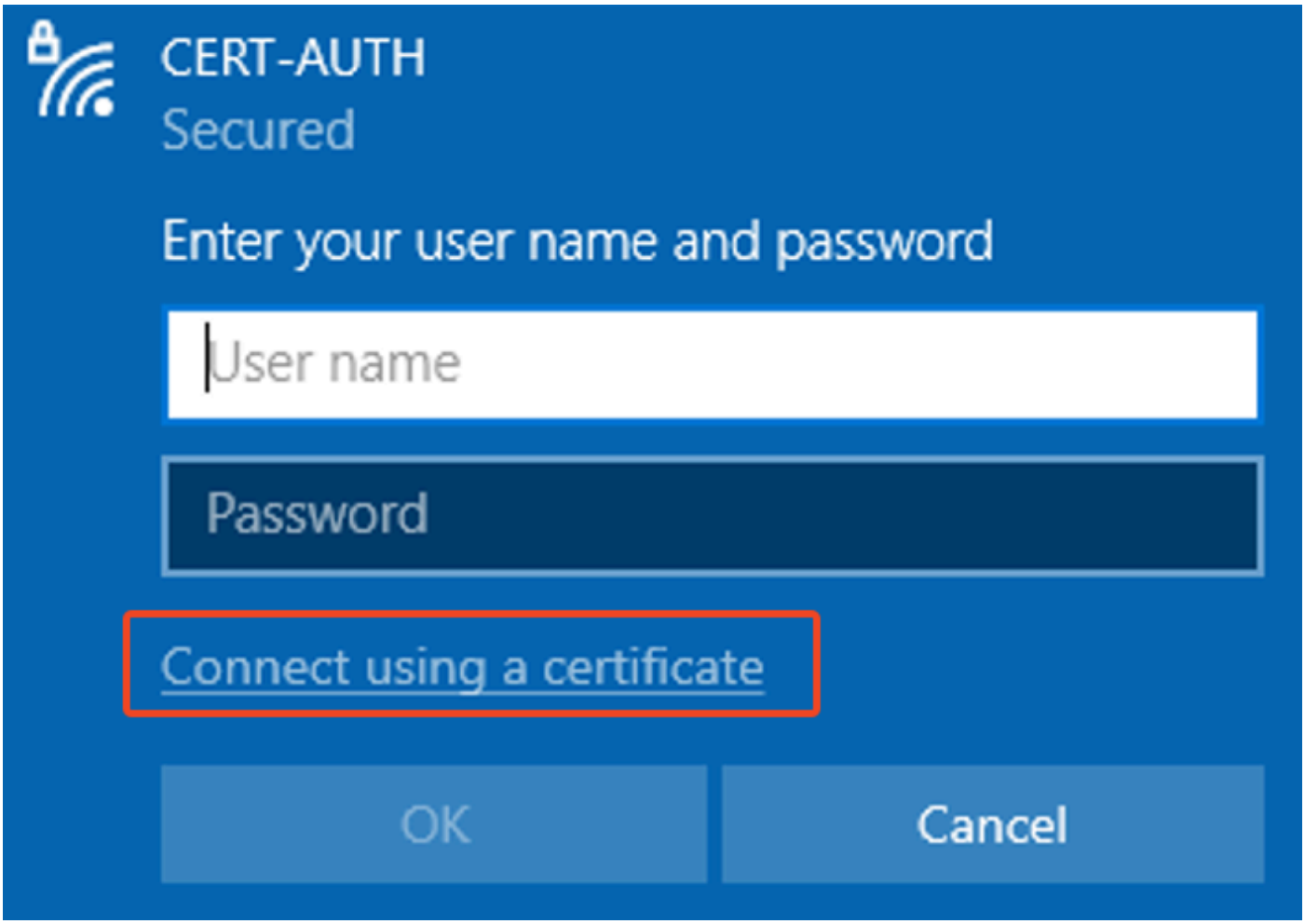
Quando os certificados forem movidos para os armazenamentos corretos, use estas etapas para se conectar à WLAN:

1. Clique no ícone de rede na bandeja do sistema para exibir as redes sem fio disponíveis.
2. Localize e clique no nome da WLAN à qual deseja se conectar.
3. Clique em Connect e continue com todos os prompts adicionais para concluir o processo de conexão usando seu certificado para autenticação.



Conexão à rede sem fio

Quando solicitado durante o processo de conexão com a WLAN, selecione a opção Connect using a certificate.



Usando certificado como credencial

Isso permite que você se conecte com êxito à rede sem fio usando o certificado.

```
C:\>netsh wlan  show interface

There is 1 interface on the system:

    Name                   : Wi-Fi 3
    Description            : TP-Link Wireless USB Adapter
    GUID                   : ee5d1c47-43cc-4873-9ae6-99e2e43c39ea
    Physical address       : 24:2f:d0:da:a5:63
    State                  : connected
    SSID                   : CERT-AUTH
    BSSID                  : a4:88:73:9e:8d:af
    Network type           : Infrastructure
    Radio type             : 802.11ac
    Authentication         : WPA2-Enterprise
    Cipher                 : CCMP
    Connection mode        : Profile
    Channel                : 36
    Receive rate (Mbps)    : 360
    Transmit rate (Mbps)   : 360
    Signal                 : 100%
    Profile                : CERT-AUTH

    Hosted network status  : Not available


C:\>netsh wlan show profiles CERT-AUTH | find "Smart"
    EAP type               : Microsoft: Smart Card or other certificate
```

Verificar o perfil sem fio

Verificar

Verifique se a WLAN está sendo transmitida pela WLC:

<#root>

```
POD6_9800#show wlan summ
Number of WLANs: 2
ID Profile Name SSID Status Security
-----------------------------------------------------------------------------------------------------------------
```

17

CERT-AUTH

CERT-AUTH

UP [WPA2][802.1x][AES]

Verifique se o AP está ativo na WLC:

```
POD6_9800#show ap summ
Number of APs: 1
CC = Country Code
RD = Regulatory Domain
AP Name Slots AP Model Ethernet MAC Radio MAC CC RD IP Address State Location
-------------------------------------------------------------------------------------------------
AP1 3 C9130AXI-D cc7f.75ae.1fc0 a488.739e.8da0 IN -D 10.78.8.78 Registered default location
```

Certifique-se de que o AP esteja transmitindo a WLAN:

<#root>

```
POD6_9800#show ap name AP1 wlan dot11 24ghz
Slot id : 0
WLAN ID BSSID
------------------------
17 a488.739e.8da0

POD6_9800#show ap name AP1 wlan dot11 5ghz
Slot id : 1
WLAN ID BSSID
------------------------
```

17

```
 a488.739e.8daf
```

Cliente conectado usando EAP-TLS:

<#root>

```
POD6_9800#show wire cli summ
Number of Clients: 1
MAC Address AP Name Type ID State Protocol Method Role
-----------------------------------------------------------------------------------------------------
242f.d0da.a563 AP1 WLAN
```

17

```
 IP Learn 11ac
```

Dot1x

```
 Local

POD6_9800#sho wireless client mac-address 242f.d0da.a563 detail | in username|SSID|EAP|AAA|VLAN
```

Wireless LAN Network Name (SSID): CERT-AUTH

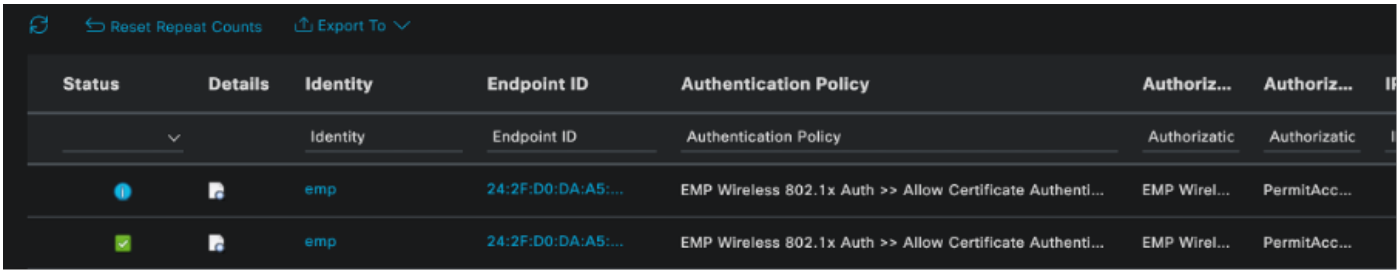
```
BSSID : a488.739e.8daf
```

EAP Type : EAP-TLS

```
VLAN : 2124
Multicast VLAN : 0
```

VLAN : 2124

Registros ao vivo do Cisco Radius ISE:

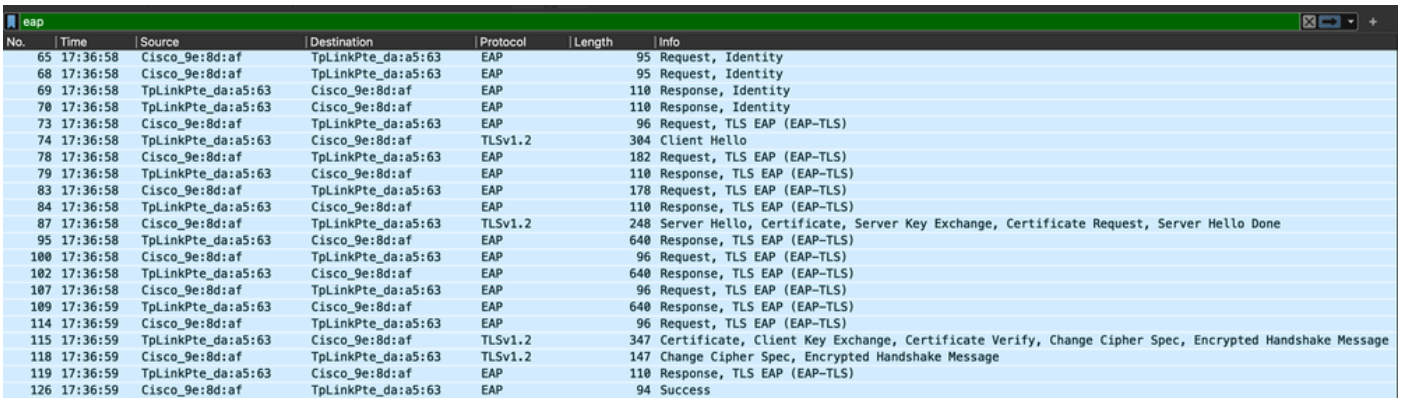


Logs ao vivo do ISE Radius

Tipo de autenticação detalhado:

Logs detalhados do ISE

Captura WLC EPC mostrando os pacotes EAP-TLS:



eap

No.	Time	Source	Destination	Protocol	Length	Info
65	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	95	Request, Identity
68	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	95	Request, Identity
69	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, Identity
70	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, Identity
73	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
74	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	TLSv1.2	304	Client Hello
78	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	182	Request, TLS EAP (EAP-TLS)
79	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
83	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	178	Request, TLS EAP (EAP-TLS)
84	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
87	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	TLSv1.2	248	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
95	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
100	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
102	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
107	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
109	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
114	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
115	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	TLSv1.2	347	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
118	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	TLSv1.2	147	Change Cipher Spec, Encrypted Handshake Message
119	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
126	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	94	Success

Captura de WLC mostrando a transação EAP

- O número de pacote 87 corresponde à etapa 8 no fluxo EAP-TLS descrito no início do documento.
- O número de pacote 115 corresponde à etapa 9 no fluxo EAP-TLS descrito no início do documento.
- O número de pacote 118 corresponde à etapa 10 no fluxo EAP-TLS descrito no início do documento.

Rastreamento Ativo por Rádio (RA) Mostrando a Conexão do Cliente: Esse rastreamento de RA é filtrado para exibir algumas das linhas relevantes da transação de autenticação.

2025/01/08 11 58 20.816875191 {wncd_x_R0-2}{1} [ewlc-capwapmsg-sess] [15655] (debug) Envio de mensagem DTLS criptografada. Dest IP 10.78.8.78[5256], length 499
2025/01/08 11 58 20.851392112 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Enviar Solicitação de Acesso para 10.106.33.23 1812 id 0/25, len 390
2025/01/08 11 58 20.871842938 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Recebido da id 1812/25 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11 58 20.872246323 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Pacote EAPOL Enviado - Versão 3,EAPOL Tipo EAP, Comprimento da Carga 6, Tipo EAP = EAP-TLS
2025/01/08 11 58 20.881960763 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Pacote EAPOL Recebido - Versão 1,EAPOL Tipo EAP, Comprimento da Carga 204, Tipo EAP = EAP-TLS
2025/01/08 11 58 20.882292551 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Enviar solicitação de acesso a 10.106.33.23 1812 id 0/26, len 663
2025/01/08 11 58 20.926204990 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Recebido da id 1812/26 10.106.33.23 0, Access-Challenge, len 1135
2025/01/08 11 58 20.927390754 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Pacote EAPOL Enviado - Versão 3,EAPOL Tipo EAP, Comprimento da Carga 1012, EAP-Type = EAP-TLS
2025/01/08 11 58 20.935081108 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Pacote EAPOL Recebido - Versão 1,EAPOL Tipo EAP, Tamanho da Carga 6, Tipo EAP = EAP-TLS
2025/01/08 11 58 20.935405770 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Enviar solicitação de acesso a 10.106.33.23 1812 id 0/27, len 465
2025/01/08 11 58 20.938485635 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Recebido da id

1812/27 10.106.33.23 0, Access-Challenge, len 1131
2025/01/08 11 58 20.939630108 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Pacote EAPOL Enviado - Versão 3,EAPOL Tipo EAP, Comprimento da Carga 1008, EAP-Type = EAP-TLS
2025/01/08 11 58 20.947417061 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Pacote EAPOL Recebido - Versão 1,EAPOL Tipo EAP, Tamanho da Carga 6, Tipo EAP = EAP-TLS
2025/01/08 11 58 20.947722851 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Enviar solicitação de acesso a 10.106.33.23 1812 id 0/28, len 465
2025/01/08 11 58 20.949913199 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Recebido da id 1812/28 10.106.33.23 0, Access-Challenge, len 275
2025/01/08 11 58 20.950432303 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Pacote EAPOL Enviado - Versão 3,EAPOL Tipo EAP, Comprimento da Carga 158, EAP-Tipo = EAP-TLS
2025/01/08 11 58 20.966862562 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Pacote EAPOL Recebido - Versão 1,EAPOL Tipo EAP, Comprimento da Carga 1492, Tipo EAP = EAP-TLS
2025/01/08 11 58 20.967209224 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Enviar Solicitação de Acesso para 10.106.33.23 1812 id 0/29, len 1961
2025/01/08 11 58 20.971337739 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Recebido da id 1812/29 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11 58 20.971708100 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Pacote EAPOL Enviado - Versão 3,EAPOL Tipo EAP, Comprimento da Carga 6, Tipo EAP = EAP-TLS
2025/01/08 11 58 20.978742828 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Pacote EAPOL Recebido - Versão 1,EAPOL Tipo EAP, Comprimento da Carga 1492, Tipo EAP = EAP-TLS
2025/01/08 11 58 20.979081544 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Enviar solicitação de acesso a 10.106.33.23 1812 id 0/30, len 1961
2025/01/08 11 58 20.982535977 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Recebido da id 1812/30 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11 58 20.982907200 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Pacote EAPOL Enviado - Versão 3,EAPOL Tipo EAP, Comprimento da Carga 6, Tipo EAP = EAP-TLS
2025/01/08 11 58 20.990141062 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Pacote EAPOL Recebido - Versão 1,EAPOL Tipo EAP, Comprimento da Carga 1492, Tipo EAP = EAP-TLS
2025/01/08 11 58 20.990472026 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Enviar Solicitação de Acesso para 10.106.33.23 1812 id 0/31, len 1961
2025/01/08 11 58 20.994358525 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Recebido da id 1812/31 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11 58 20.994722151 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Pacote EAPOL Enviado - Versão 3,EAPOL Tipo EAP, Comprimento da Carga 6, Tipo EAP = EAP-TLS
2025/01/08 11 58 21.001735553 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Pacote EAPOL Recebido - Versão 1,EAPOL Tipo EAP, Comprimento da

Carga 247, EAP-Tipo = EAP-TLS
2025/01/08 11 58 21.002076369 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Enviar Solicitação de Acesso para 10.106.33.23 1812 id 0/32, len 706
2025/01/08 11 58 21.013571608 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Recebido da id 1812/32 10.106.33.23 0, Access-Challenge, len 174
2025/01/08 11 58 21.013987785 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Pacote EAPOL Enviado - Versão 3,EAPOL Tipo EAP, Comprimento da Carga 57, EAP-Type = EAP-TLS
2025/01/08 11 58 21.024429150 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Pacote EAPOL Recebido - Versão 1,EAPOL Tipo EAP, Tamanho da Carga 6, Tipo EAP = EAP-TLS
2025/01/08 11 58 21.024737996 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Enviar Solicitação de Acesso para 10.106.33.23 1812 id 0/33, len 465
2025/01/08 11 58 21.057794929 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Recebido da id 1812/33 10.106.33.23 0, Access-Accept, len 324
2025/01/08 11 58 21.058149893 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Evento de atualização de identidade levantada para método EAP-TLS

Troubleshooting

Não há etapas de Troubleshooting específicas para este problema além dos procedimentos de Troubleshooting 802.1x Wireless típicos:

1. Use depurações de rastreamento do RA do cliente para verificar o processo de autenticação.
2. Execute uma captura EPC de WLC para examinar os pacotes entre o cliente, a WLC e o servidor RADIUS.
3. Verifique os logs ao vivo do ISE para verificar se a solicitação corresponde à política correta.
4. Verifique no ponto de extremidade do Windows se o certificado está instalado corretamente e se toda a cadeia de confiança está presente.

Referências

- Perguntas frequentes do Portal de provisionamento de certificado, versão 3.2
- Entender os serviços de autoridade de certificação interna do ISE
- Entender e configurar o EAP-TLS com uma WLC e um ISE

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.