

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

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configuración en ME](#)

[Declarar ME en ISE](#)

[Crear un nuevo usuario en ISE](#)

[Crear la regla de autenticación](#)

[Crear la regla de autorización](#)

[Configuración del dispositivo final](#)

[Verificación](#)

[Proceso de autenticación en ME](#)

[Proceso de autenticación en ISE](#)

Introducción

Este documento describe cómo configurar una WLAN (red de área local inalámbrica) con seguridad empresarial Wi-Fi Protected Access 2 (WPA2) 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) utilizado en esta guía es el protocolo de autenticación extensible protegido (PEAP). Además, el cliente se asigna a una VLAN específica (distinta de la asignada a la WLAN y a la predeterminada).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- 802.1x
- PEAP
- Autoridad 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

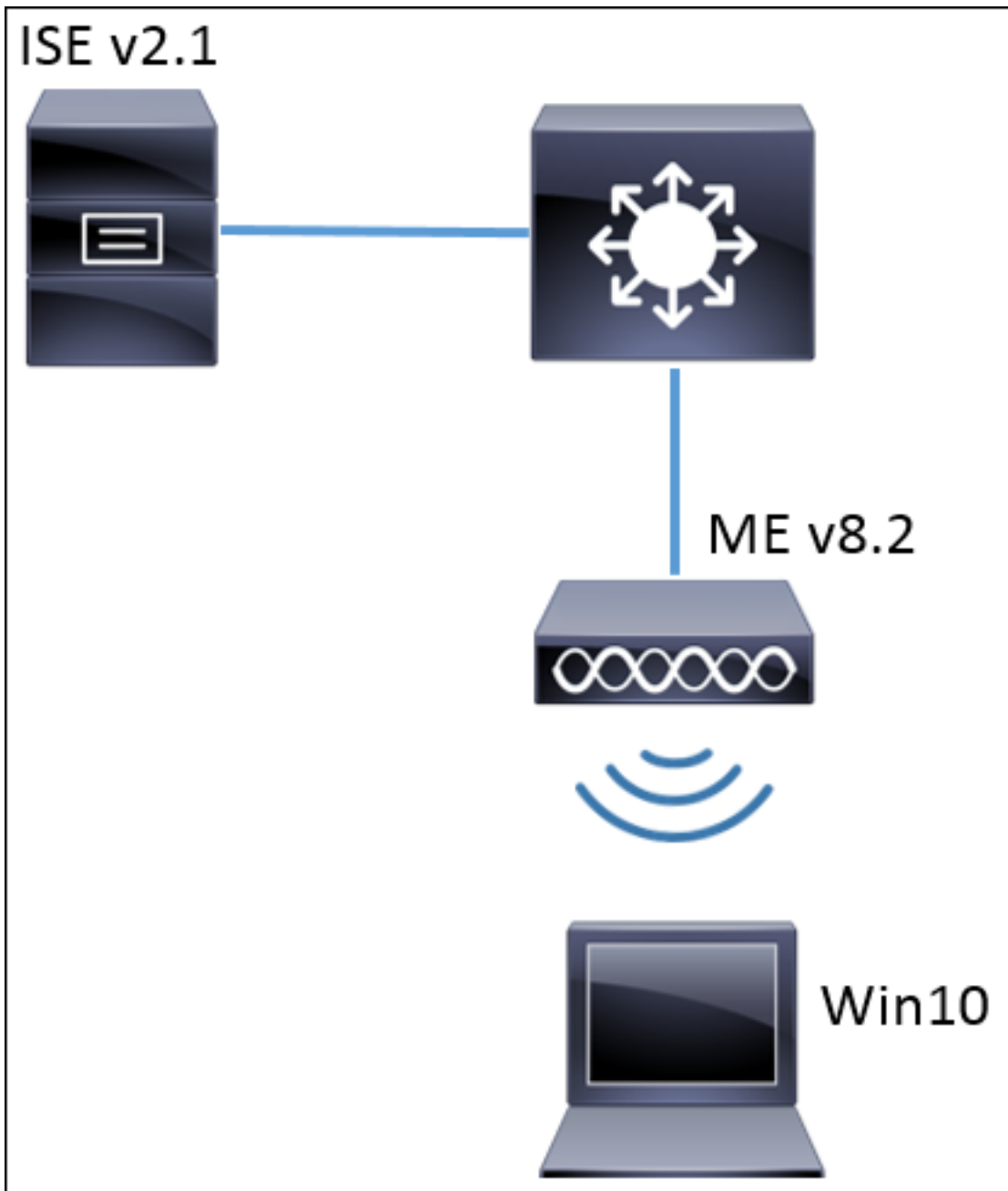
ISE v2.1

Portátil Windows 10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. 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 de 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. Configurar el 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 de ME y navegue hasta **Wireless Settings (Parámetros inalámbricos)** >

WLANs > Add new WLAN (WLAN > WLAN > Agregar nueva WLAN).

The screenshot displays the Cisco Aironet 1850 S management interface. On the left, a dark sidebar contains navigation options: 'Monitoring' (with a globe icon), 'Wireless Settings' (with a gear icon, highlighted in red), 'WLANs' (with a Wi-Fi icon, highlighted in red), 'Access Points' (with an antenna icon), 'WLAN Users' (with a group of people icon), 'Guest WLANs' (with a group of people icon), 'Management' (with a puzzle piece icon), and 'Advanced' (with a download icon). The main content area is titled 'WLAN CONFIGURATION' and features a large blue box with a white Wi-Fi icon, the text 'Active WLANs', and a large blue number '2'. At the bottom of the main content area, a button with a plus sign and the text '+ Add new WLAN' is highlighted in red.

Paso 2. Seleccione un nombre para la WLAN.

The image shows a configuration window titled "Add New WLAN" with a blue header and a close button (X) in the top right corner. Below the header are four tabs: "General", "WLAN Security", "VLAN & Firewall", and "QoS". The "General" tab is currently selected and underlined. The configuration area contains the following fields:

- WLAN Id**: A dropdown menu with the value "3".
- Profile Name ***: A text input field containing "me-ise".
- SSID ***: A text input field containing "me-ise".
- Admin State**: A dropdown menu with the value "Enabled".
- Radio Policy**: A dropdown menu with the value "ALL".

At the bottom right of the window, there are two buttons: "Apply" (with a checkmark icon) and "Cancel" (with an X icon).

Paso 3. Especifique la configuración de seguridad en la pestaña **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 de RADIUS y elegir una clave **secreta compartida**.



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

Add New WLAN

General WLAN Security VLAN & Firewall QoS

Security WPA2 Enterprise

Authentication Server External Radius

Radius IP ▲ Radius Port Shared Secret

a.b.c.d 1812

Please enter valid IPv4 address

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 (que no sea la VLAN de AP), habilite **Use VLAN Tagging** y asigne el **ID de VLAN** deseado.

Add New WLAN

General WLAN Security **VLAN & Firewall** QoS

Use VLAN Tagging Yes

VLAN ID * 2400

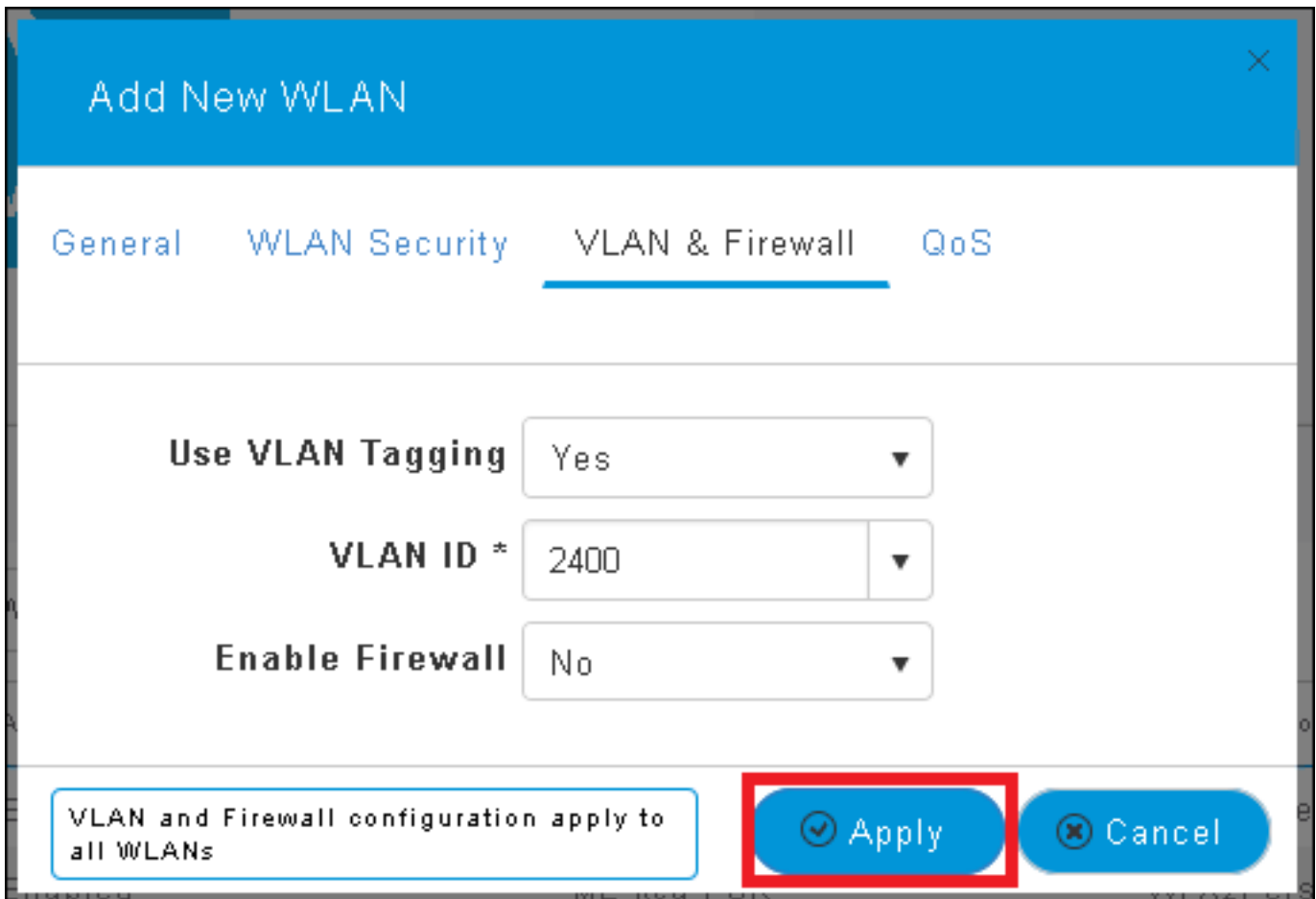
Enable Firewall No

VLAN and Firewall configuration apply to all WLANs

Apply Cancel

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

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



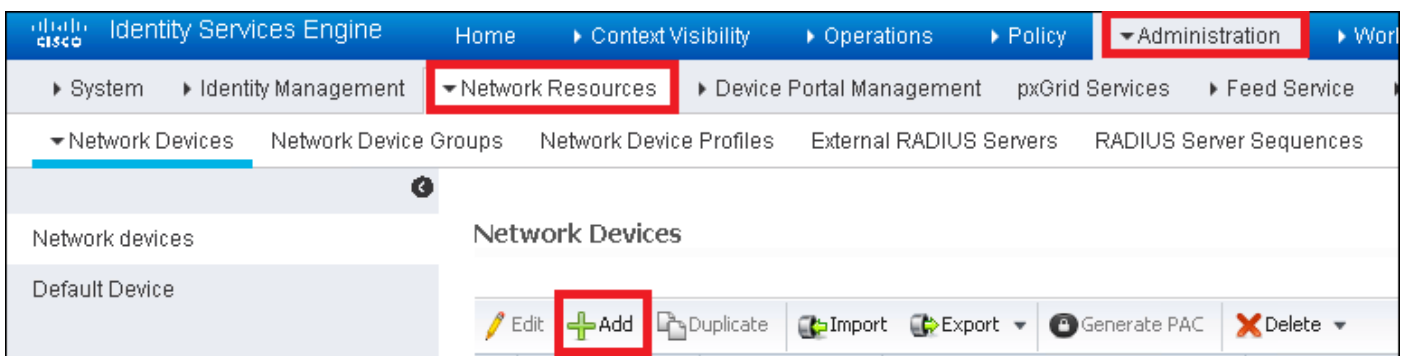
Paso 6. Opcional, configure la WLAN para aceptar la invalidación de VLAN.

Habilite la anulación de AAA en la WLAN y agregue las VLAN necesarias. Para ello, deberá abrir una sesión CLI a 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>
```

Declarar ME en ISE

Paso 1. Abra la consola ISE y navegue hasta **Administration > Network Resources > Network Devices > Add**.



Paso 2. Introduzca la información.

Opcionalmente se puede especificar un nombre de modelo, una versión de software, una

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 de ME.

Network Devices List > **New Network Device**

Network Devices

* Name

Description

* IP Address: /

* Device Profile

Model Name

Software Version

* Network Device Group

Device Type

Location

WLCs

RADIUS Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

* Shared Secret

Enable KeyWrap

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

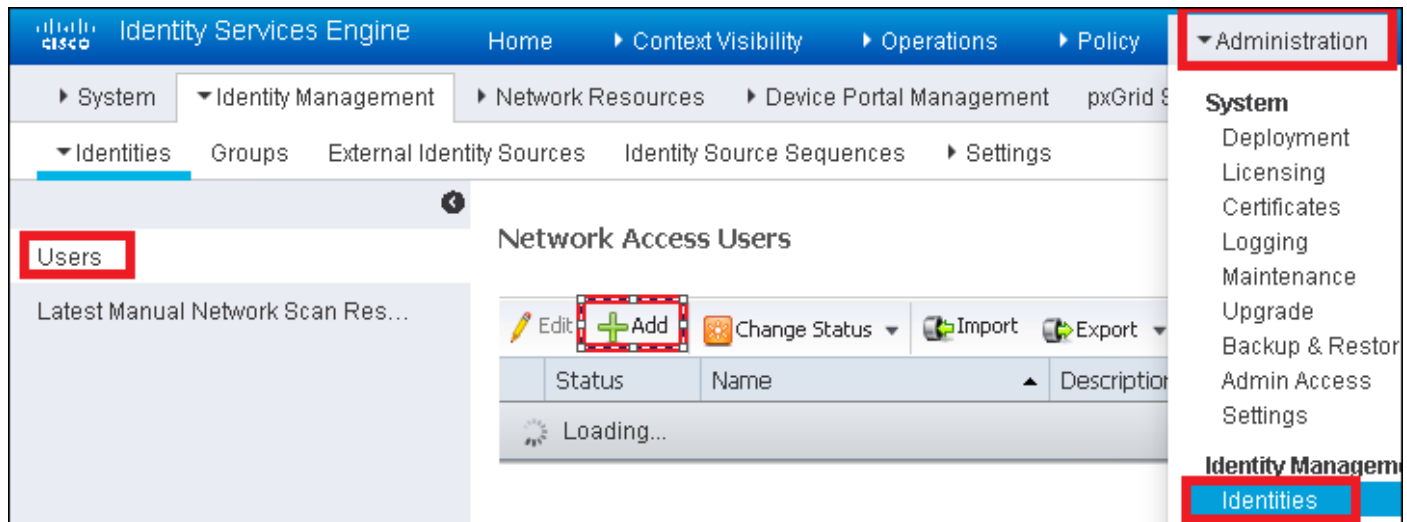
CoA Port

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

[ISE - Grupos de dispositivos de red](#)

Crear un nuevo usuario en ISE

Paso 1. Vaya a **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 User**

* Name

Status Enabled ▼

Email

▼ **Passwords**

Password Type: ▼

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

▼ **User Groups**

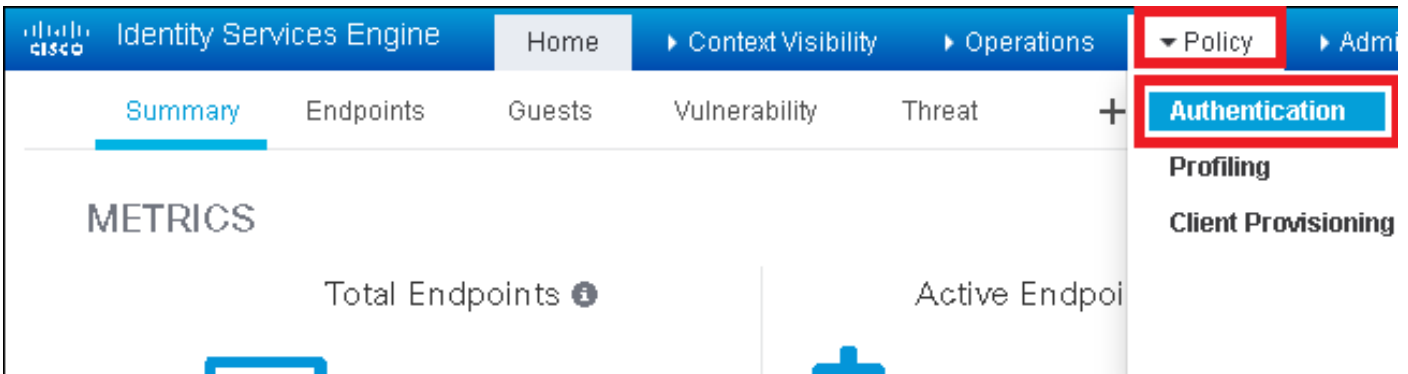


Crear la regla de autenticación

Las reglas de autenticación se utilizan para verificar si las credenciales de los usuarios son correctas (verifique si el usuario es realmente quien dice ser) y limitar los métodos de

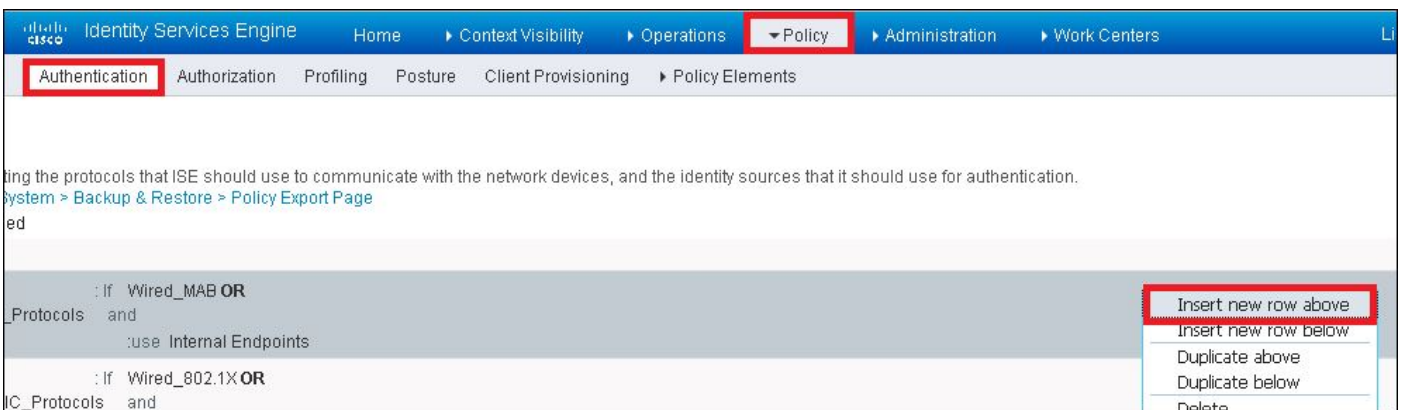
autenticación que puede utilizar.

Paso 1. Navegar a **Política > Autenticación**.



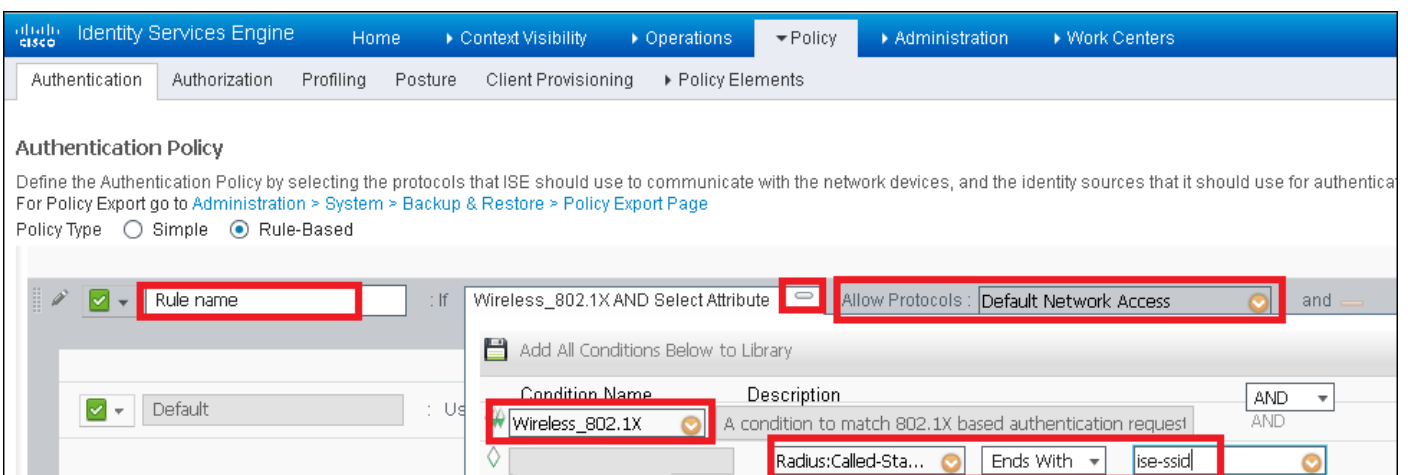
Paso 2. Inserte una nueva regla de autenticación.

Para hacerlo, navegue hasta **Política > Autenticación > Insertar nueva fila arriba/abajo**.

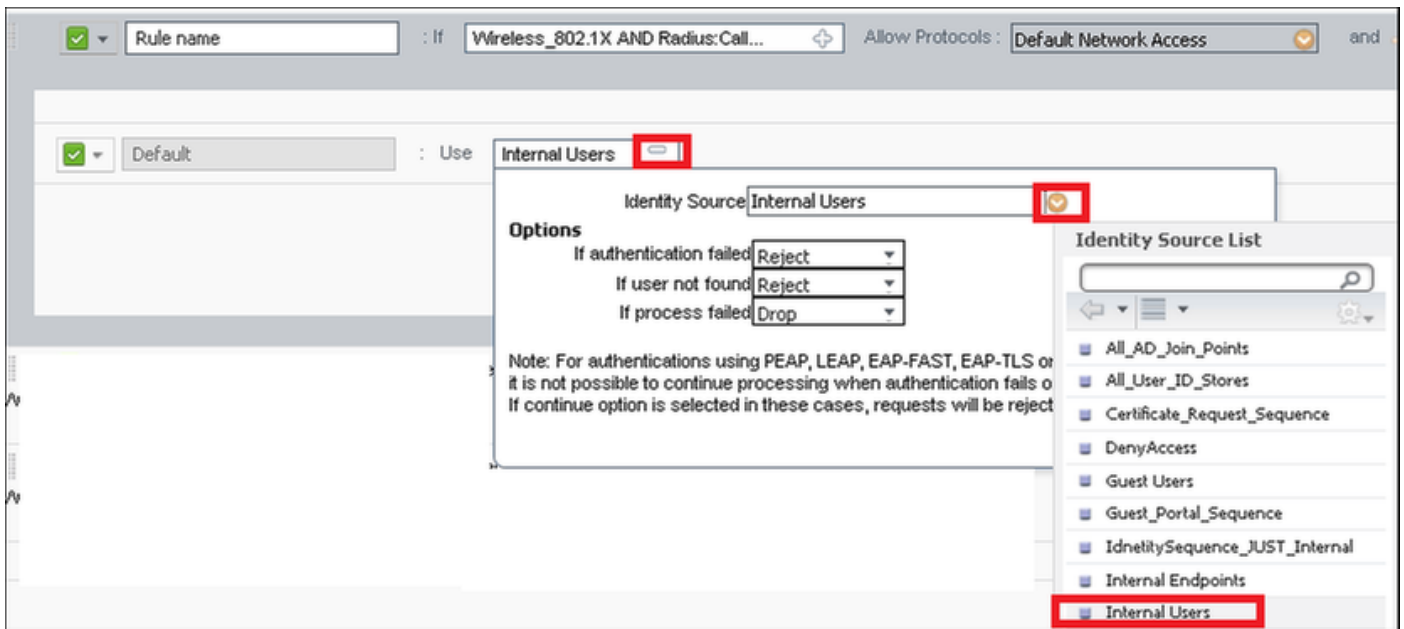


Paso 3. Introduzca la información necesaria

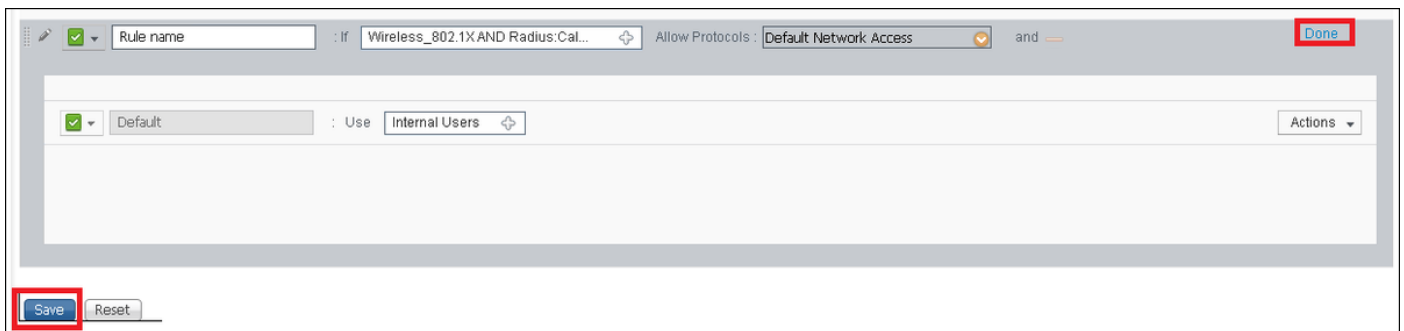
Este ejemplo de regla de autenticación permite todos los protocolos enumerados en la lista **Acceso de red predeterminado**, esto se aplica a la solicitud de autenticación para clientes Wireless 802.1x y con Called-Station-ID y termina con *ise-ssid*.



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



Quando haya terminado, haga clic en **Finalizado** y **Guardar**



Para obtener más información sobre las políticas de permisos de protocolos, consulte este enlace:

[Servicio de protocolos permitidos](#)

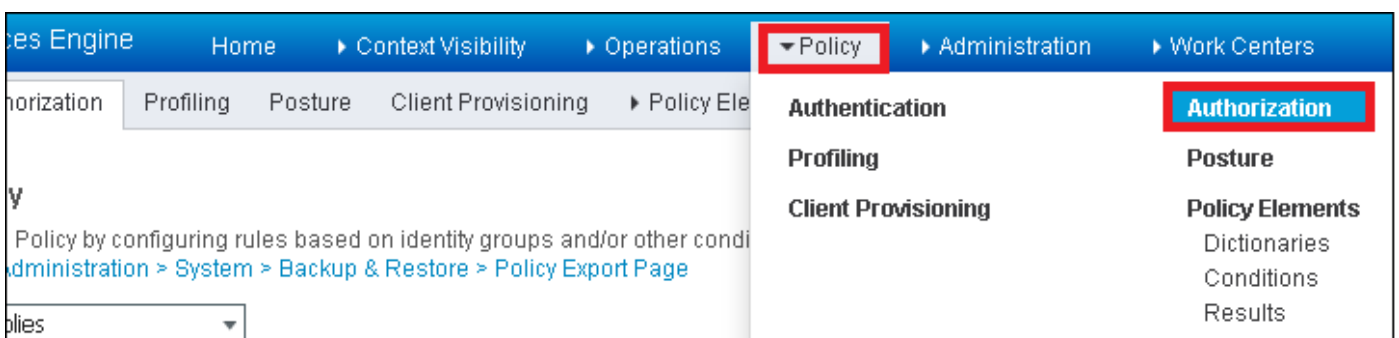
Para obtener más información sobre las fuentes de identidad, consulte este enlace:

[Crear un grupo de identidad de usuario](#)

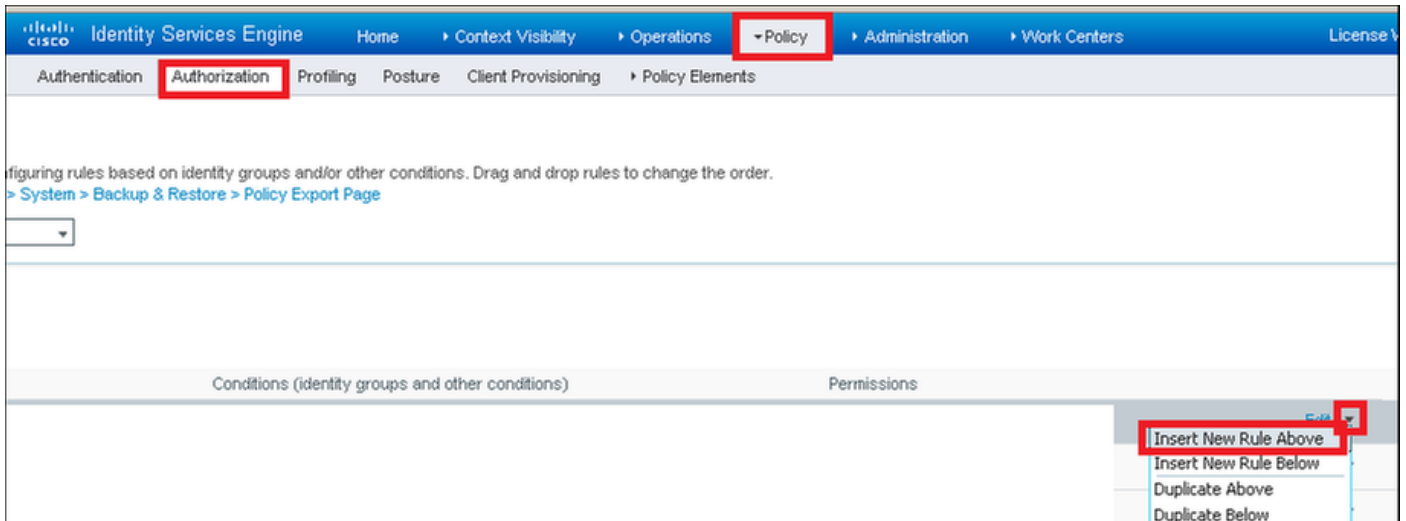
Crear la regla de autorización

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

Paso 1. Vaya a **Política > Autorización**.

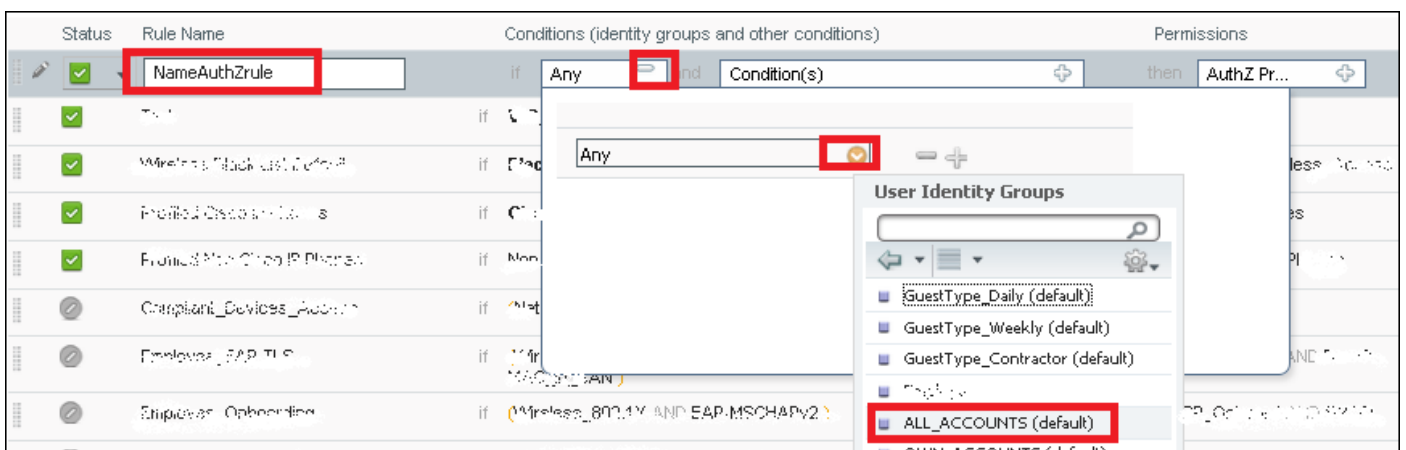


Paso 2. Inserte una nueva regla. Vaya a **Política > Autorización > Insertar Nueva Regla Arriba/Abajo**.

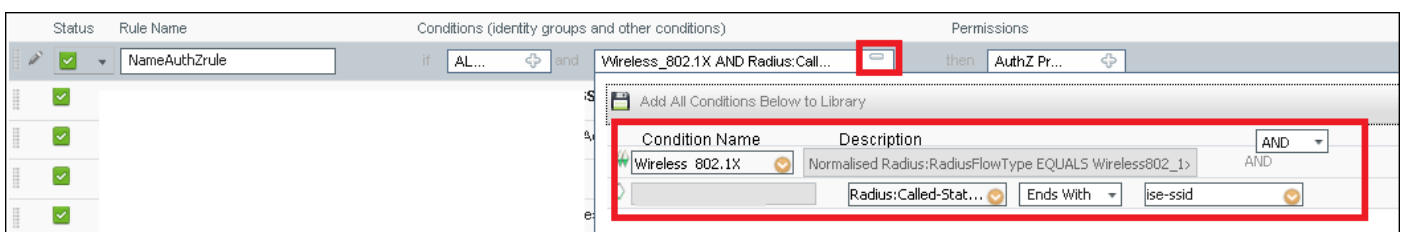


Paso 3. Introduzca la información.

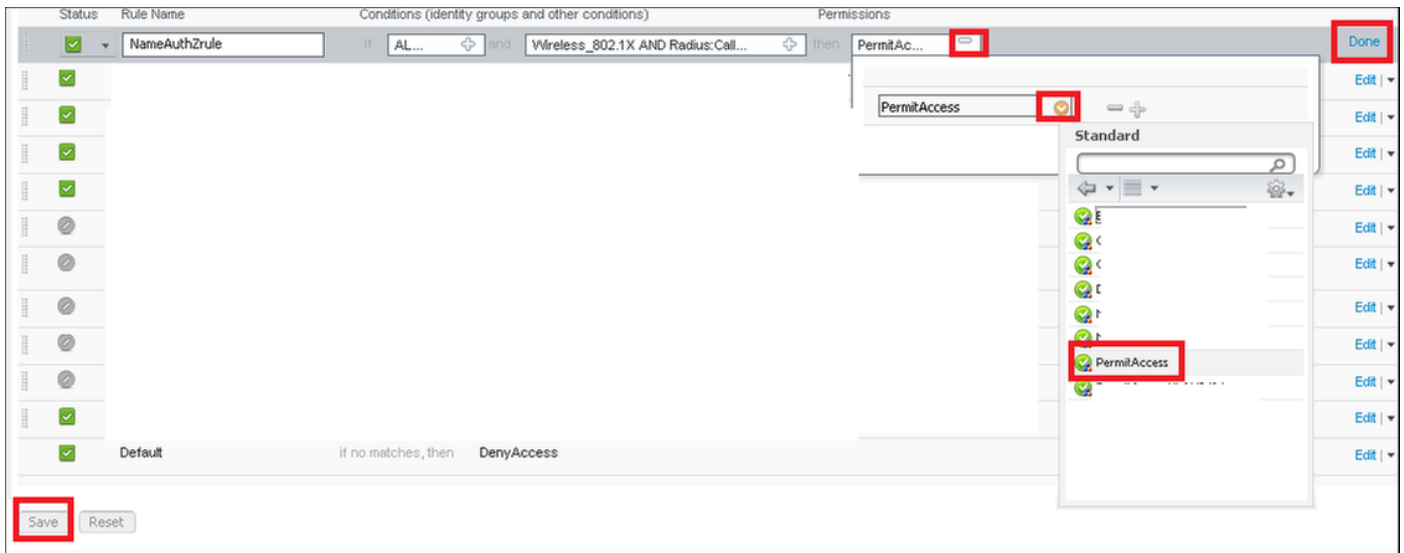
Primero elija un nombre para la regla y los grupos de identidad donde se almacena el usuario. En este ejemplo, el usuario se almacena en el grupo **ALL_ACCOUNTS**.



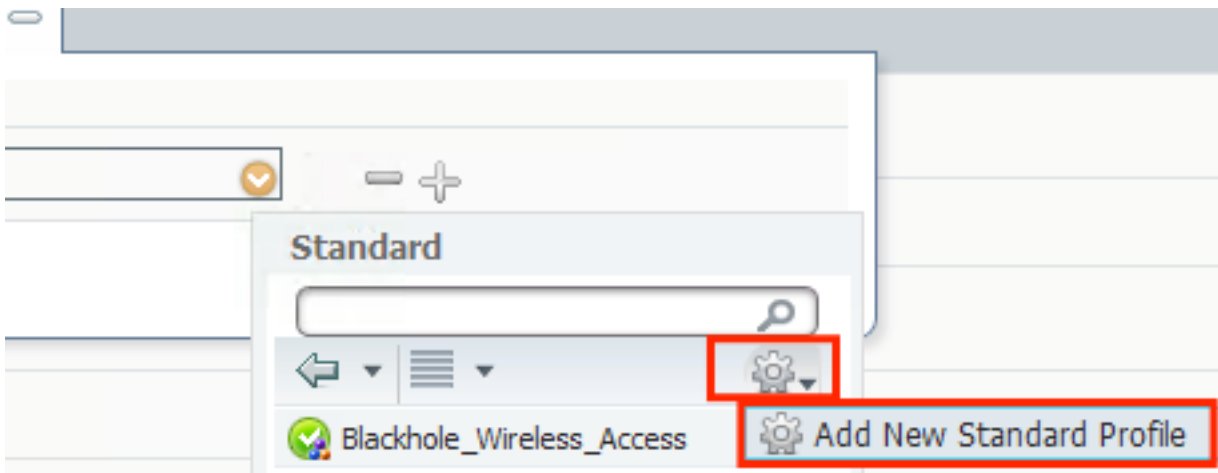
Después de eso, elija otras condiciones que hacen que el proceso de autorización caiga en esta regla. En este ejemplo, el proceso de autorización llega a esta regla si utiliza 802.1x Wireless y se denomina ID de estación termina con **ise-ssid**.



Finalmente elija el perfil de autorización que permite a los clientes unirse a la red, haga clic en **Finalizado** y **Guardar**.



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



Introduzca la información:

Add New Standard Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

DAACL Name

ACL (Filter-ID)

VLAN Tag ID IDName

Voice Domain Permission

Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:vlan-id
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6

Configuración del dispositivo final

Configure un portátil 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 el equipo 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 recomendado, ya que puede convertirse en un problema de seguridad)

La configuración para 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 de 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**.

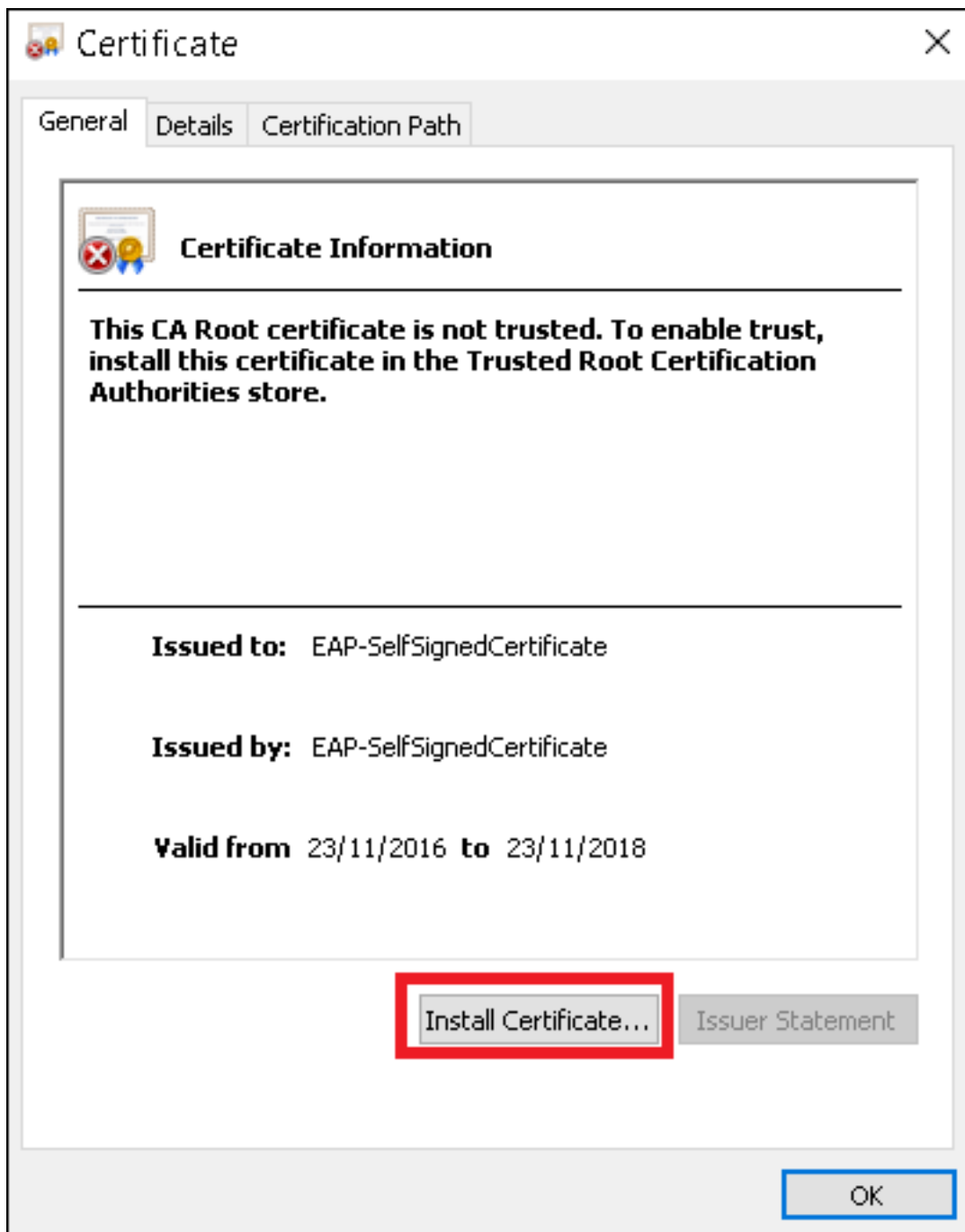
The screenshot shows the Cisco Identity Services Engine Administration interface. The top navigation bar includes 'Administration' and 'Work'. The left sidebar shows 'System' and 'Certificates' under 'Certificate Management'. The main content area displays 'System Certificates' with a warning icon and a note: 'For disaster recovery it is recommended to export certificate ar...'. Below this are buttons for 'Edit', 'Generate Self Signed Certificate', 'Import', 'Export', and 'Delete'. The 'Export' button is highlighted in red. A table below shows a list of certificates, with one certificate selected (checkbox checked) and its 'EAP Authentication' label highlighted in red.

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

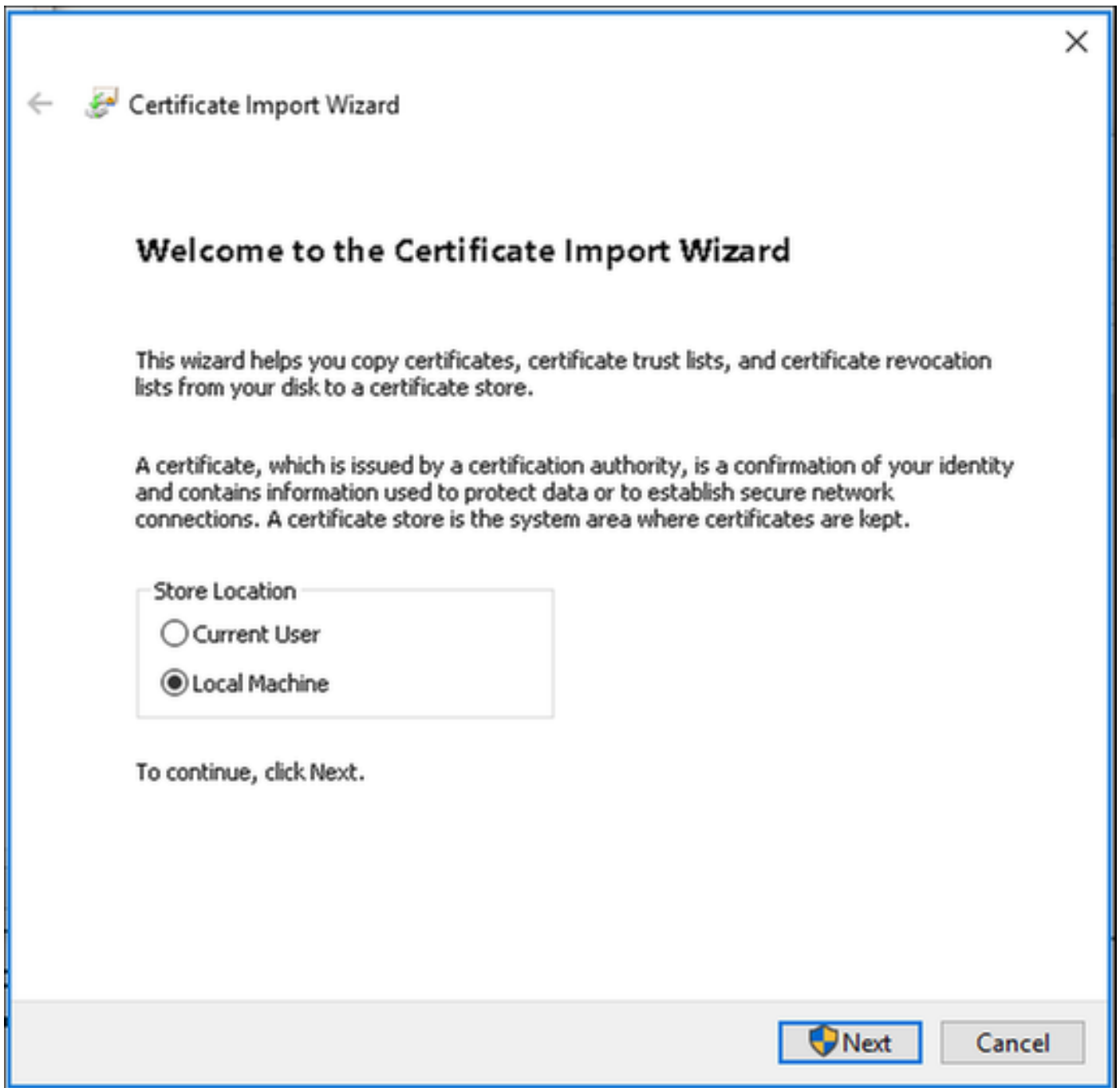
The screenshot shows a dialog box titled 'Export Certificate 'EAP-SelfSignedCertificate#EAP-SelfSignedCertificate#00001''. It contains two radio buttons: 'Export Certificate Only' (selected and highlighted in red) and 'Export Certificate and Private Key'. Below the radio buttons are two input fields: '*Private Key Password' and '*Confirm Password'. A warning message is displayed: 'Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private key.' At the bottom right, there are 'Export' and 'Cancel' buttons, with the 'Export' button highlighted in red.

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

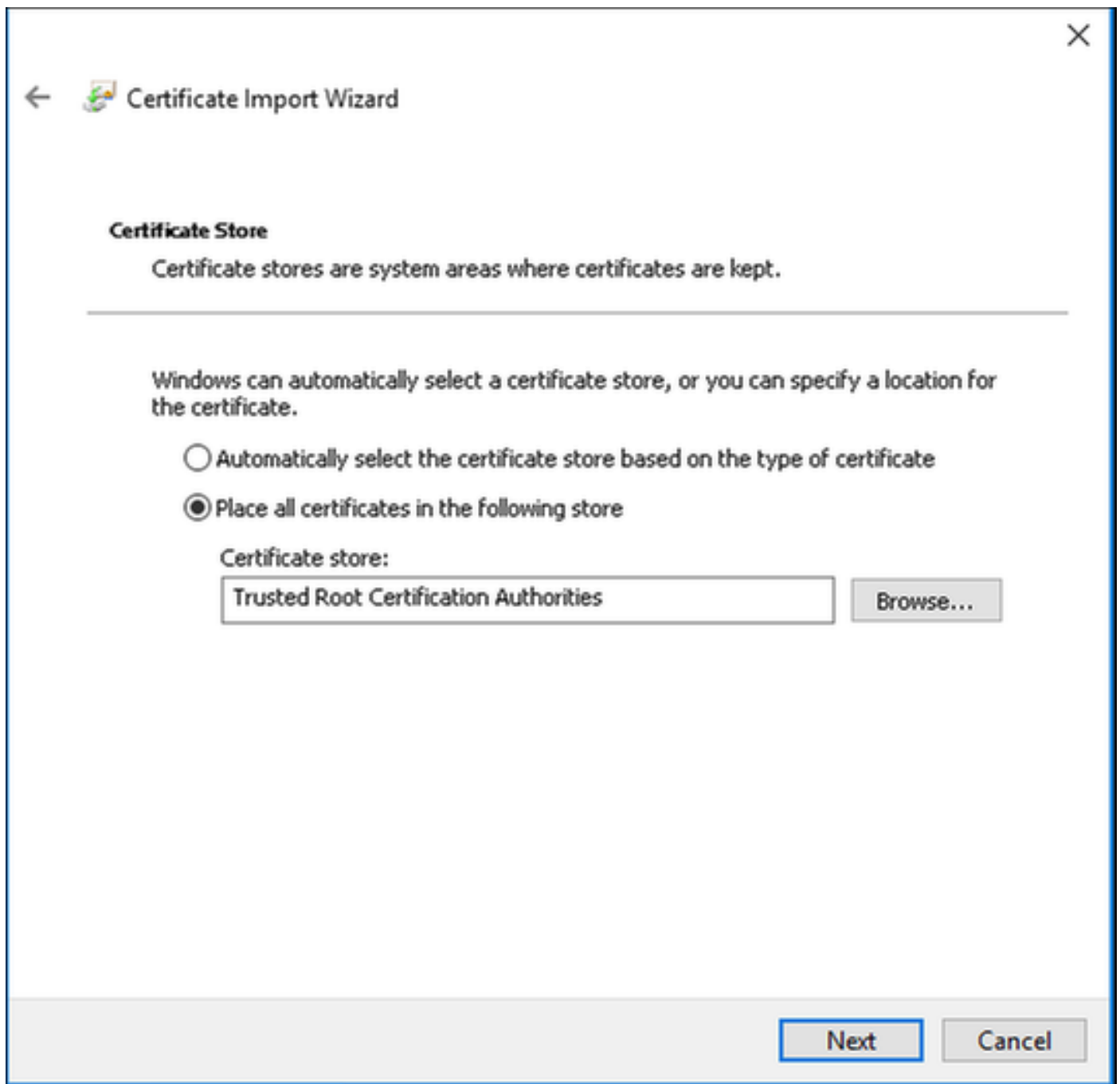
Copie el certificado exportado antes en el equipo de Windows, cambie la extensión del archivo de .pem a .crt, después de hacer doble clic en él y seleccione **Instalar certificado...**



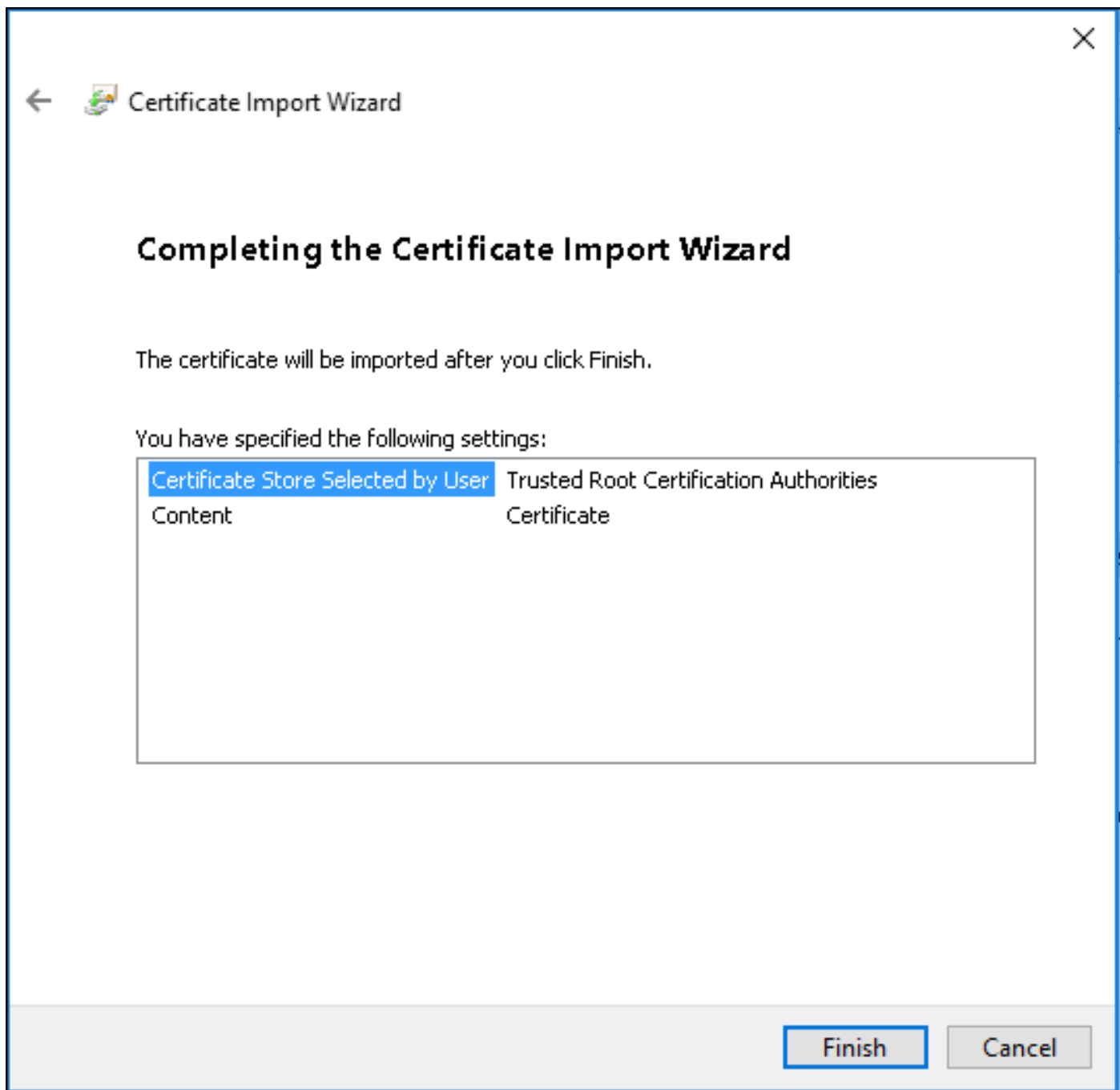
Elija instalarlo en **Local Machine** y luego haga clic en **Next**.



Seleccione **Colocar todos los certificados en el siguiente almacén** y, a continuación, busque y elija **Autoridades de certificación raíz de confianza**. Después de eso, haga clic en **Next**.



A continuación, haga clic en **Finalizar**.



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

Security Warning



You are about to install a certificate from a certification authority (CA) claiming to represent:

EAP-SelfSignedCertificate

Windows cannot validate that the certificate is actually from "EAP-SelfSignedCertificate". You should confirm its origin by contacting "EAP-SelfSignedCertificate". The following number will assist you in this process:

Thumbprint (sha1): 011A193D 70C7713D 0204E3D0 4759215D
4294213C

Warning:

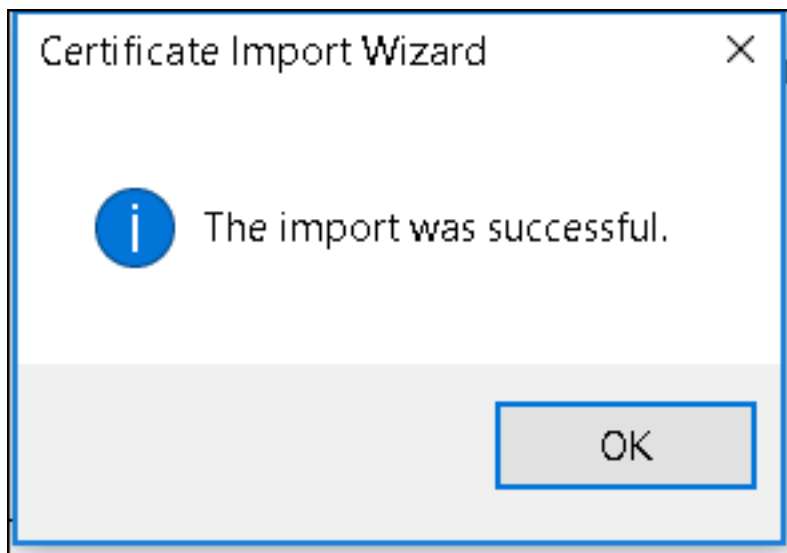
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Yes

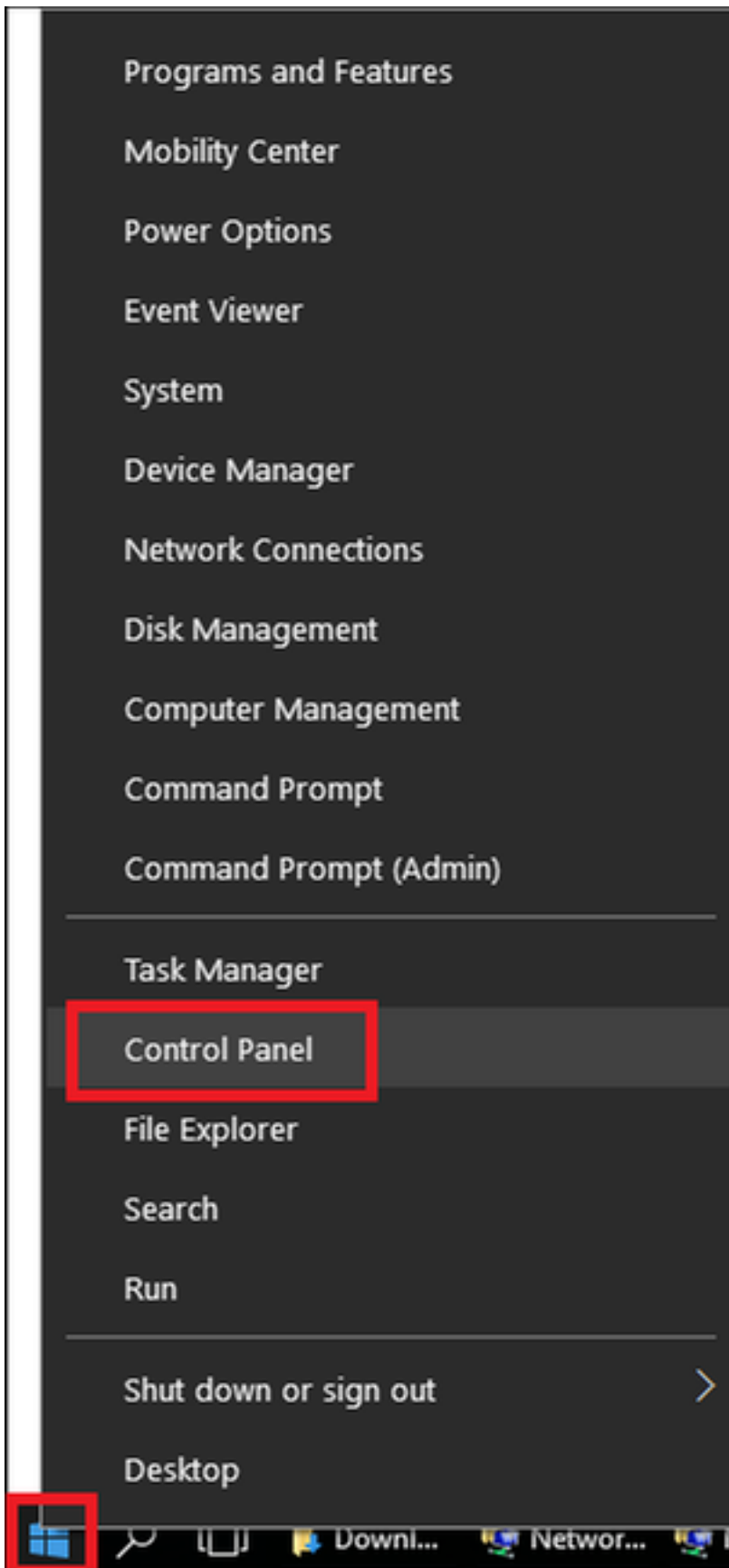
No

Por último, haga clic en **Aceptar**.

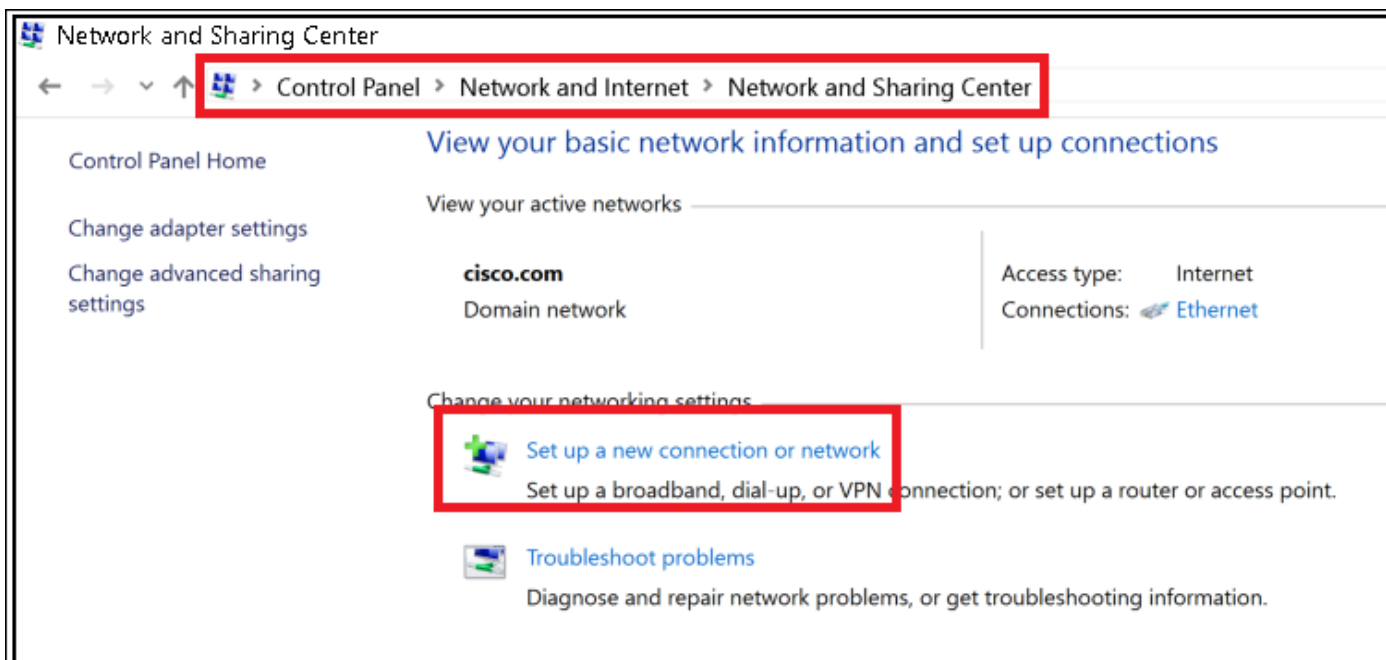


Configuración del dispositivo final: creación del perfil WLAN

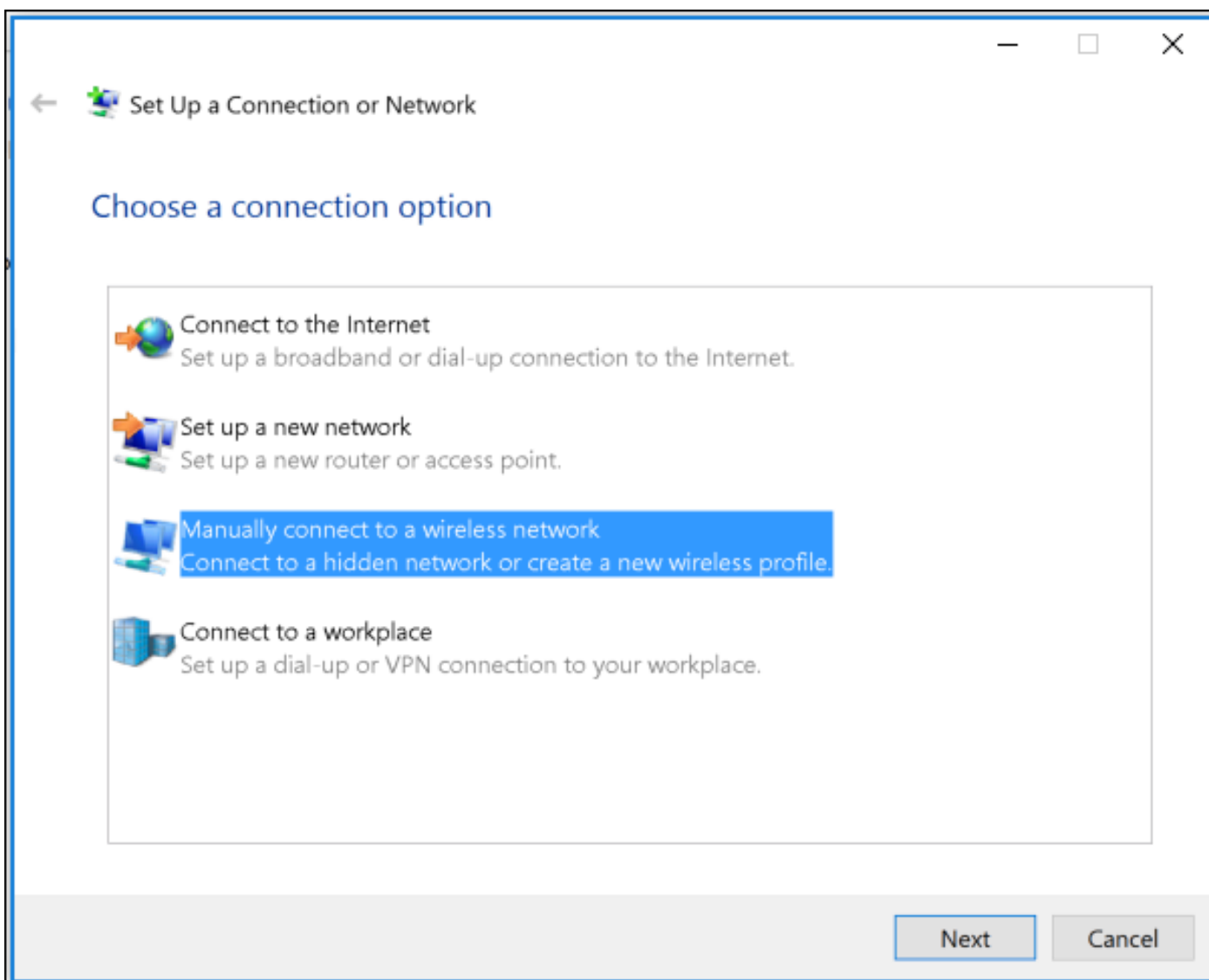
Paso 1. Haga clic con el botón derecho del ratón en el icono **Inicio** y seleccione **Panel de control**.



Paso 2. Navegue hasta Red e Internet y luego Centro de Red y Uso Compartido y haga clic en Configurar una nueva conexión o red.



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**.

← Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name:

Security type:

Encryption type:

Security Key: Hide characters

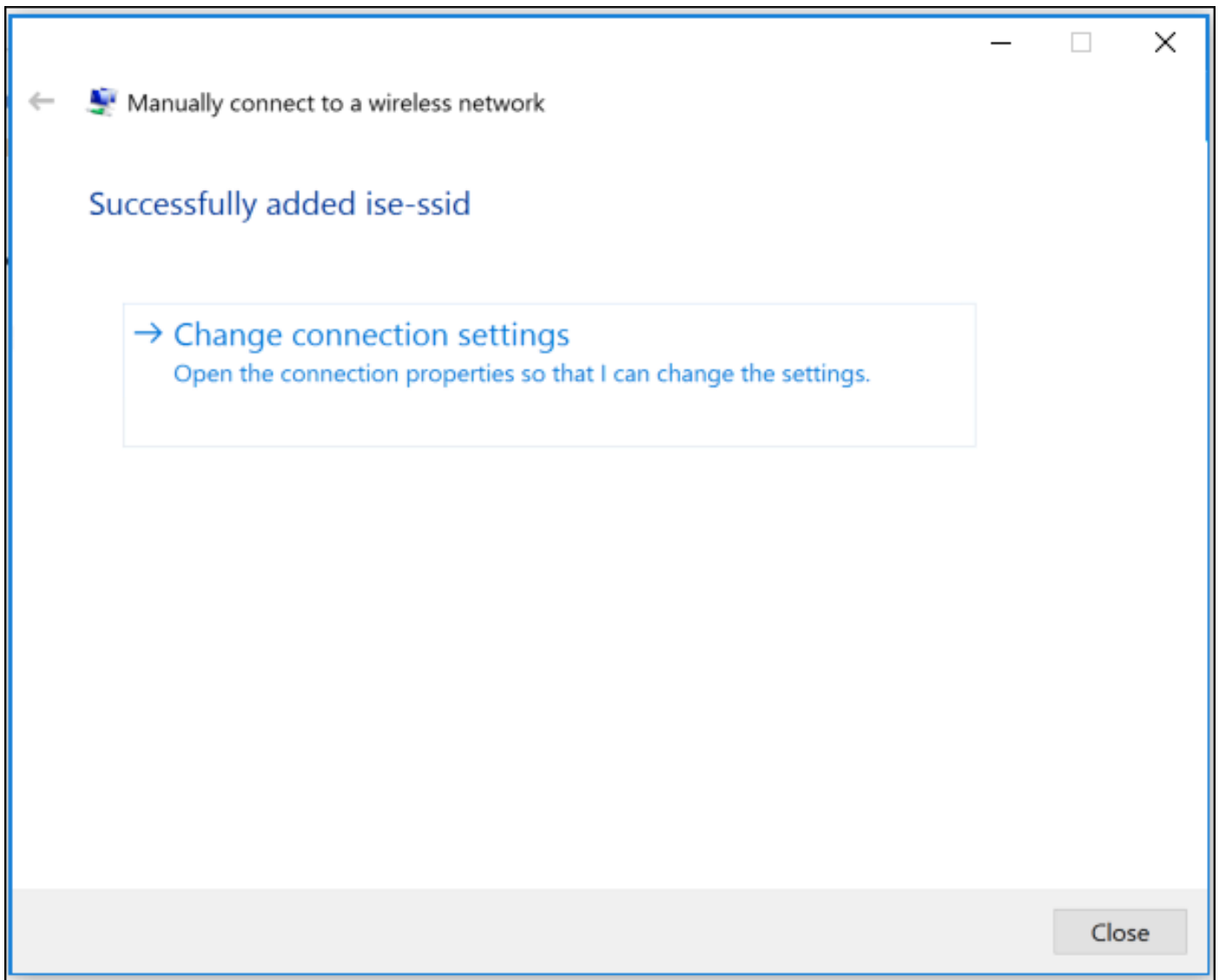
Start this connection automatically

Connect even if the network is not broadcasting

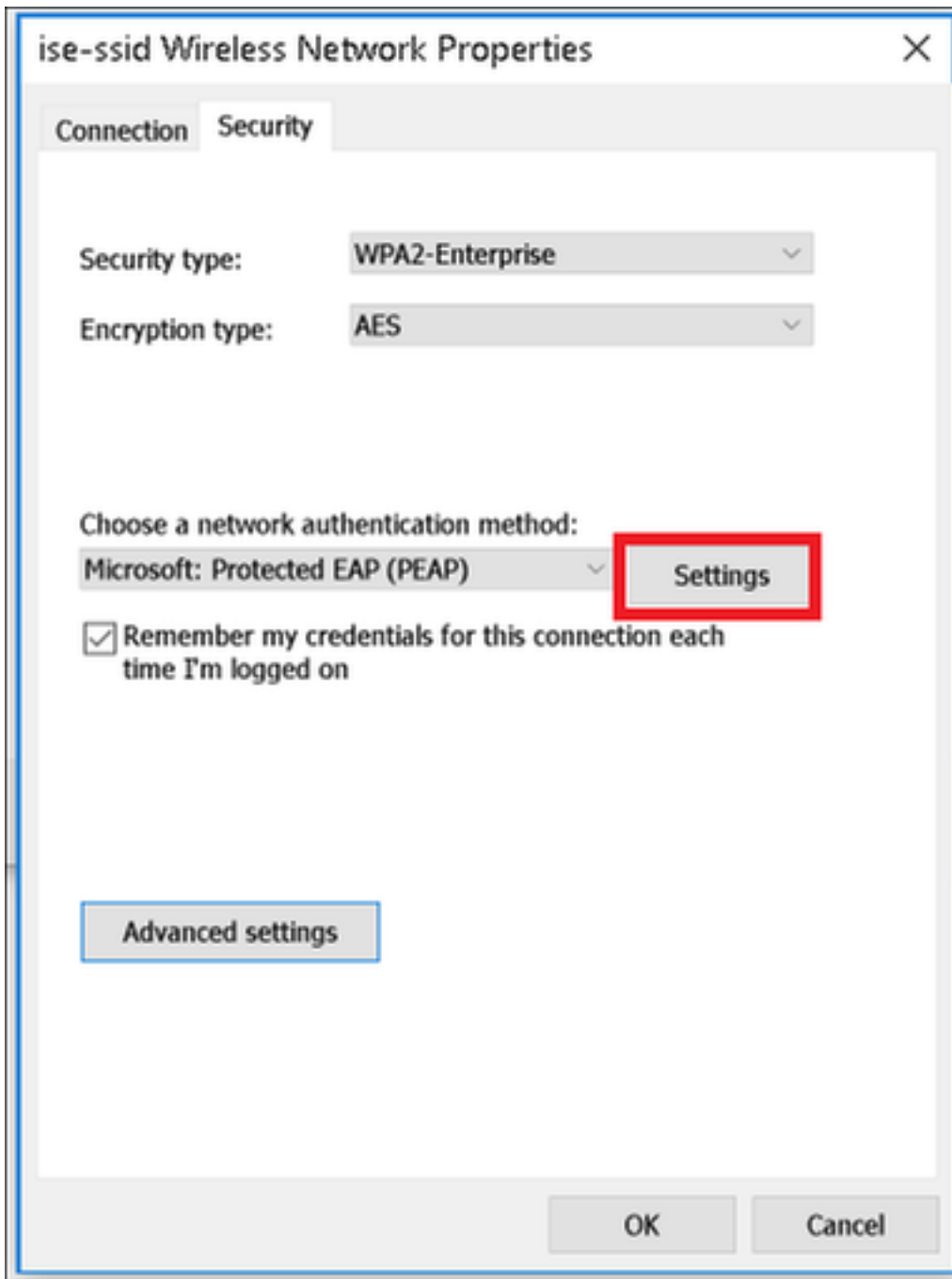
Warning: If you select this option, your computer's privacy might be at risk.

Next Cancel

Paso 5. Seleccione **Cambiar configuración de conexión** para personalizar la configuración del perfil WLAN.



Paso 6. Vaya a la ficha **Seguridad** y haga clic en **Configuración**.



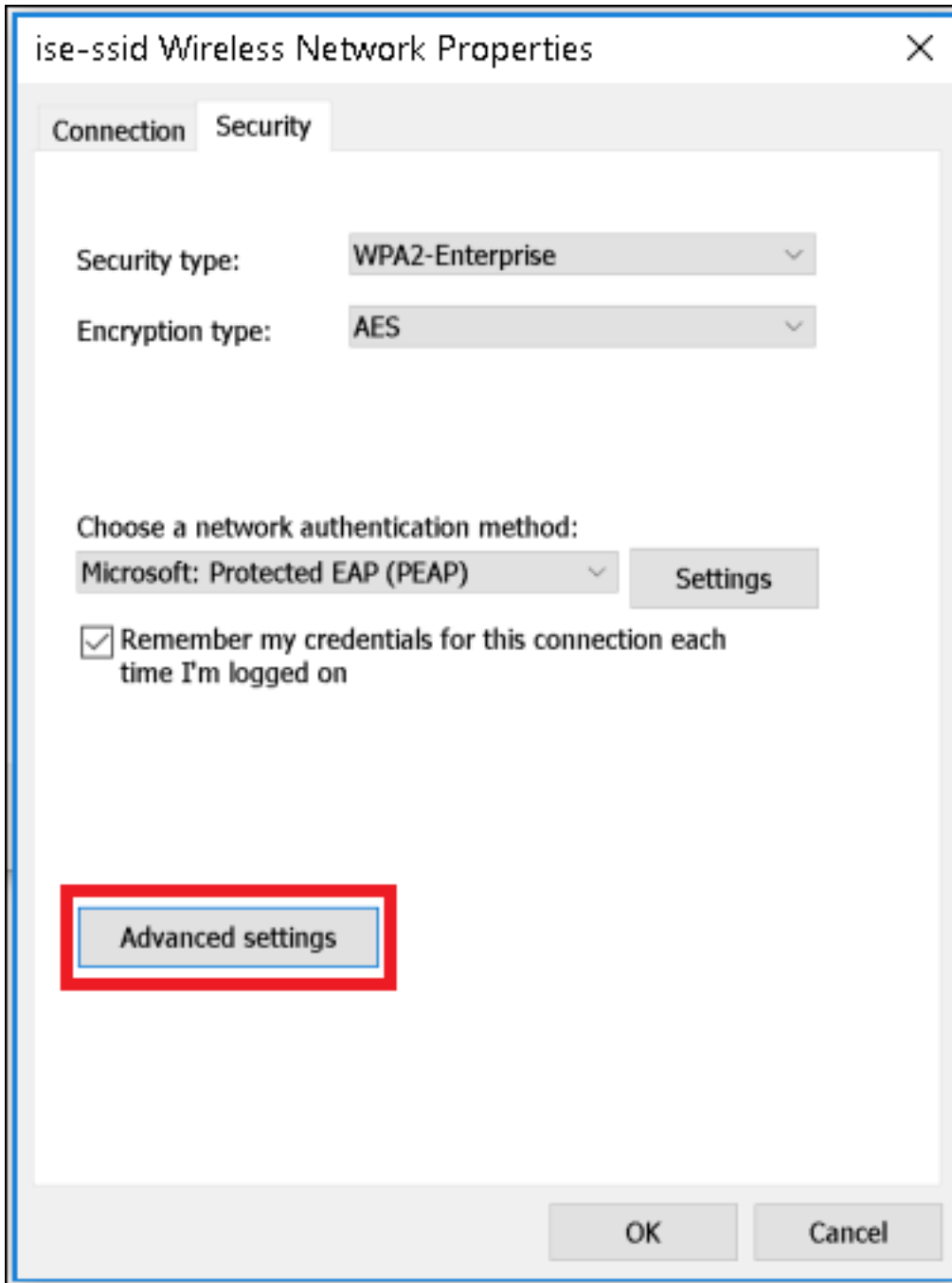
Paso 7. Elija si el servidor RADIUS está validado o no.

Si la respuesta es afirmativa, habilite **Verificar la identidad del servidor validando el certificado** y de **Autoridades de certificación raíz de confianza**: seleccione el certificado autofirmado de ISE.

Después de seleccionar **Configurar** y deshabilitar **Usar automáticamente mi nombre de inicio de sesión y contraseña de Windows...**, luego haga clic en **Aceptar**

Paso 8. Configurar las credenciales del usuario

Una vez que vuelva a la ficha **Seguridad**, seleccione **Configuración avanzada**, especifique el modo de autenticación como **Autenticación de usuario** y guarde las credenciales configuradas en ISE para autenticar al usuario.



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):

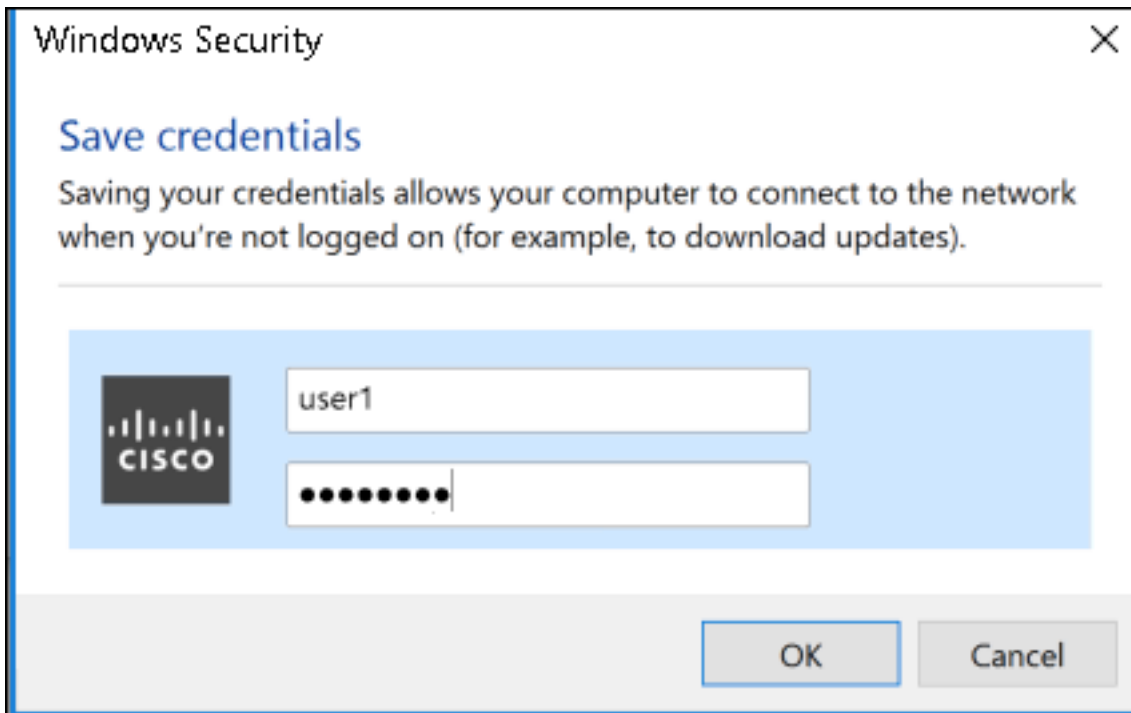
10

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 el WLC o desde la perspectiva de ISE.

Proceso de autenticación en ME

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

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

Ejemplo de una autenticación correcta (se ha omitido alguna salida):

```
*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:ed:18:c6:7b:4d AP 1852-4
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Applying site-specific Local Bridging
override for station 08:74:02:77:13:45 - vapId 3, site 'FlexGroup', interface 'management'
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Applying Local Bridging Interface
Policy for station 08:74:02:77:13:45 - vlan 0, interface id 0, interface 'management'
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Set Clinet Non AP specific
apfMsAccessVlan = 2400
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 This apfMsAccessVlan may be changed
later from AAA after L2 Auth
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Received 802.11i 802.1X key management
suite, enabling dot1x Authentication
*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: 08:74:02:77:13:45 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 client

*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 apfPemAddUser2:session timeout forstation 08:74:02:77:13:45 - Session Tout 0, apfMsTimeOut '0' and sessionTimerRunning flag is 0

*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Stopping deletion of Mobile Station: (callerId: 48)

*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Func: apfPemAddUser2, Ms Timeout = 0, Session Timeout = 0

*apfMsConnTask_0: Nov 25 16:36:24.335: **08:74:02:77:13:45 Sending assoc-resp with status 0 station:08:74:02:77:13:45 AP:38:ed:18:c6:7b:40-01 on apVapId 3**

*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 1**

*spamApTask0: Nov 25 16:36:24.341: 08:74:02:77:13:45 Sent dot1x auth initiate message for mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 reauth_sm state transition 0 ---> 1 for mobile 08:74:02:77:13:45 at 1x_reauth_sm.c:47

*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 is disabled - applying Global eap timers and retries

*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 reauth timeout = 1800

*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 into Connecting state

*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 reauth timeout = 1800

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Creating a PKC PMKID Cache entry for station 08:74:02:77:13:45 (RSN 2)

*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 cache at index 0 for station 08:74:02:77:13:45

*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 handoff

*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 take care of same.

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Sending EAP-Success to mobile 08:74:02:77:13:45 (EAP Id 70)

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Freeing AAACB from Dot1xCB as AAA auth is done for mobile 08:74:02:77:13:45

*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:c6:7b:4d in PMKID cache at index 0 of station 08:74:02:77:13:45

*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:c6:7b:4d in PMKID cache at index 0 of station 08:74:02:77:13:45

*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 retransmission to mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Entering Backend Auth Success state (id=70) for mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Received Auth Success while in Authenticating state for mobile 08:74:02:77:13:45

*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 into Authenticated state

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received EAPOL-Key from mobile 08:74:02:77:13:45

*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 08:74:02:77:13:45

*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 retransmission to mobile 08:74:02:77:13:45

*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 08:74:02:77:13:45

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

*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 : 255.255.255.224

*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 AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3for this client

*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 LWAPP rule on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3 flex-acl-name:

*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, Adding TMP rule

*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 request from Unassociated to Local
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-Incomplete to Mobility-Complete, mobility role=Local, client
state=APF_MS_STATE_ASSOCIATED
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) pemAdvanceState2
6261, Adding TMP rule
*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 mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*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_type 1, add_or_delete 1
*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 Invalid src IP address, 0.0.0.0 is part of reserved ip address range (caller
apf_ms.c:3593)
*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_type 1, add_or_delete 1
*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 obtener una manera fácil de leer los resultados de debug client, utilice la herramienta *Wireless debug analyzer*.

[Analizador de depuración inalámbrica](#)

Proceso de autenticación en ISE

Navigate hasta **Operaciones > RADIUS > Registros en directo** para ver qué política de autenticación, política de autorización y perfil de autorización se asignan al usuario.

The screenshot shows the Cisco ISE interface with the following elements highlighted in red:

- The **Operations** menu item in the top navigation bar.
- The **RADIUS** menu item in the sub-navigation bar.
- The **Live Logs** sub-menu item.
- The **Details** column header in the log table.
- The content of the **Details** column for the selected log entry, which includes:

Authentication Policy	Authorization Policy	Authorization Profiles
Default >> Rule name >> Default	Default >> NameAuthZrule	PermitAccess

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