Anulación de WLAN + VLAN 802.1x con Mobility Express (ME) 8.2 e ISE 2.1

Contenido

Introducción

En este documento se describe cómo configurar una red WLAN (red de área local inalámbrica) con seguridad Wi-Fi Protected Access 2 (WPA2) Enterprise con un controlador Mobility Express y un servidor externo Remote Authentication Dial-In User Service (RADIUS). Identity Service Engine (ISE) se utiliza como ejemplo de servidores RADIUS externos.

El protocolo de autenticación extensible (EAP) que se utiliza en esta guía es el protocolo de autenticación extensible protegido (PEAP). Además, el cliente está asignado a una VLAN específica (distinta de la asignada a la WLAN de forma predeterminada).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- 802.1x
- PEAP
- Entidad de certificación (CA)
- Certificados

Componentes Utilizados

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

ME v8.2

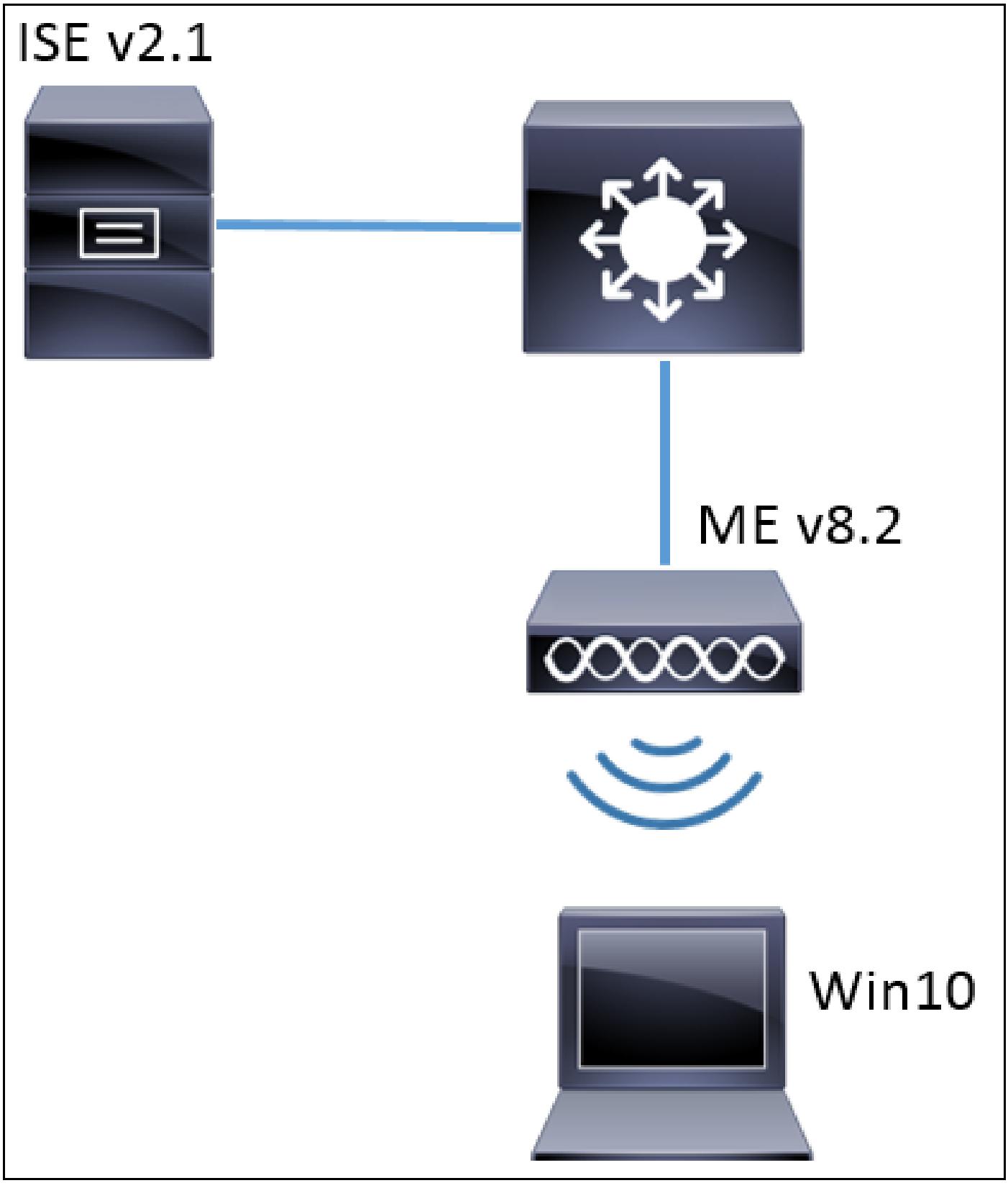
ISE v2.1

Portátil Windows 10

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). If your network is live, make sure that you understand the potential impact of any command.

Configurar

Diagrama de la red



Configuraciones

Los pasos generales son:

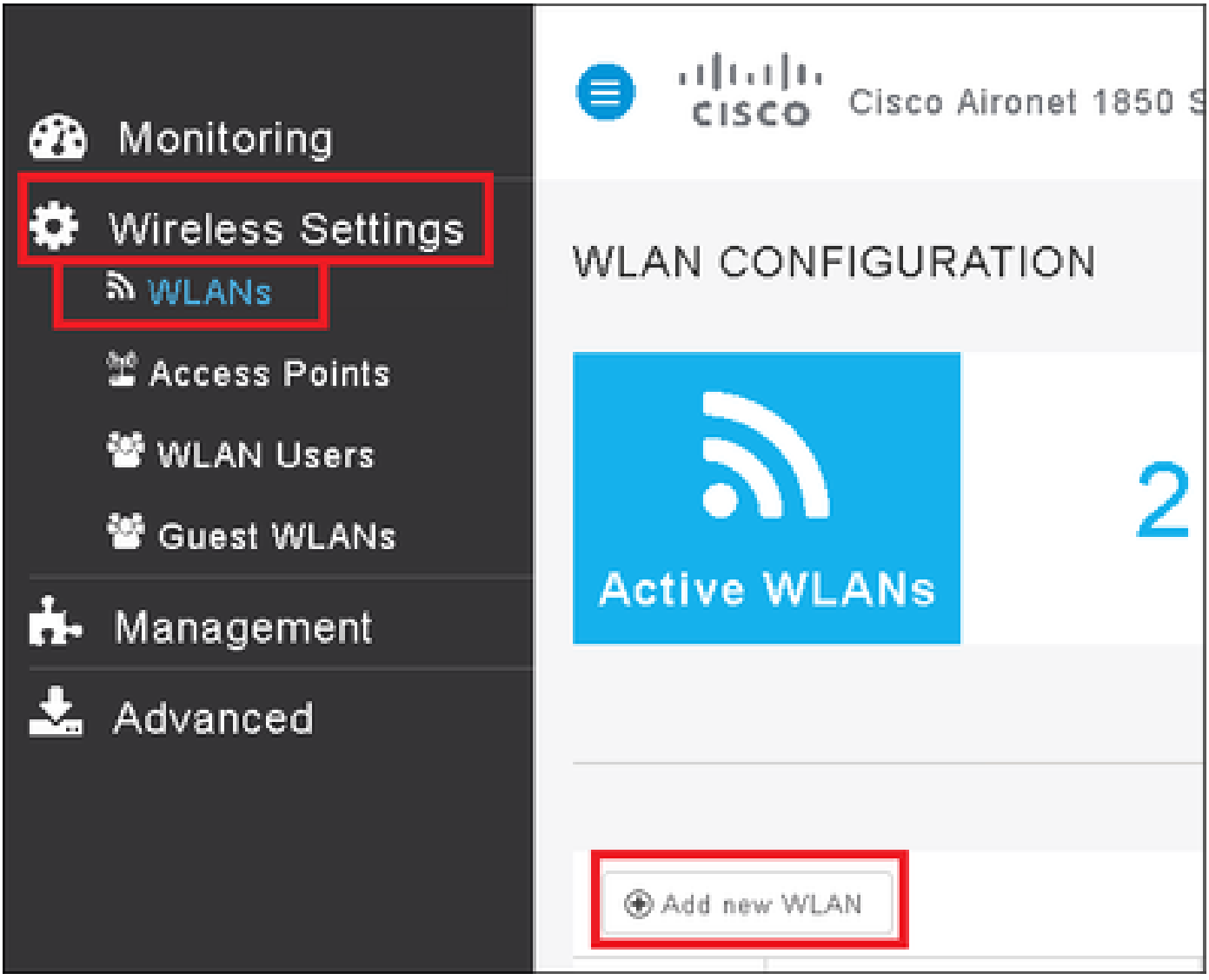
1. Cree el identificador del conjunto de servicios (SSID) en ME y declare el servidor RADIUS (ISE en este ejemplo) en ME
2. Declarar ME en servidor RADIUS (ISE)

3. Crear la regla de autenticación en ISE
4. Crear la regla de autorización en ISE
5. Configuración del terminal

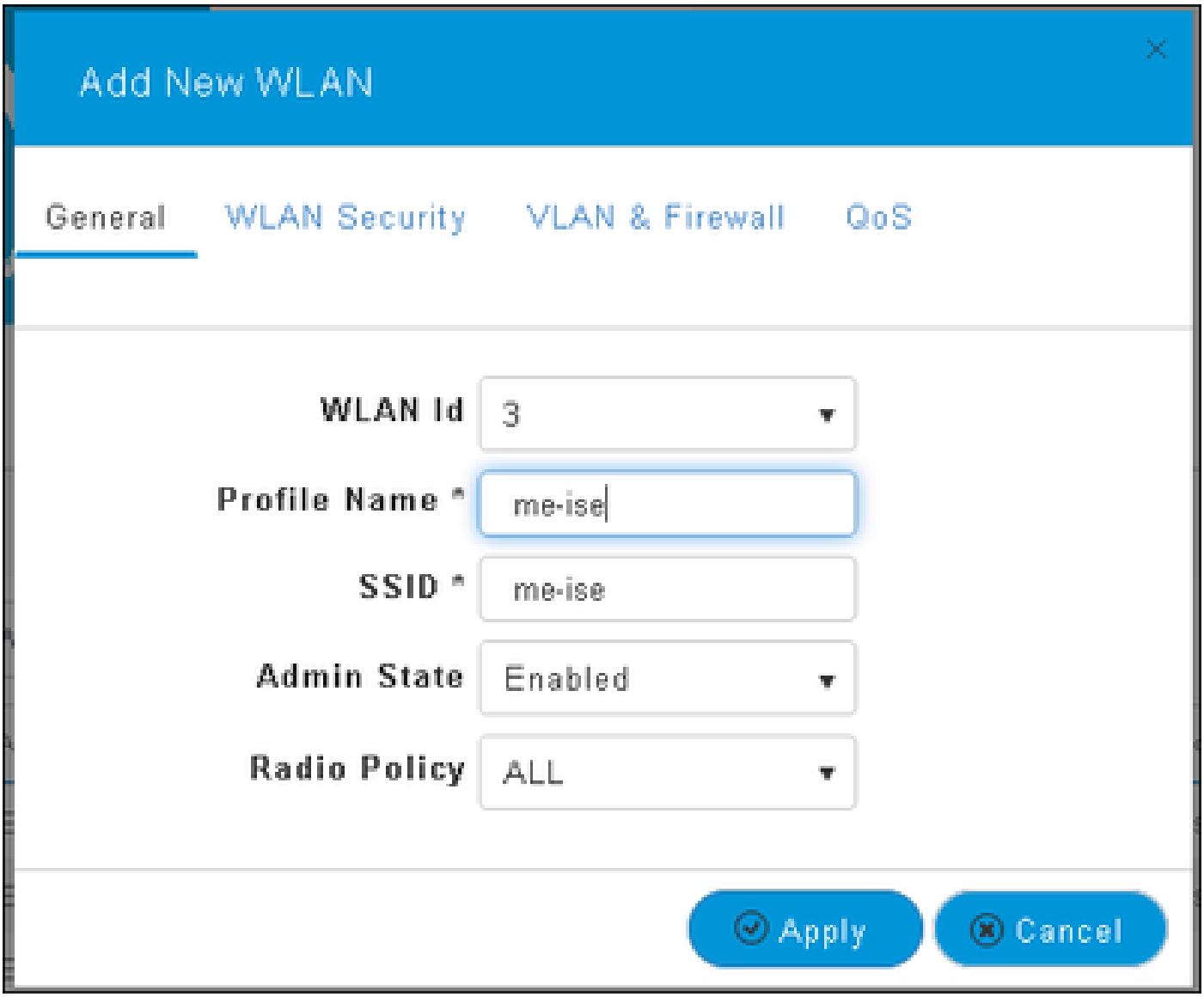
Configuración en ME

Para permitir la comunicación entre el servidor RADIUS y ME es necesario registrar el servidor RADIUS en ME y viceversa. Este paso muestra cómo registrar el servidor RADIUS en ME.

Paso 1. Abra la GUI del ME y navegue hasta Parámetros inalámbricos > WLAN > Agregar nueva WLAN.

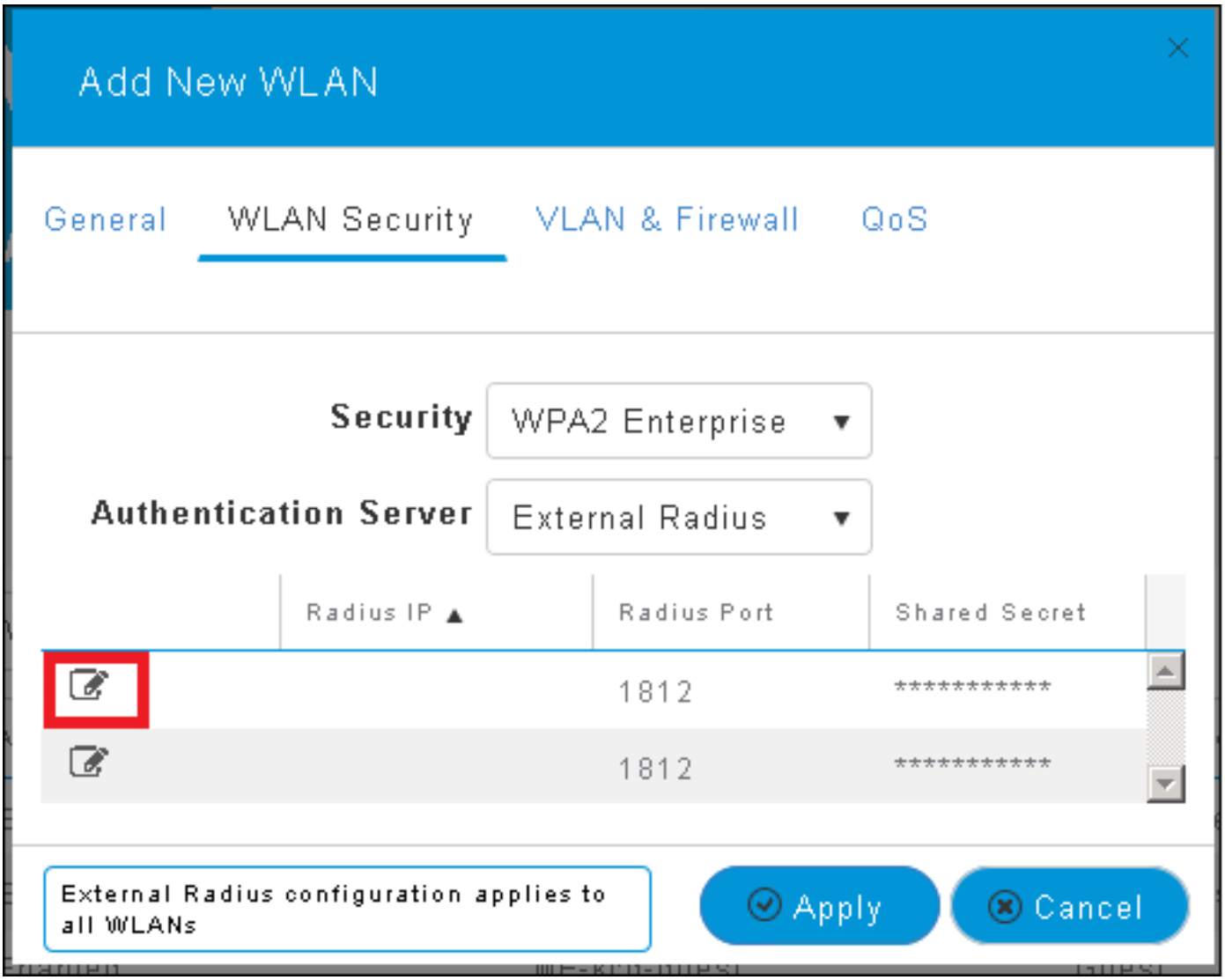


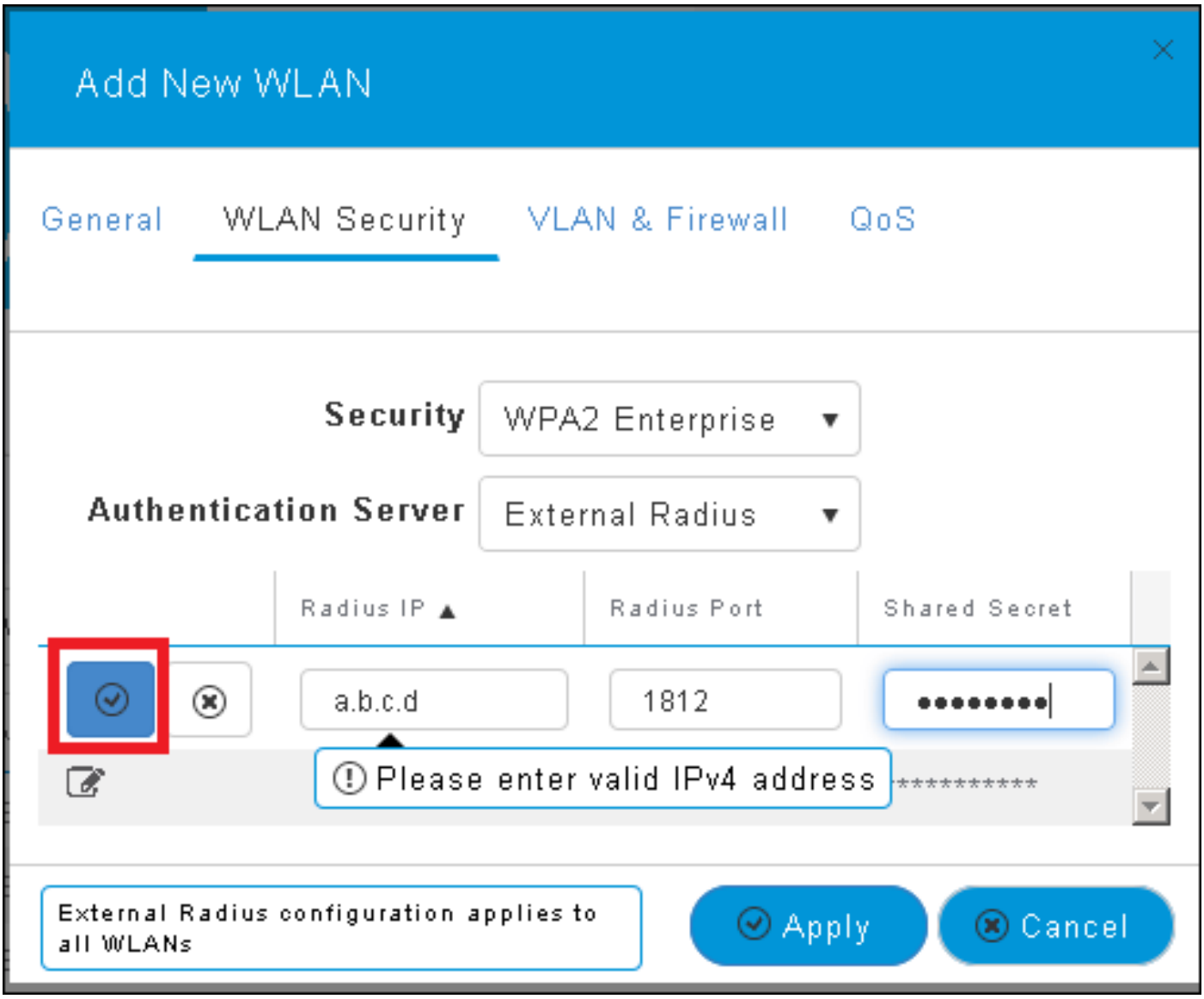
Paso 2. Seleccione un nombre para la WLAN.



Paso 3. Especifique la configuración de seguridad en la ficha Seguridad WLAN.

Elija WPA2 Enterprise, para el servidor de autenticación elija External RADIUS. Haga clic en la opción edit (editar) para agregar la dirección IP del RADIUS y elija una clave Shared Secret.


Add New WLAN
General
WLAN Security
VLAN & Firewall
QoS
Security
WPA2 Enterprise
Authentication Server
External Radius
Radius IP
Radius Port
Shared Secret
1812
****
1812
****
External Radius configuration applies to all WLANs
Apply
Cancel

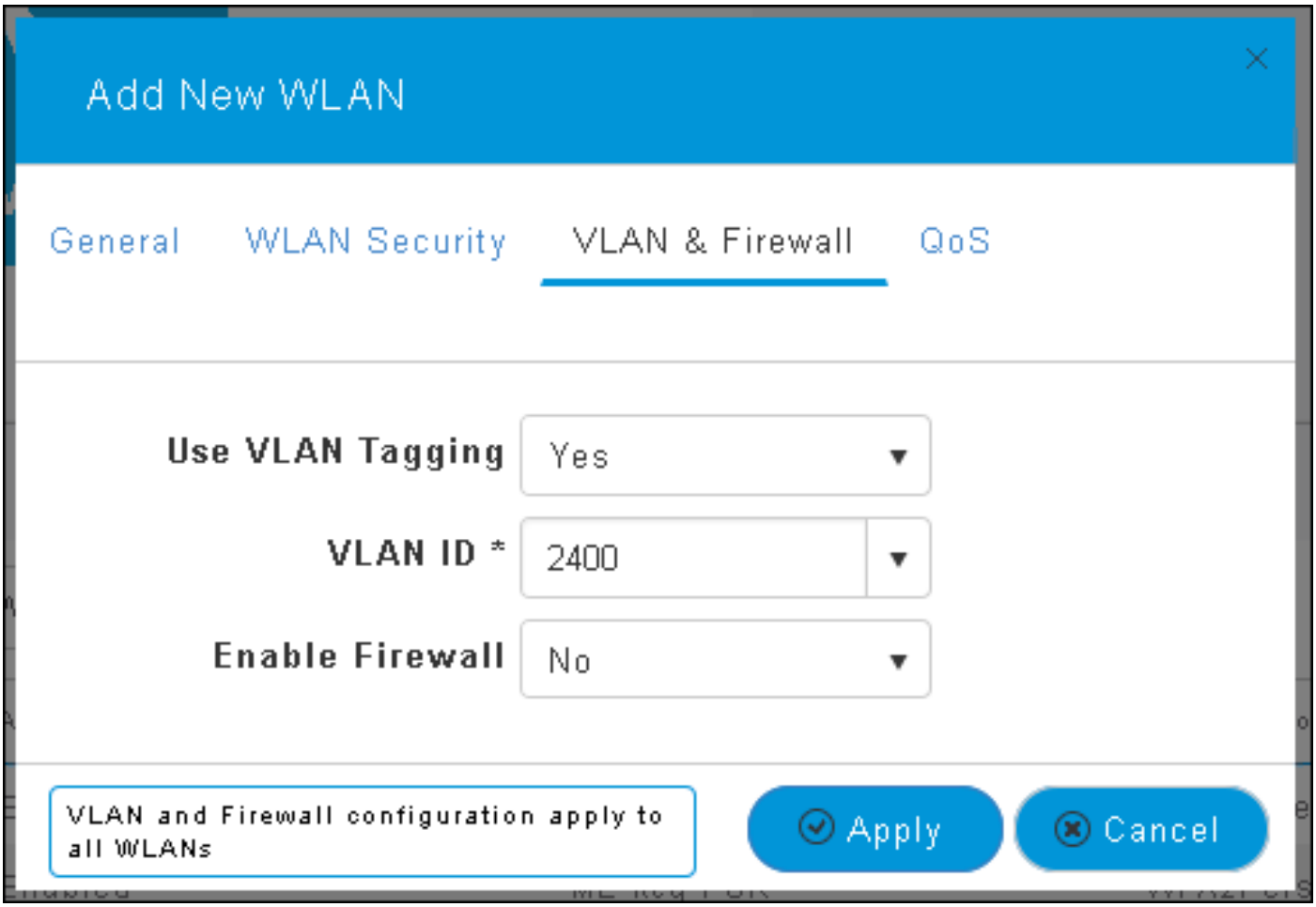


<a.b.c.d> corresponde al servidor RADIUS.

Paso 4. Asigne una VLAN al SSID.

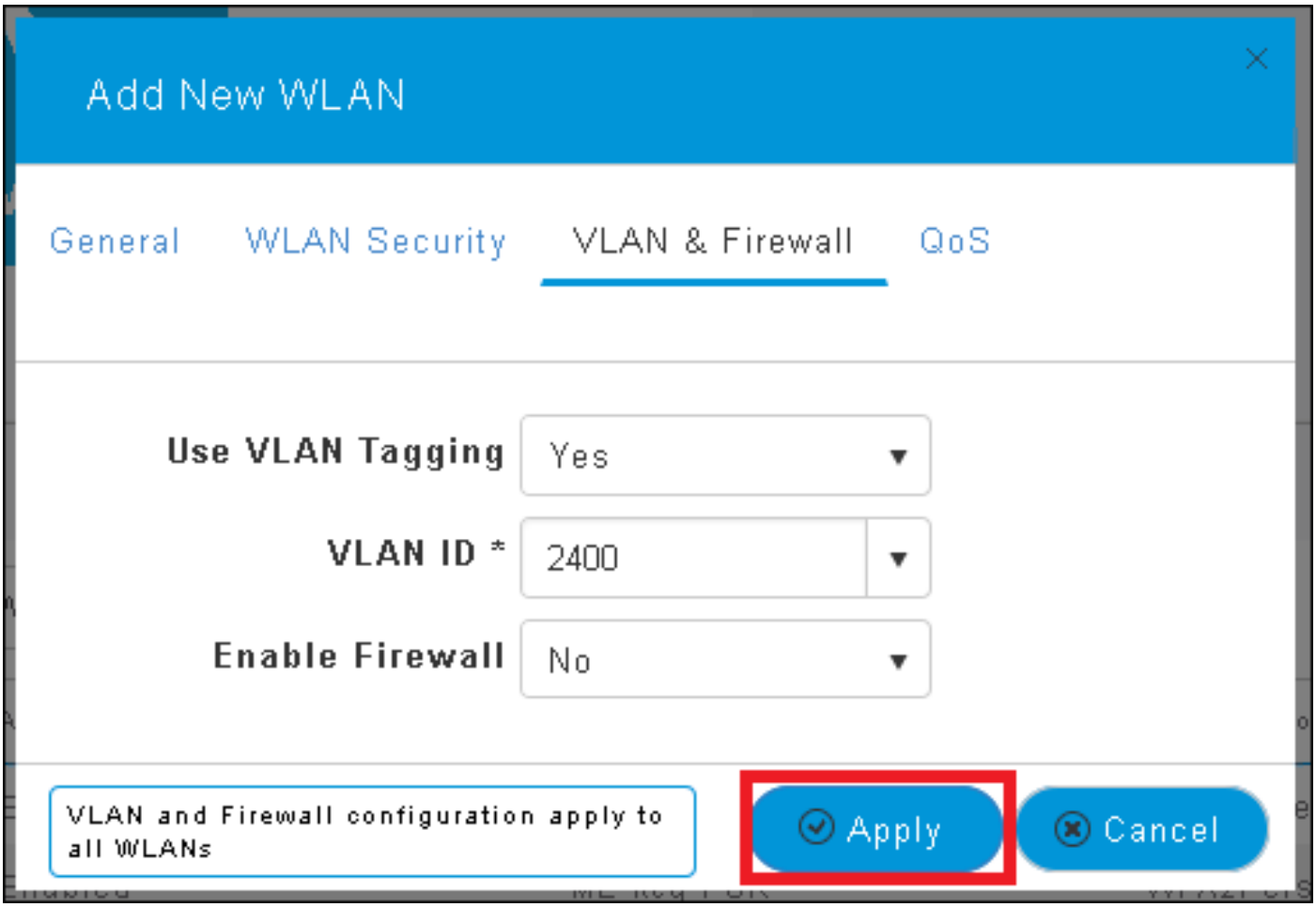
Si el SSID necesita ser asignado a la VLAN del AP, este paso puede ser omitido.

Para asignar los usuarios para este SSID a una VLAN específica (distinta de la VLAN del AP), habilite Use VLAN Tagging y asigne el ID de VLAN deseado.



Nota: Si se utiliza etiquetado VLAN, asegúrese de que el puerto de switch al que se conecta el punto de acceso esté configurado como puerto troncal y que la VLAN de AP esté configurada como nativa.

Paso 5. Haga clic en Aplicar para finalizar la configuración.



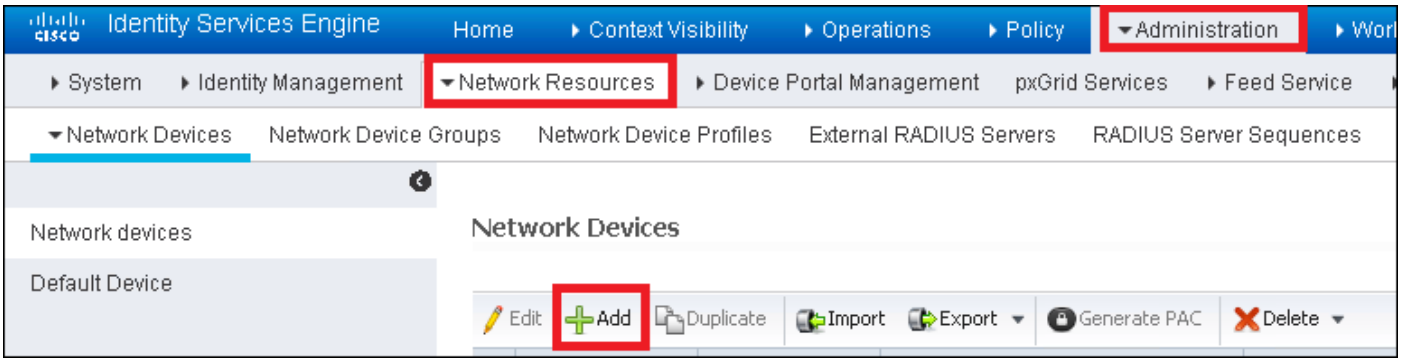
Paso 6. Opcional, configure la WLAN para aceptar la anulación de VLAN.

Active la anulación de AAA en la WLAN y agregue las VLAN necesarias. Para ello, deberá abrir una sesión CLI en la interfaz de administración de ME y ejecutar estos comandos:

```
>config wlan disable <wlan-id>
>config wlan aaa-override enable <wlan-id>
>config wlan enable <wlan-id>
>config flexconnect group default-flexgroup vlan add <vlan-id>
```

Declararme en ISE

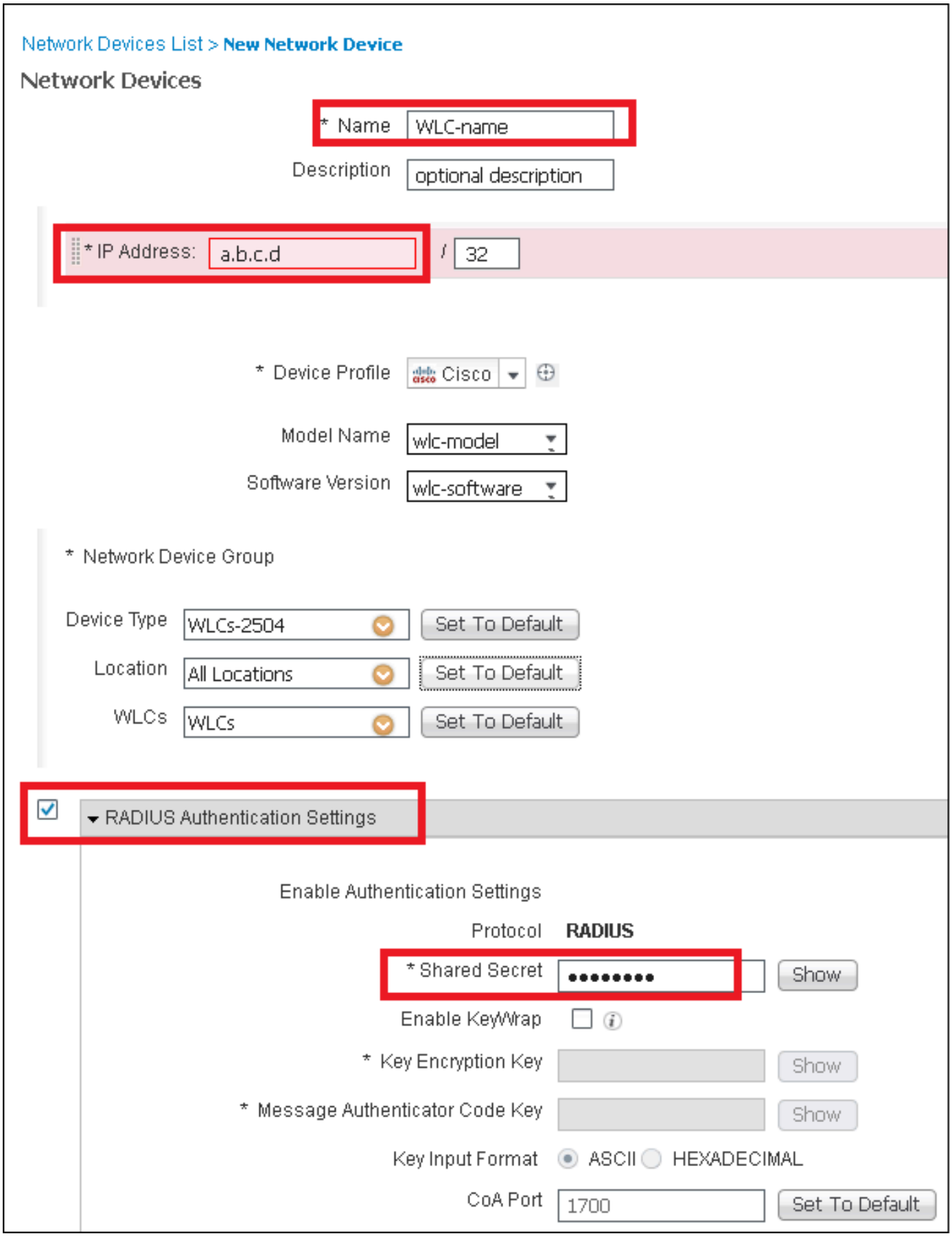
Paso 1. Abra la consola de ISE y navegue hasta Administración > Recursos de red > Dispositivos de red > Agregar.



Paso 2. Introduzca la información.

Opcionalmente se puede especificar un nombre de modelo, versión de software, descripción y asignar grupos de dispositivos de red basados en tipos de dispositivos, ubicación o WLC.

a.b.c.d corresponde a la dirección IP del ME.

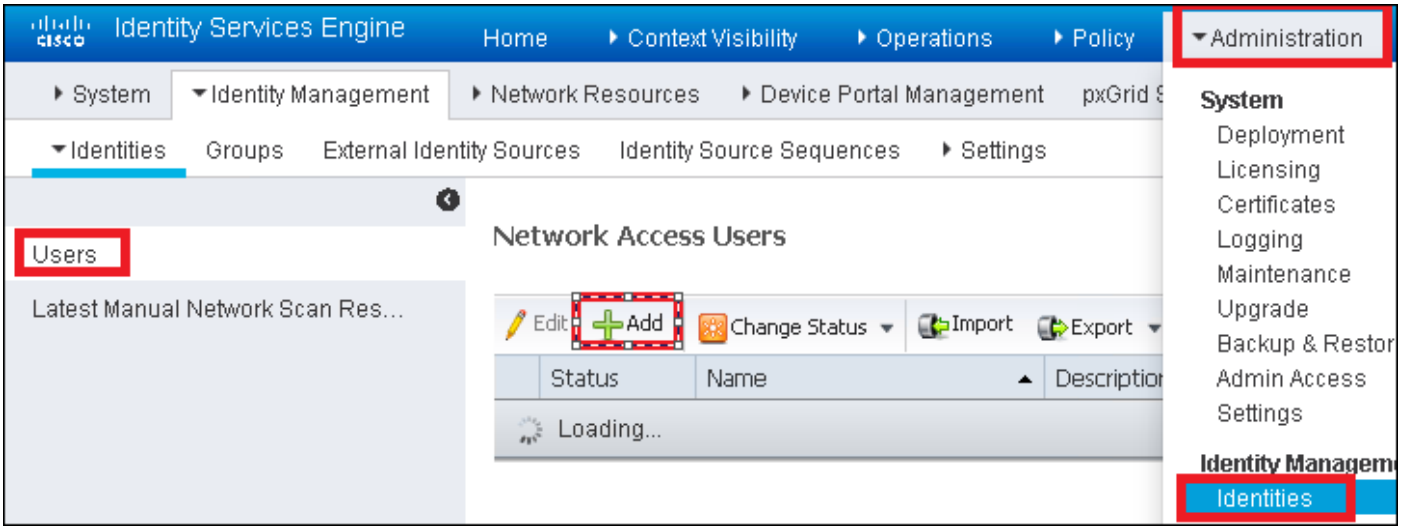


Para obtener más información sobre los grupos de dispositivos de red, consulte este enlace:

[ISE: grupos de dispositivos de red]

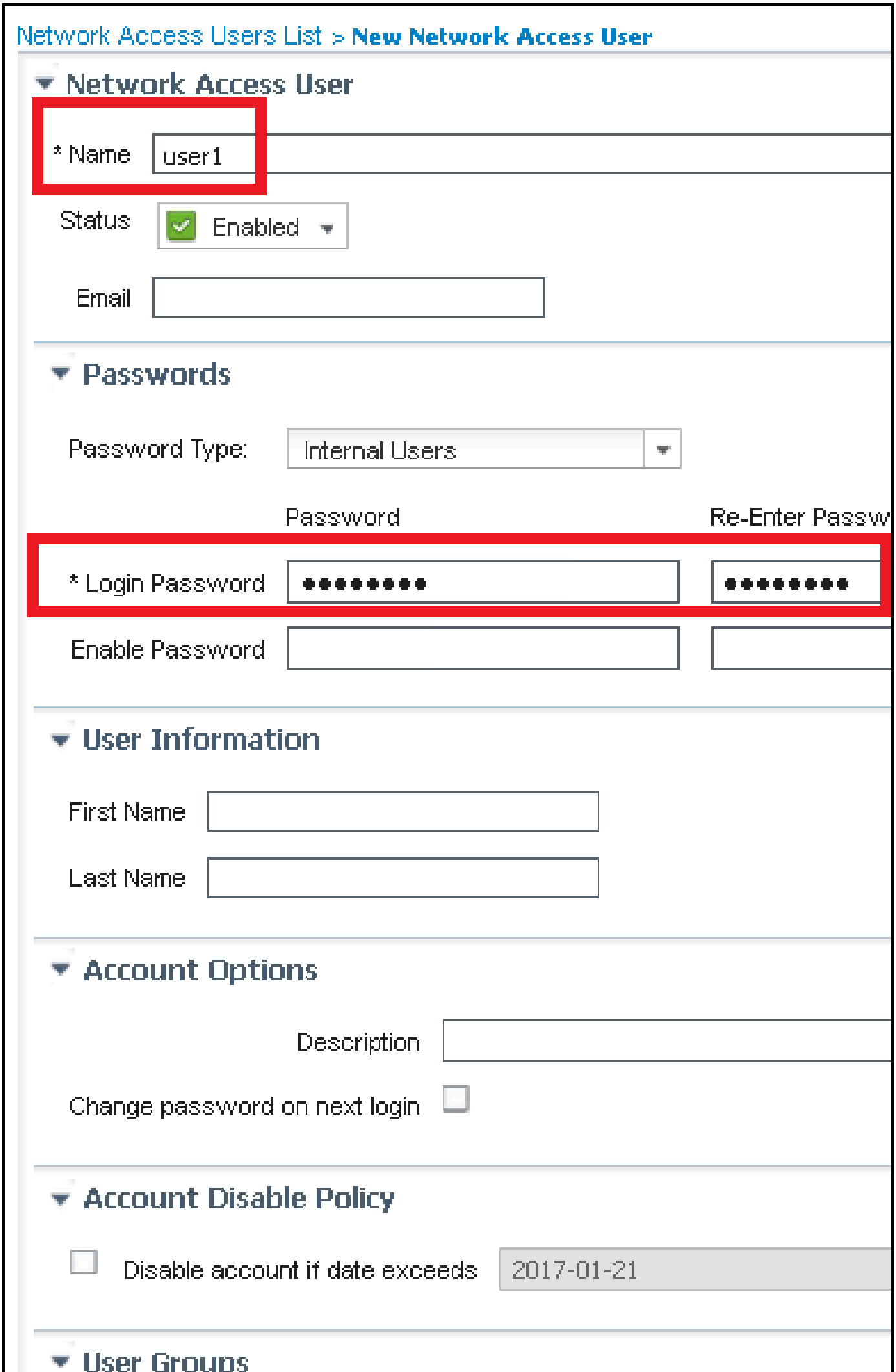
Crear un nuevo usuario en ISE

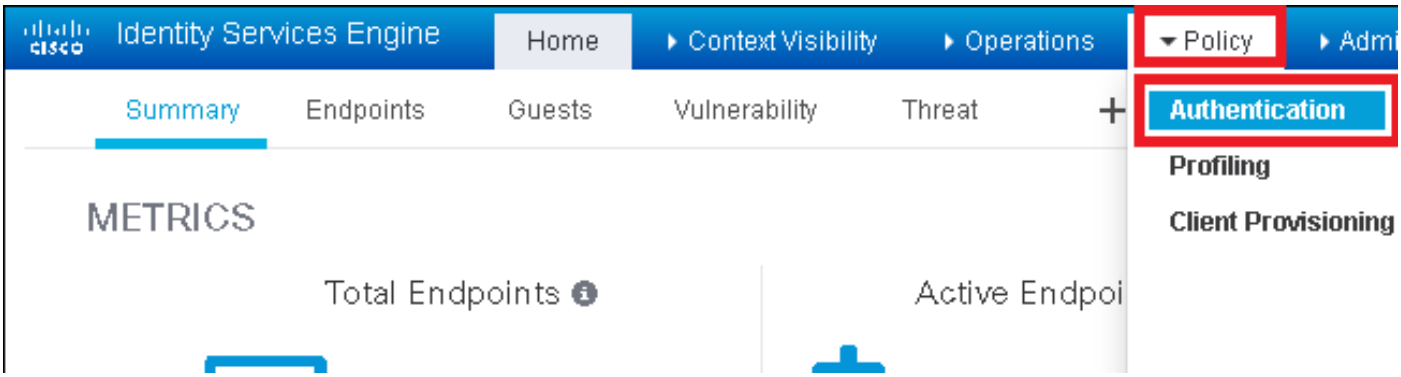
Paso 1. Desplácese hasta Administration > Identity Management > Identities > Users > Add.



Paso 2. Introduzca la información.

En este ejemplo, este usuario pertenece a un grupo denominado ALL_ACCOUNTS, pero se puede ajustar según sea necesario.


Network Access Users List > New Network Access User
Network Access User
* Name
user1
Status
Enabled
Email
Passwords
Password Type:
Internal Users
Password
Re-Enter Passw
* Login Password
Enable Password
User Information
First Name
Last Name
Account Options
Description
Change password on next login
Account Disable Policy
Disable account if date exceeds
2017-01-21
User Groups

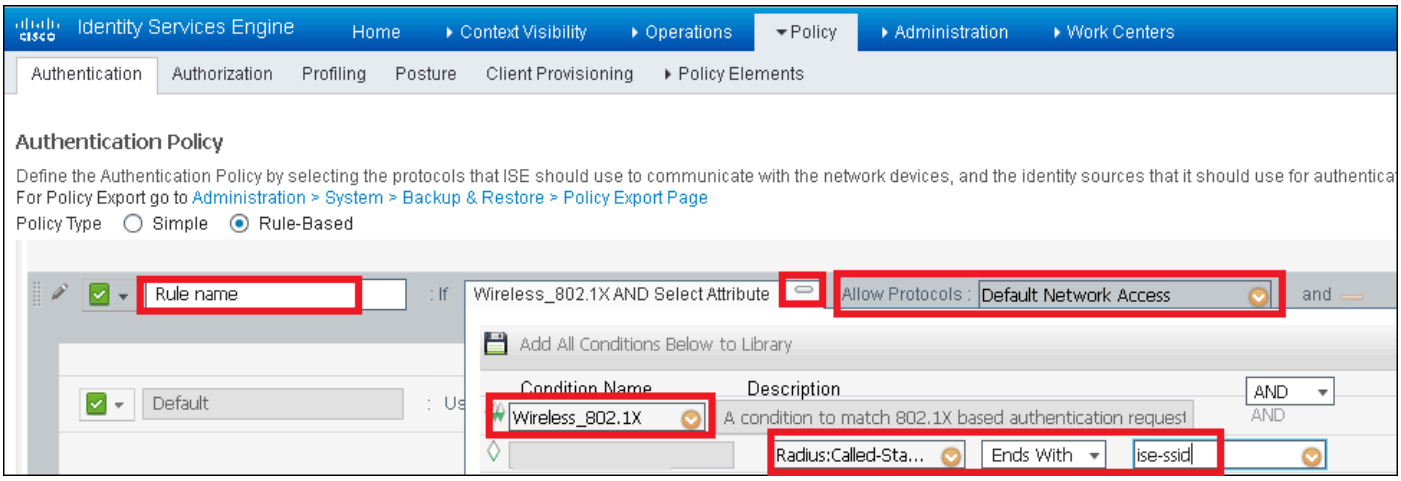


Paso 2. Inserte una nueva regla de autenticación.

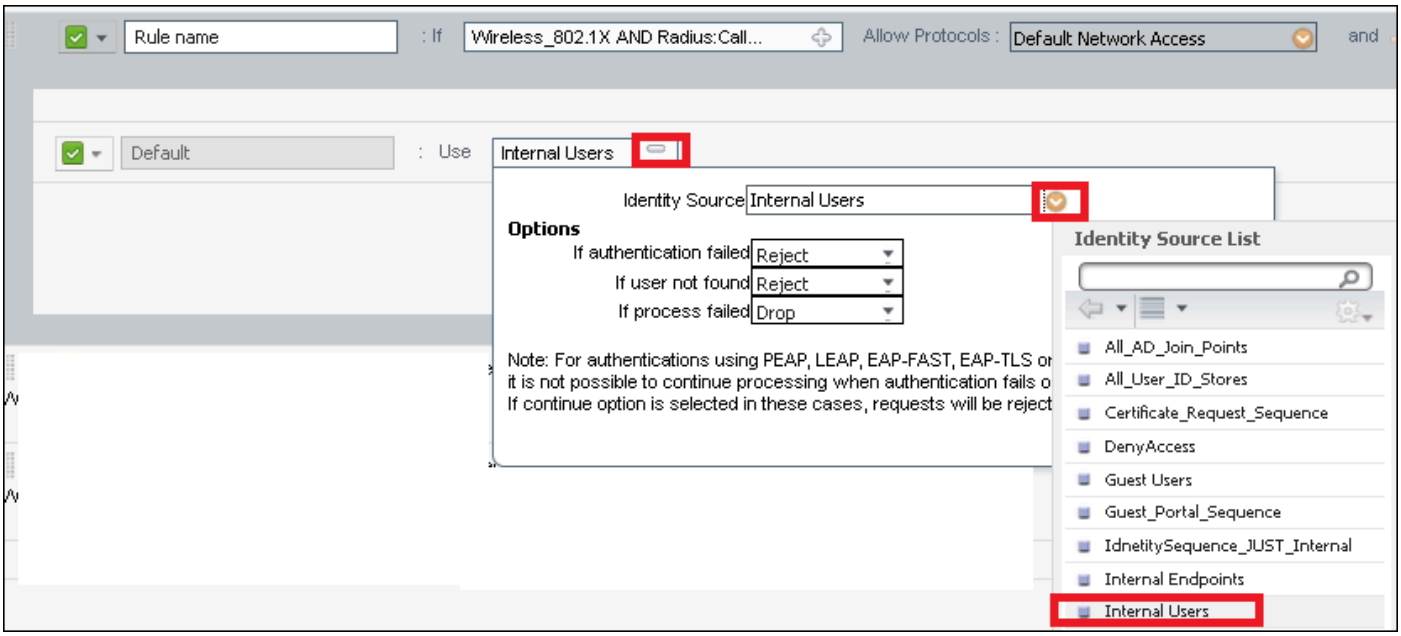
Para hacerlo, navegue hasta Policy > Authentication > Insert new row above/below.

Paso 3. Introduzca la información necesaria

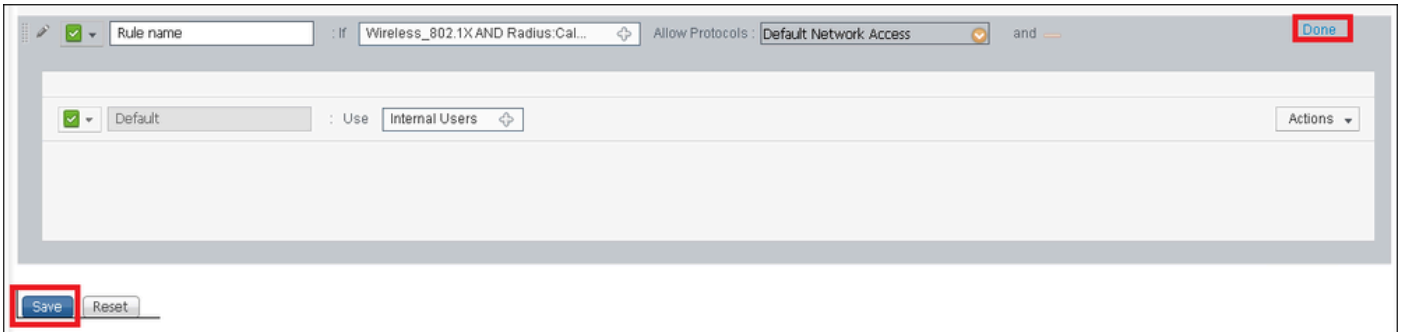
Este ejemplo de regla de autenticación permite todos los protocolos enumerados en la lista Default Network Access, esto se aplica a la solicitud de autenticación para clientes Wireless 802.1x y con Called-Station-ID y termina con ise-ssid.



Además, elija el origen de identidad para los clientes que coincide con esta regla de autenticación, en este ejemplo se utiliza Usuarios internos



Una vez que haya terminado, haga clic en Finalizado y Guardar



Para obtener más información sobre las directivas de permitidos protocolos, consulte este enlace:

Servicio de protocolos permitidos

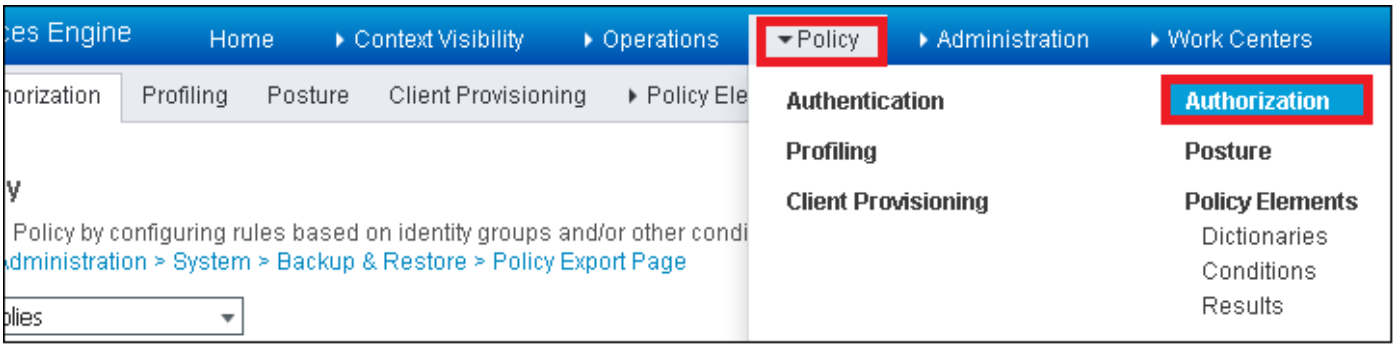
Para obtener más información sobre los orígenes de identidad, consulte este enlace:

Crear un grupo de identidad de usuario

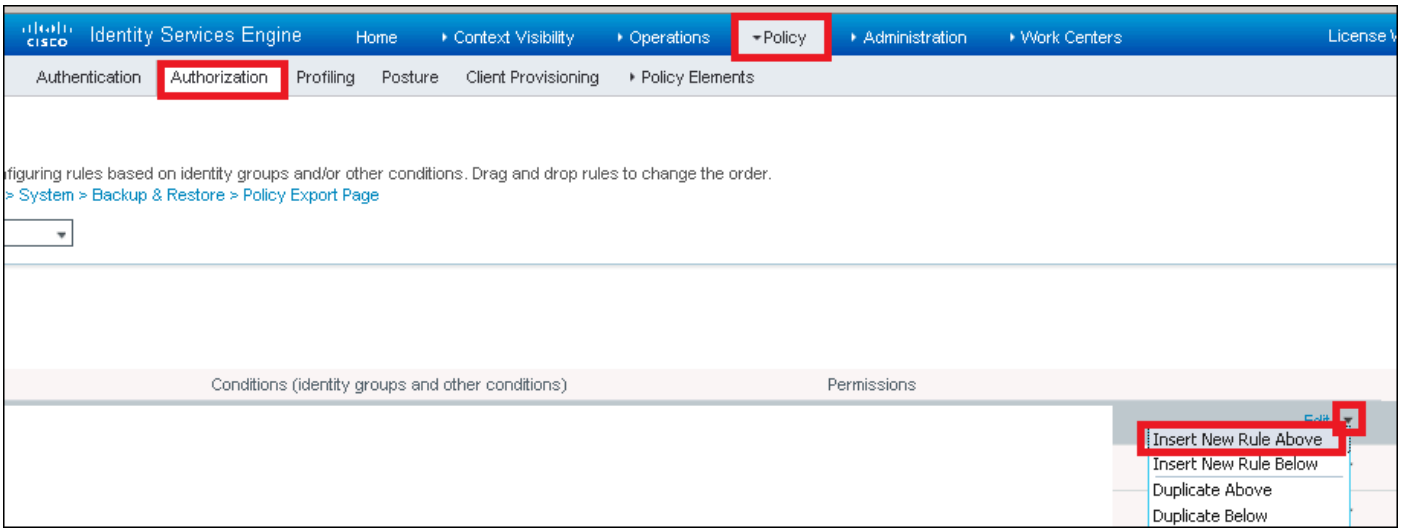
Crear la regla de autorización

La regla de autorización es la encargada de determinar si el cliente puede o no unirse a la red

Paso 1. Navegue hasta Política > Autorización.

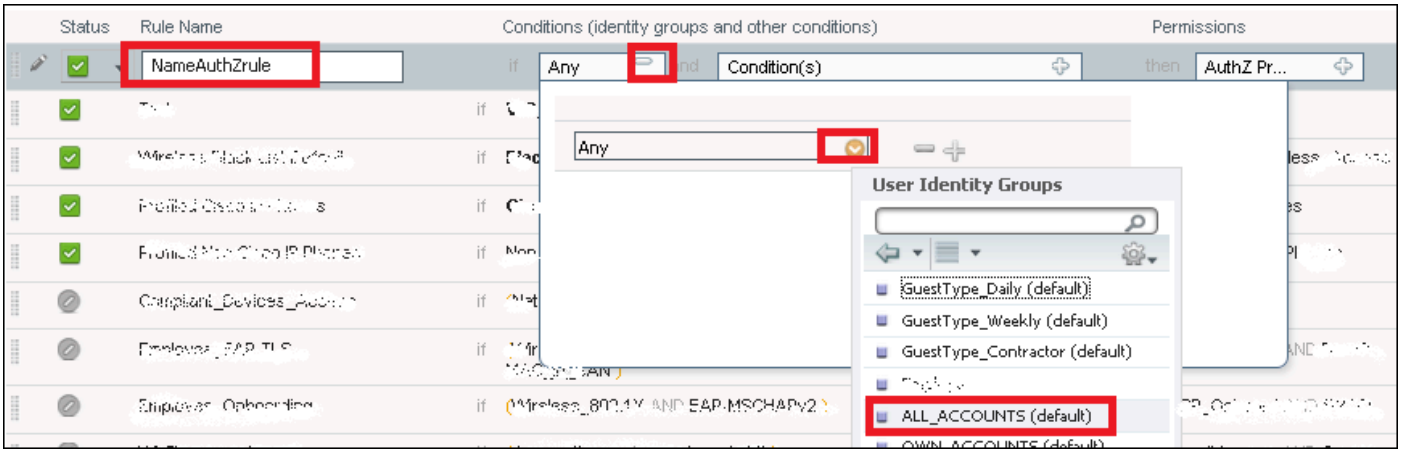


Paso 2. Inserte una nueva regla. Vaya a Política > Autorización > Insertar nueva regla arriba/abajo.

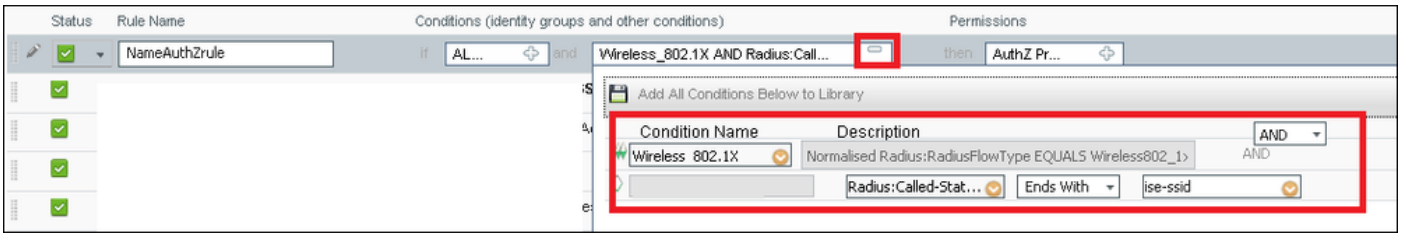


Paso 3. Introduzca la información.

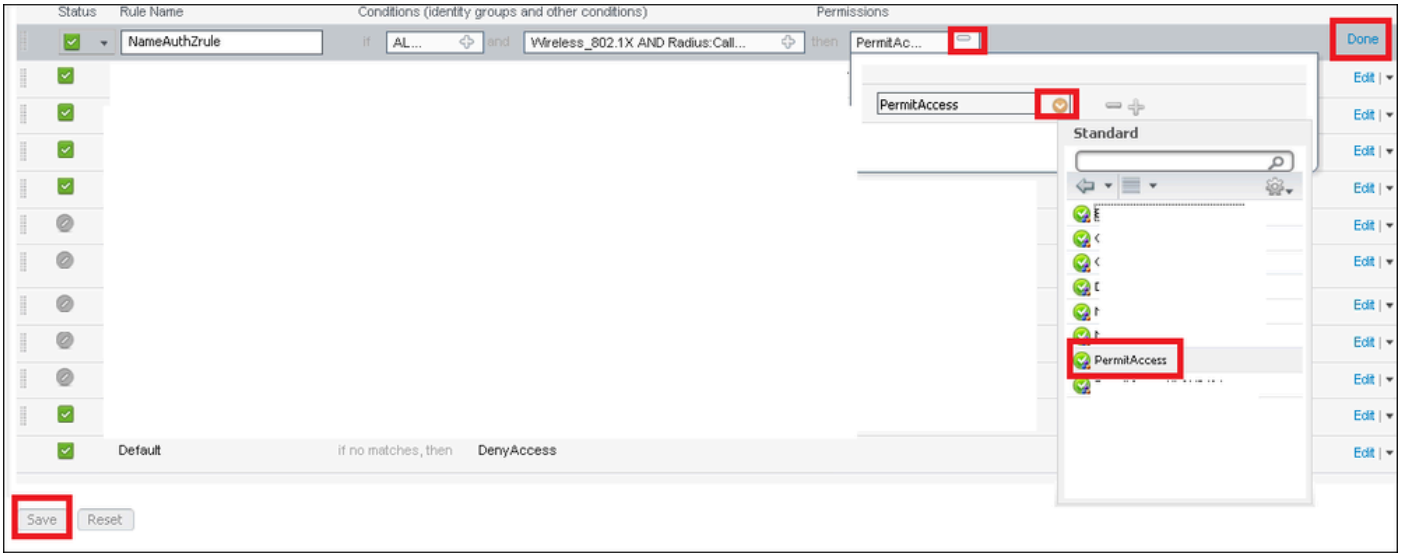
En primer lugar, elija un nombre para la regla y los grupos de identidad donde se almacena el usuario. En este ejemplo, el usuario se almacena en el grupo ALL_ACCOUNTS.



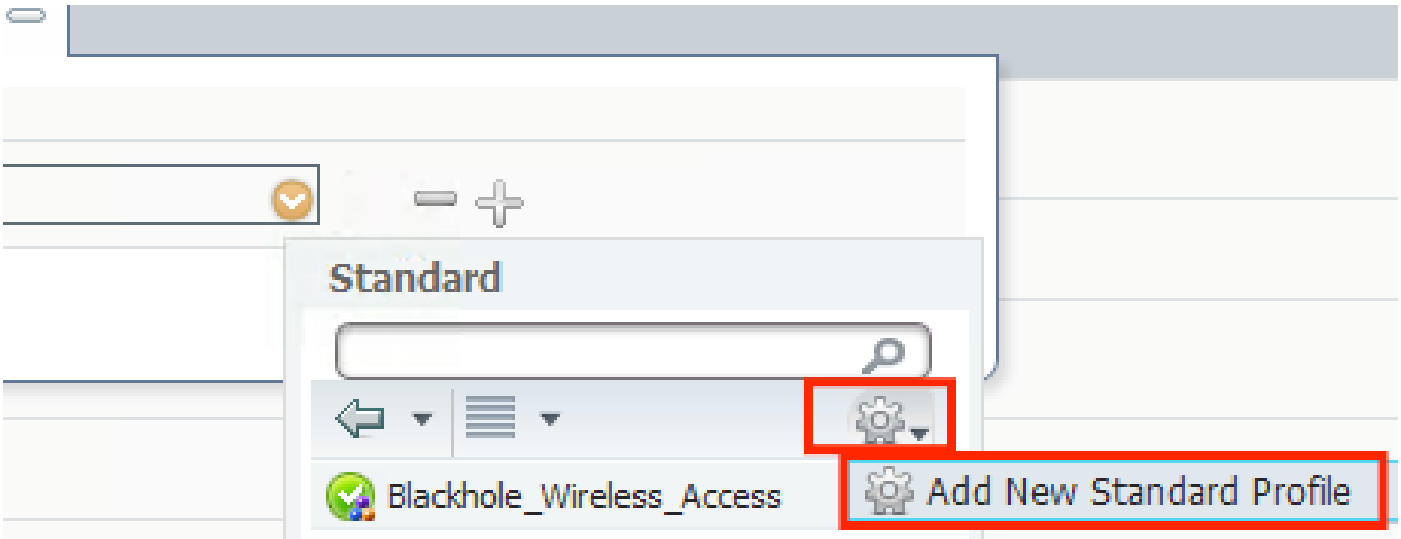
A continuación, elija otras condiciones que hagan que el proceso de autorización se ajuste a esta regla. En este ejemplo, el proceso de autorización llega a esta regla si utiliza 802.1x Wireless y se denomina station ID termina con ise-ssid.



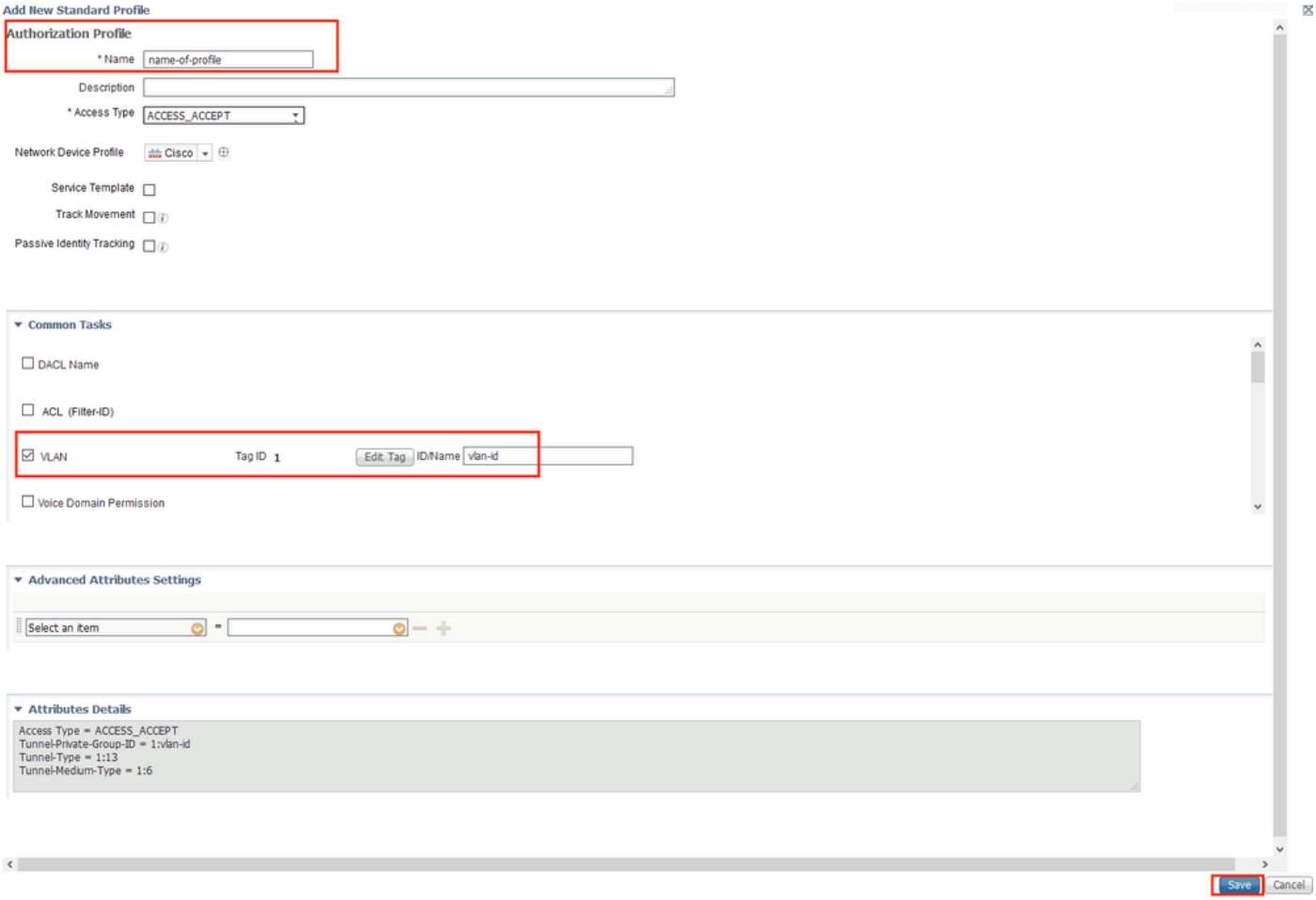
Por último, elija el perfil de autorización que permite que los clientes se unan a la red, haga clic en Finalizado y Guardar.



Opcionalmente, cree un nuevo perfil de autorización que asignará el cliente inalámbrico a una VLAN diferente:



Introduzca la información:



Configuración del dispositivo final

Configure un portátil con Windows 10 para conectarse a un SSID con autenticación 802.1x mediante PEAP/MS-CHAPv2 (versión de Microsoft del protocolo de autenticación por desafío mutuo versión 2).

En este ejemplo de configuración, ISE utiliza su certificado autofirmado para realizar la autenticación.

Para crear el perfil WLAN en la máquina de Windows hay dos opciones:

1. Instale el certificado autofirmado en el equipo para validar y confiar en el servidor ISE para completar la autenticación
2. Omitir la validación del servidor RADIUS y confiar en cualquier servidor RADIUS utilizado para realizar la autenticación (no se recomienda, ya que puede convertirse en un problema de seguridad)

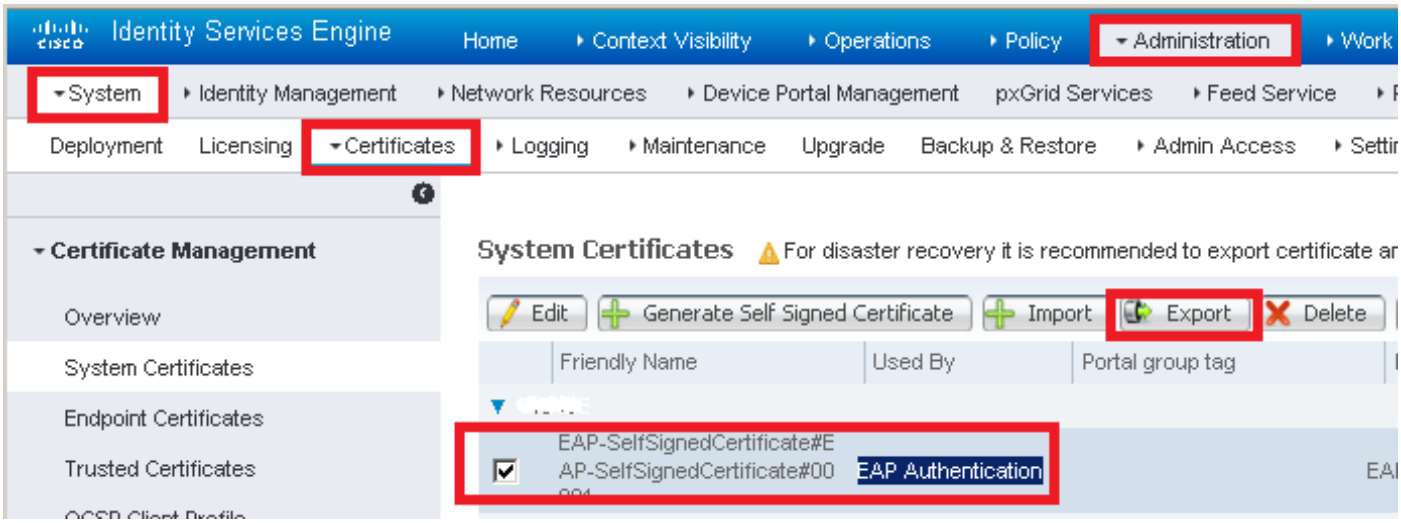
La configuración de estas opciones se explica en End device configuration - Create the WLAN Profile - Step 7.

Configuración del dispositivo final: instalación del certificado autofirmado de ISE

Paso 1. Exportar certificado autofirmado desde ISE.

Inicie sesión en ISE y navegue hasta Administration > System > Certificates > System Certificates.

A continuación, seleccione el certificado utilizado para la autenticación EAP y haga clic en Exportar.

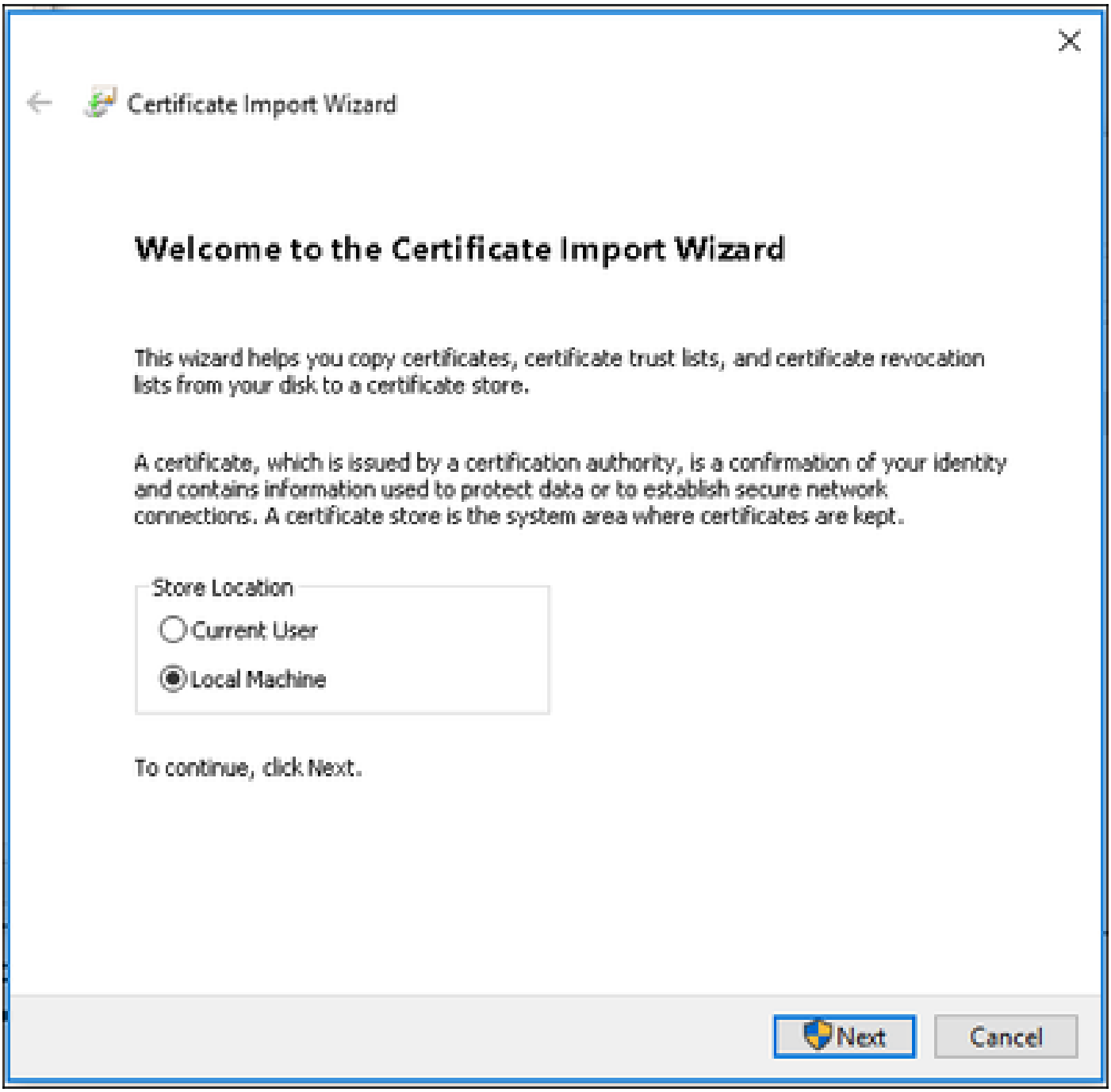


Guarde el certificado en la ubicación necesaria. Este certificado está instalado en el equipo con Windows.

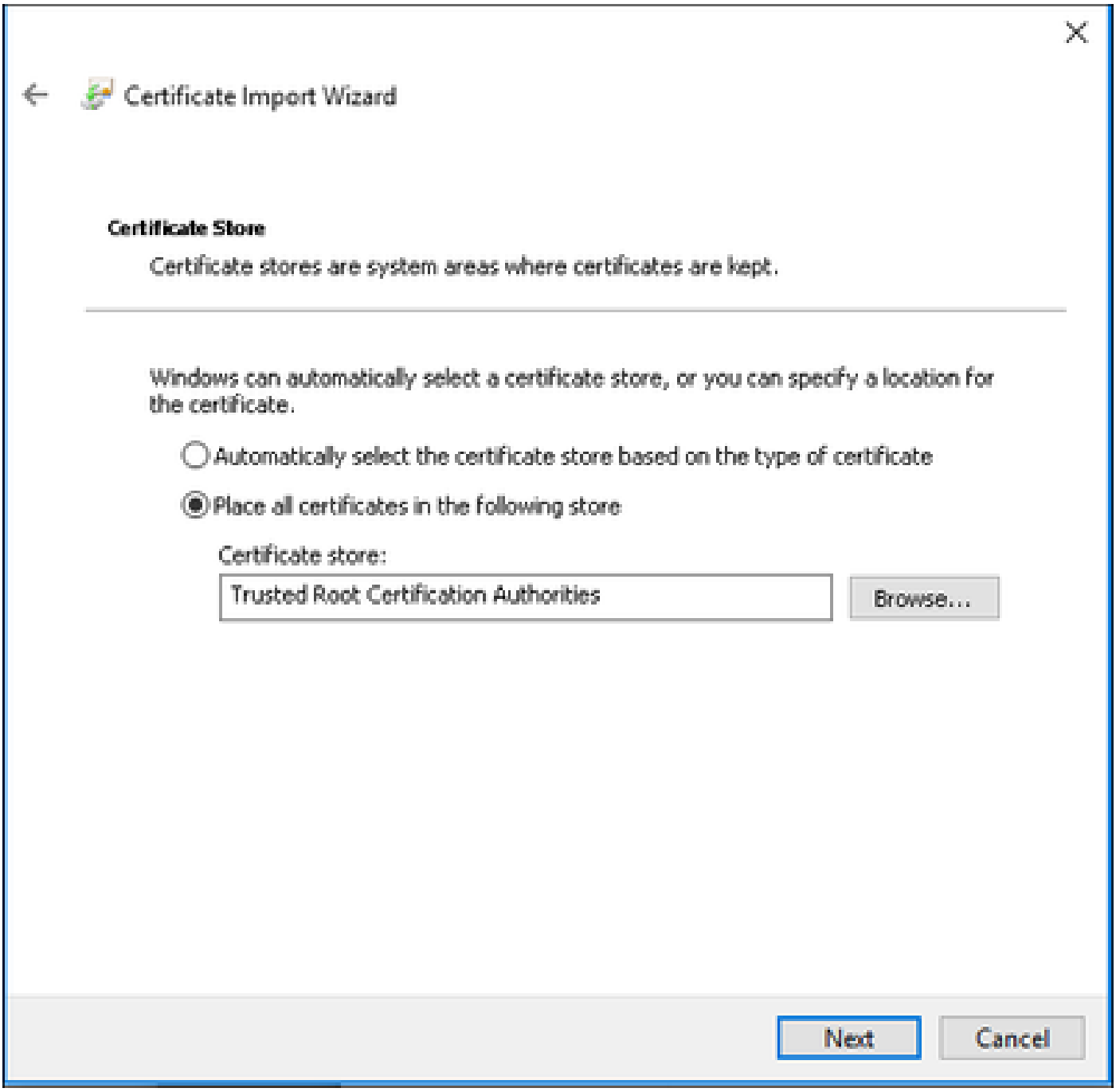
Paso 2. Instale el certificado en el equipo con Windows.

Copie el certificado exportado antes en la máquina de Windows, cambie la extensión del archivo de .pem a .crt, después de que haga doble clic en él y seleccione Instalar certificado....

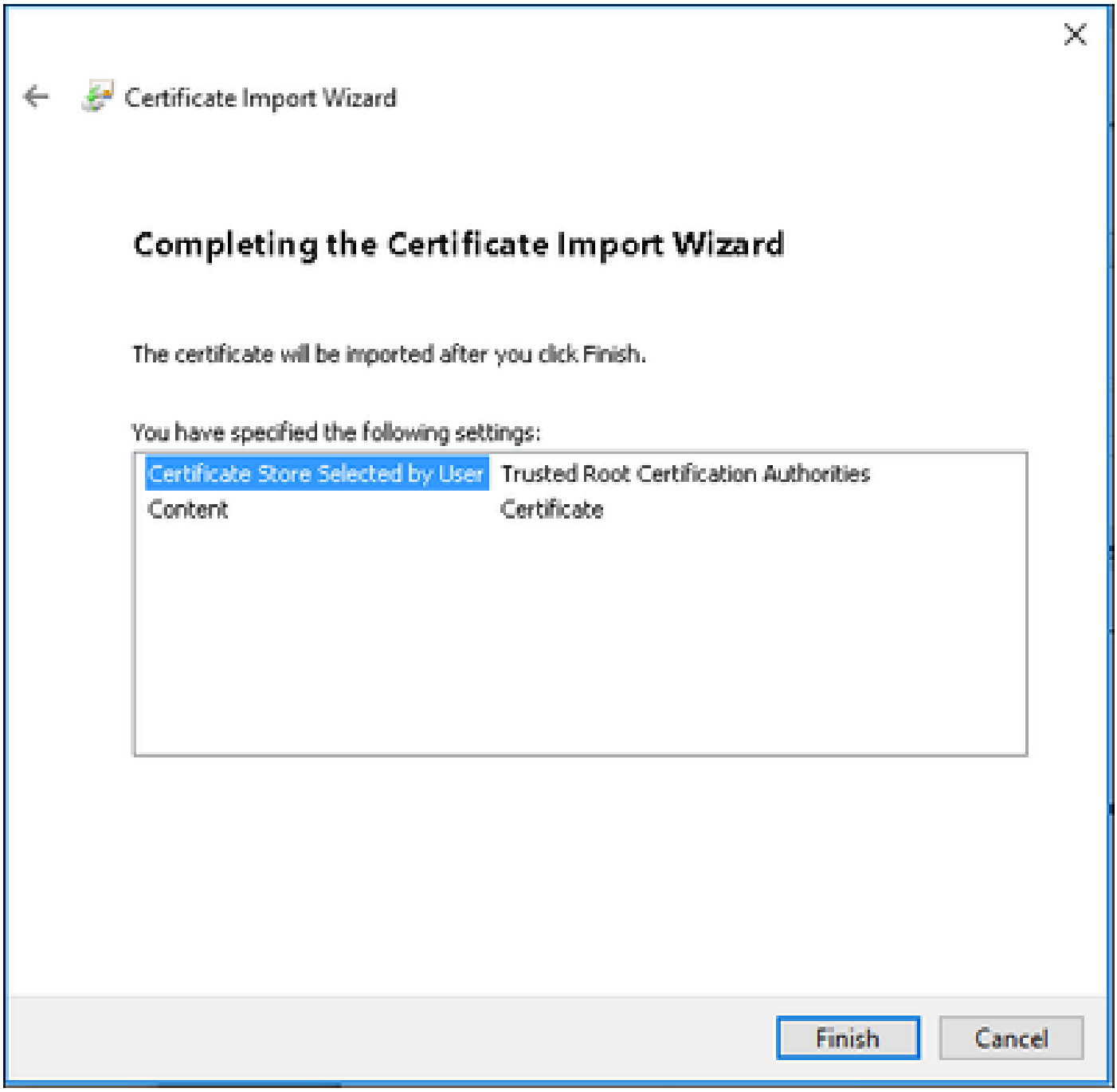
Elija instalarlo en el equipo local y, a continuación, haga clic en Siguiente.



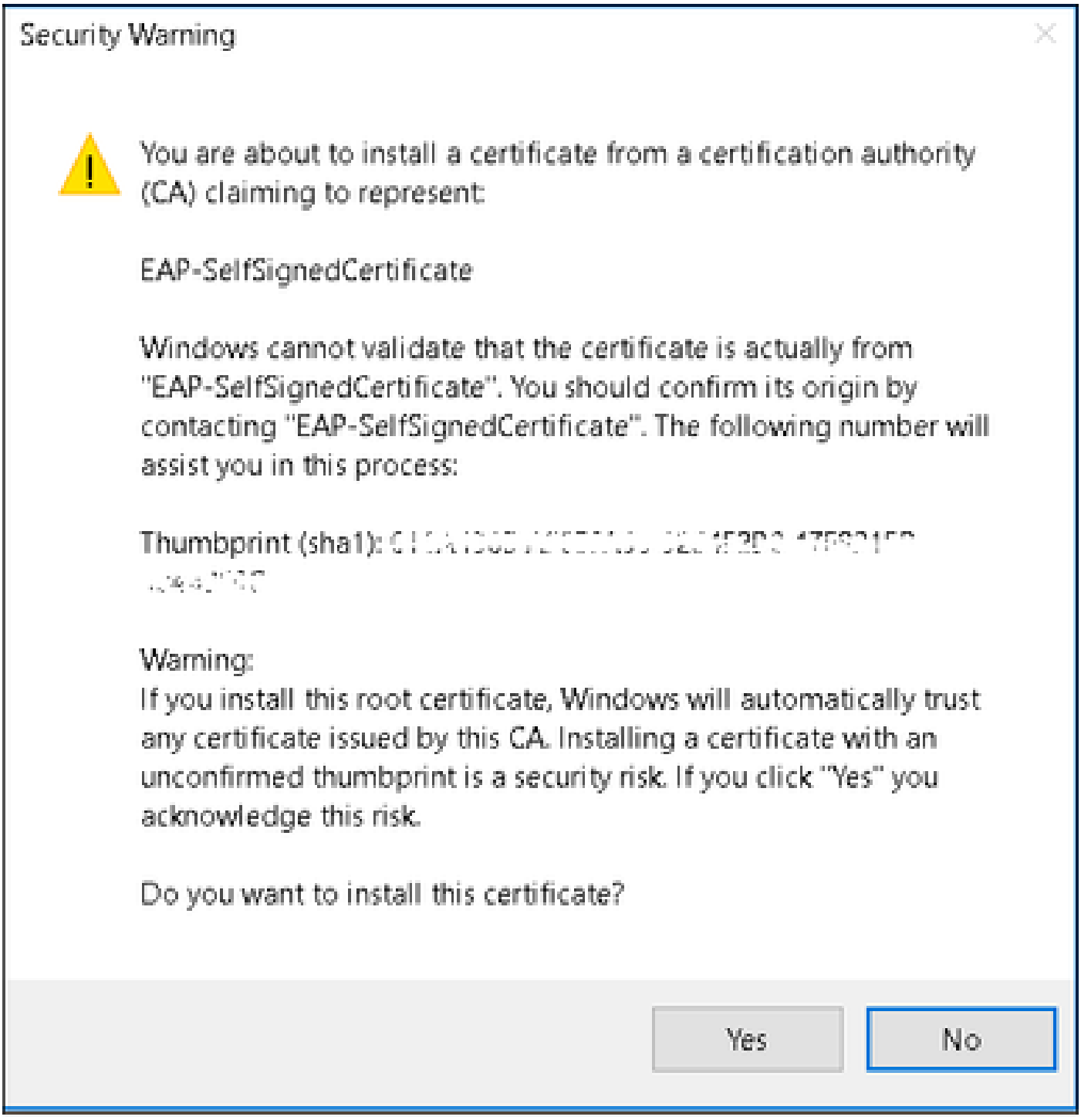
Seleccione Colocar todos los certificados en el siguiente almacén, busque y elija Entidades emisoras raíz de confianza. Después de eso, haga clic en Siguiente.



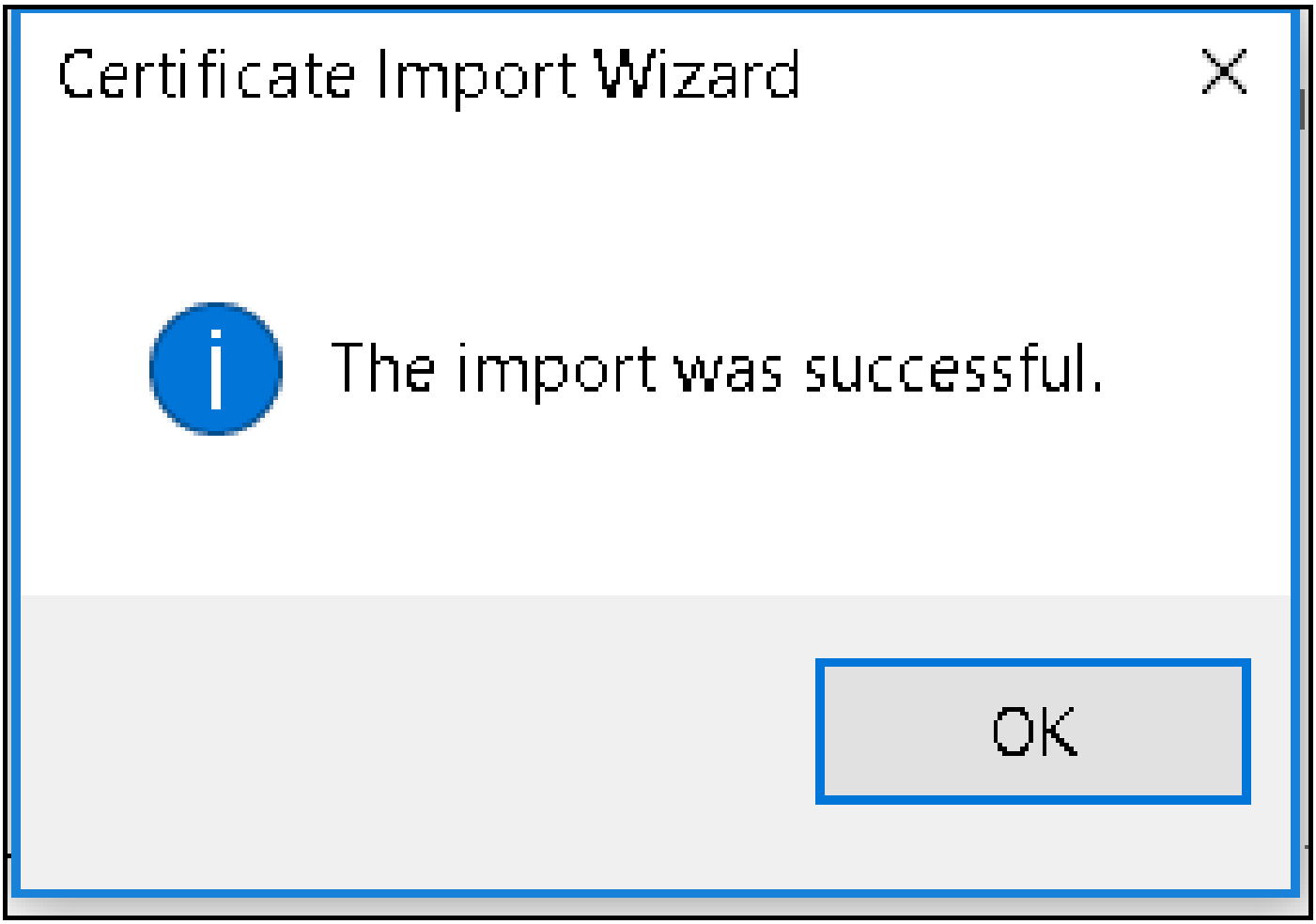
A continuación, haga clic en Finalizar.



Al final, haga clic en Yes para confirmar la instalación del certificado.

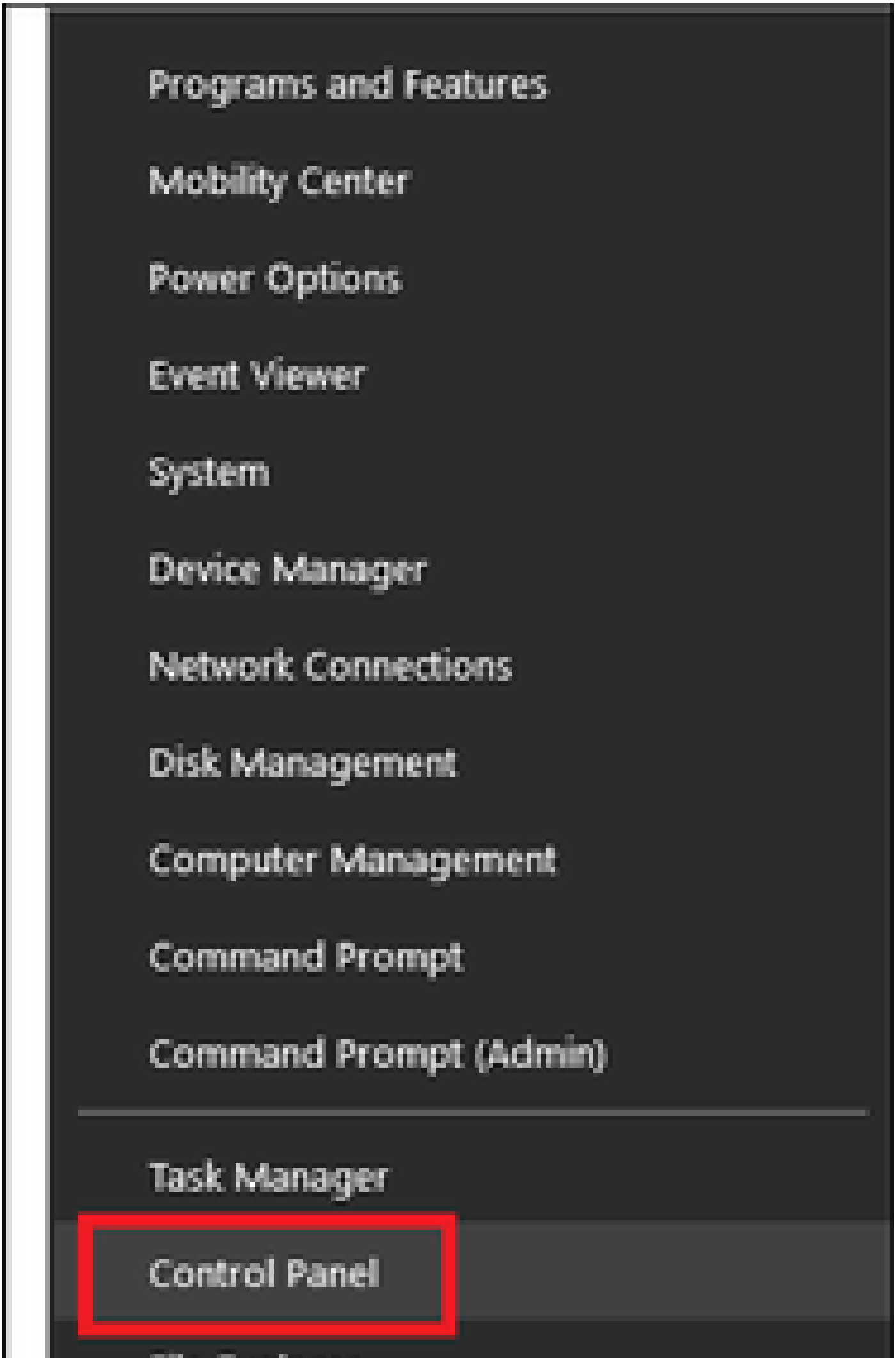


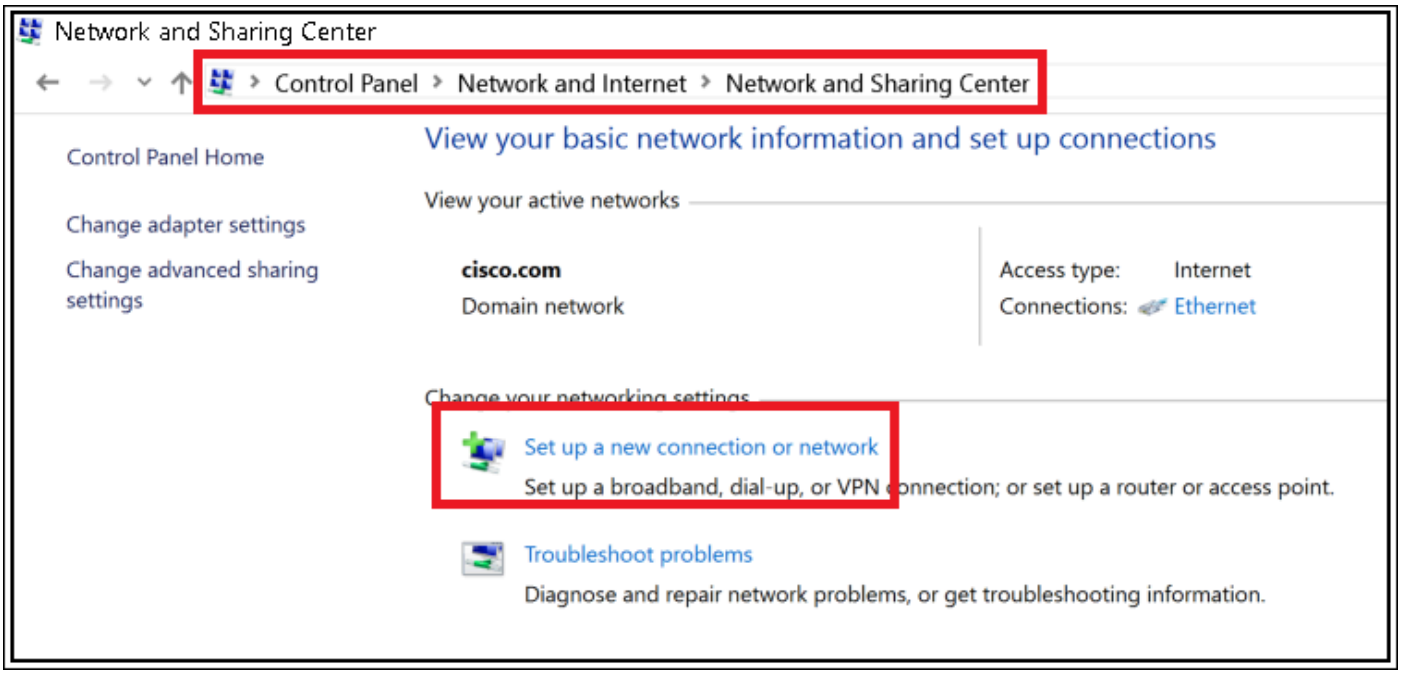
Por último, haga clic en Aceptar.



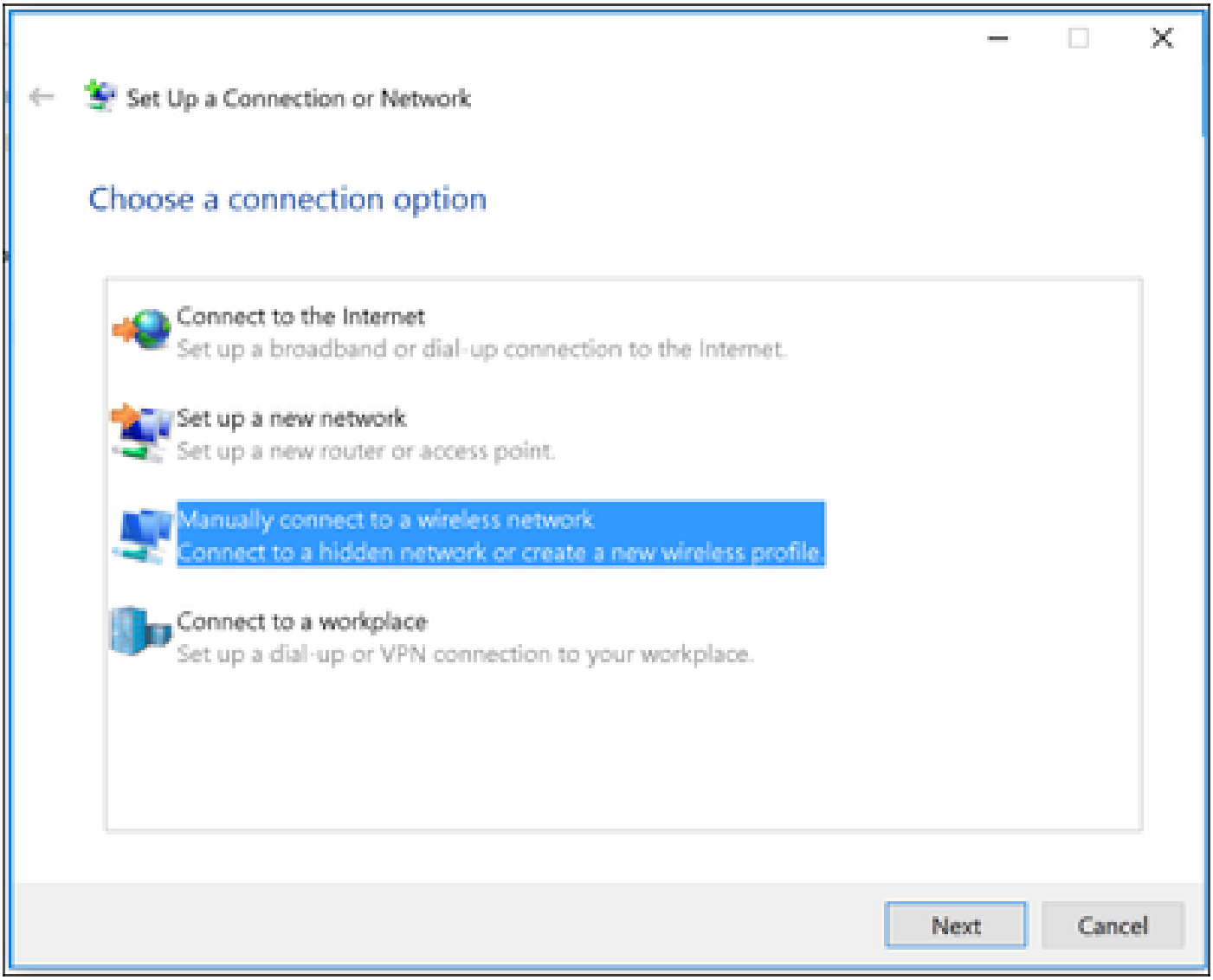
Configuración del dispositivo final: creación del perfil WLAN

Paso 1. Haga clic con el botón derecho en el icono Inicio y seleccione Panel de control.

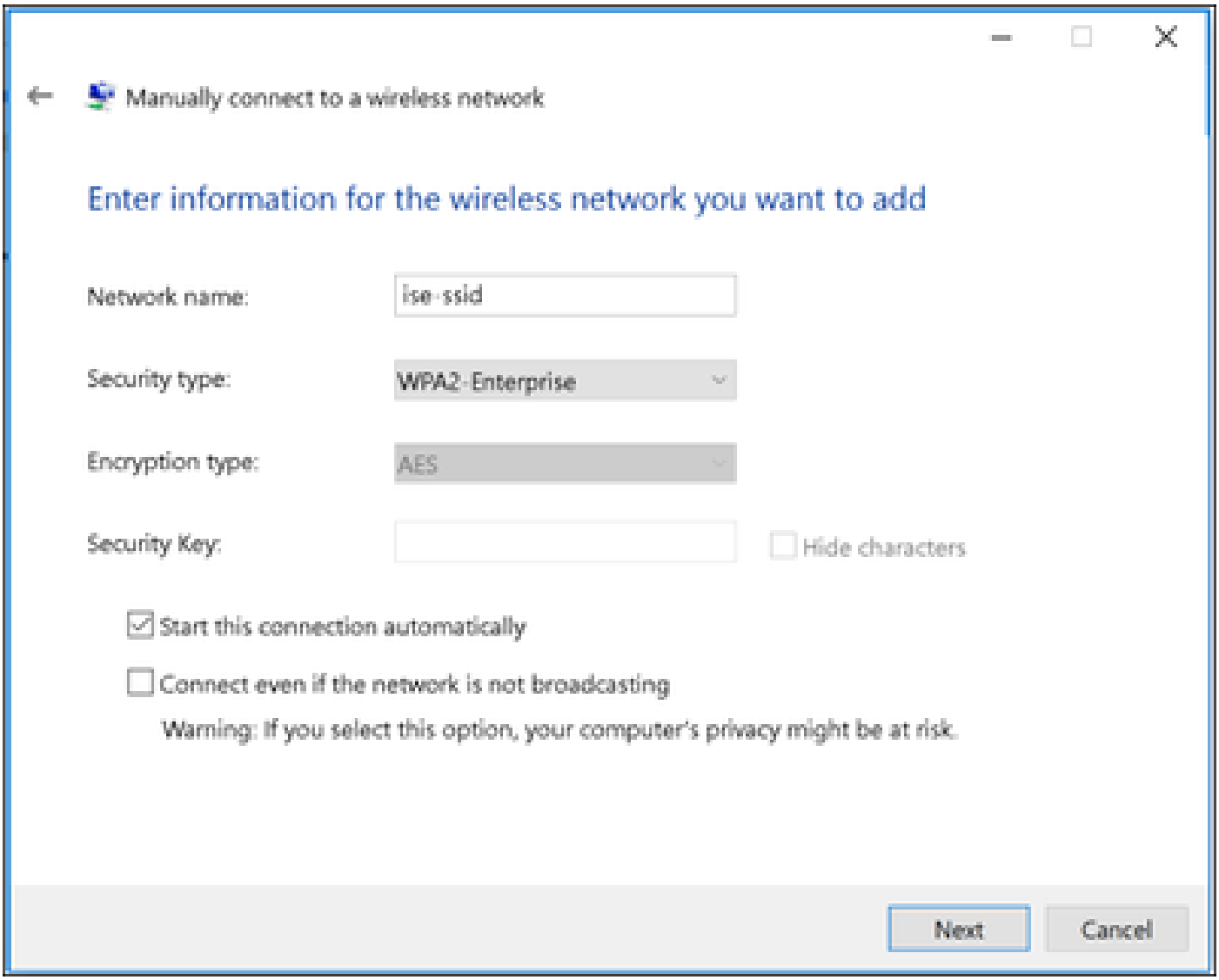

Programs and Features
Mobility Center
Power Options
Event Viewer
System
Device Manager
Network Connections
Disk Management
Computer Management
Command Prompt
Command Prompt (Admin)
Task Manager
Control Panel



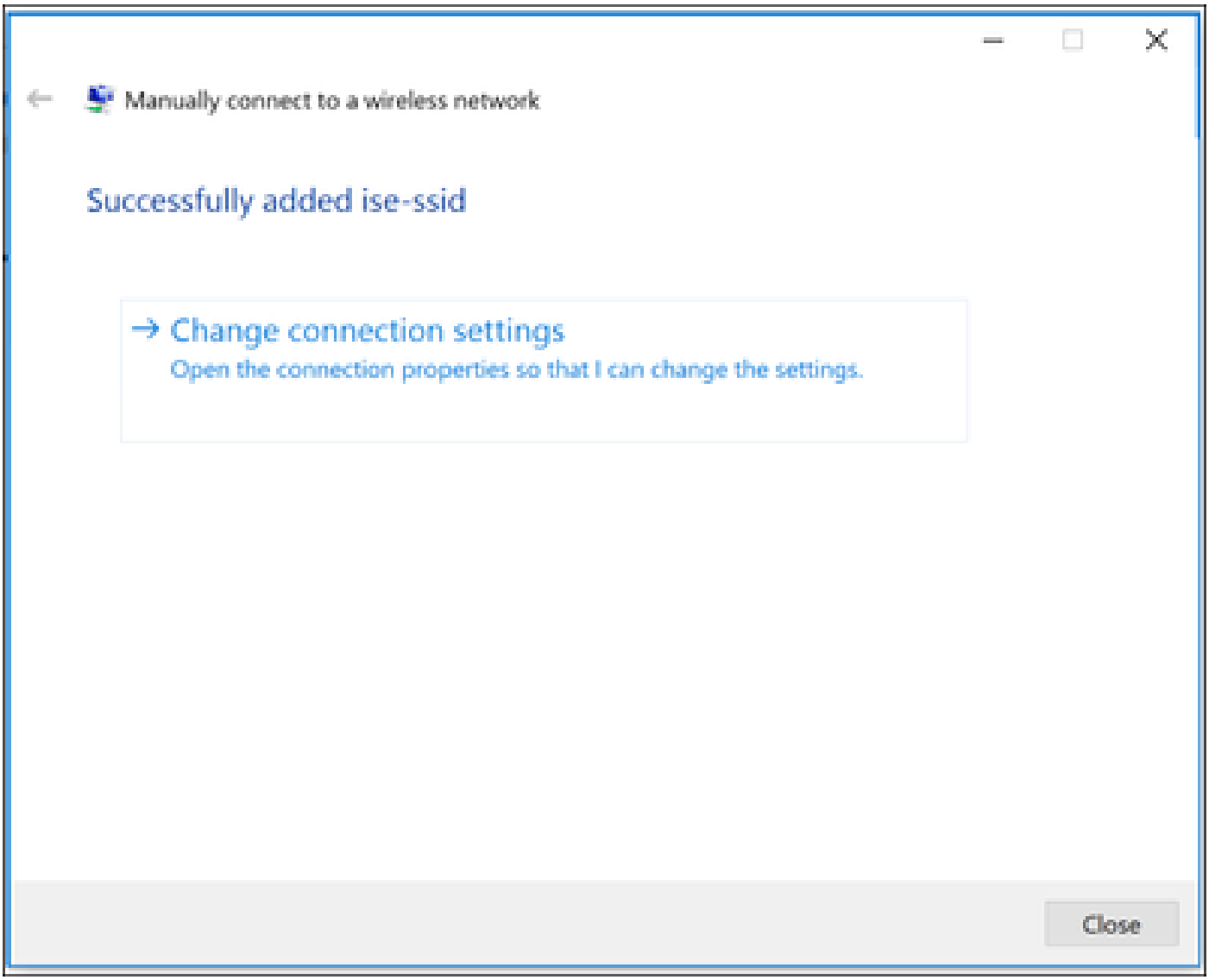
Paso 3. Seleccione Manually connect to a wireless network y haga clic en Next.



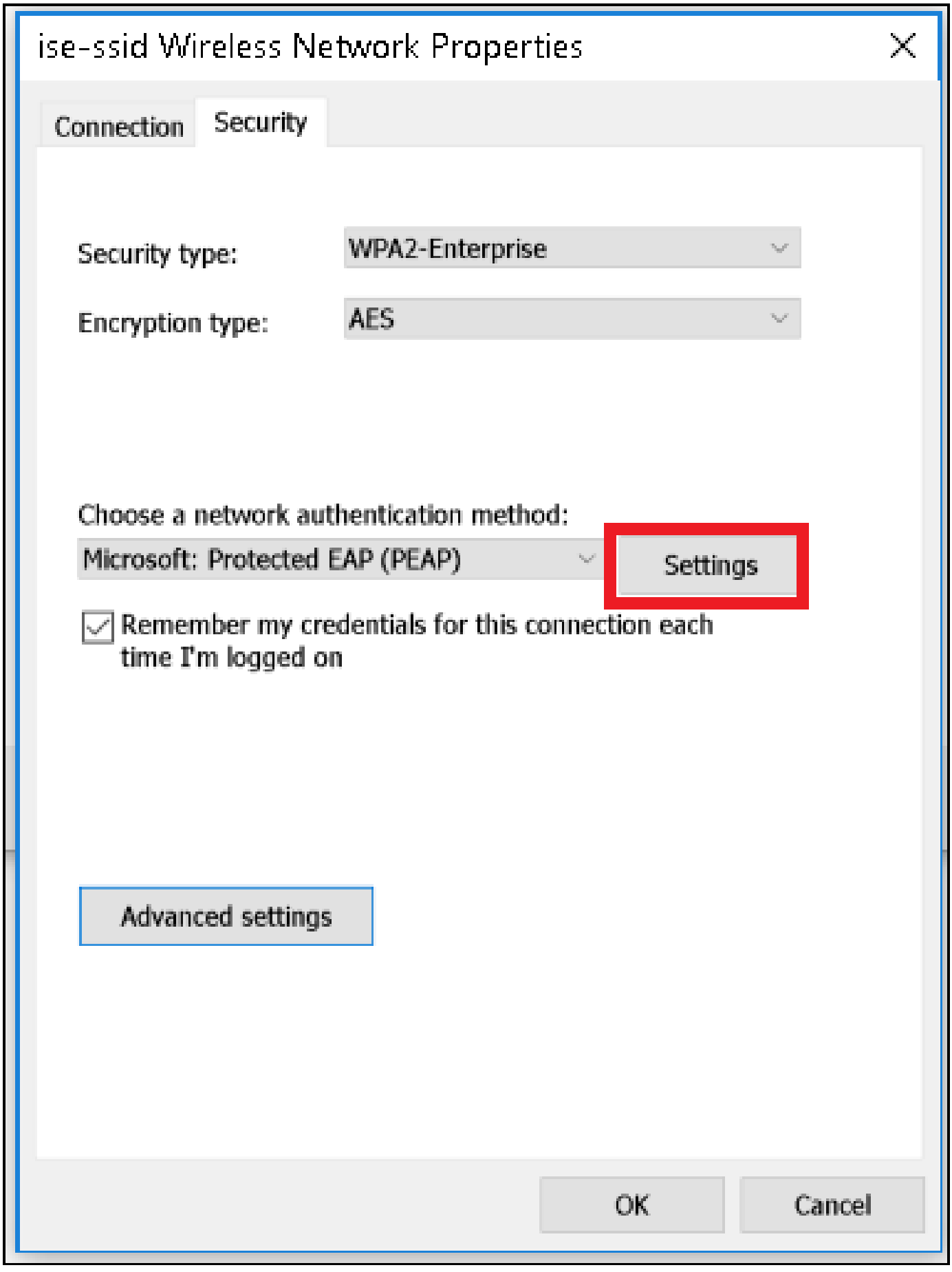
Paso 4. Introduzca la información con el nombre del SSID y el tipo de seguridad WPA2-Enterprise y haga clic en Siguiente.



Paso 5. Seleccione Change connection settings para personalizar la configuración del perfil WLAN.



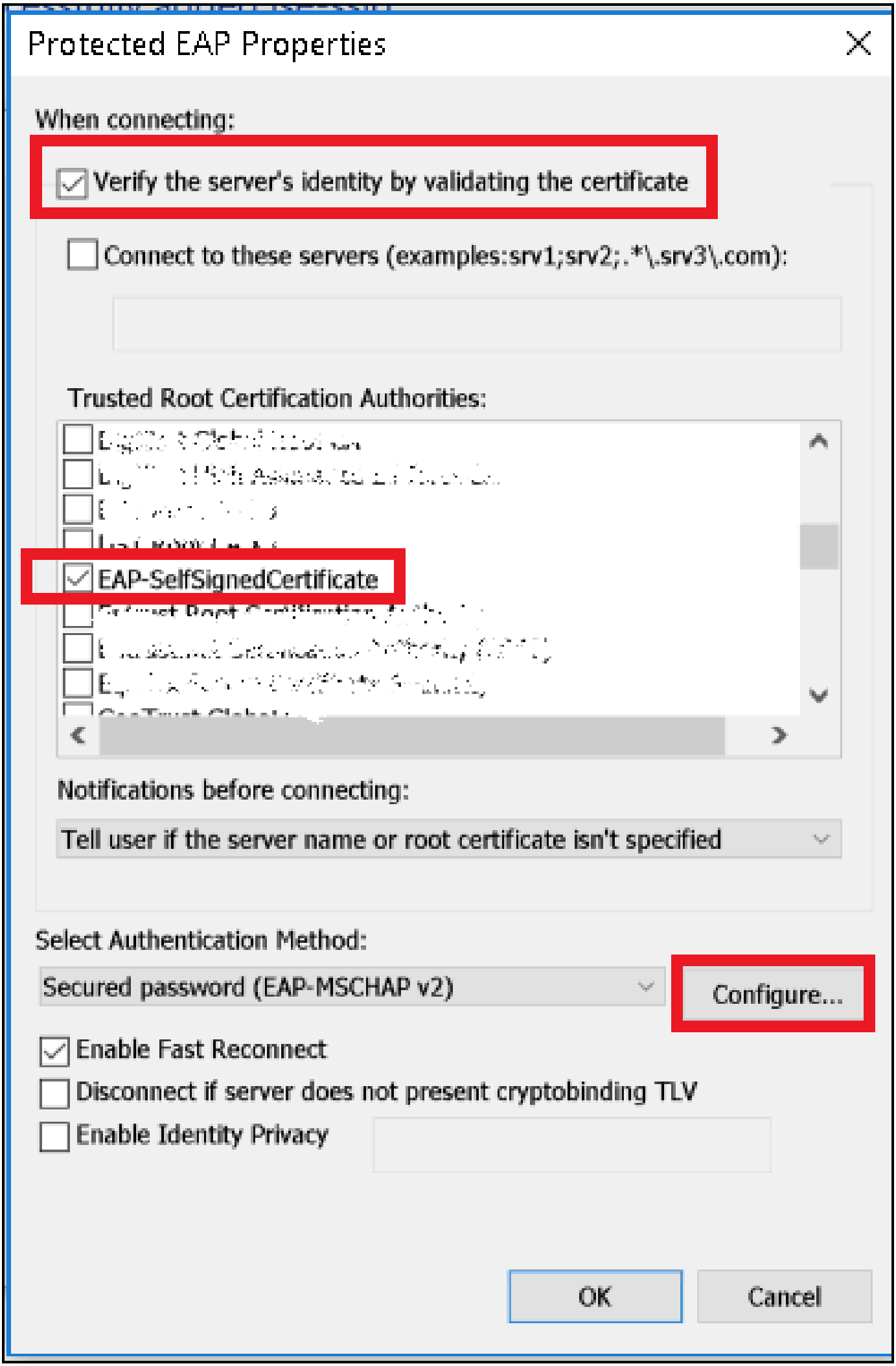
Paso 6. Navegue hasta la pestaña Seguridad y haga clic en Configuración.



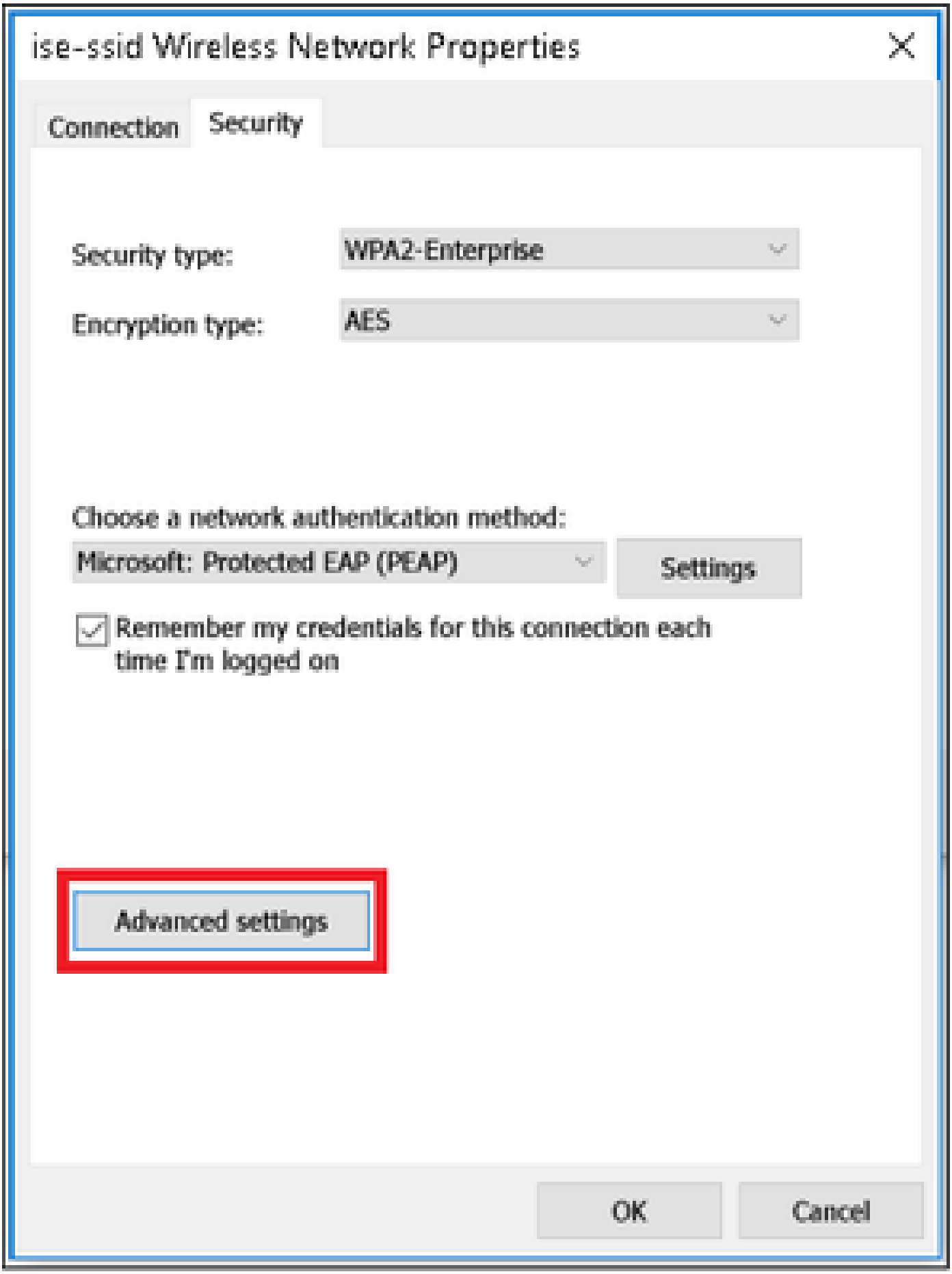
Paso 7. Seleccione si el servidor RADIUS está validado o no.

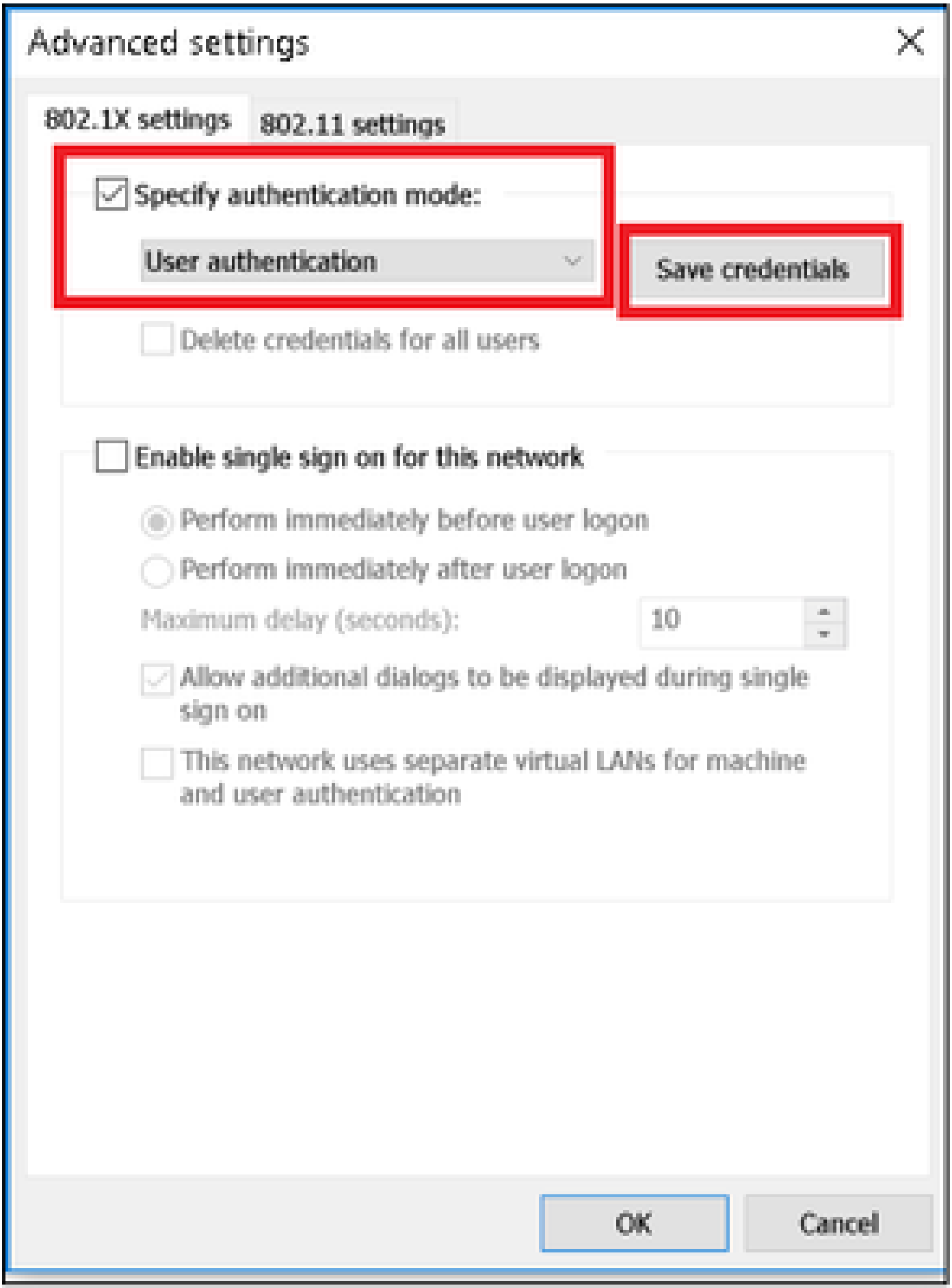
En caso afirmativo, active Verificar la identidad del servidor validando el certificado y en la lista Entidades de certificación raíz de confianza: seleccione el certificado autofirmado de ISE.

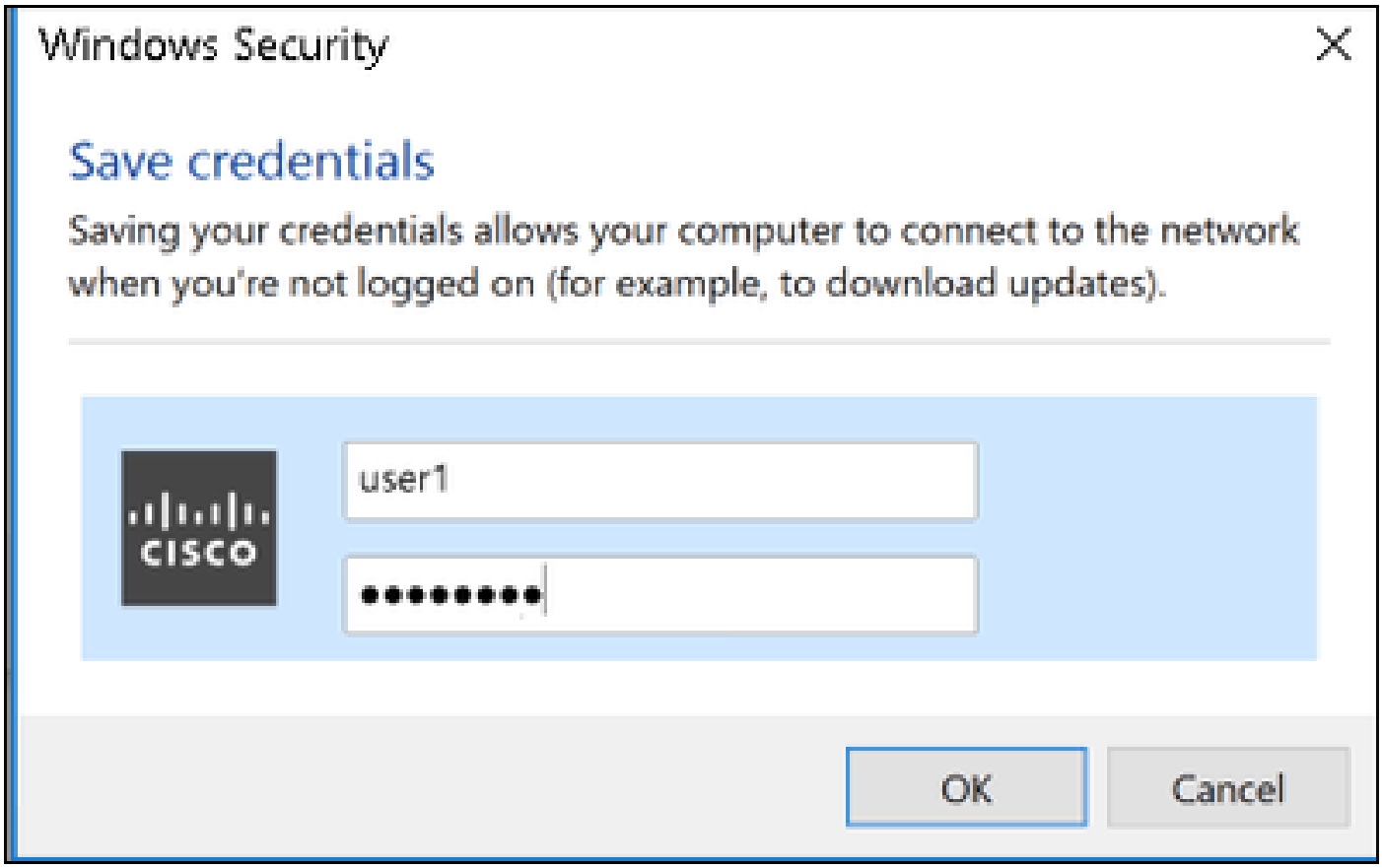
Después seleccione Configure y desactive Automatically use my Windows logon name and password..., y haga clic en OK.


Protected EAP Properties
When connecting:
Verify the server's identity by validating the certificate
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):
Trusted Root Certification Authorities:
EAP-SelfSignedCertificate
Notifications before connecting:
Tell user if the server name or root certificate isn't specified
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
Configure...
Enable Fast Reconnect
Disconnect if server does not present cryptobinding TLV
Enable Identity Privacy
OK
Cancel

Una vez en la pestaña Security, seleccione Advanced settings, especifique el modo de autenticación como User authentication y guarde las credenciales que se configuraron en ISE para autenticar al usuario.


ise-ssid Wireless Network Properties
Connection
Security
Security type:
WPA2-Enterprise
Encryption type:
AES
Choose a network authentication method:
Microsoft: Protected EAP (PEAP)
Settings
Remember my credentials for this connection each time I'm logged on
Advanced settings
OK
Cancel


Advanced settings
802.1X settings
802.11 settings
Specify authentication mode:
User authentication
Save credentials
Delete credentials for all users
Enable single sign on for this network
Perform immediately before user logon
Perform immediately after user logon
Maximum delay (seconds):
10
Allow additional dialogs to be displayed during single sign on
This network uses separate virtual LANs for machine and user authentication
OK
Cancel



Verificación

El flujo de autenticación se puede verificar desde la perspectiva de WLC o ISE.

Proceso de autenticación en ME

Ejecute este comando para monitorear el proceso de autenticación para un usuario específico:

```
> debug client <mac-add-client>
```

Ejemplo de una autenticación exitosa (se omitieron algunos resultados):

<#root>

```
*apfMsConnTask_0: Nov 25 16:36:24.333:
08:74:02:77:13:45 Processing assoc-req station:08:74:02:77:13:45 AP:38:ed:18:c6:7b:40-01 thread:669ba80

*apfMsConnTask_0: Nov 25 16:36:24.333: 08:74:02:77:13:45 Association received from mobile on BSSID 38:e
```

*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Applying site-specific Local Bridging override
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Applying Local Bridging Interface Policy for s
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Set Clinet Non AP specific apfMsAccessVlan = 2
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 This apfMsAccessVlan may be changed later from
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Received 802.11i 802.1X key management suite,
*apfMsConnTask_0: Nov 25 16:36:24.335:

08:74:02:77:13:45 0.0.0.0 START (0) Change state to AUTHCHECK (2) last state START (0)

*apfMsConnTask_0: Nov 25 16:36:24.335: 0

8:74:02:77:13:45 0.0.0.0 AUTHCHECK (2) Change state to 8021X_REQD (3) last state AUTHCHECK (2)

*apfMsConnTask_0: Nov 25 16:36:24.335:

08:74:02:77:13:45 0.0.0.0 8021X_REQD (3) DHCP required on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3for this

*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 apfPemAddUser2:session timeout forstation 08:7
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Stopping deletion of Mobile Station: (callerId
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Func: apfPemAddUser2, Ms Timeout = 0, Session
*apfMsConnTask_0: Nov 25 16:36:24.335: 0

8:74:02:77:13:45 Sending assoc-resp with status 0 station:08:74:02:77:13:45 AP:38:ed:18:c6:7b:40-01 on a

*apfMsConnTask_0: Nov 25 16:36:24.335:

08:74:02:77:13:45 Sending Assoc Response to station on BSSID 38:ed:18:c6:7b:4d (status 0) ApVapId 3 Slot

*spamApTask0: Nov 25 16:36:24.341: 08:74:02:77:13:45 Sent dot1x auth initiate message for mobile 08:74:
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 reauth_sm state transition 0 ---> 1 for mob
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 EAP-PARAM Debug - eap-params for Wlan-Id :3
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Disable re-auth, use PMK lifetime.
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Station 08:74:02:77:13:45 setting dot1x rea
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 dot1x - moving mobile 08:74:02:77:13:45 int
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342:

08:74:02:77:13:45 Sending EAP-Request/Identity to mobile 08:74:02:77:13:45 (EAP Id 1)

*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.401:

08:74:02:77:13:45 Received EAPOL EAPPKT from mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.401:

08:74:02:77:13:45 Received Identity Response (count=1) from mobile 08:74:02:77:13:45

.
.
.
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978:

08:74:02:77:13:45 Processing Access-Accept for mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978:

08:74:02:77:13:45 Username entry (user1) created in mscb for mobile, length = 253

```
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Station 08:74:02:77:13:45 setting dot1x rea
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Creating a PKC PMKID Cache entry for statio
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Adding BSSID 38:ed:18:c6:7b:4d to PMKID cac
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: New PMKID: (16)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] 80 3a 20 8c 8f c2 4c 18 7d 4c 28 e7 7f 10 11 03
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Adding Audit session ID payload in Mobility
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 0 PMK-update groupcast messages sent
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 PMK sent to mobility group
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Disabling re-auth since PMK lifetime can ta
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Sending EAP-Success to mobile 08:74:02:77:1
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Freeing AAACB from Dot1xCB as AAA auth is d
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Found an cache entry for BSSID 38:ed:18:c6:
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Found an cache entry for BSSID 38:ed:18:c6:
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: Including PMKID in M1 (16)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] 80 3a 20 8c 8f c2 4c 18 7d 4c 28 e7 7f 10 11 03
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: M1 - Key Data: (22)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] dd 14 00 0f ac 04 80 3a 20 8c 8f c2 4c 18 7d 4c
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0016] 28 e7 7f 10 11 03
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979:
```

08:74:02:77:13:45 Starting key exchange to mobile 08:74:02:77:13:45, data packets will be dropped

```
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980:
```

08:74:02:77:13:45 Sending EAPOL-Key Message to mobile 08:74:02:77:13:45

state INITPMK (message 1)

```
, replay counter 00.00.00.00.00.00.00.00
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Reusing allocated memory for EAP Pkt for re
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Entering Backend Auth Success state (id=70)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Received Auth Success while in Authenticati
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 dot1x - moving mobile 08:74:02:77:13:45 int
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received EAPOL-Key from mobile 08:74:02:77:
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983:
```

08:74:02:77:13:45 Received EAPOL-key in PTK_START state (message 2) from mobile 08:74:02:77:13:45

```
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Successfully computed PTK from PMK!!!
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received valid MIC in EAPOL Key Message M2!
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000000: 30 14 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00 0..
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000010: 00 0f ac 01 0c 00 ......
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000000: 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00 00 0f ...
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000010: ac 01 0c 00 ....
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 PMK: Sending cache add
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Stopping retransmission timer for mobile 08
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984:
```

08:74:02:77:13:45 Sending EAPOL-Key Message to mobile 08:74:02:77:13:45

state PTKINITNEGOTIATING (message 3),

```
replay counter 00.00.00.00.00.00.00.01
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Reusing allocated memory for EAP Pkt for re
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988:
```

08:74:02:77:13:45 Received EAPOL-key in PTKINITNEGOTIATING state (message 4) from mobile 08:74:02:77:13:

```
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Stopping retransmission timer for mobile 08
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988:
```

08:74:02:77:13:45 0.0.0.0 8021X_REQD (3) Change state to L2AUTHCOMPLETE (4) last state 8021X_REQD (3)

```
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Mobility query, PEM State: L2AUTHCOMPLETE
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building Mobile Announce :
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building Client Payload:
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Ip: 0.0.0.0
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Vlan Ip: 172.16.0.136, Vlan mask : 2
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Vap Security: 16384
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Virtual Ip: 192.0.2.1
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 ssid: ise-ssid
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building VlanIpPayload.
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) DHCP required on
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Not Using WMM Compliance code qosCap 00
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile LW
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988:
```

08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4)

```
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6623
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Adding Fast Path rule
 type = Airespace AP - Learn IP address
 on AP 38:ed:18:c6:7b:40, slot 1, interface = 1, QOS = 0
 IPv4 ACL ID = 255, IPv
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) mobility role update requ
 Peer = 0.0.0.0, Old Anchor = 0.0.0.0, New Anchor = 172.16.0.136
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) State Update from Mobility
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6261, Ad
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Replacing Fast Path rule
 type = Airespace AP - Learn IP address
 on AP 38:ed:18:c6:7b:40, slot 1, interface = 1, QOS = 0
 IPv4 ACL ID = 255,
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobi
*pemReceiveTask: Nov 25 16:36:25.990: 08:74:02:77:13:45 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0
*pemReceiveTask: Nov 25 16:36:25.990: 08:74:02:77:13:45 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 WcdbClientUpdate: IP Binding from WCDB ip_learn
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 IPv4 Addr: 0:0:0:0
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 In apfRegisterIpAddrOnMscb_debug: regType=1 Inva
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 IPv4 Addr: 0:0:0:0
*apfReceiveTask: Nov 25 16:36:27.840: 08:74:02:77:13:45 WcdbClientUpdate: IP Binding from WCDB ip_learn
*apfReceiveTask: Nov 25 16:36:27.841:
```

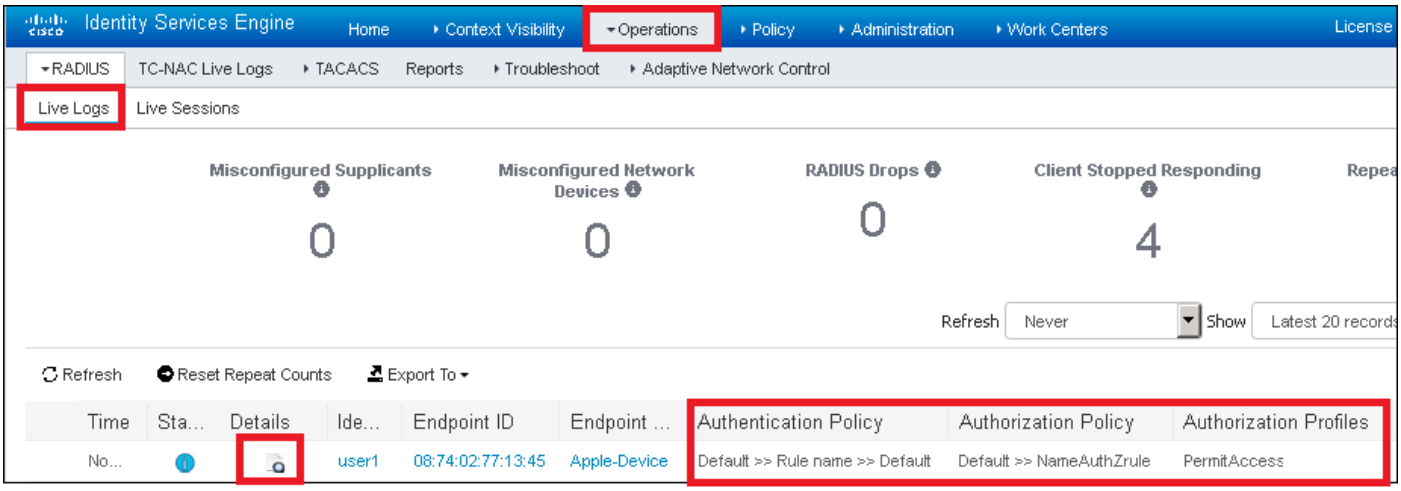
08:74:02:77:13:45 172.16.0.16 DHCP_REQD (7) Change state to RUN (20) last state DHCP_REQD (7)

Para una manera fácil de leer los resultados del cliente de depuración, utilice la herramienta Wireless debug analyzer:

[Analizador de depuración de errores inalámbrico]

Proceso de autenticación en ISE

Navegue hasta Operaciones > RADIUS > Live Logs para ver qué política de autenticación, política de autorización y perfil de autorización se asignaron al usuario.



Para obtener más información, haga clic en Details para ver un proceso de autenticación más detallado.

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).