Configuración de EAP-TLS en el WLC 9800 con CA interna de ISE

Contenido

Introducción

Este documento describe la autenticación EAP-TLS mediante la Autoridad de certificación de

Identity Services Engine para autenticar a los usuarios.

Prerequisites

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Controlador inalámbrico: C9800-40-K9 que ejecuta 17.09.04a
- Cisco ISE: Ejecución del Parche 4 de la Versión 3
- Modelo de PA: C9130AXI-D
- Switch: 9200-L-24P

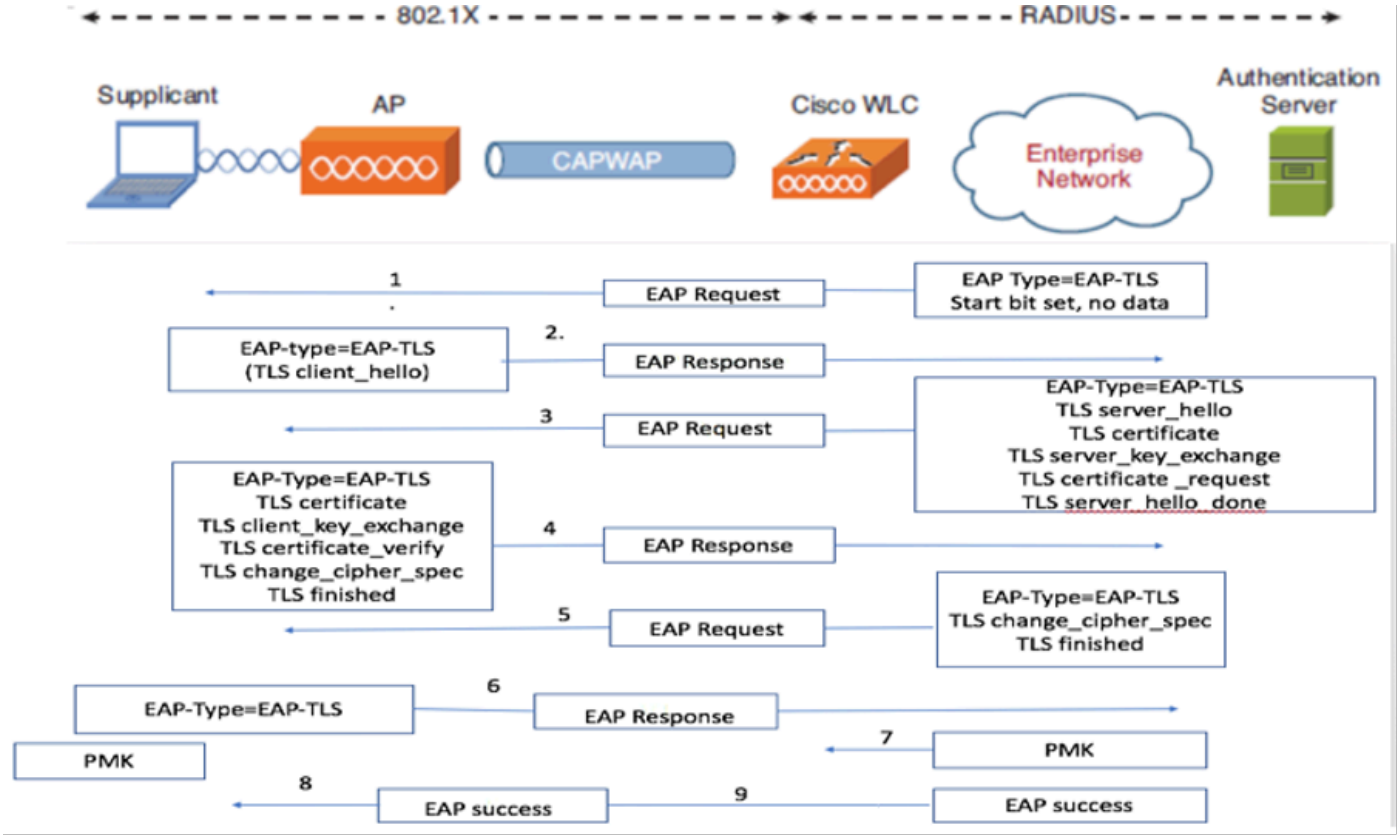
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La mayoría de las organizaciones tienen su propia CA que emite certificados para los usuarios finales para la autenticación EAP-TLS. ISE incluye una autoridad de certificación integrada que se puede utilizar para generar certificados para los usuarios que se utilizarán en la autenticación EAP-TLS. En situaciones en las que no es posible utilizar una CA completa, resulta ventajoso utilizar la CA de ISE para la autenticación de usuarios.

Este documento describe los pasos de configuración requeridos para utilizar de manera efectiva la CA ISE para autenticar a los usuarios inalámbricos. Flujo de autenticación EAP-TLS

Flujo de autenticación EAP-TLS



Flujo de autenticación EAP-TLS

Pasos del flujo EAP-TLS

1. El cliente inalámbrico se asocia al punto de acceso (AP).
2. En esta etapa, el AP no permite la transmisión de datos y envía una solicitud de autenticación.
3. El cliente, actuando como solicitante, responde con una identidad de respuesta EAP.
4. El controlador de LAN inalámbrica (WLC) reenvía la información de ID de usuario al servidor de autenticación.
5. El servidor RADIUS responde al cliente con un paquete de inicio EAP-TLS.
6. La conversación EAP-TLS comienza a partir de este punto.
7. El cliente envía una respuesta EAP al servidor de autenticación, incluyendo un mensaje de entrada en contacto client_hello con un cifrado establecido en NULL.
8. El servidor de autenticación responde con un paquete Access-Challenge que contiene:

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

9. El cliente responde con un mensaje EAP-Response que incluye:

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

10. Tras una autenticación de cliente exitosa, el servidor RADIUS envía un Access-Challenge que contiene:

```
Change_cipher_spec
Handshake finished message
```

11. El cliente verifica el hash para autenticar el servidor RADIUS.

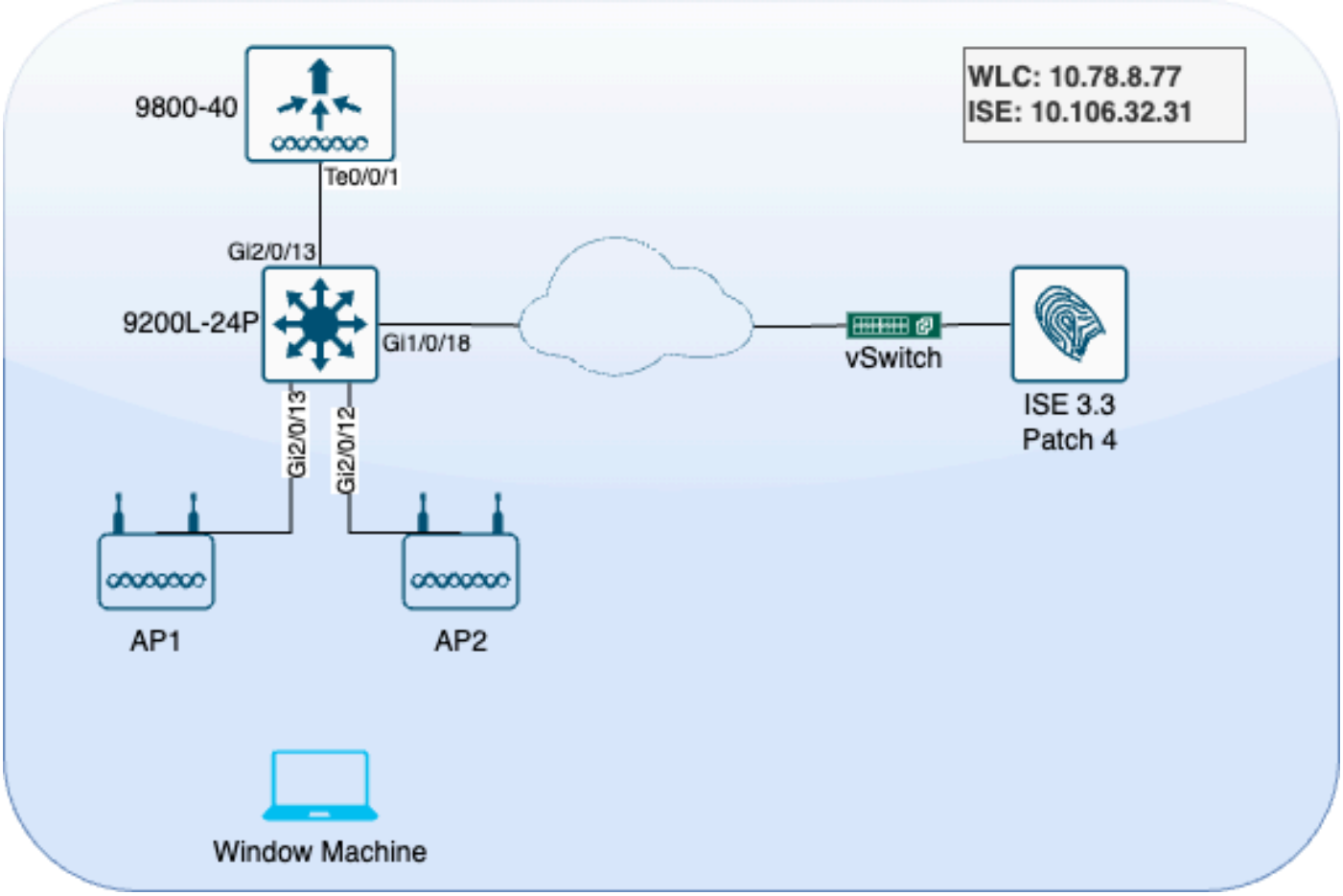
12. Una nueva clave de cifrado se deriva dinámicamente del secreto durante el intercambio de señales TLS.

13. Se envía un mensaje EAP-Success desde el servidor al autenticador y luego al solicitante.

14. El cliente inalámbrico habilitado para EAP-TLS ahora puede acceder a la red inalámbrica.

Configurar

Diagrama de la red



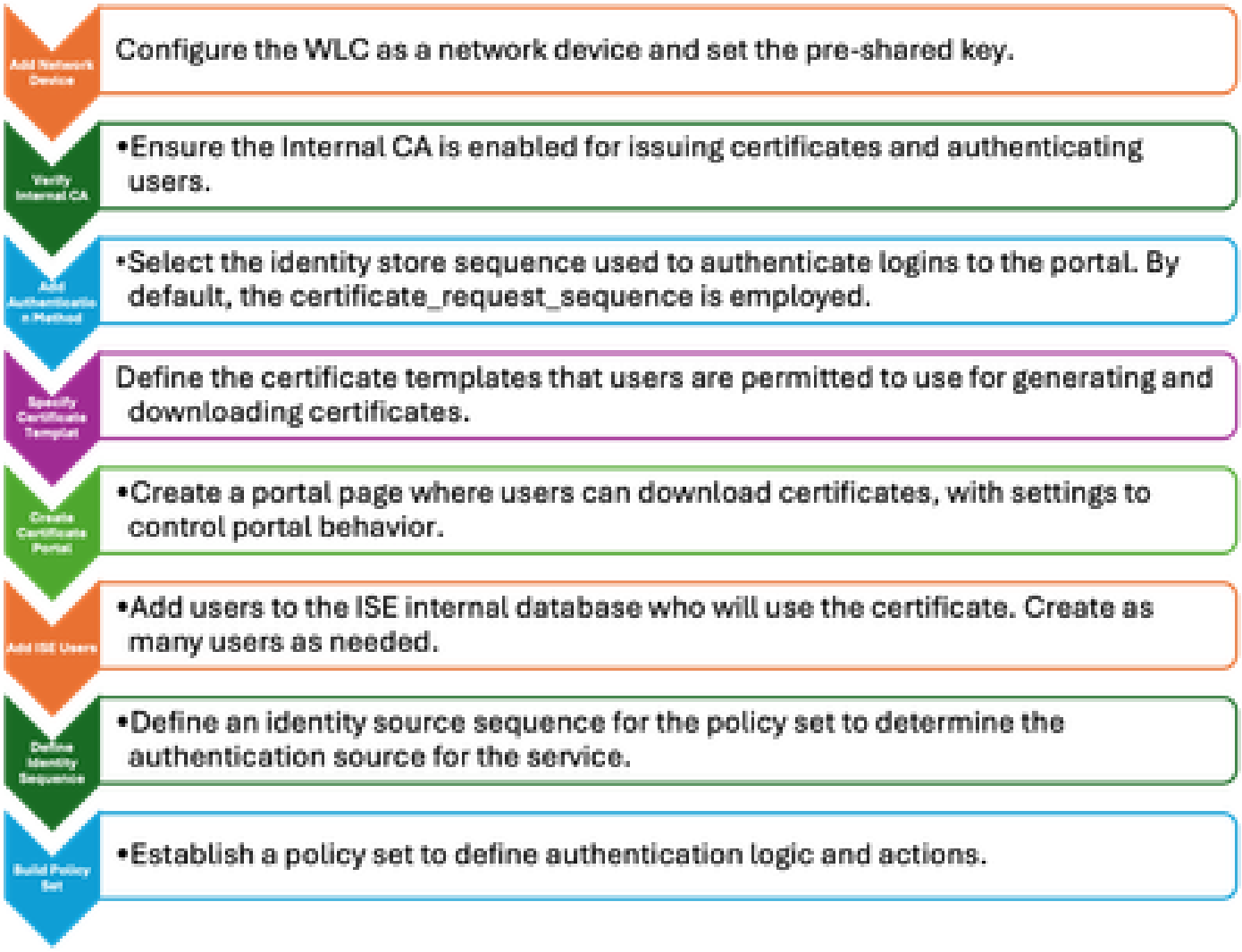
Topología de laboratorio

Configuraciones

En esta sección, configuramos dos componentes: ISE y 9800 WLC.

Configuración de ISE

Estos son los pasos de configuración para el servidor ISE. Cada paso se acompaña de capturas de pantalla en esta sección para proporcionar orientación visual.

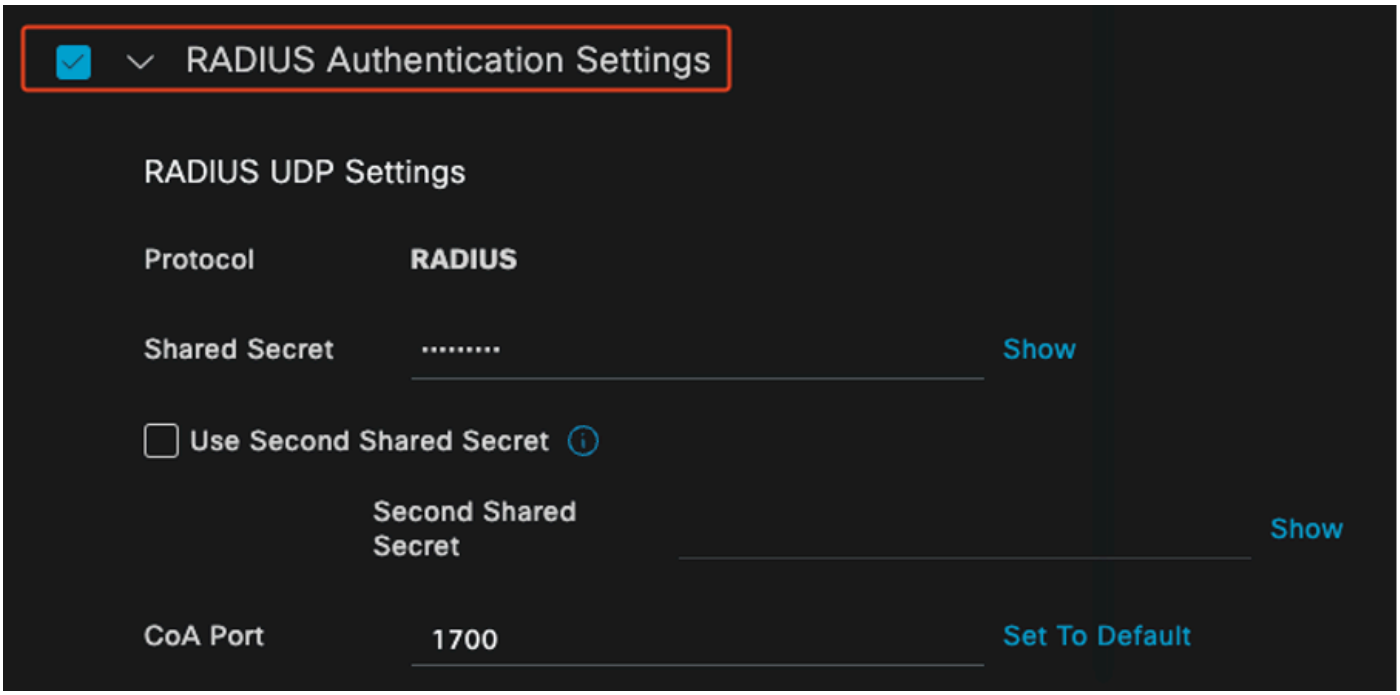


Pasos de configuración del servidor ISE

Adición de un dispositivo de red

Para agregar el controlador de LAN inalámbrica (WLC) como dispositivo de red, siga estas instrucciones:

1. Vaya a Administration > Network Resources > Network Devices.
2. Haga clic en el icono +Add para iniciar el proceso de agregar el WLC.
3. Asegúrese de que la clave previamente compartida coincida tanto con el WLC como con el servidor ISE para habilitar una comunicación adecuada.
4. Una vez introducidos correctamente todos los detalles, haga clic en Submit en la esquina inferior izquierda para guardar la configuración

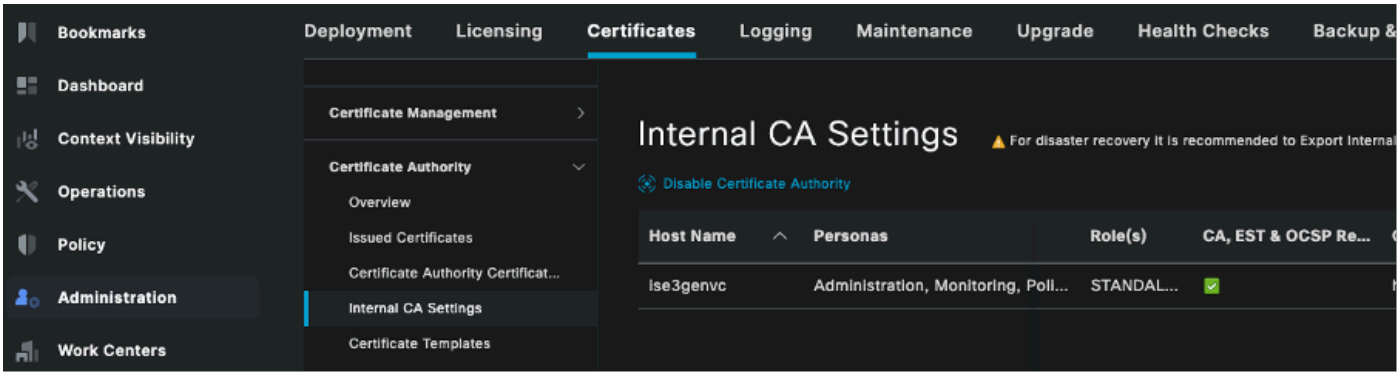


Adición de un dispositivo de red

Verificar CA interna

Para comprobar la configuración de la Autoridad de certificación interna (CA), siga estos pasos:

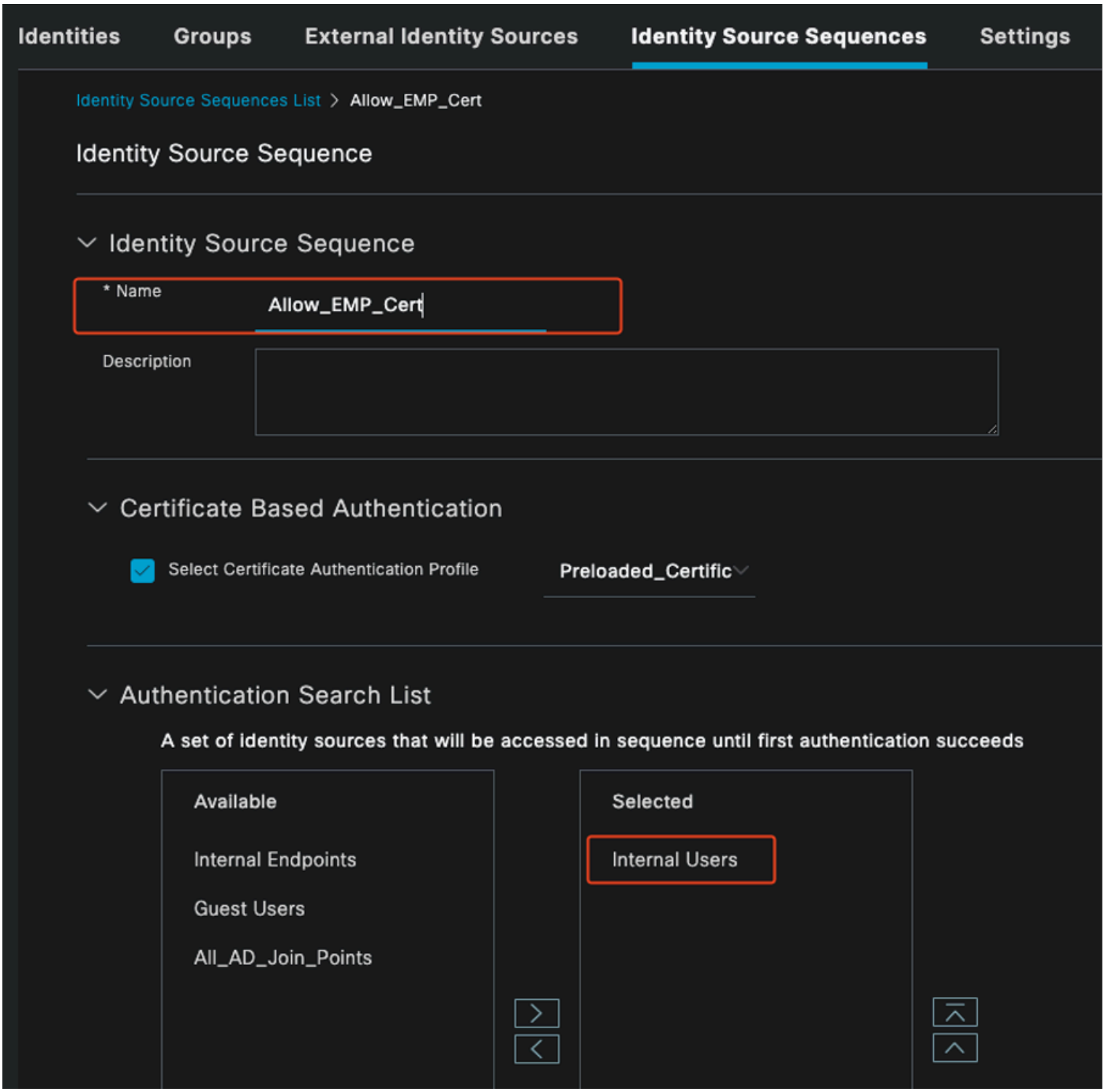
1. Vaya a Administration > System > Certificates > Certificate Authority > Internal CA Settings.
2. Asegúrese de que la columna CA esté habilitada para confirmar que la CA interna está activa.



Verificar CA interna

Agregar método de autenticación

Vaya a Administration > Identity Management > Identity Source Sequences. Agregue una secuencia de identidad personalizada para controlar el origen de inicio de sesión del portal.



método de autentificación

Especificar plantilla de certificado

Para especificar una plantilla de certificado, siga estos pasos:

Paso 1. Navegue hasta Administración > Sistema > Certificados > Autoridad de Certificados > Plantillas de Certificados.

Paso 2. Haga clic en el icono +Agregar para crear una nueva plantilla de certificado:

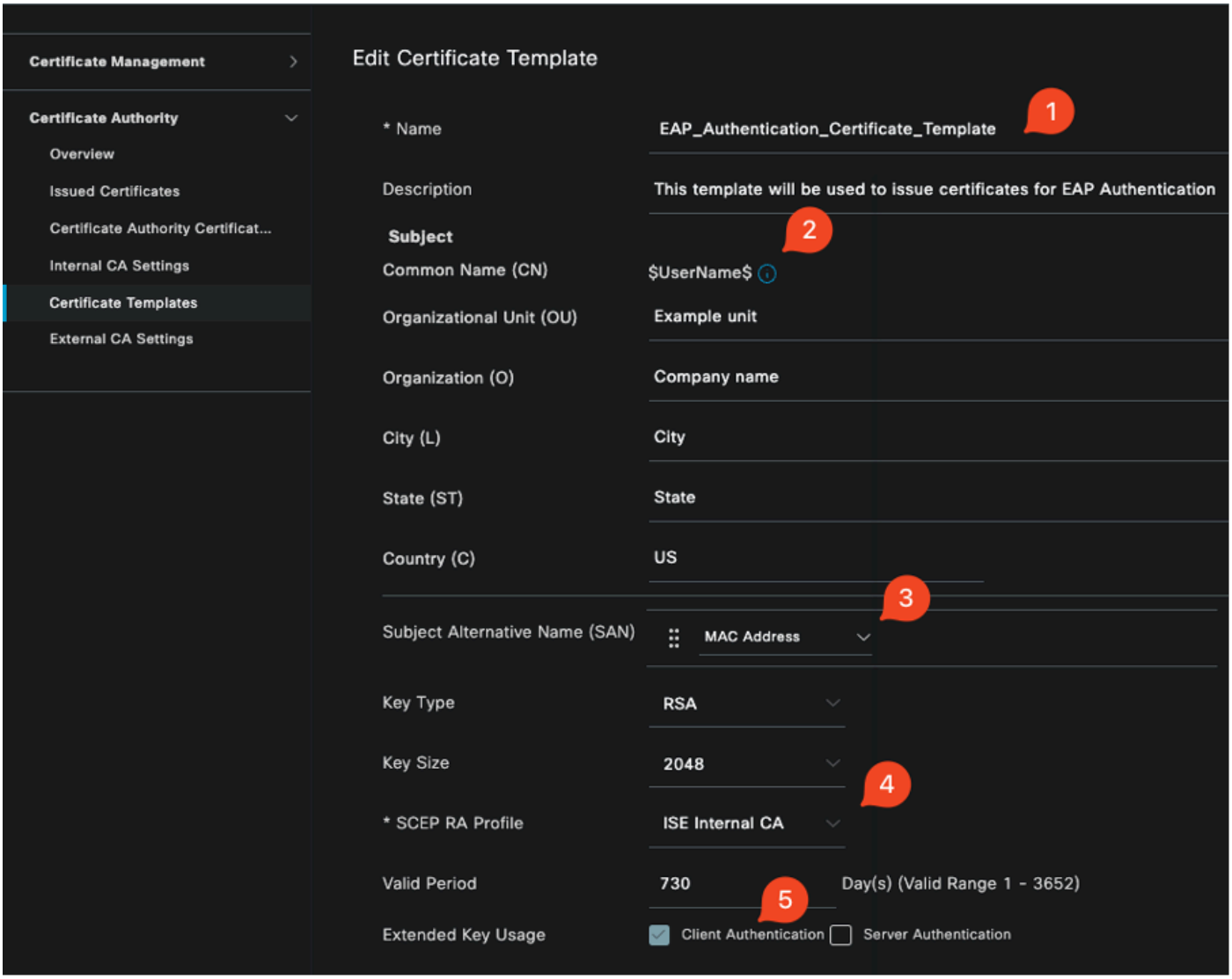
2.1 Proporcione un nombre único local para la plantilla en el servidor ISE.

2.2 Asegúrese de que Common Name (CN) está establecido en $UserName$.

2.3 Compruebe que el nombre alternativo del sujeto (SAN) está asignado a la dirección MAC.

2.4 Establezca el perfil SCEP RA en CA interna de ISE.

2.5 En la sección de uso de clave ampliada, habilite la autenticación de cliente.



Plantilla de certificado

Crear portal de certificados

Para crear un portal de certificados para la generación de certificados de cliente, siga estos pasos:

Paso 1. Vaya a Administración > Administración del portal de dispositivos > Aprovisionamiento de certificados.

Paso 2. Haga clic en Crear para configurar una nueva página del portal.

Paso 3. Proporcione un nombre único para que el portal lo identifique fácilmente.

3.1. Elija el número de puerto para que el portal funcione; configure esto en 8443.

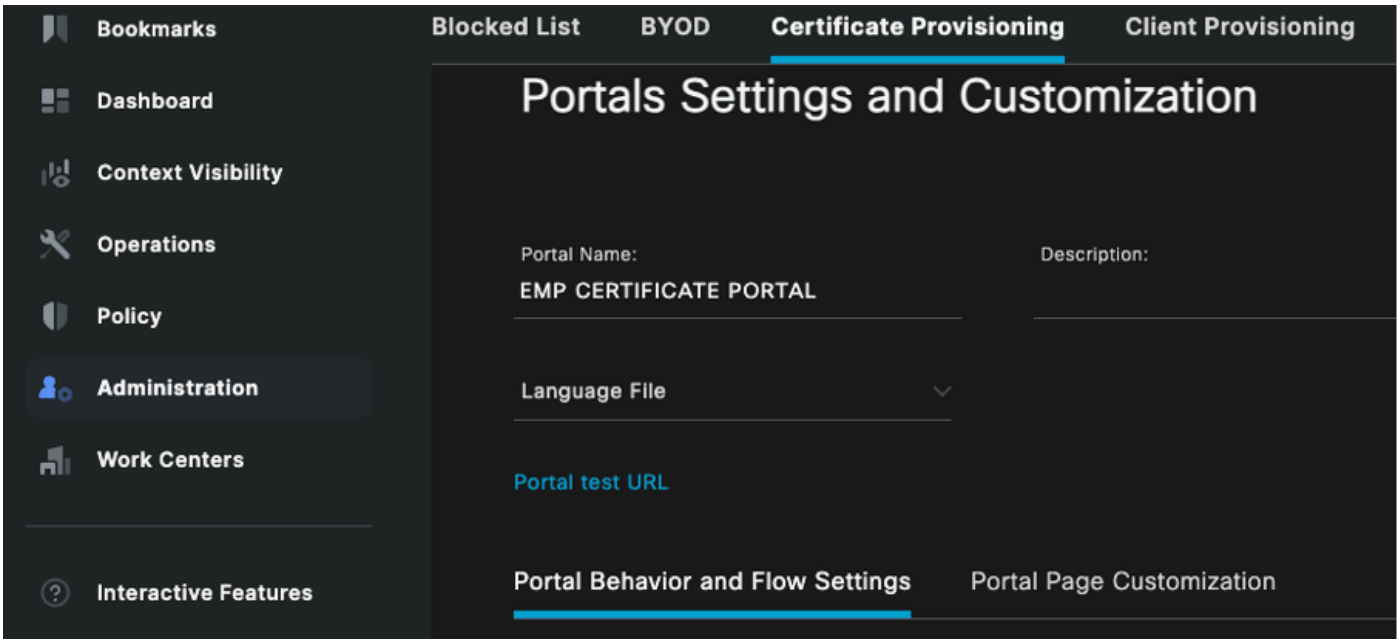
3.2. Especifique las interfaces en las que ISE escucha este portal.

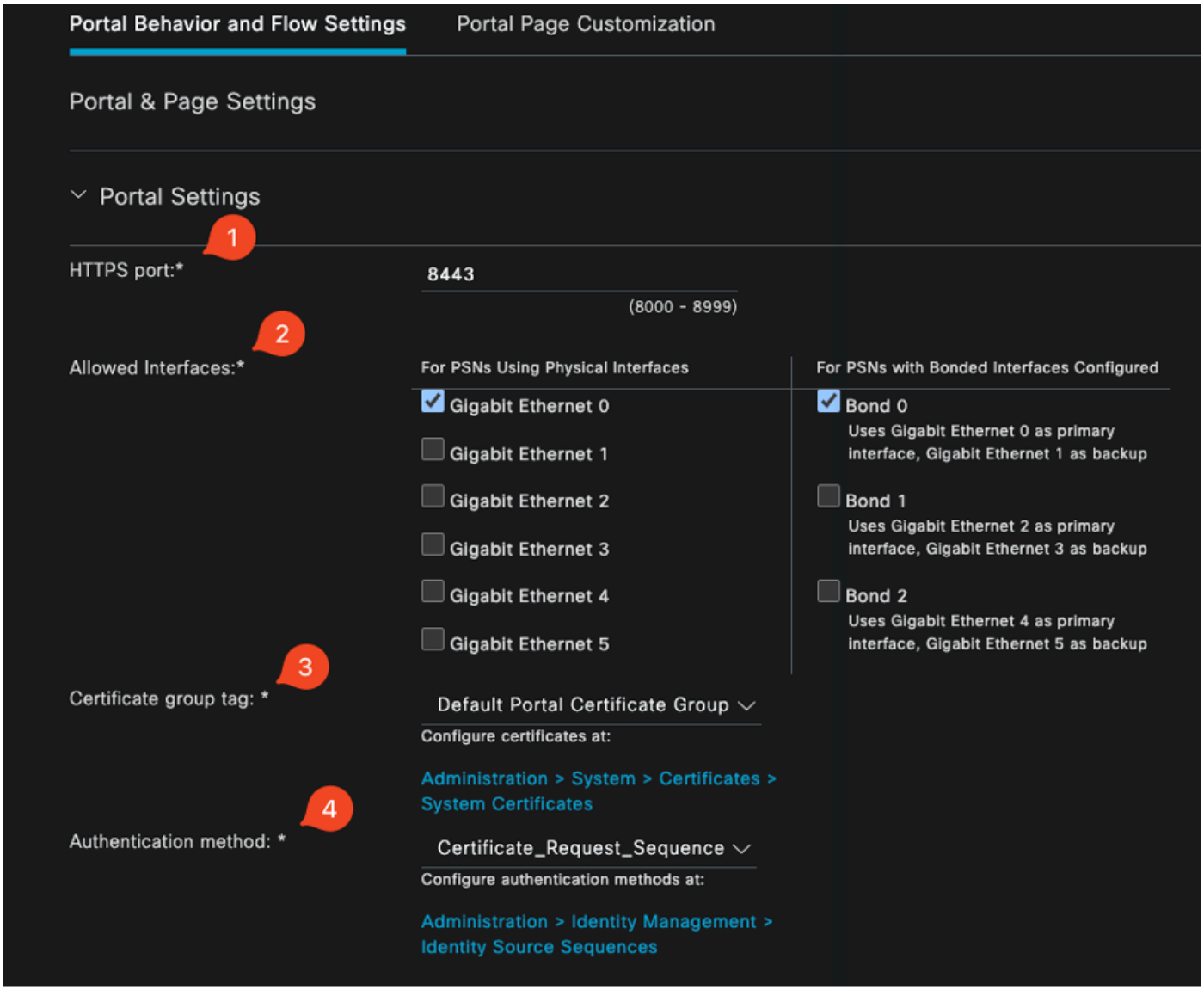
3.3. Seleccione la Etiqueta de Grupo de Certificados como el Grupo de Certificados del Portal Predeterminado.

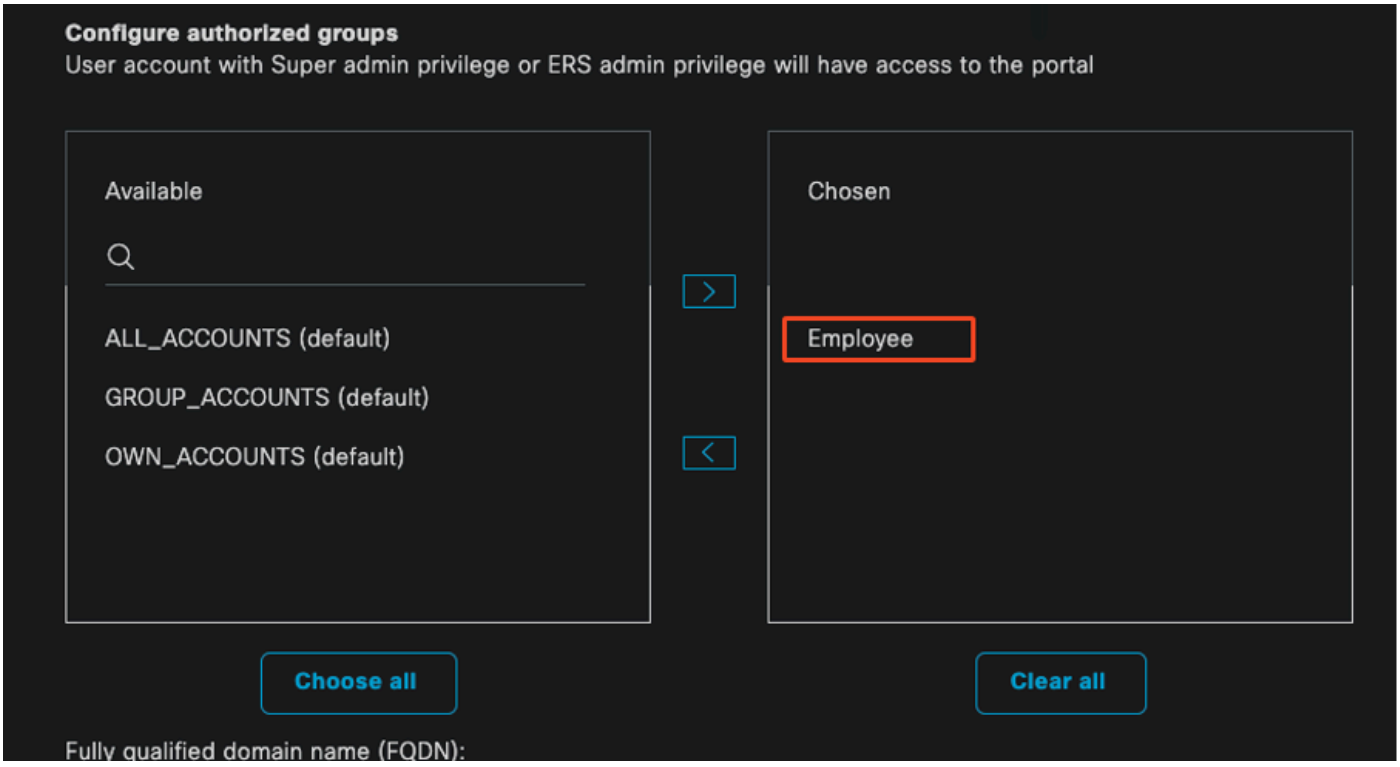
3.4. Seleccione el método de autenticación, que indica la secuencia de almacenamiento de identidad utilizada para autenticar el inicio de sesión en este portal.

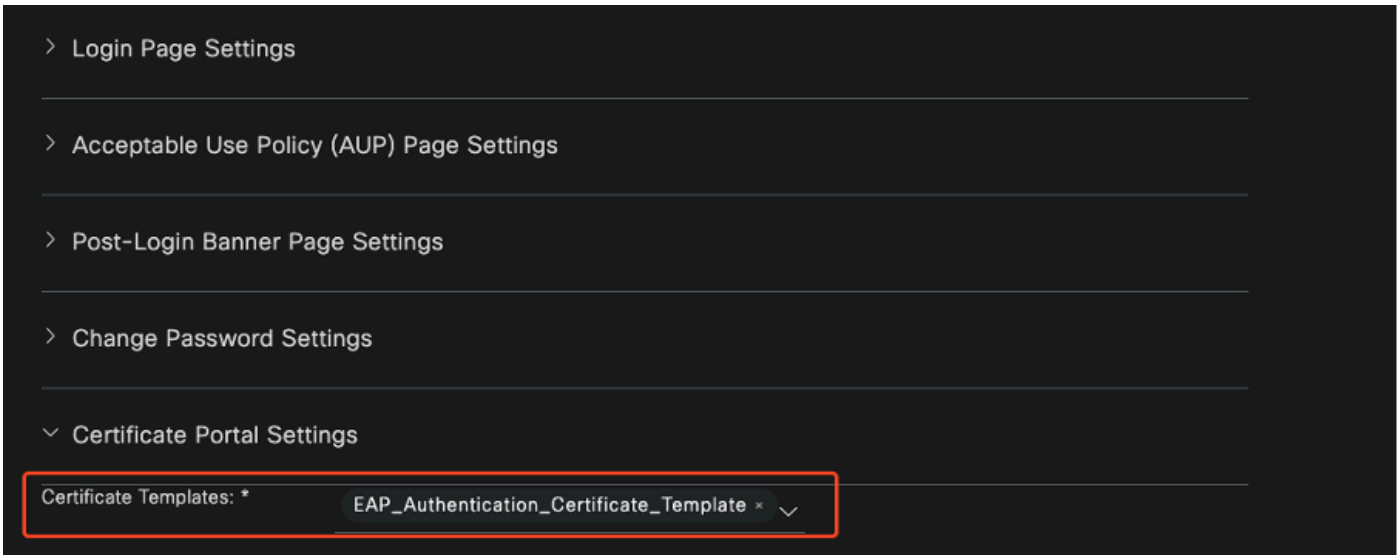
3.5. Incluir los grupos autorizados cuyos miembros puedan acceder al portal. Por ejemplo, seleccione el grupo de usuarios Empleados si los usuarios pertenecen a este grupo.

3.6. Defina las plantillas de certificado que se permiten en la configuración de aprovisionamiento de certificados.



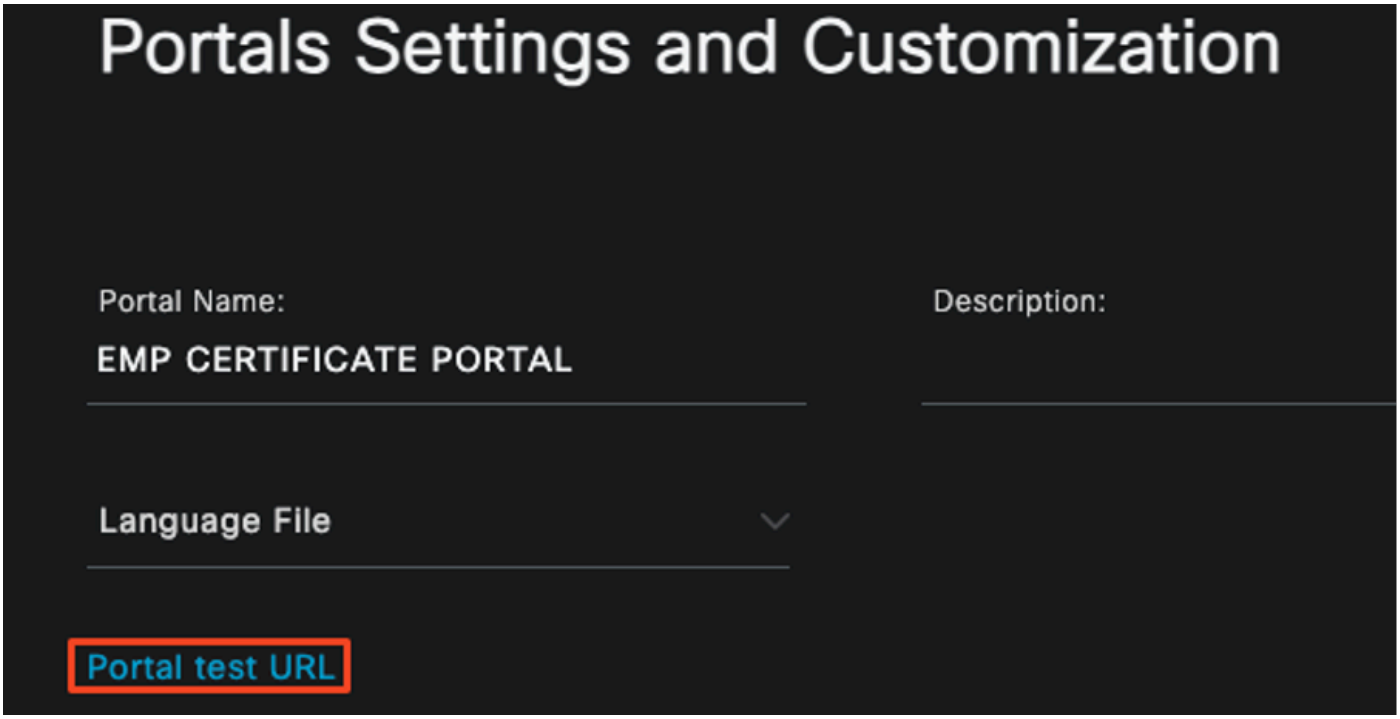

Portal Behavior and Flow Settings
Portal Page Customization
Portal & Page Settings
Portal Settings
1
HTTPS port:*
8443
(8000 - 8999)
2
Allowed Interfaces:*
For PSNs Using Physical Interfaces
Gigabit Ethernet 0
Gigabit Ethernet 1
Gigabit Ethernet 2
Gigabit Ethernet 3
Gigabit Ethernet 4
Gigabit Ethernet 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):

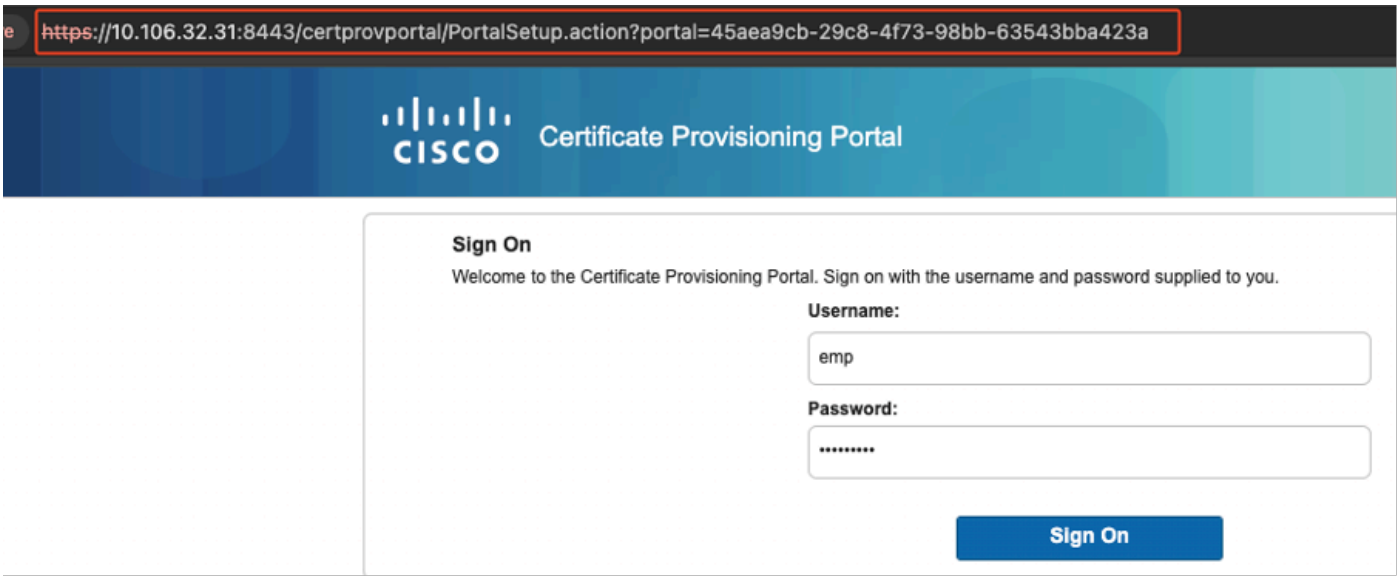


Configuración del portal de certificados

Una vez finalizada esta configuración, puede probar el portal haciendo clic en la URL de prueba del portal. Esta acción abre la página del portal.



URL de la página Test Portal

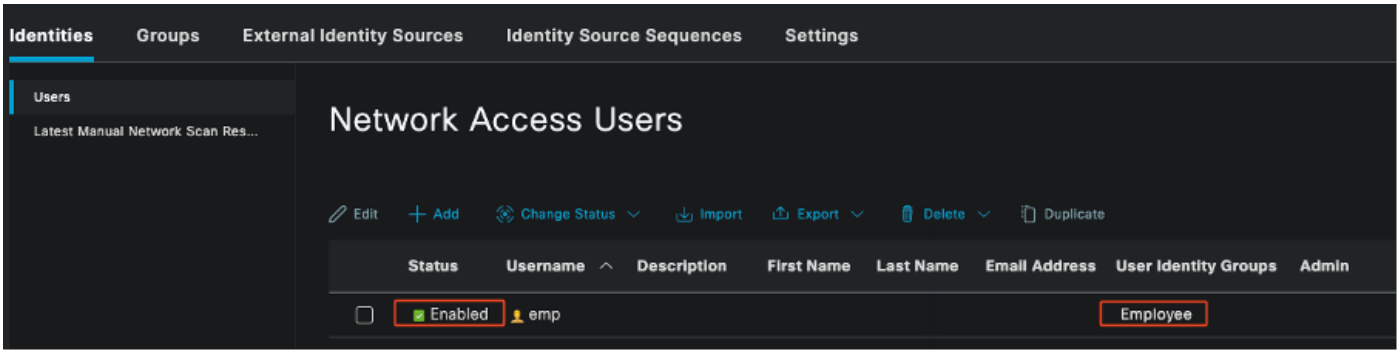


Página del portal

Agregar usuario interno

Para crear un usuario para la autenticación a través del portal de certificados, siga estos pasos:

1. Vaya a Administration > Identity Management > Identities > Users.
2. Haga clic en la opción para agregar un usuario al sistema.
3. Seleccione los grupos de identidad de usuario a los que pertenece el usuario. En este ejemplo, asigne el usuario al grupo Empleado.



Adición de usuario interno

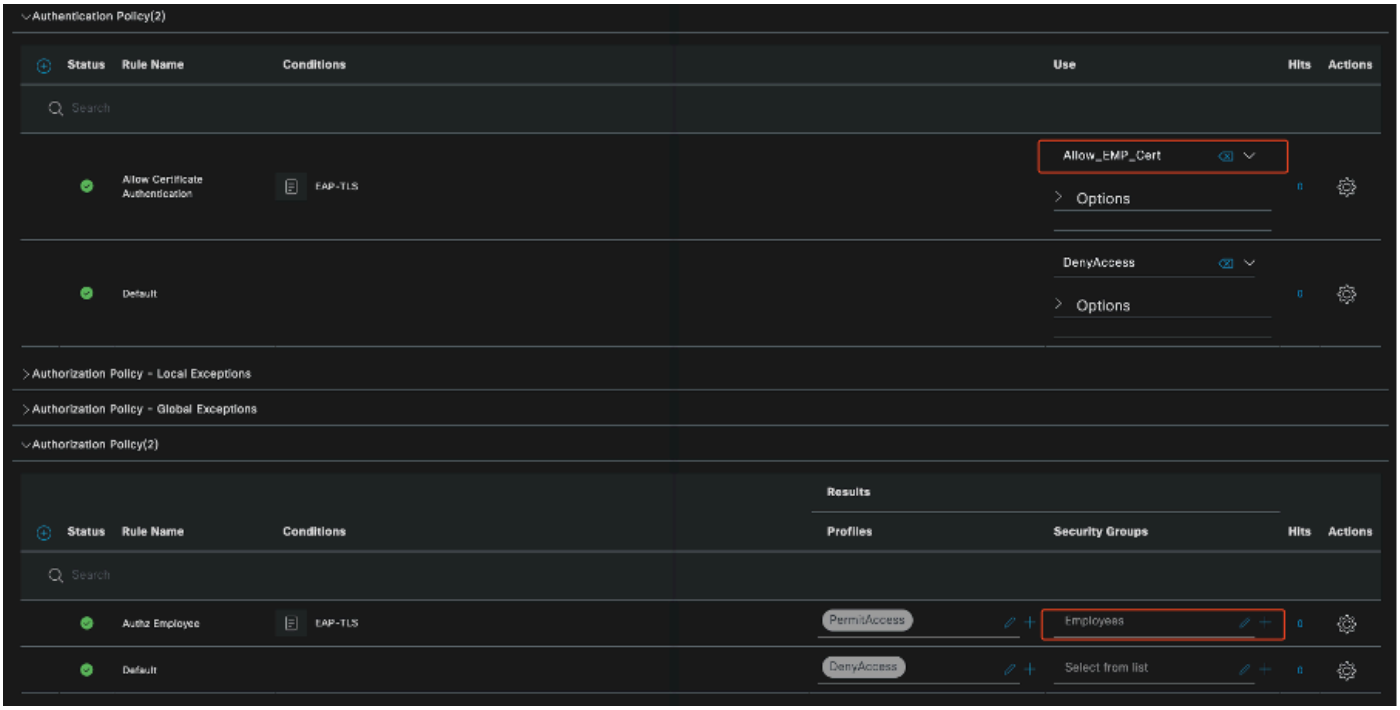
Configuración de ISE Certificate Provisioning Portal y RADIUS Policy

La sección anterior trataba sobre la configuración del portal de aprovisionamiento de certificados de ISE. Ahora, configuramos los conjuntos de políticas RADIUS de ISE para permitir la autenticación de usuarios.

1. Configuración de conjuntos de políticas RADIUS de ISE
2. Vaya a Política > Conjuntos de políticas.
3. Haga clic en el signo más (+) para crear un nuevo conjunto de directivas.

En este ejemplo, configure un conjunto de directivas simple diseñado para autenticar a los usuarios mediante sus certificados.

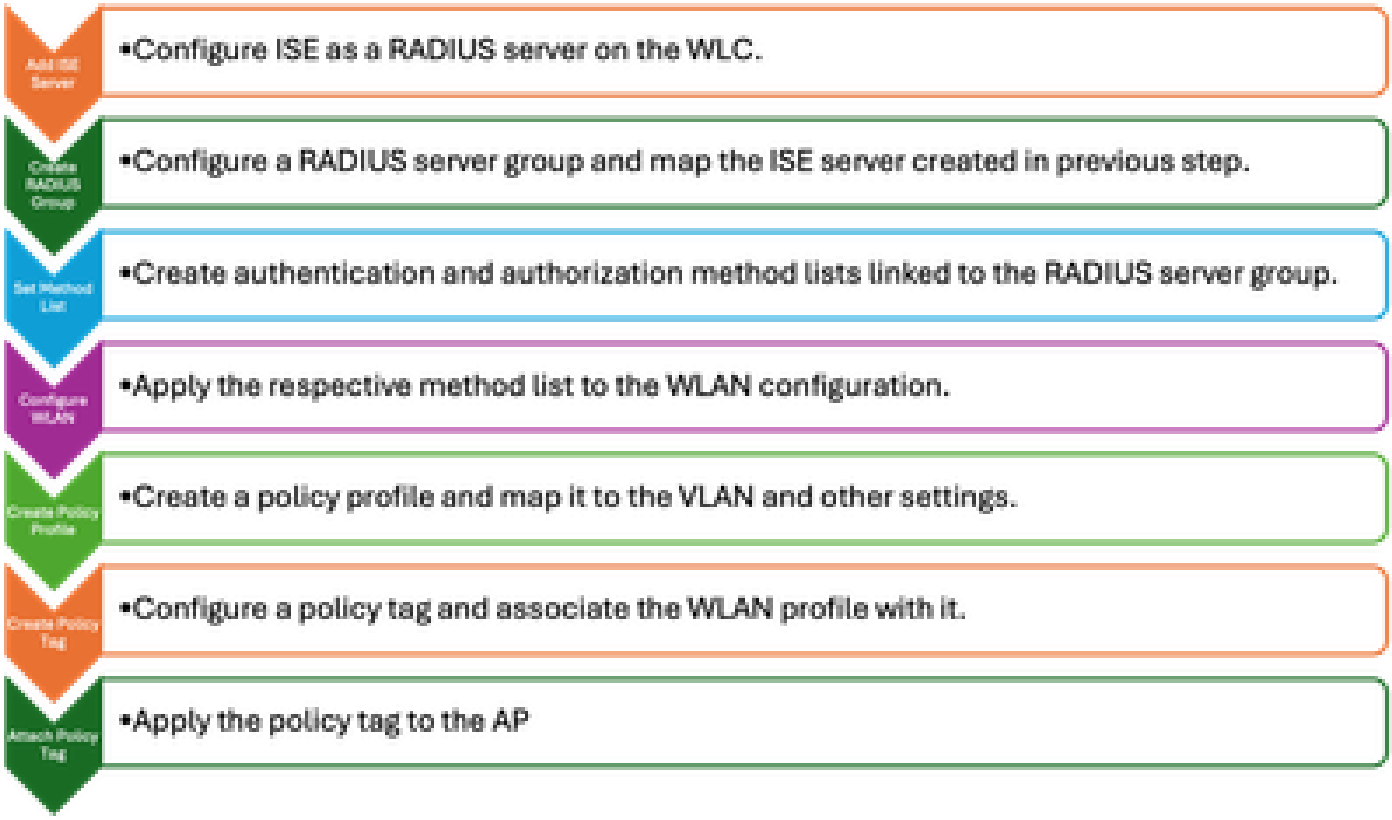
Conjunto de políticas



Conjunto de políticas que muestra las políticas de autenticación y autorización

Configuración de 9800 WLC

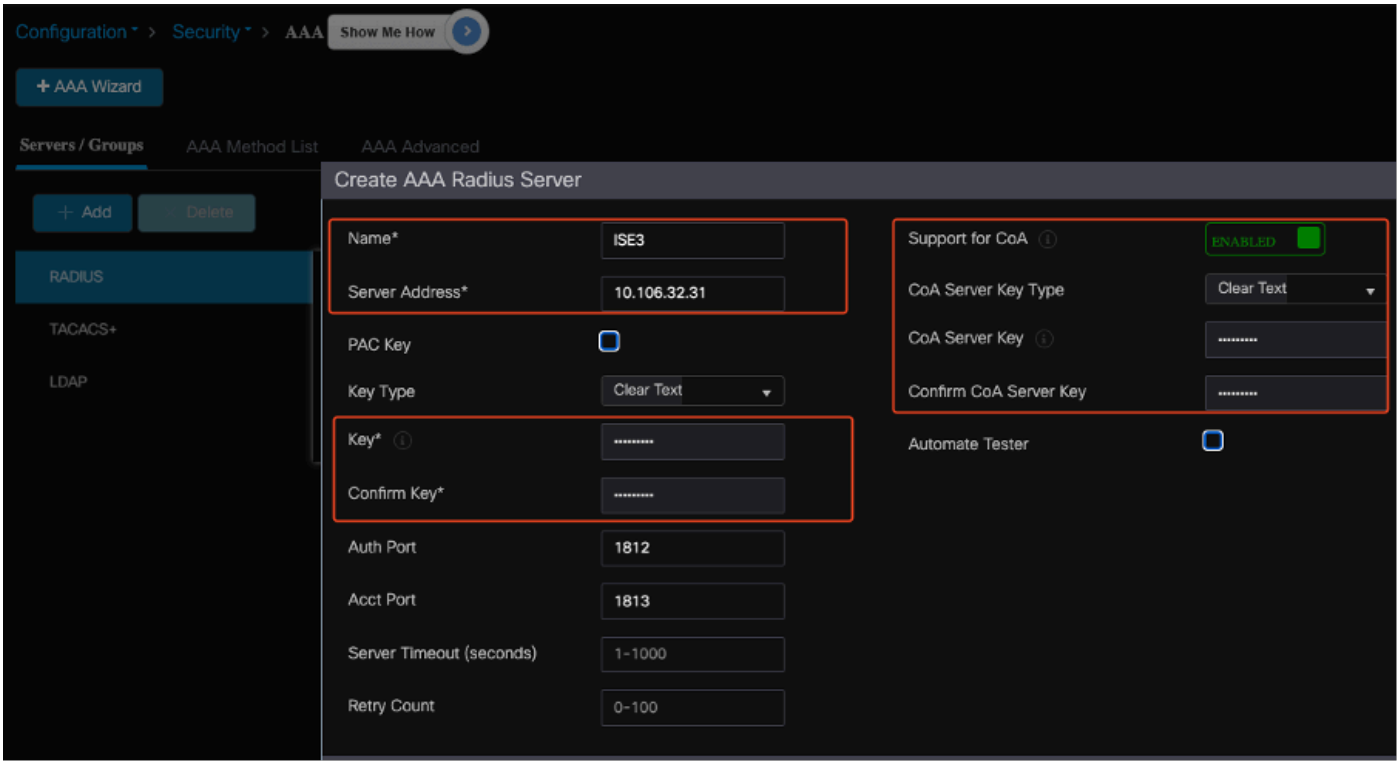
Estos son los pasos de configuración para el WLC 9800. Cada paso se acompaña de capturas de pantalla en esta sección para proporcionar orientación visual.



Pasos de configuración del WLC

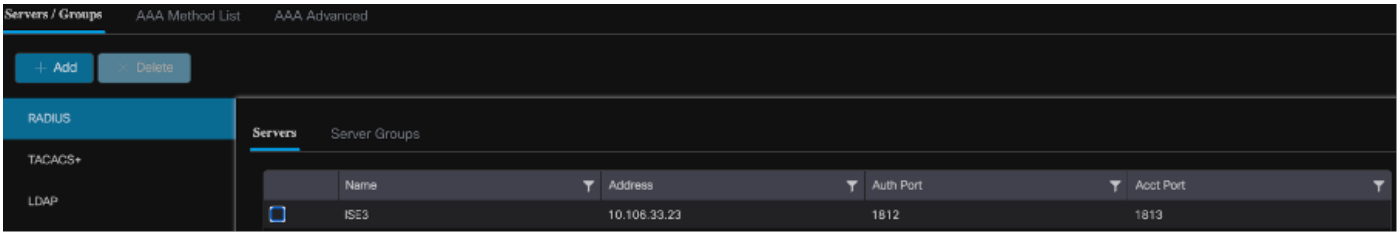
Adición de un servidor ISE al WLC 9800

1. Para integrar el servidor ISE con el controlador de LAN inalámbrica (WLC) 9800, siga estos pasos:
2. Vaya a Configuration > Security > AAA.
3. Haga clic en el botón Add para incluir el servidor ISE en la configuración del WLC.



Adición de un servidor ISE en el WLC

Una vez agregado el servidor, aparece en la lista de servidores.

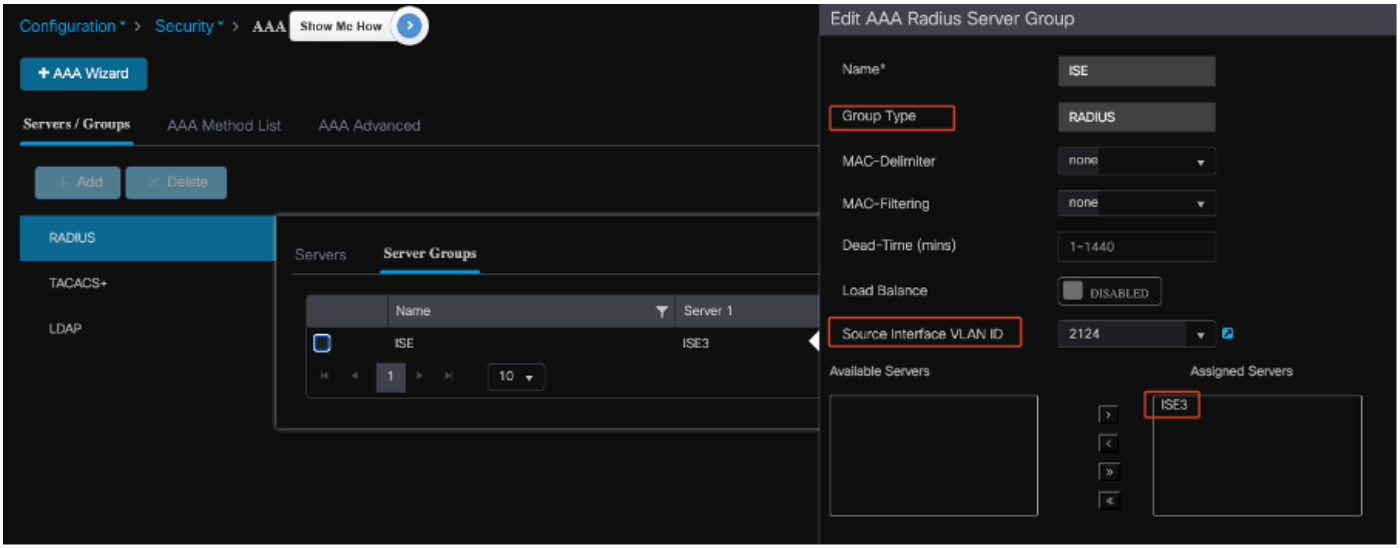


Visualización de servidores Radius

Agregar grupo de servidores en 9800 WLC

Para agregar un grupo de servidores en el controlador de LAN inalámbrica 9800, siga estos pasos:

1. Vaya a Configuration > Security > AAA.
2. Haga clic en la pestaña Server Group y, a continuación, haga clic en Add para crear un nuevo grupo de servidores.

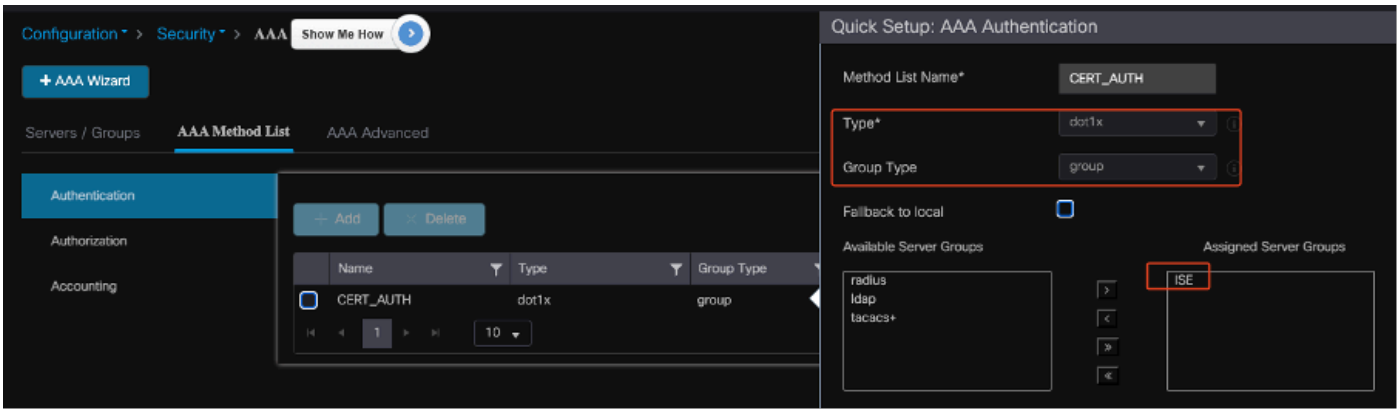


Asignación de servidores ISE a un grupo de servidores Radius

Configuración de la lista de métodos AAA en el WLC 9800

Después de crear el grupo de servidores, configure la lista de métodos de autenticación mediante estos pasos:

1. Vaya a Configuration > Security > AAA > AAA Method List.
2. En la ficha Autenticación, agregue una nueva lista de métodos de autenticación.
3. Establezca el tipo en dot1x.
4. Seleccione group como tipo de grupo.
5. Incluya los grupos de servidores ISE que creó anteriormente como grupos de servidores.

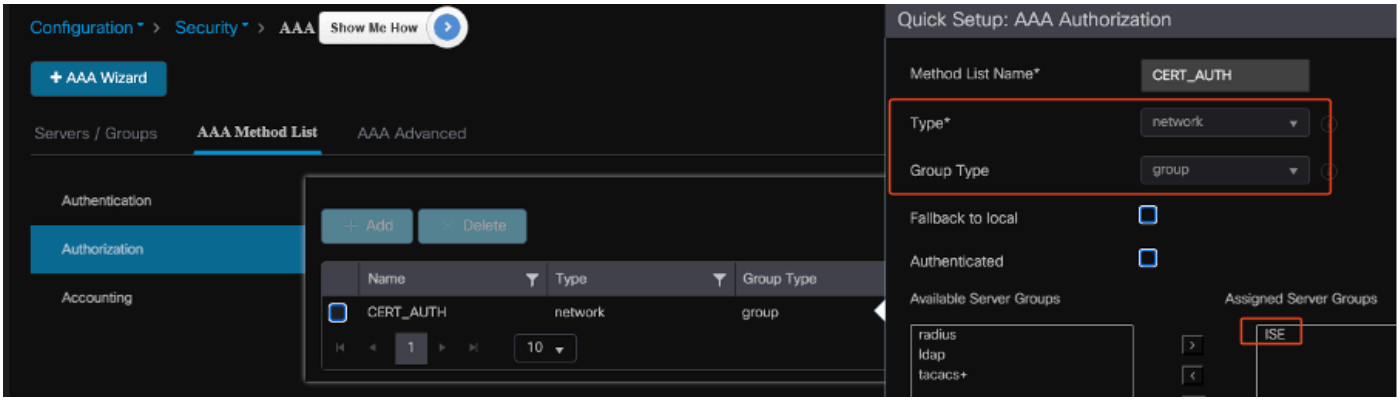


Creación de Listas de Métodos de Autenticación

Configuración de la lista de métodos de autorización en el WLC 9800

Para configurar la lista de métodos de autorización, siga estos pasos:

1. Navegue hasta la pestaña Autorización dentro de la sección Lista de Métodos AAA.
2. Haga clic en Agregar para crear una nueva lista de métodos de autorización.
3. Elija network como tipo.
4. Seleccione group como tipo de grupo.
5. Incluya el grupo de servidores ISE como grupo de servidores.

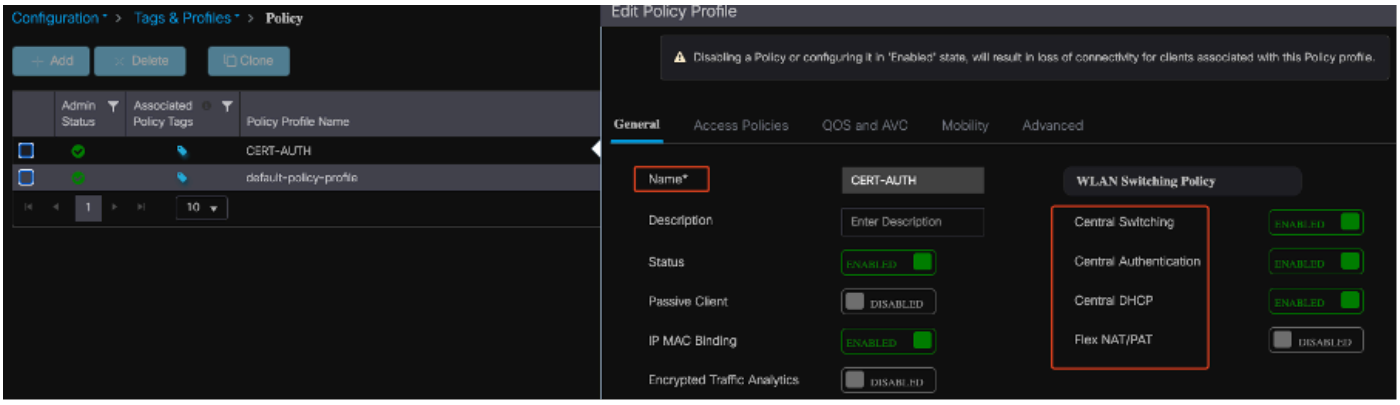


Agregar lista de métodos de autorización

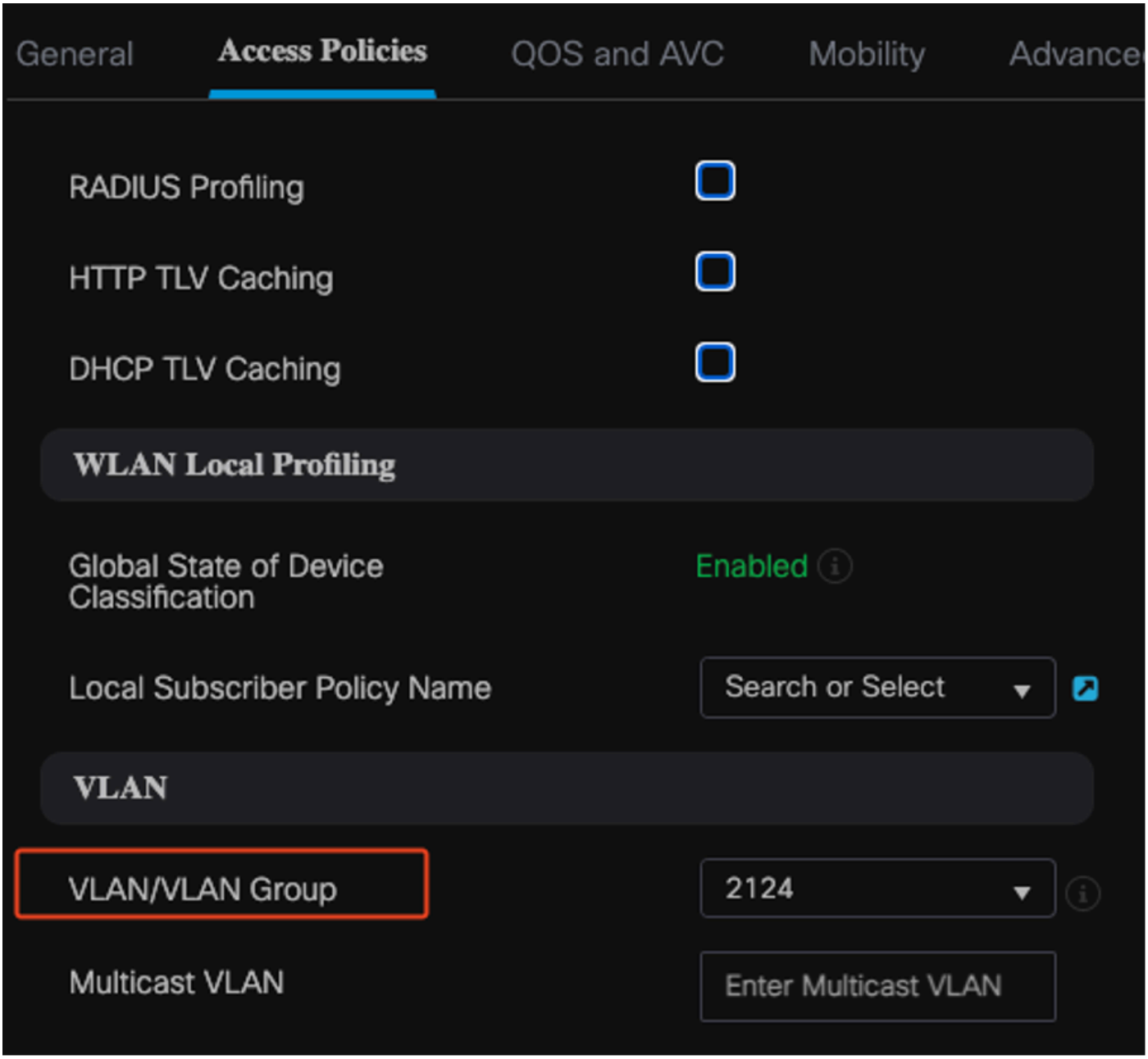
Cree un perfil de política en el WLC 9800

Una vez finalizada la configuración del grupo RADIUS, continúe con la creación de un perfil de política:

1. Vaya a Configuración > Etiquetas y perfiles > Política.
2. Haga clic en Agregar para crear un nuevo perfil de directiva.
3. Elija los parámetros adecuados para su perfil de política. En este ejemplo, todo es central y LAB VLAN se utiliza como la VLAN del cliente.



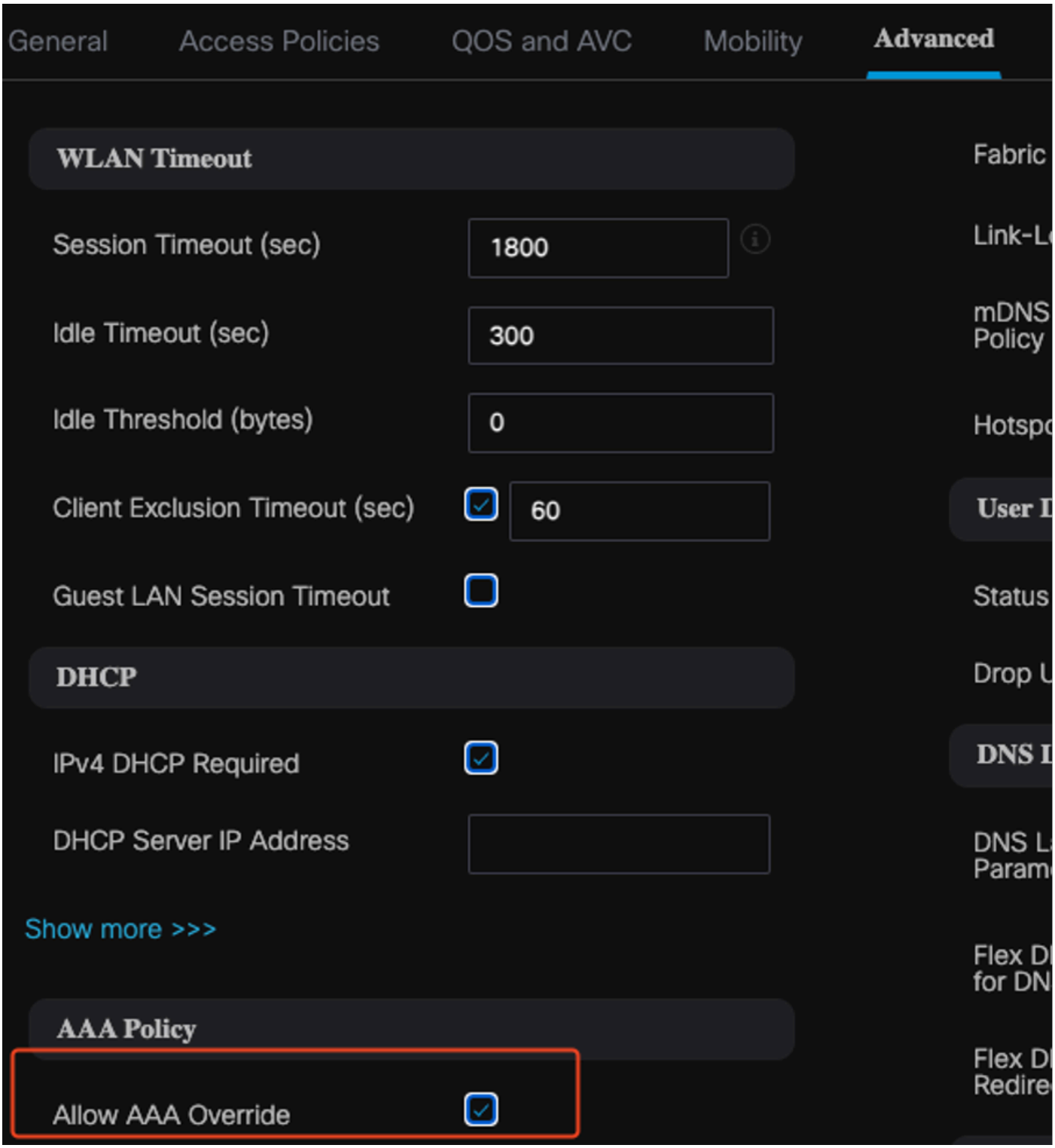
Configuración del Perfil de Política



VLAN para asignación de políticas

Al configurar la autorización RADIUS, asegúrese de que la opción AAA Override esté habilitada en la ficha advanced de la configuración del perfil de política. Este ajuste permite al controlador de

LAN inalámbrica aplicar políticas de autorización basadas en RADIUS a usuarios y dispositivos.

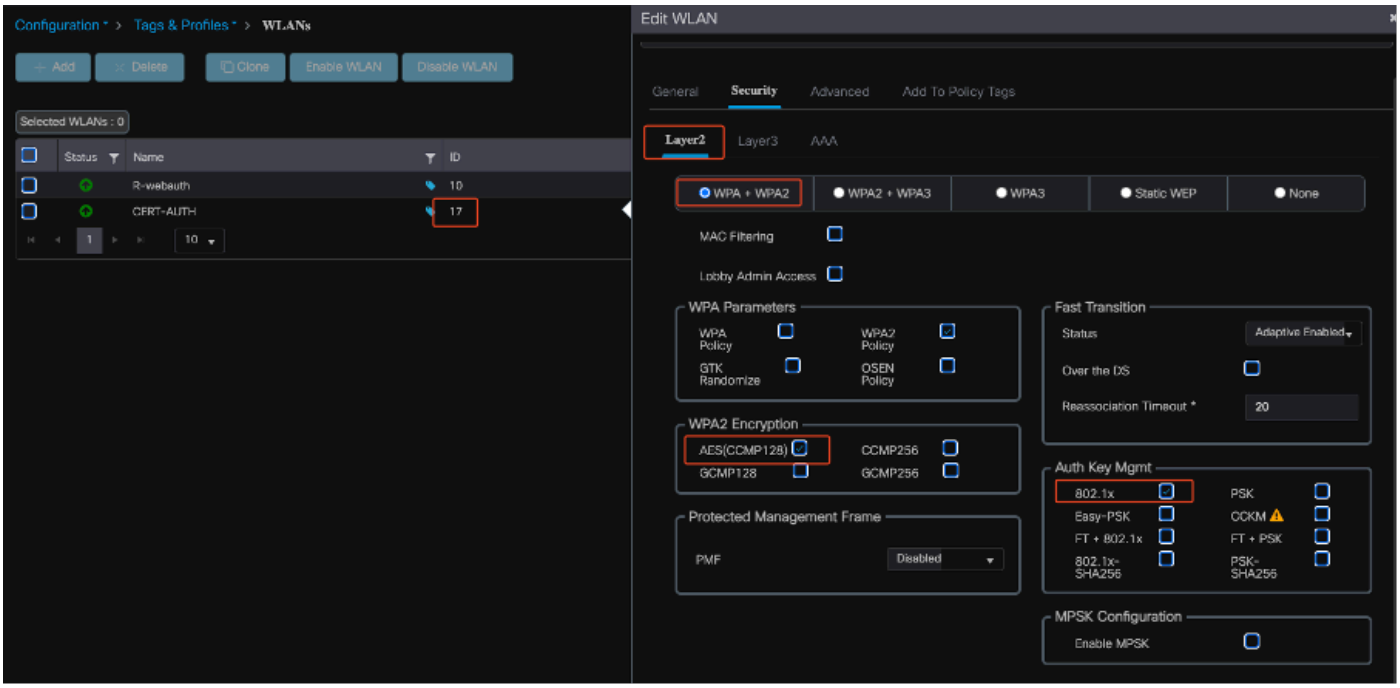


Anulación de AAA

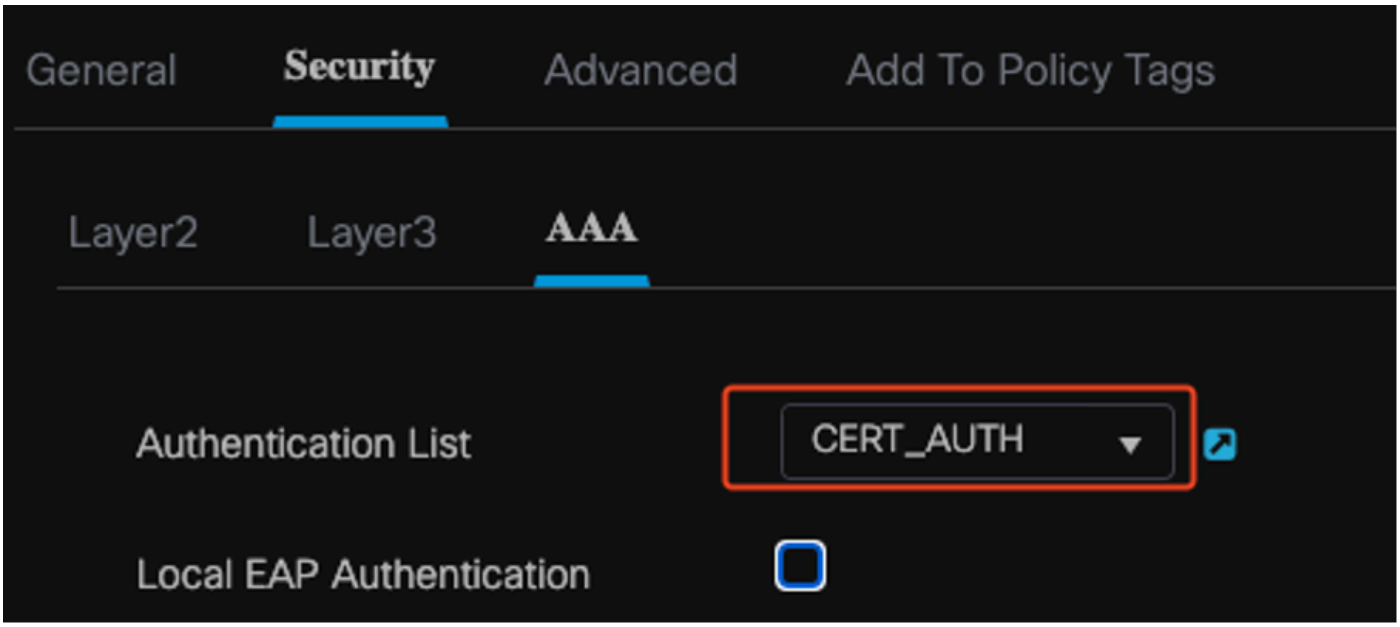
Cree una WLAN en el WLC 9800

Para configurar una nueva WLAN con autenticación 802.1x, siga estos pasos:

1. Vaya a Configuration > Tags & Profiles > WLANs.
2. Haga clic en Add para crear una nueva WLAN.
3. Seleccione los parámetros de autenticación de capa 2 y active la autenticación 802.1x.



Configuración del perfil WLAN

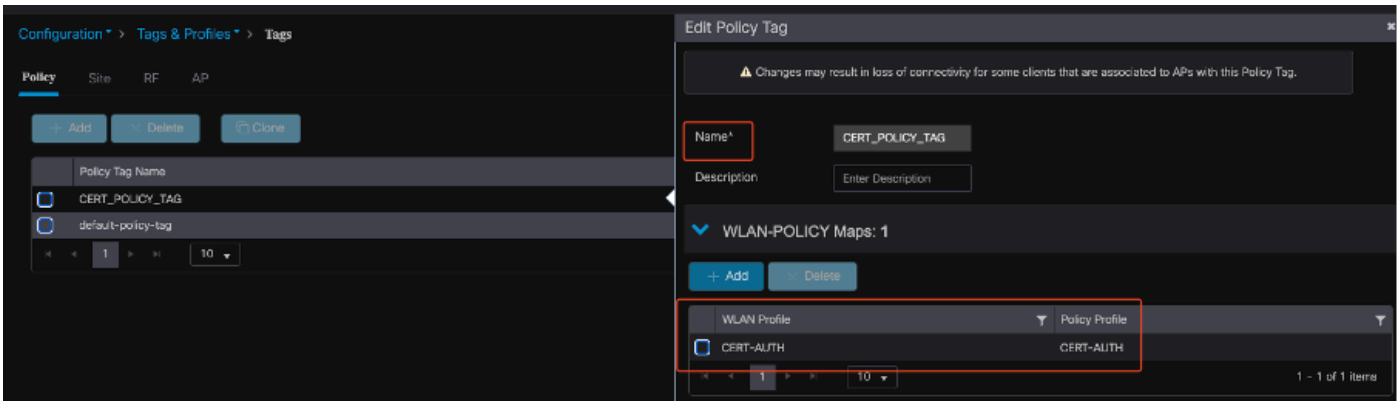


Perfil WLAN a mapa de lista de métodos

Asignar WLAN con el perfil de la política en el WLC 9800

Para asociar su WLAN con un perfil de política, siga estos pasos:

1. Vaya a Configuration > Tags & Profiles > Tags.
2. Haga clic en Agregar para agregar una nueva etiqueta.
3. En la sección WLAN-POLICY, asigne la WLAN recién creada al perfil de política apropiado.

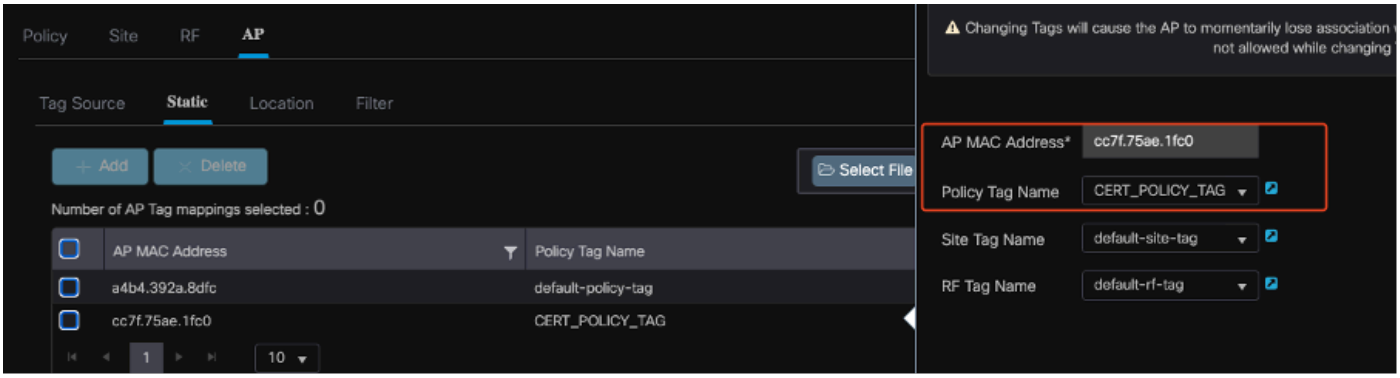


Configuración de etiquetas de políticas

Asignar etiqueta de política al punto de acceso en el WLC 9800

Para asignar la etiqueta de directiva a un punto de acceso (AP), siga estos pasos:

1. Vaya a Configuración > Etiquetas y perfiles > Etiquetas > AP.
2. Vaya a la sección Static dentro de la configuración AP.
3. Haga clic en el AP específico que desea configurar.
4. Asigne la etiqueta de política que creó al AP seleccionado.



Asignación de ETIQUETA AP

Configuración en ejecución del WLC después de la finalización de la instalación

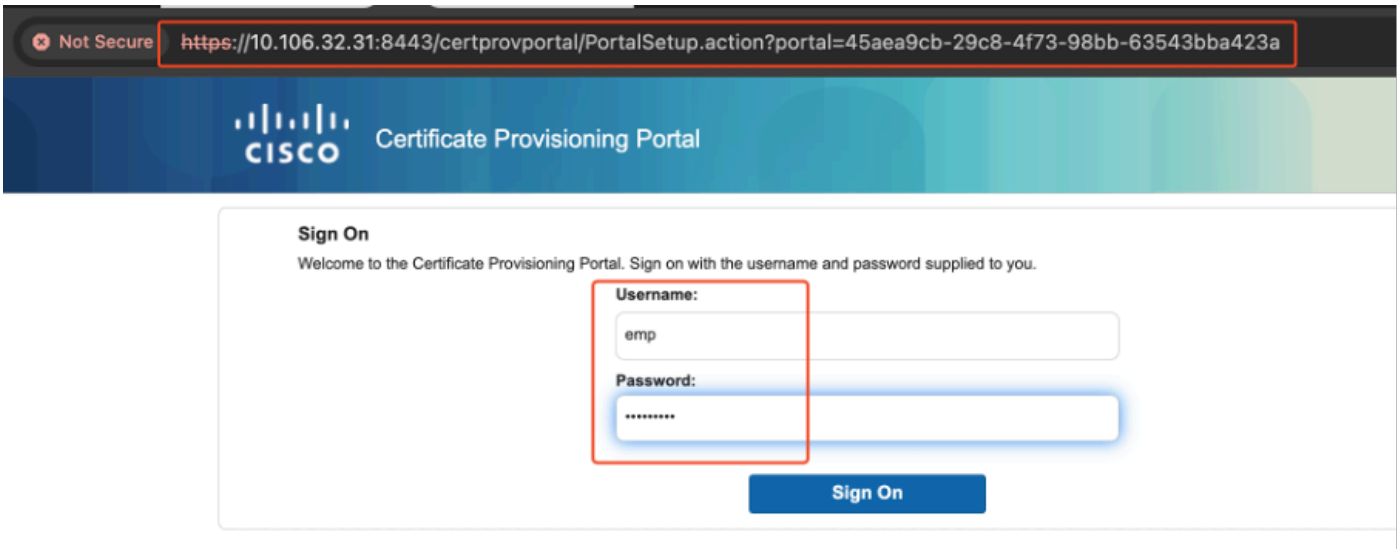
```
aaa group server radius ISE
 server name ISE3
 ip radius source-interface Vlan2124
aaa authentication dot1x CERT_AUTH group ISE
aaa authorization network CERT_AUTH group ISE
aaa server radius dynamic-author
 client 10.106.32.31 server-key Cisco!123
!

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
```

Crear y descargar certificado para el usuario

Para crear y descargar un certificado para un usuario, siga estos pasos:

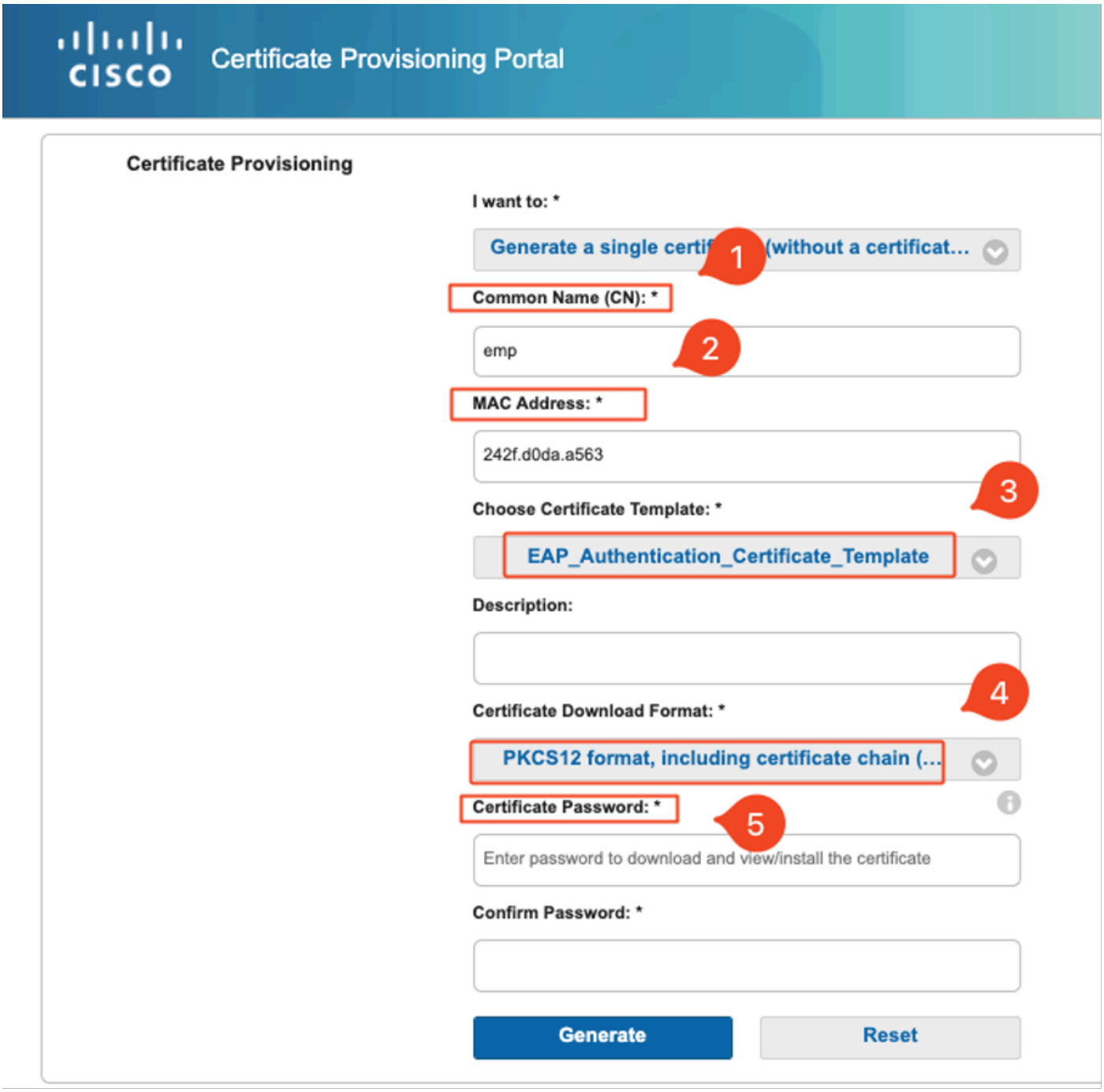
1. Haga que el usuario inicie sesión en el portal de certificados que se configuró anteriormente.



Acceso al portal de certificados

2. Acepte la política de uso aceptable (AUP). A continuación, ISE presenta una página para la generación de certificados.

3. Seleccione Generar un solo certificado (sin solicitud de firma de certificado).



Generando certificado

Para generar un certificado a través del Portal de aprovisionamiento de certificados, asegúrese de que se rellenan estos campos obligatorios:

- CN: El servidor de autenticación utiliza el valor que se presenta en el campo Nombre común del certificado de cliente para autenticar a un usuario. En el campo Common Name (Nombre común), introduzca el nombre de usuario (que utilizó para iniciar sesión en el Portal de aprovisionamiento de certificados).
- Dirección MAC: Los nombres alternativos de sujeto (SAN) son una extensión X.509 que permite asociar varios valores a un certificado de seguridad. Cisco ISE, versión 2.0 solo admite direcciones MAC. Por lo tanto, en el campo de dirección SAN/MAC.
    - Plantilla de certificado: La plantilla de certificado define un conjunto de campos que la CA utiliza al validar una solicitud y emitir un certificado. Campos como el nombre

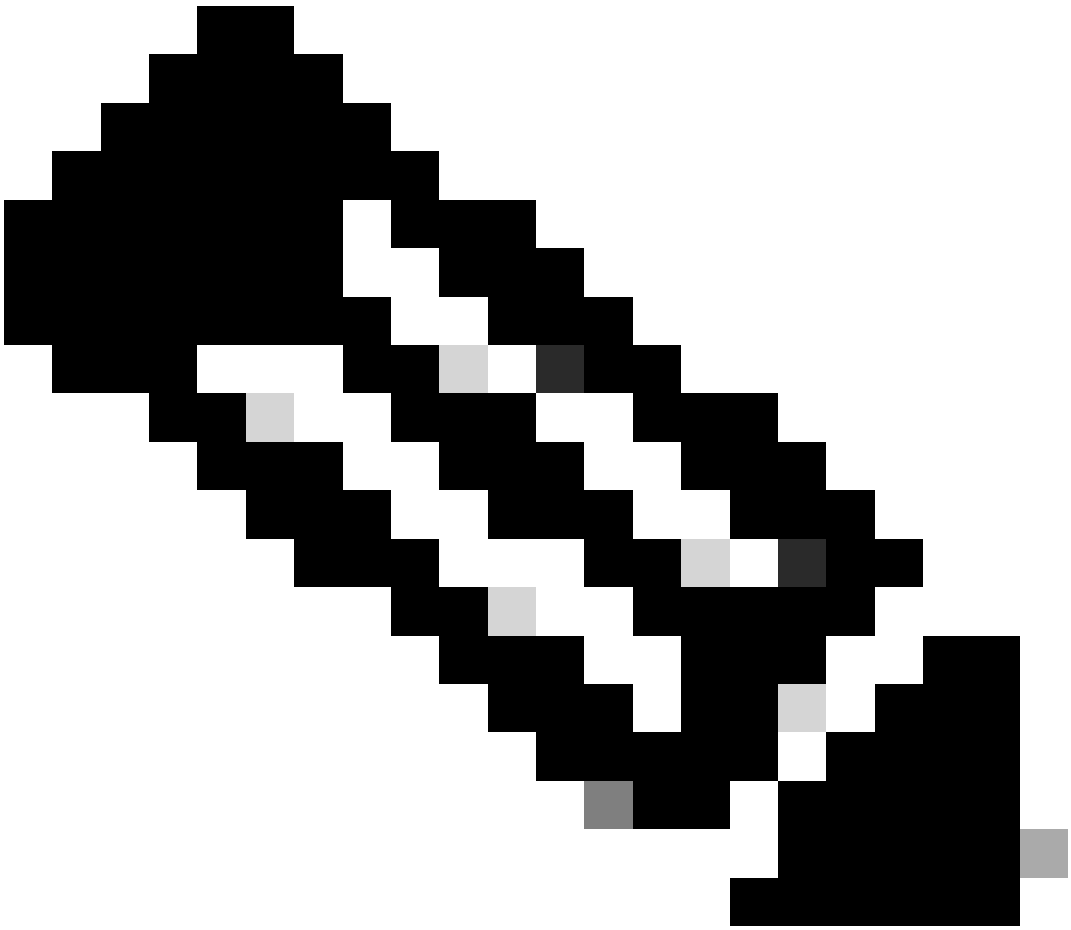
común (CN) se utilizan para validar la solicitud (CN debe coincidir con el nombre de usuario). La CA utiliza otros campos al emitir el certificado.

- Contraseña del certificado: Necesita una contraseña de certificado para proteger el certificado. Debe proporcionar la contraseña del certificado para ver el contenido del certificado e importar el certificado en un dispositivo.
- La contraseña debe cumplir estas reglas:
- La contraseña debe contener al menos una letra mayúscula, una letra minúscula y un dígito
    - La contraseña debe tener entre 8 y 15 caracteres
    - Los caracteres permitidos incluyen A-Z, a-z, 0-9, _, #

Una vez rellenados todos los campos, seleccione Generate para crear y descargar el certificado.

Instalación de certificados en un equipo con Windows 10

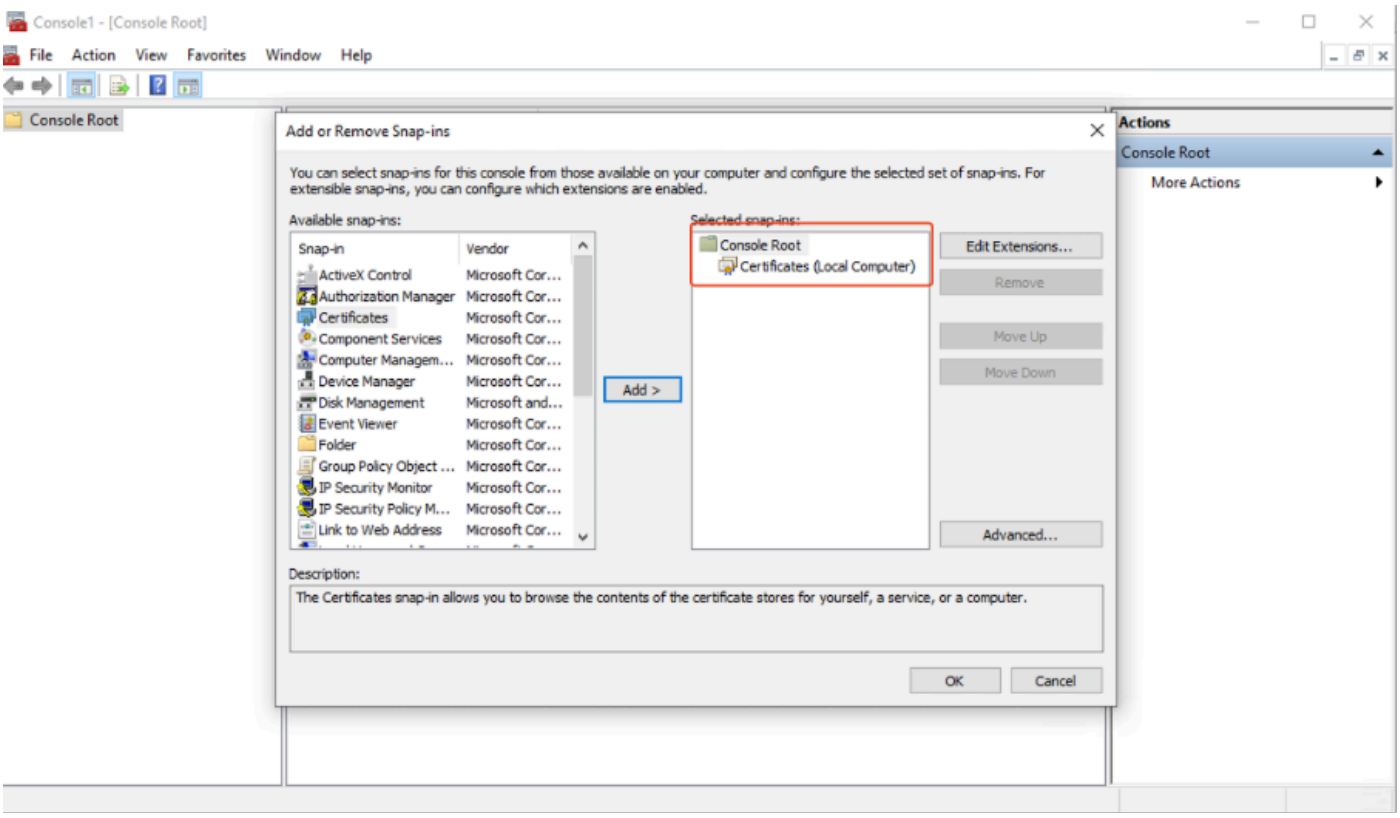
Para instalar un certificado en un equipo con Windows 10, abra Microsoft Management Console (MMC) siguiendo estos pasos:



Nota: Estas instrucciones pueden variar en función de la configuración de Windows, por lo que se recomienda consultar la documentación de Microsoft para obtener detalles específicos.

1. Haga clic en Inicio y luego en Ejecutar.
2. Escriba mmc en el cuadro Ejecutar y presione Intro. Se abre Microsoft Management Console.
3. Agregar complemento de certificado:
4. Vaya a Archivo > Agregar o quitar complemento.
5. Seleccione Add, luego elija Certificates y haga clic en Add.
6. Seleccione Cuenta de equipo, luego Equipo local y haga clic en Finalizar.

Estos pasos permiten administrar certificados en el equipo local.



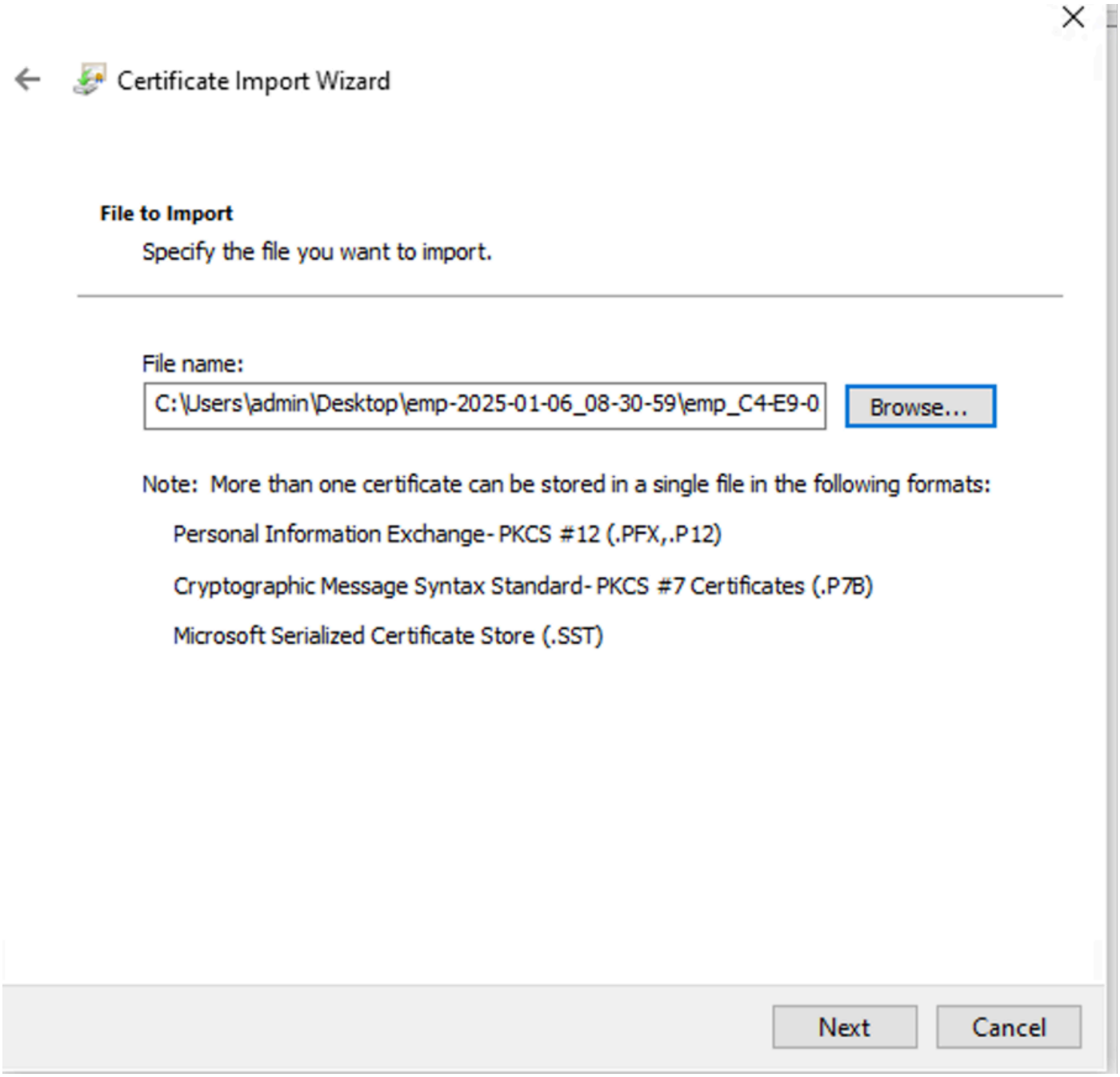
Consola MMC de Windows

Paso 1. Importar el certificado:

1.1. Haga clic en Acción en el menú.

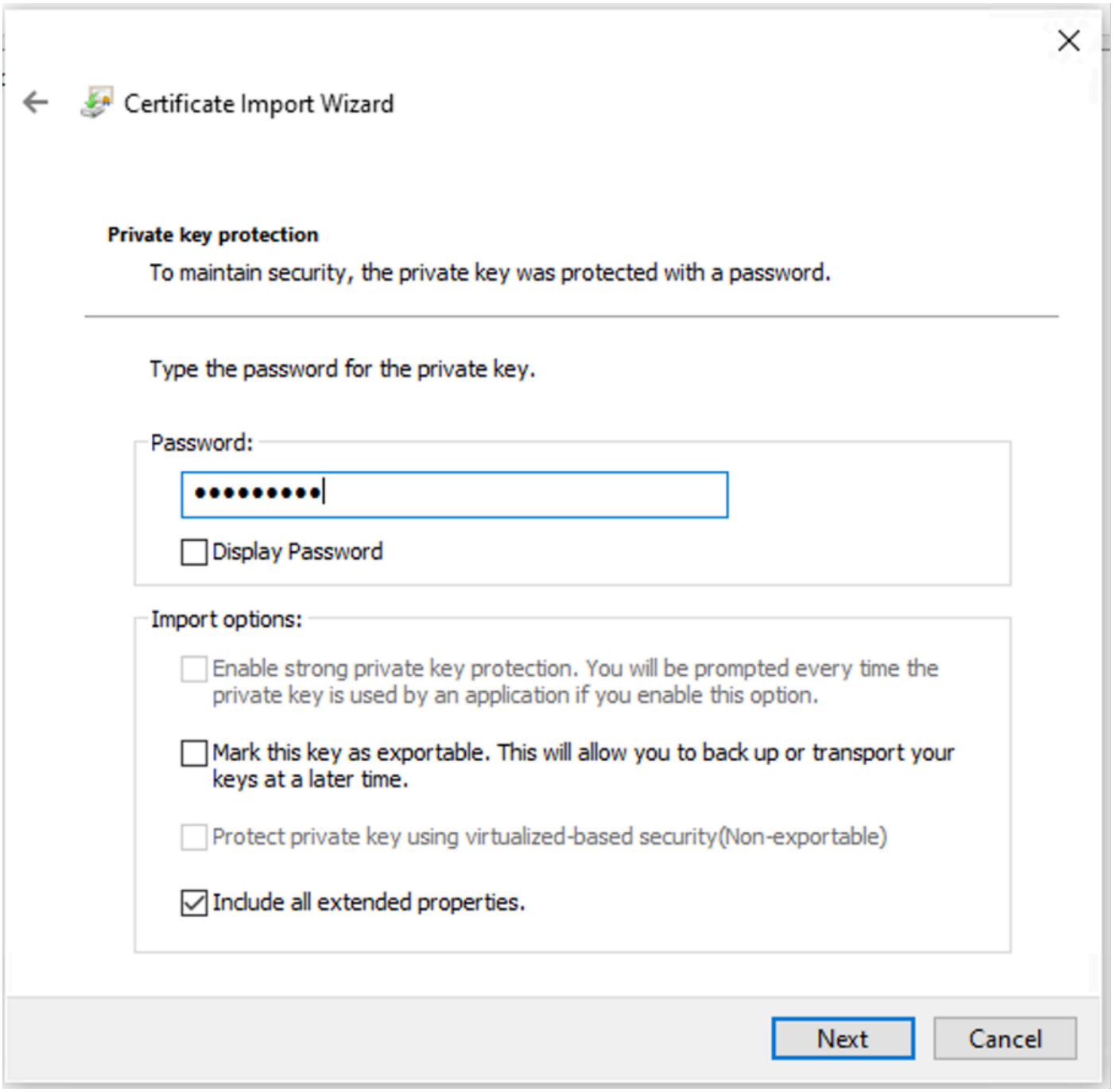
1.2. Vaya a Todas las tareas y seleccione Importar.

1.3. Consulte las indicaciones para localizar y seleccionar el archivo de certificado almacenado en el equipo.



Importando certificado

Durante el proceso de importación de certificados, se le pedirá que escriba la contraseña que creó al generar el certificado en el portal. Asegúrese de escribir esta contraseña correctamente para importar e instalar correctamente el certificado en el equipo.



Introducción de la contraseña del certificado

Paso 2. Traslade los certificados a las carpetas apropiadas:

2.1. Abra Microsoft Management Console (MMC) y vaya a la carpeta Certificados (equipo local) > Personal.

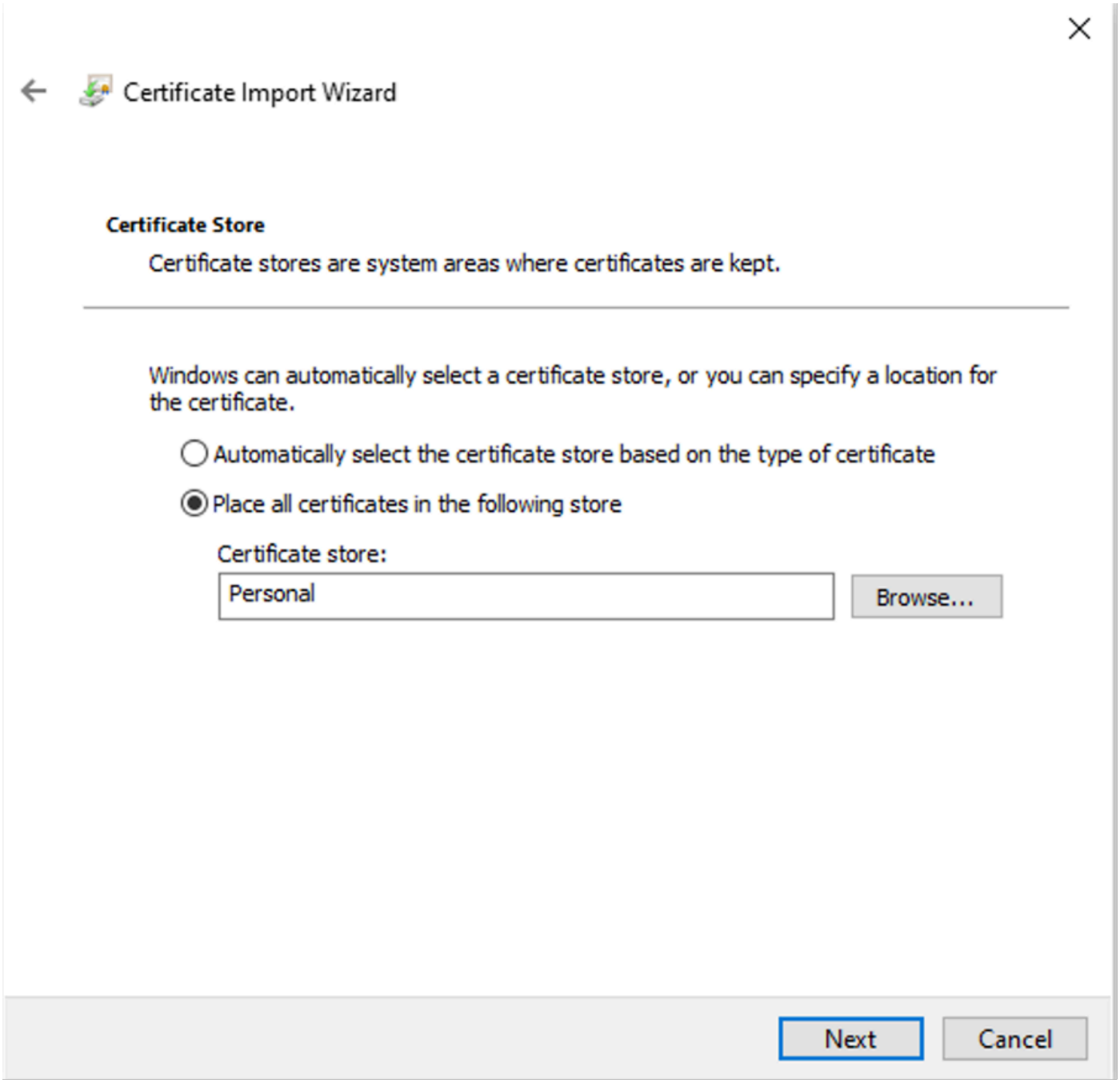
2.2. Revise los certificados y determine sus tipos (por ejemplo, CA raíz, CA intermedia o personal).

2.3. Trasladar cada certificado al almacén adecuado:

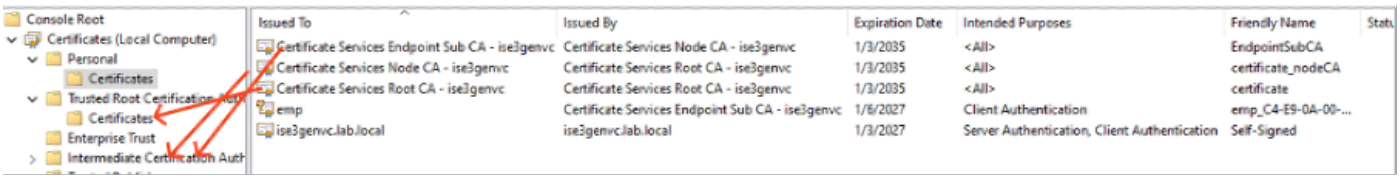
2.4. Certificados CA raíz: Pasar a Entidades emisoras raíz de confianza.

2.5. Certificados CA intermedios: Pasar a Entidades de certificación intermedias.

2.6. Certificados personales: Deje la carpeta Personal.



Almacenamiento de certificados en la carpeta personal

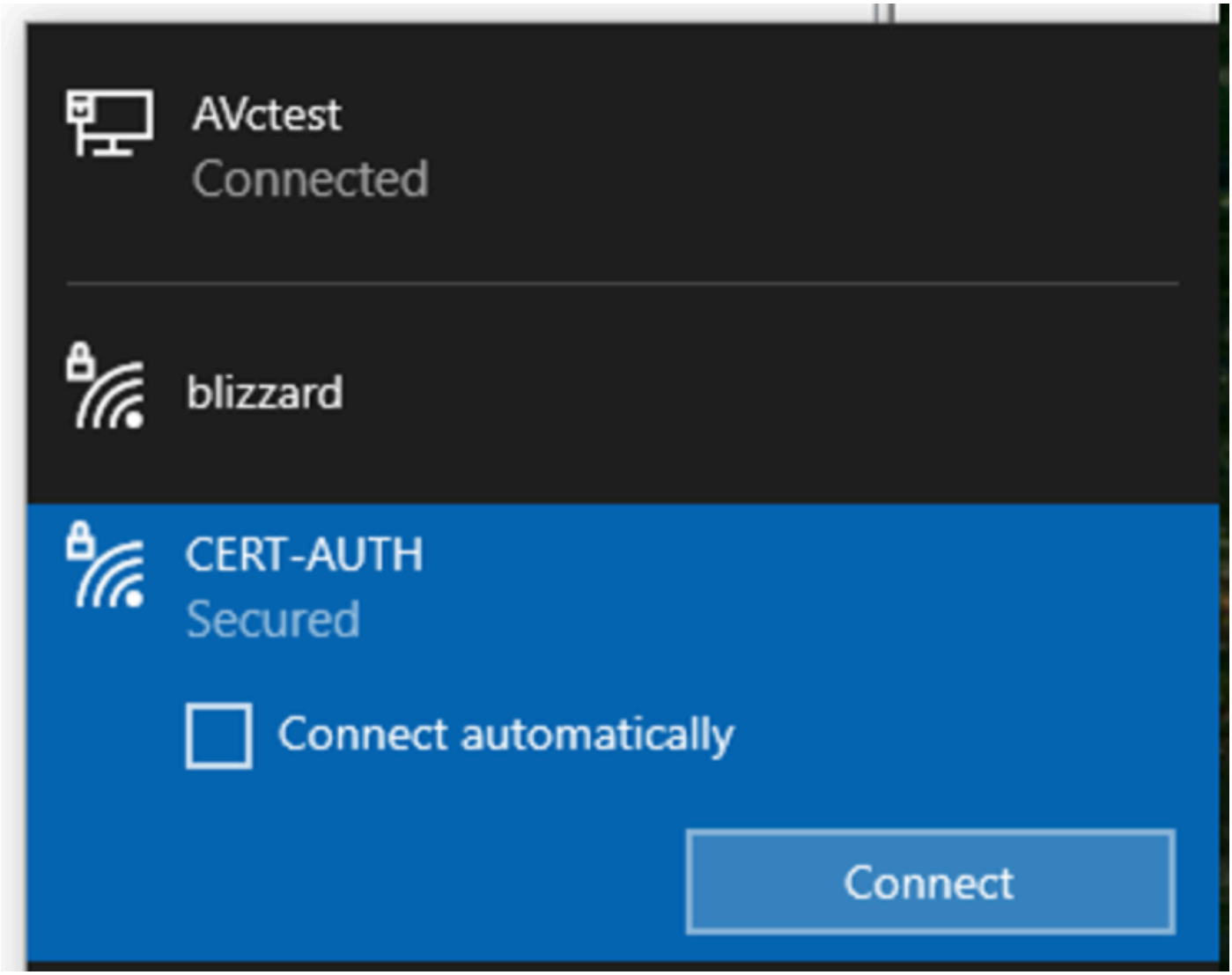


Traslado de certificados a sus tiendas

Conexión del equipo con Windows

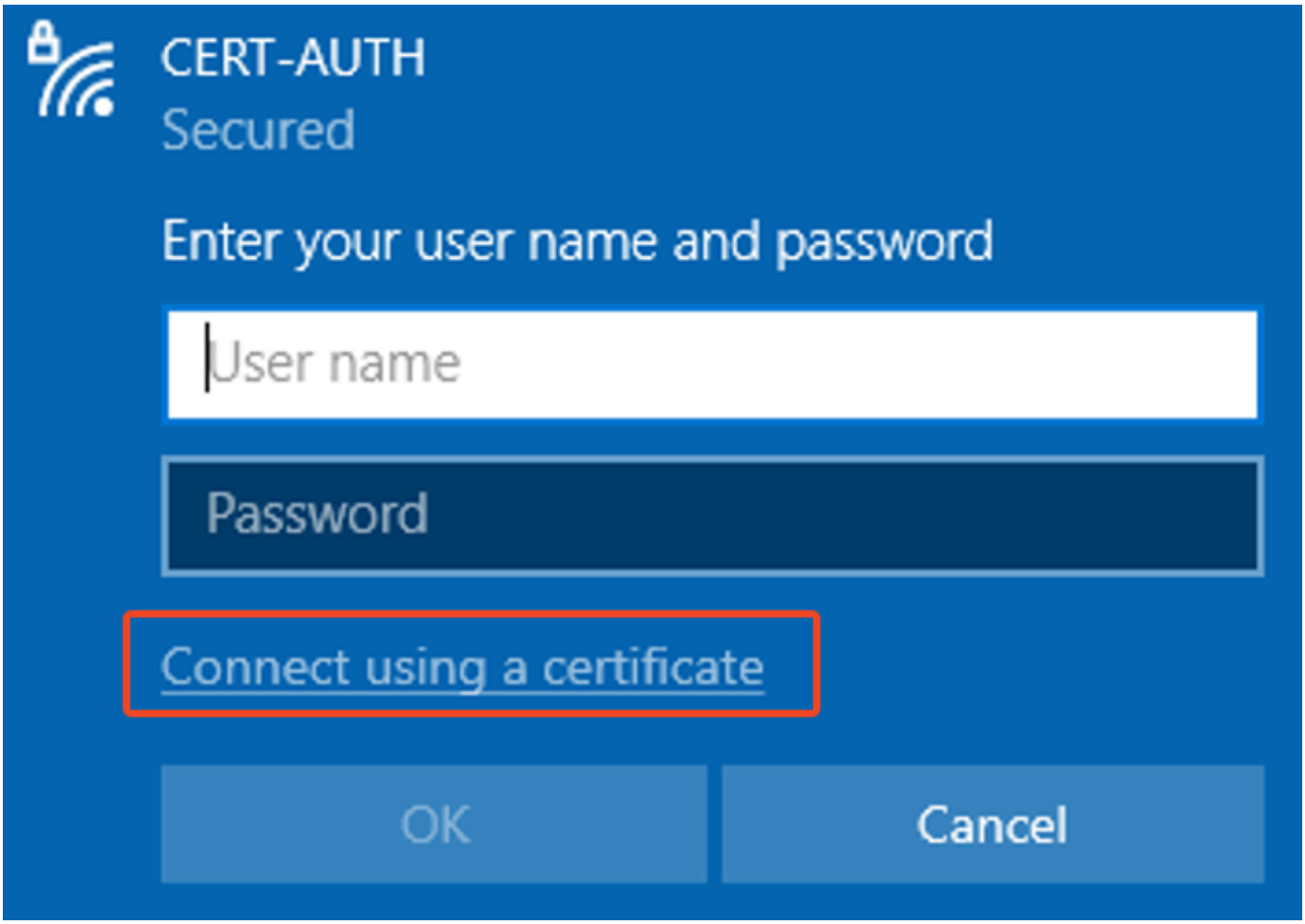
Una vez que los certificados se mueven a los almacenes correctos, utilice estos pasos para conectarse a la WLAN:

1. Haga clic en el icono de red en la bandeja del sistema para ver las redes inalámbricas disponibles.
2. Busque y haga clic en el nombre de la WLAN a la que desea conectarse.
3. Haga clic en Connect y continúe con cualquier solicitud adicional para completar el proceso de conexión utilizando su certificado para la autenticación.



Conexión a la red inalámbrica

Cuando se le solicite durante el proceso de conexión a la WLAN, seleccione la opción Connect using a certificate (Conectar usando un certificado).



Utilizar certificado como credencial

Esto le permite conectarse correctamente a la red inalámbrica mediante el 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 perfil inalámbrico

Verificación

Verifique que el WLC esté transmitiendo la WLAN:

<#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 que el AP esté activo en el 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
```

Asegúrese de que el AP esté transmitiendo la 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 mediante 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

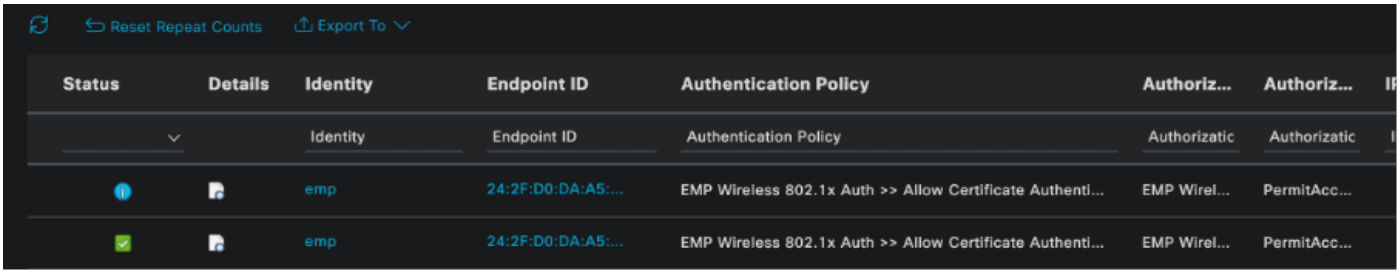
```
BSSID : a488.739e.8daf
```

EAP Type : EAP-TLS

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

VLAN : 2124

Registros en directo de Cisco Radius ISE:

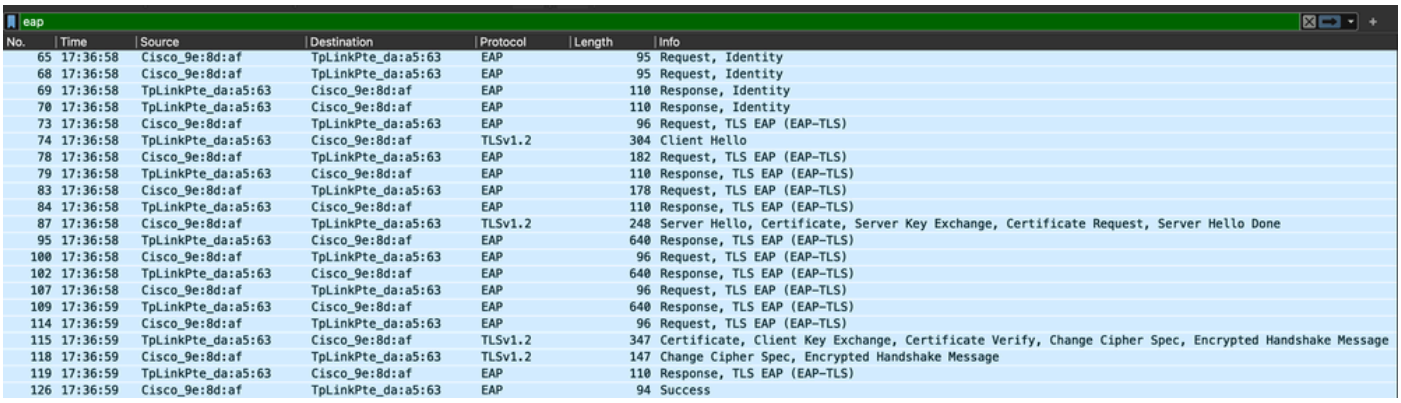


Registros en directo de ISE Radius

Tipo de autenticación detallada:

Registros detallados de ISE

Captura WLC EPC que muestra los paquetes 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 que muestra la transacción EAP

- El paquete número 87 corresponde al paso 8 del flujo EAP-TLS descrito al principio del documento.
- El número de paquete 115 corresponde al paso 9 del flujo EAP-TLS descrito al principio del documento.
- El número de paquete 118 corresponde al paso 10 del flujo EAP-TLS descrito al principio del documento.

Seguimiento de radio activa (RA) que muestra la conexión del cliente: Este seguimiento de RA se filtra para mostrar algunas de las líneas relevantes de la transacción de autenticación.

2025/01/08 11 58 20.816875191 {wncd_x_R0-2}{1} [ewlc-capwapmsg-sess] [15655] (debug) Envío de mensaje DTLS cifrado. Dest IP 10.78.8.78[5256], longitud 499
2025/01/08 11 58 20.851392112 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 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 recibido desde 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] Paquete EAPOL enviado - Versión 3,EAP tipo EAPOL, longitud de carga 6, EAP-tipo = EAP-TLS
2025/01/08 11 58 20.881960763 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Paquete EAPOL recibido - Versión 1,EAP tipo EAPOL, longitud de carga 204, EAP-tipo = EAP-TLS
2025/01/08 11 58 20.882292551 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 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 recibido desde 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] Paquete EAPOL enviado - Versión 3,EAPOL Tipo EAP, Longitud de 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] Paquete EAPOL recibido - Versión 1,EAP tipo EAPOL, longitud de carga 6, EAP-tipo = EAP-TLS
2025/01/08 11 58 20.935405770 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 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 recibido desde

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] Paquete EAPOL enviado - Versión 3,EAP tipo EAPOL, longitud de carga 1008, EAP-tipo = EAP-TLS
2025/01/08 11 58 20.947417061 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Paquete EAPOL recibido - Versión 1,EAP tipo EAPOL, longitud de carga 6, EAP-tipo = EAP-TLS
2025/01/08 11 58 20.947722851 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 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 recibido desde 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] Paquete EAPOL enviado - Versión 3,EAPOL tipo EAP, longitud de 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] Paquete EAPOL recibido - Versión 1,EAP tipo EAPOL, longitud de carga 1492, EAP-tipo = EAP-TLS
2025/01/08 11 58 20.967209224 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 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 recibido desde 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] Paquete EAPOL enviado - Versión 3,EAP tipo EAPOL, longitud de carga 6, EAP-tipo = EAP-TLS
2025/01/08 11 58 20.978742828 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Paquete EAPOL recibido - Versión 1,EAP tipo EAPOL, longitud de carga 1492, EAP-tipo = EAP-TLS
2025/01/08 11 58 20.979081544 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 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 recibido desde 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] Paquete EAPOL enviado - Versión 3,EAP tipo EAPOL, longitud de carga 6, EAP-tipo = EAP-TLS
2025/01/08 11 58 20.990141062 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Paquete EAPOL recibido - Versión 1,EAP tipo EAPOL, longitud de carga 1492, EAP-tipo = EAP-TLS
2025/01/08 11 58 20.990472026 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 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 recibido desde 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] Paquete EAPOL enviado - Versión 3,EAP tipo EAPOL, longitud de carga 6, EAP-tipo = EAP-TLS
2025/01/08 11 58 21.001735553 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Paquete EAPOL recibido - Versión 1,EAP tipo EAPOL, longitud de carga 247,

EAP-tipo = EAP-TLS
2025/01/08 11 58 21.002076369 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 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 recibido desde 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] Paquete EAPOL enviado - Versión 3,EAP tipo EAPOL, longitud de carga 57, EAP-tipo = EAP-TLS
2025/01/08 11 58 21.024429150 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Paquete EAPOL recibido - Versión 1,EAP tipo EAPOL, longitud de carga 6, EAP-tipo = EAP-TLS
2025/01/08 11 58 21.024737996 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 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 recibido desde 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 actualización de identidad provocada para el método EAP EAP-TLS

Troubleshoot

No hay pasos específicos para solucionar este problema aparte de los procedimientos habituales de solución de problemas de la tecnología inalámbrica 802.1x:

1. Tome los debugs de seguimiento de RA del cliente para verificar el proceso de autenticación.
2. Realice una captura WLC EPC para examinar los paquetes entre el cliente, el WLC, y el servidor RADIUS.
3. Verifique los registros en directo de ISE para verificar que la solicitud coincide con la política correcta.
4. Compruebe en el extremo de Windows que el certificado está instalado correctamente y que toda la cadena de confianza está presente.

Referencias

- Preguntas frecuentes de Certificate Provisioning Portal, versión 3.2
- Comprender los servicios de autoridad de certificación interna de ISE
- Comprensión y configuración de EAP-TLS con un WLC e ISE

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).