

Configuración de Secure Client NAM para Dot1x con Windows e ISE 3.2

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

- [1. Descargue e instale Secure Client NAM \(Administrador de acceso de red\)](#)
- [2. Descargue e instale Secure Client NAM Profile Editor.](#)
- [3. Configuraciones generales por defecto](#)
- [4. Escenario 1: Configuración del Suplicante NAM de Secure Client para la Autenticación de Usuario PEAP \(MS-CHAPv2\)](#)
- [5. Escenario 2: Configuración del Suplicante NAM de Secure Client para la Autenticación de Usuario y Máquina Simultánea EAP-FAST](#)
- [6. Escenario 3: Configuración del Suplicante NAM de Secure Client para la Autenticación de Certificado de Usuario EAP TLS](#)
- [7. Configure ISR 1100 e ISE para permitir las autenticaciones basadas en el escenario 1 PEAP MSCHAPv2](#)

[Verificación](#)

[Troubleshoot](#)

[Problema: Secure Client no utiliza el perfil NAM.](#)

[Problema 2: Los registros deben recopilarse para realizar análisis adicionales.](#)

- [1. Activar registro extendido NAM](#)
- [2. Reproduzca el problema.](#)
- [3. Recopile el paquete DART de Secure Client.](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar Secure Client Network Analysis Module (NAM) en Windows.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Comprensión básica de qué es un suplicante RADIUS
- Punto1x
- PEAP
- PKI

Componentes Utilizados

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

- Windows 10 Pro Versión 22H2 Construido 19045.3930
- ISE 3.2
- Cisco C1117 Cisco IOS® XE Software, versión 17.12.02
- Active Directory 2016

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

Este documento describe cómo configurar Secure Client NAM en Windows. Se utilizan la opción de implementación previa y el Editor de perfiles para realizar la autenticación dot1x. Asimismo, se proporcionan algunos ejemplos de cómo se logra.

En la red, un suplicante es una entidad en un extremo de un segmento LAN punto a punto que busca ser autenticado por un autenticador conectado al otro extremo de ese link. El estándar IEEE 802.1X utiliza el término suplicante para referirse al hardware o al software. En la práctica, un solicitante es una aplicación de software instalada en un equipo de usuario final. El usuario invoca al solicitante y envía las credenciales para conectar el equipo a una red segura. Si la autenticación se realiza correctamente, el autenticador normalmente permite que el equipo se conecte a la red.

Acerca del Administrador de acceso de red

Network Access Manager es un software cliente que proporciona una red segura de capa 2 de acuerdo con sus políticas. Detecta y selecciona la red de acceso de capa 2 óptima y realiza la autenticación de dispositivos para acceder a redes por cable e inalámbricas. Network Access Manager gestiona la identidad de usuarios y dispositivos, así como los protocolos de acceso a la red necesarios para un acceso seguro. Funciona de forma inteligente para evitar que los usuarios finales realicen conexiones que infrinjan las políticas definidas por el administrador.

El administrador de acceso de red está diseñado para ser de enlace único, lo que permite una sola conexión de red a la vez. Además, las conexiones con cables tienen mayor prioridad que las inalámbricas, por lo que si se conecta a la red mediante una conexión con cables, el adaptador inalámbrico se desactiva sin dirección IP.

Configurar

Diagrama de la red

Es crucial entender que para las autenticaciones dot1x se necesitan 3 partes; el suplicante que puede hacer dot1x, el autenticador también conocido como NAS/NAD que sirve como proxy encapsulando el tráfico dot1x dentro de RADIUS, y el servidor de autenticación.

En este ejemplo, el suplicante se instala y configura de diferentes maneras. Más adelante, se muestra un escenario con la configuración del dispositivo de red y el servidor de autenticación.

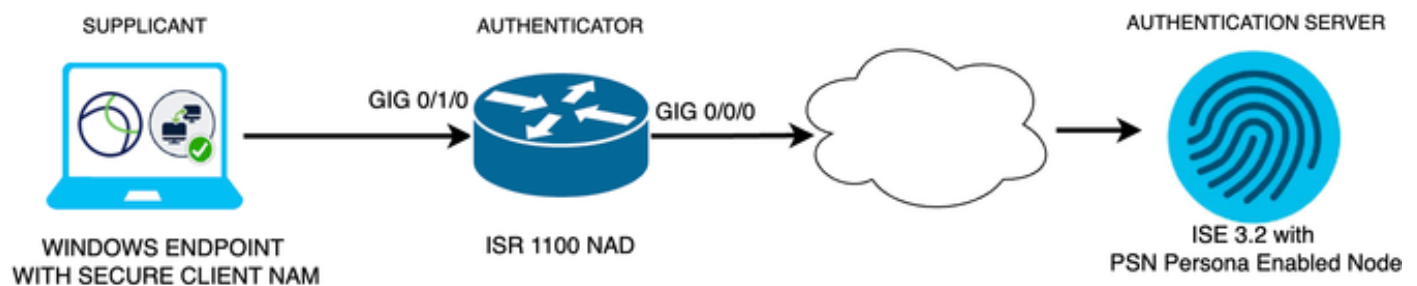


Diagrama de la red

Configuraciones

1. Descargue e instale Secure Client NAM (Network Access Manager).
2. Descargue e instale el editor de perfiles NAM de Secure Client.
3. Configuraciones predeterminadas generales
4. Situación 1: configurar el suplicante NAM de cliente seguro para la autenticación de usuario PEAP (MS-CHAPv2).
5. Situación 2: Configure el Suplicante NAM de Secure Client para EAP-FAST simultáneamente mientras se configuran la Autenticación del Usuario y la Máquina.
6. Escenario 3 Parte 1: Configuración del Suplicante NAM de Secure Client para EAP-TLS.
7. Situación 3, parte 2: configurar la demostración de NAD e ISE.

1. Descargue e instale Secure Client NAM (Administrador de acceso de red)

[Descarga de software de Cisco](#)

En la barra de búsqueda del nombre del producto, escriba Secure Client 5.




Inicio > Seguridad > VPN and Endpoint Security Clients > Secure Client (incluido AnyConnect) > Secure Client 5 > AnyConnect VPN Client Software.

En este ejemplo de configuración, se utiliza la versión 5.1.2.42.


Hay varias formas de implementar Secure Client en dispositivos Windows; desde SCCM, desde Identity Service Engine y desde la cabecera VPN. Sin embargo, en este artículo, el método de

instalación utilizado es el método previo a la implementación.

En la página, busque el archivo Paquete de implementación de cabecera de Cisco Secure Client (Windows).















Cisco Secure Client Pre-Deployment Package (Windows) - includes individual MSI files  06-Feb-2024 108.30 MB  

[cisco-secure-client-win-5.1.2.42-predeploy-k9.zip](#)

[Advisories](#) 

archivo zip Msi

Una vez descargado y extraído, haga clic en Setup.

 Profiles	4/4/2024 7:16 PM
 Setup	4/4/2024 7:16 PM
 cisco-secure-client-win-1.182.3-thousandeyes-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-core-vpn-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-dart-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-iseposture-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-nam-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-nvm-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-posture-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-sbl-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-umbrella-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.5191-zta-predeploy-k9	4/4/2024 7:16 PM
 Setup	4/4/2024 7:16 PM
 setup	4/4/2024 7:16 PM

Archivos de Secure Client

Instale el Administrador de acceso de red y los módulos de la Herramienta de diagnóstico e informes.



Advertencia: Si utiliza el Asistente de Cisco Secure Client, el módulo VPN se instala automáticamente y se oculta en la GUI. El NAM no funciona si el módulo VPN no está instalado. Si utiliza archivos MSI individuales o un método de instalación diferente, asegúrese de instalar el módulo VPN.

Select the Cisco Secure Client 5.1.2.42 modules you wish to install:

- Core & AnyConnect VPN
- Start Before Login
- Network Access Manager
- Secure Firewall Posture
- Network Visibility Module
- Umbrella
- ISE Posture
- ThousandEyes
- Zero Trust Access
- Select All
- Diagnostic And Reporting Tool
- Lock Down Component Services

Install Selected

Selector de instalación

Haga clic en Instale la opción seleccionada.

Acepte el CLUF.

Supplemental End User License Agreement

IMPORTANT: READ CAREFULLY

By clicking accept or using the Cisco Technology, you agree that such use is governed by the Cisco End User License Agreement and the applicable Product Specific Terms (collectively, the "EULA"). You also acknowledge and agree that you have read the Cisco Privacy Statement.

If you do not have authority to bind your company and its affiliates, or if you do not agree with the terms of the EULA, do not click 'accept' and do not use the Cisco Technology. If you are a Cisco channel partner accepting on behalf of an end customer ("customer"), you must inform the customer that the EULA applies to customer's use of the Cisco Technology and provide the customer with access to all relevant terms.

The latest version of documents can be found at the following locations.

- Cisco End User License Agreement: https://www.cisco.com/c/en/us/about/legal/cloud-and-software/end_user_license_agreement.html
- Applicable Product Specific Terms: <https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html>
- Cisco Privacy Statement: <https://www.cisco.com/c/en/us/about/legal/privacy-full.html>

Ventana EULA

Es necesario reiniciar después de la instalación de NAM.

Cisco Secure Client Install Selector

You must reboot your system for the installed changes to take effect.

OK

Ventana de requisitos de reinicio

Una vez instalado, se puede encontrar y abrir desde la barra de búsqueda de Windows.



Cisco Secure Client
App

2. Descargue e instale Secure Client NAM Profile Editor.

Se necesita el editor de perfiles del administrador de acceso de red de Cisco para configurar las preferencias Dot1x.

Desde la misma página donde se descarga Secure Client, se encuentra la opción Profile Editor.

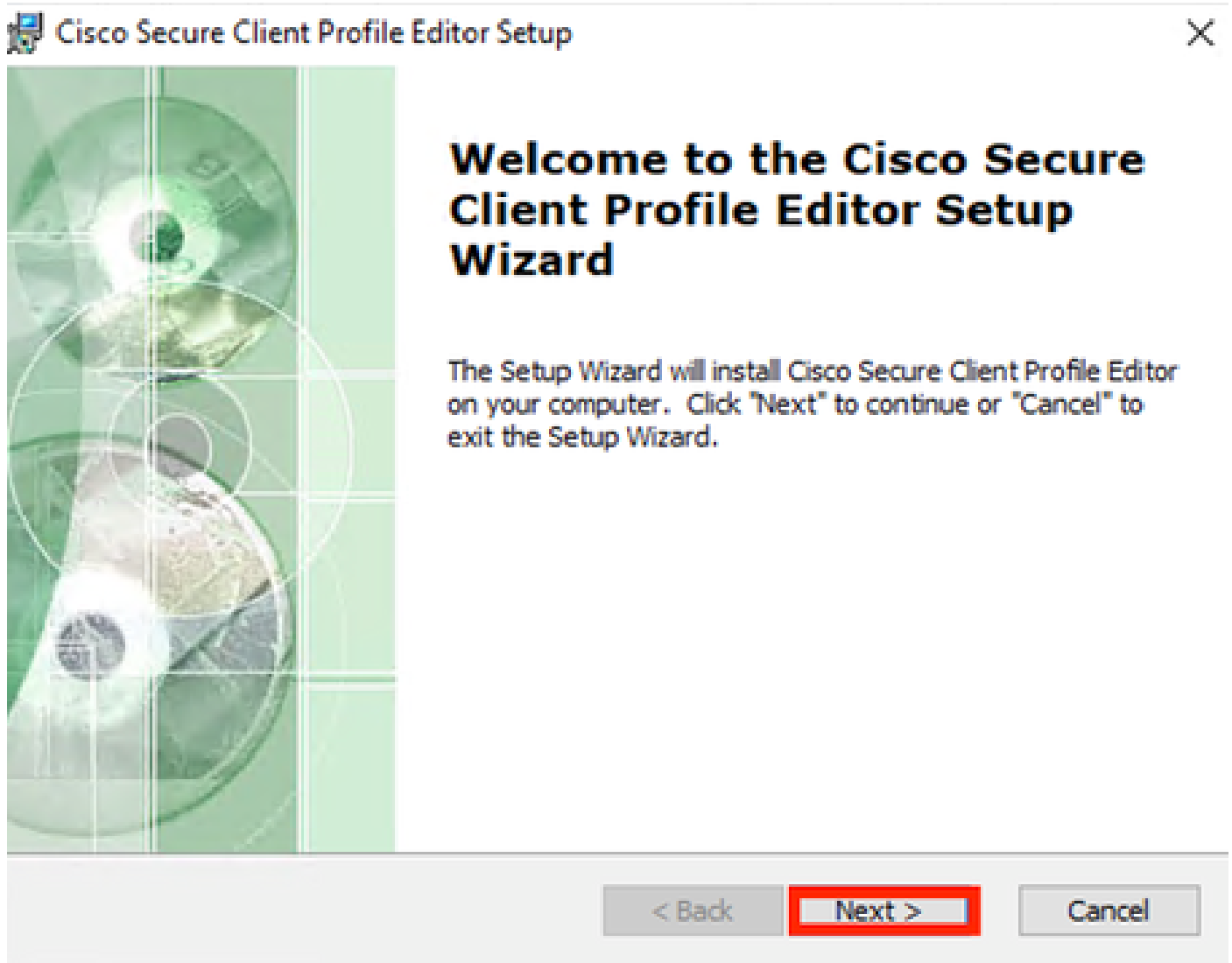
Este ejemplo utiliza la opción con la versión 5.1.2.42.



Editor de perfiles

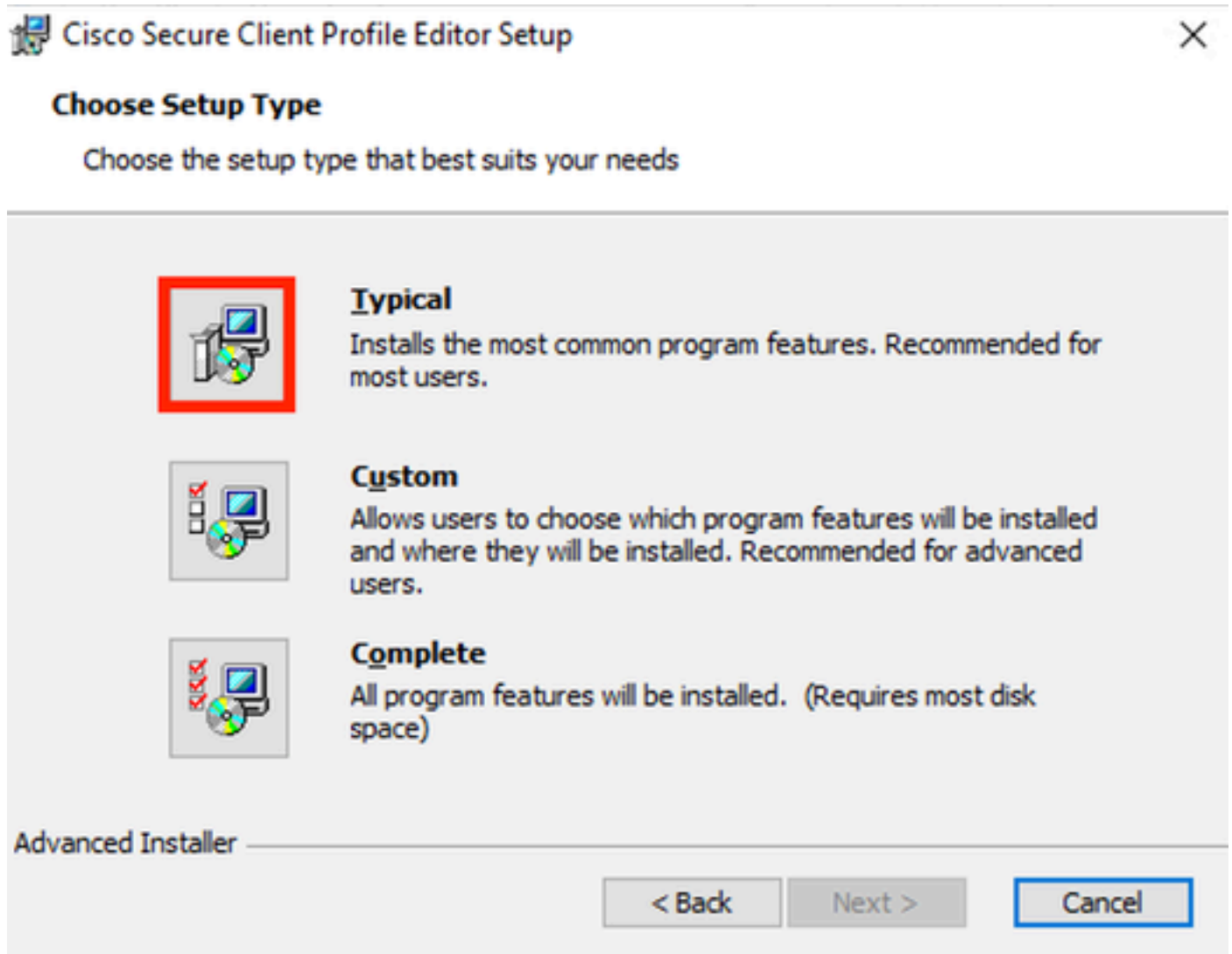
Una vez descargado, continúe con la instalación.

Ejecute el archivo msi.

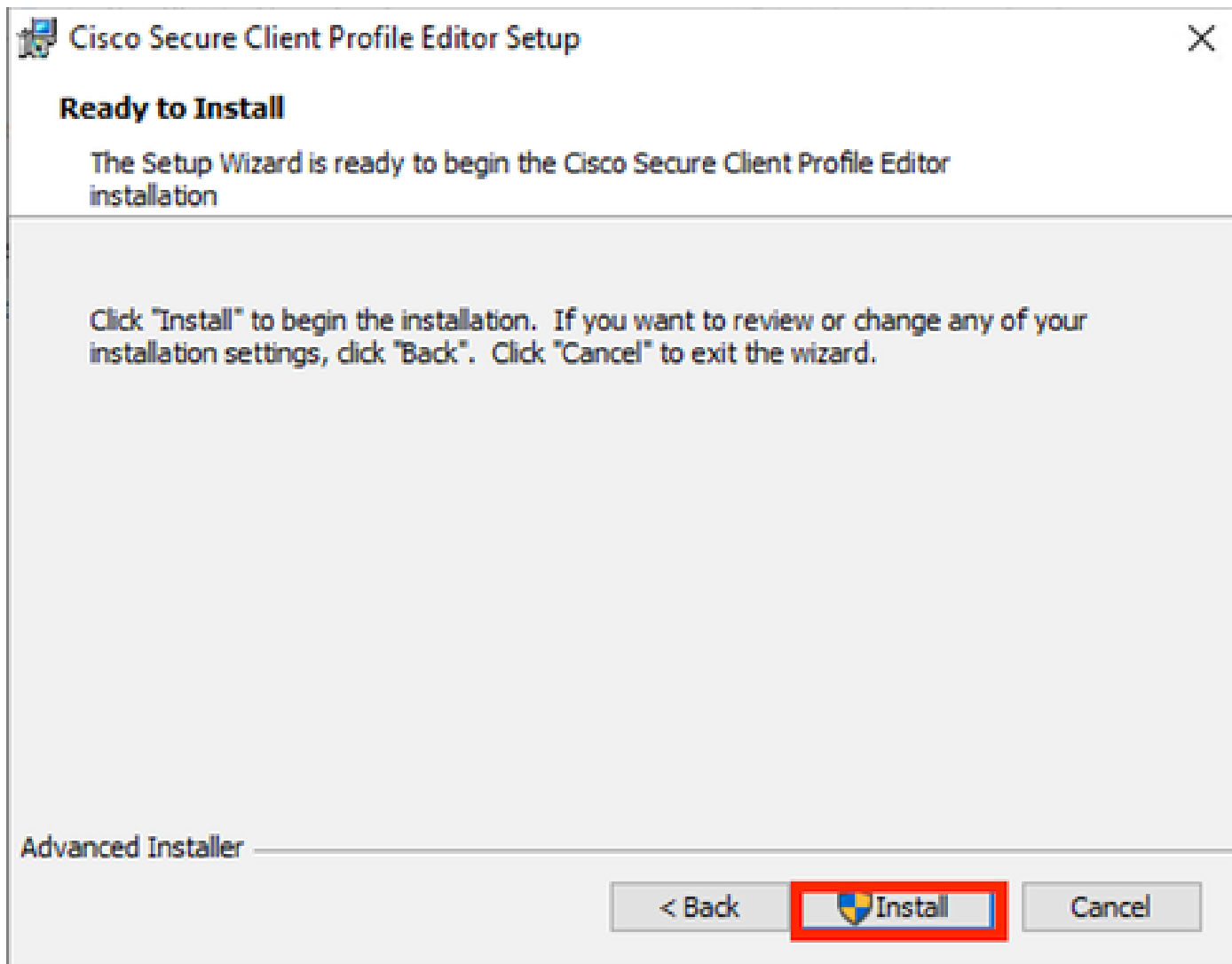


Ventana de configuración del Editor de perfiles

Utilice la opción de configuración Típica.



Configuración del Editor de perfiles



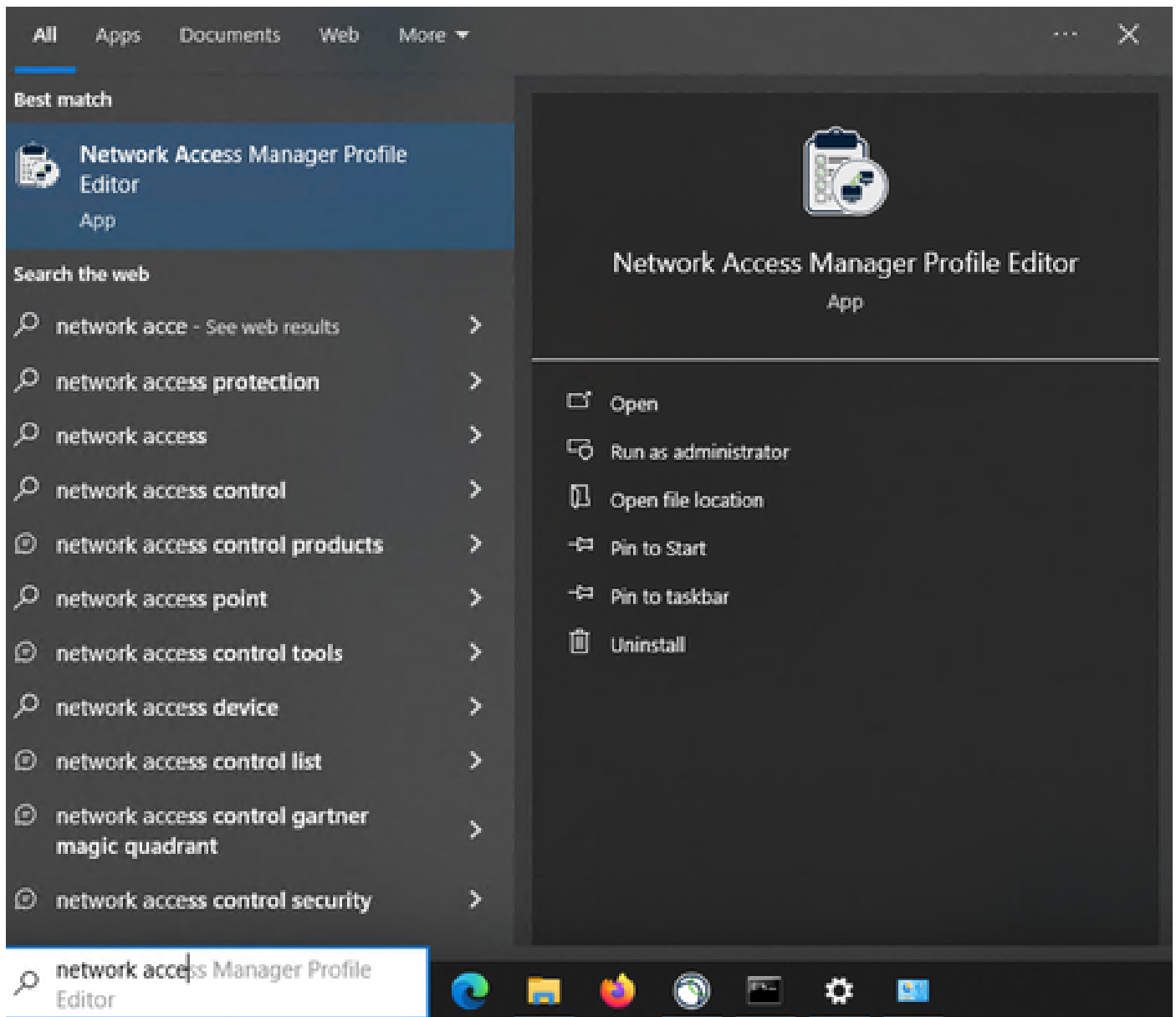
Ventana de instalación

Haga clic en Finish (Finalizar).



Fin de la configuración del Editor de perfiles

Una vez instalado, abra Network Access Manager Profile Editor desde la barra de búsqueda.



Editor de perfiles para NAM en la barra de búsqueda

La instalación de Network Access Manager y Profile Editor ha finalizado.

3. Configuraciones generales por defecto

Todos los escenarios presentados en este artículo contienen configuraciones para:

- Directiva de cliente
- Política de autenticación
- Grupos de red

Network Access Manager

- Client Policy
- Authentication Policy
- Networks
- Network Groups

Client Policy

Profile: Untitled

Connection Settings

Default Connection Timeout (sec.)

Connection Attempt:

Before user logon

Time to wait before allowing user to logon (sec.)

After user logon

Media

Manage Wi-Fi (wireless) Media

- Enable validation of WPA/WPA2/WPA3 handshake
- Enable Randomized MAC Address

Default Association Timeout (sec.)

Manage Wired (802.3) Media

Manage Mobile Broadband (3G) Media

- Enable Data Roaming

End-user Control

Allow end-user to:

- Disable Client
- Display user groups
- Specify a script or application to run when connected
- Auto-connect

Select machine connection type

Enable by default

Administrative Status

Service Operation: Enable Disable

FIPS Mode: Enable Disable

Captive Portal Detection: Enable Disable

Directiva de cliente del Editor de perfiles NAM

- Network Access Manager
 - Client Policy
 - Authentication Policy**
 - Networks
 - Network Groups

Authentication Policy

Profile: Untitled

Allow Association Modes

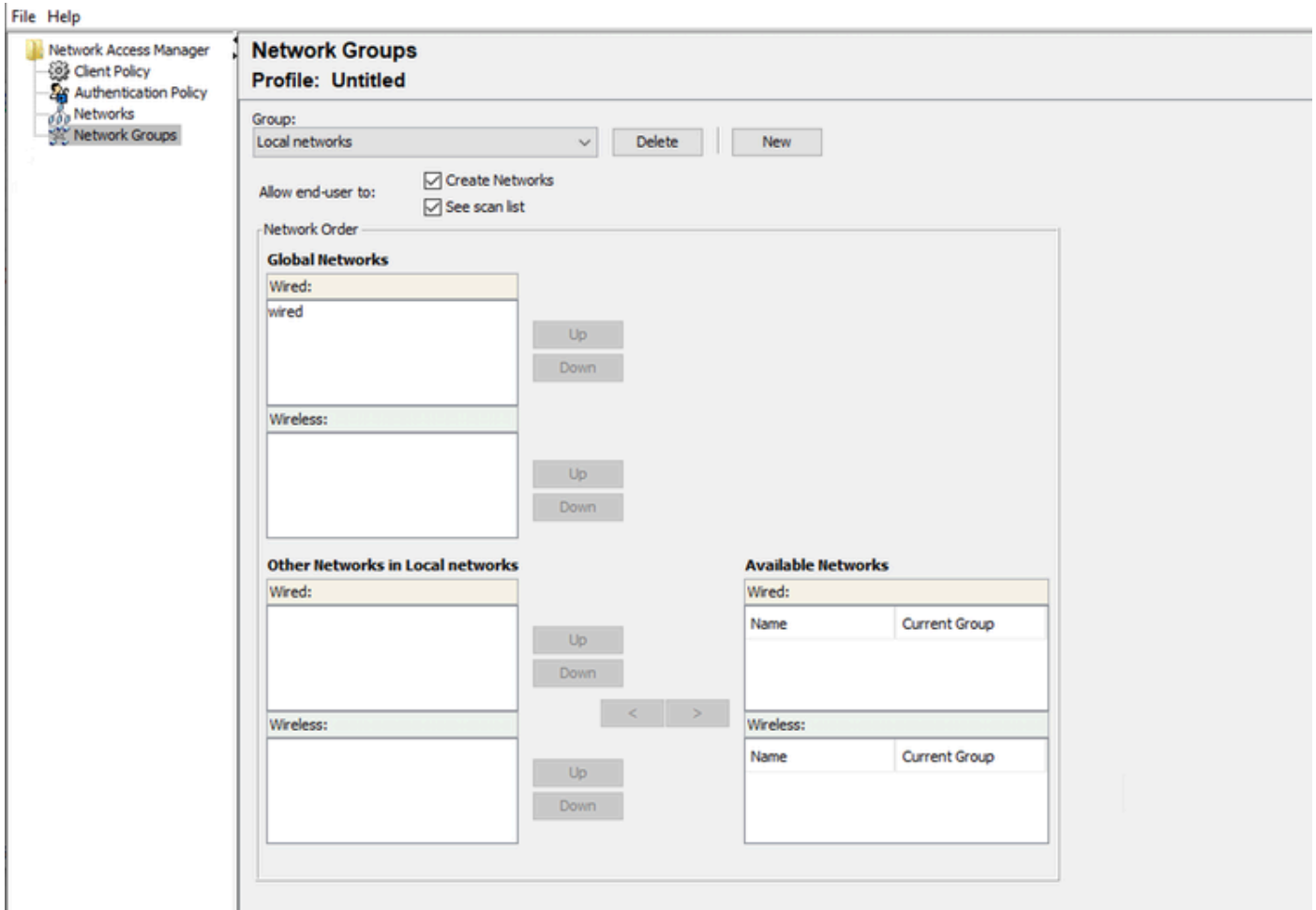
- Select All (Personal)
 - Open (no encryption)
 - Open (Static WEP)
 - Shared (WEP)
 - WPA Personal TKIP
 - WPA Personal AES
 - WPA2 Personal TKIP
 - WPA2 Personal AES
 - WPA3 Open (OWE)
 - WPA3 Personal AES (SAE)
- Select All (Enterprise)
 - Open (Dynamic (802.1X) WEP)
 - WPA Enterprise TKIP
 - WPA Enterprise AES
 - WPA2 Enterprise TKIP
 - WPA2 Enterprise AES
 - CKKM Enterprise TKIP
 - CKKM Enterprise AES
 - WPA3 Enterprise AES

Allowed Authentication Modes

- Select All Outer
 - EAP-FAST
 - EAP-GTC
 - EAP-MSCHAPv2
 - EAP-TLS
 - EAP-TLS
 - EAP-TTLS
 - EAP-MD5
 - EAP-MSCHAPv2
 - PAP (legacy)
 - CHAP (legacy)
 - MSCHAP (legacy)
 - MSCHAPv2 (legacy)
 - LEAP
 - PEAP
 - EAP-GTC
 - EAP-MSCHAPv2
 - EAP-TLS

Allowed Wired Security

- Select All
 - Open (no encryption)
 - 802.1x only
 - 802.1x with MacSec
 - AES-GCM-128
 - AES-GCM-256



Ficha Grupos de red

4. Escenario 1: Configuración del Suplicante NAM de Secure Client para la Autenticación de Usuario PEAP (MS-CHAPv2)

Vaya a la sección Redes.

El perfil de red predeterminado se puede eliminar.

Haga clic en Add (Agregar).

Networks

Profile: Untitled

Network

Name	Media Type	Group*
------	------------	--------

Add...

Edit...

Delete

* A network in group 'Global' is a member of *all* groups.

Creación de perfiles de red

Asigne un nombre al perfil de red.

Seleccione Global para Membership Group. Seleccione medios de red con cables.

Networks

Profile: Untitled

Name:	<input type="text" value="PEAP MSCHAPv2"/>	Media Type
Group Membership	<input type="radio"/> In group: <input type="text" value="Local networks"/>	Security Level
	<input checked="" type="radio"/> In all groups (Global)	
Choose Your Network Media	<input checked="" type="radio"/> Wired (802.3) Network Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.	
	<input type="radio"/> Wi-Fi (wireless) Network Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.	
	SSID (max 32 chars): <input type="text"/>	
	<input type="checkbox"/> Hidden Network	
	<input type="checkbox"/> Corporate Network	
Association Timeout	<input type="text" value="5"/> seconds	
Common Settings	Script or application on each user's machine to run when connected. <input type="text"/>	
	<input type="button" value="Browse Local Machine"/>	
Connection Timeout	<input type="text" value="40"/> seconds	
<input type="button" value="Next"/> <input type="button" value="Cancel"/>		

Sección Tipo de medio del perfil de red

Haga clic en Next (Siguiete).

Seleccione Authenticating Network y utilice el valor predeterminado para el resto de las opciones de la sección Security Level.

Networks
Profile: Untitled

Security Level

Open Network
Open networks have no security, and are open to anybody within range. This is the least secure type of network.

Authenticating Network
Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

Media Type
Security Level
Connection Type

802.1X Settings

authPeriod (sec.) 30 startPeriod (sec.) 3
heldPeriod (sec.) 60 maxStart 2

Security

Key Management
None

Encryption

AES GCM 128
 AES GCM 256

Port Authentication Exception Policy

Enable port exceptions

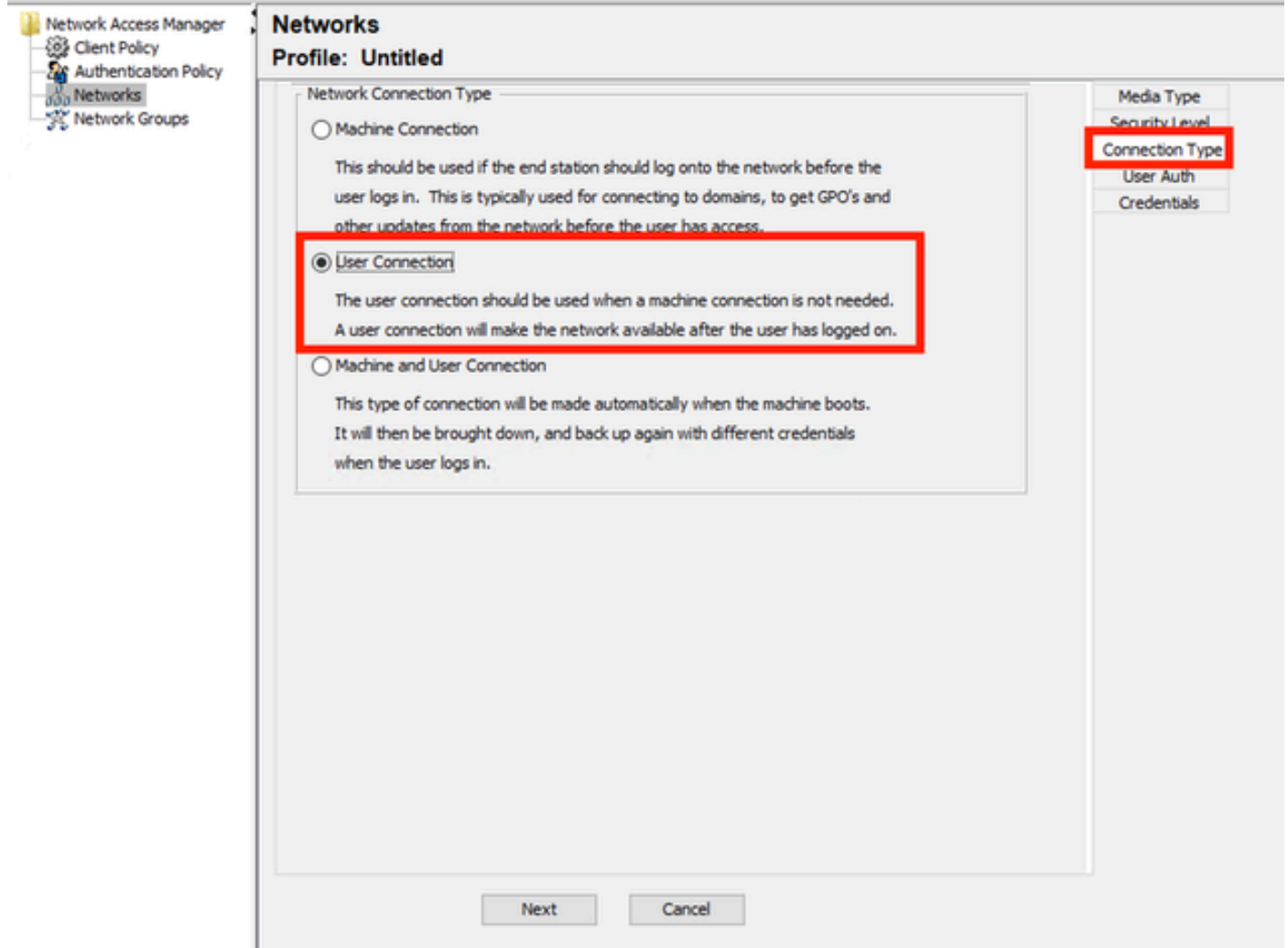
Allow data traffic before authentication
 Allow data traffic after authentication even if

EAP fails
 EAP succeeds but key management fails

Next Cancel

Nivel de seguridad del perfil de red

Haga clic en Siguiente para continuar con la sección Tipo de conexión.



Tipo de conexión del perfil de red

Seleccione el tipo de conexión Conexión de usuario.

Haga clic en Next para continuar con la sección User Auth que ahora está disponible.

Seleccione PEAP como el método EAP general.

Networks
Profile: Untitled

EAP Methods

- EAP-MD5
- EAP-MSCHAPv2
- EAP-GTC
- EAP-TLS
- EAP-TTLS
- PEAP
- EAP-FAST

Extend user connection beyond log off

EAP-PEAP Settings

- Validate Server Identity
- Enable Fast Reconnect
- Disable when using a Smart Card

Inner Methods based on Credentials Source

- Authenticate using a Password
 - EAP-MSCHAPv2
 - EAP-GTC
- EAP-TLS, using a Certificate
- Authenticate using a Token and EAP-GTC

Media Type
Security Level
Connection Type
User Auth
Certificates
Credentials

Next Cancel

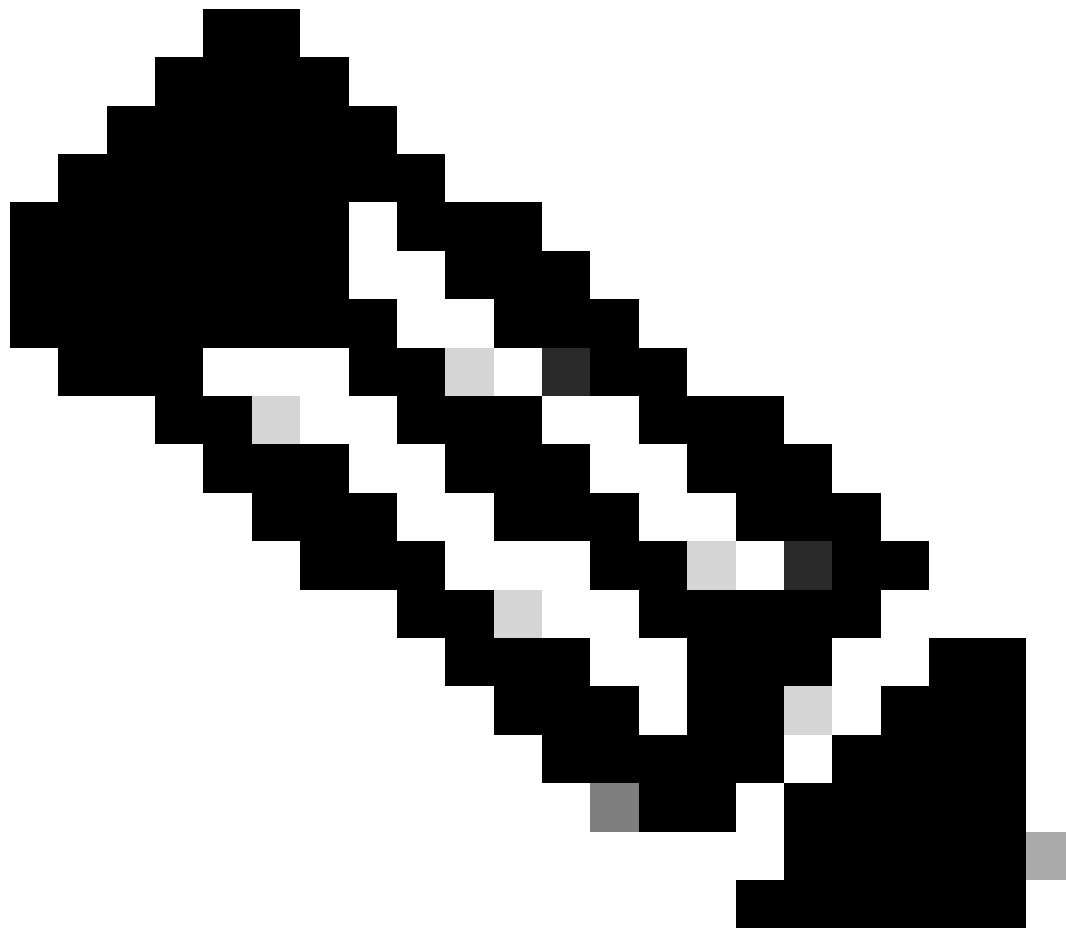
Autenticación de usuario de perfil de red

No cambie los valores predeterminados en la configuración EAP-PEAP.

Continúe con la sección Métodos internos basados en el origen de credenciales.

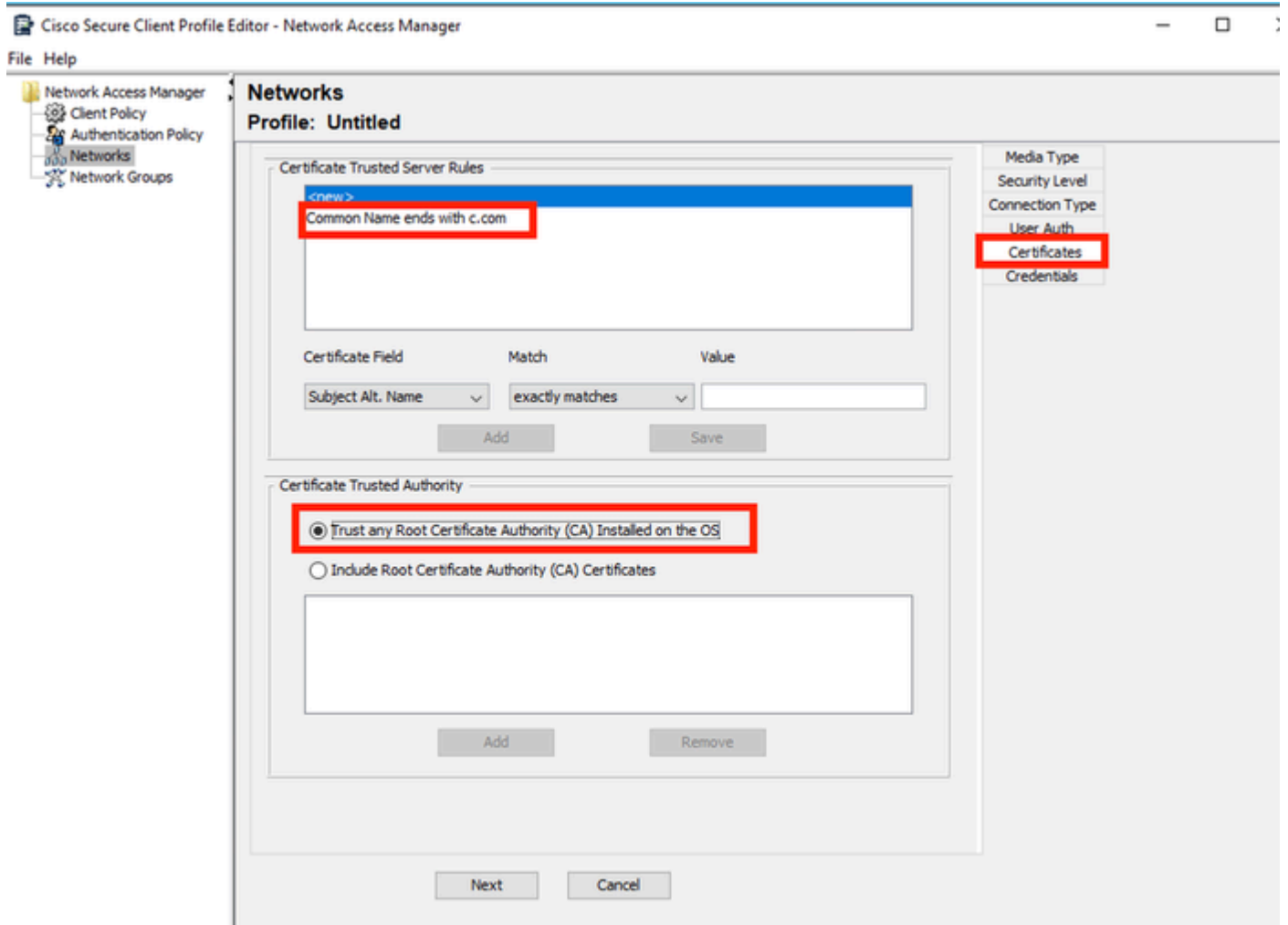
De los múltiples métodos internos que existen para EAP-PEAP, seleccione Authenticate using a Password y seleccione EAP-MSCHAPv2.

Haga clic en Siguiente para continuar con la sección Certificado.



Nota: se muestra la sección Certificate porque la opción Validate Server Identity en EAP-PEAP Settings está seleccionada. Para EAP-PEAP, realiza la encapsulación utilizando el certificado del servidor.

En la sección Certificados, en Reglas de servidor de confianza de certificados, se utiliza la regla Nombre común que termina con c.com. Esta sección de la configuración hace referencia al certificado que el servidor utiliza durante el flujo PEAP EAP. Si se utiliza Identity Service Engine (ISE) en su entorno, puede utilizar el nombre común del certificado EAP de nodo de servidor de políticas.

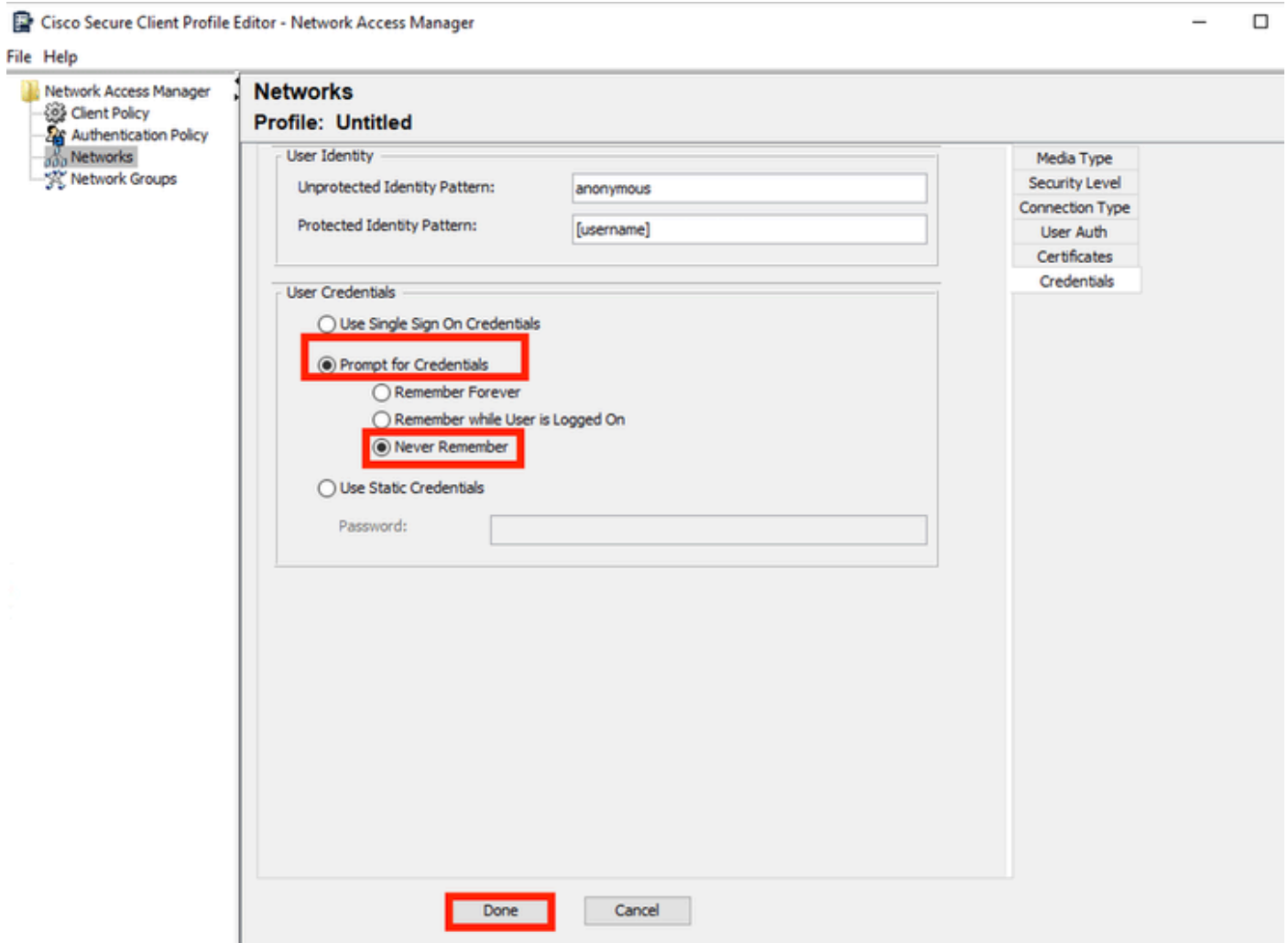


Sección Certificado de Perfil de Red

Se pueden seleccionar dos opciones en Certificate Trusted Authority. Para este escenario, en lugar de agregar un certificado de CA específico que firmó el certificado EAP RADIUS, se utiliza la opción Confiar en cualquier autoridad de certificación raíz (CA) instalada en el sistema operativo.

Con esta opción, el dispositivo Windows confía en cualquier certificado EAP firmado por un certificado incluido en el programa Administrar certificados de usuario Certificados: Usuario actual > Entidades de certificación raíz de confianza > Certificados.

Haga clic en Next (Siguiete).



Sección Credenciales de Perfil de Red

En la sección Credenciales sólo se cambia la sección Credenciales de Usuario.

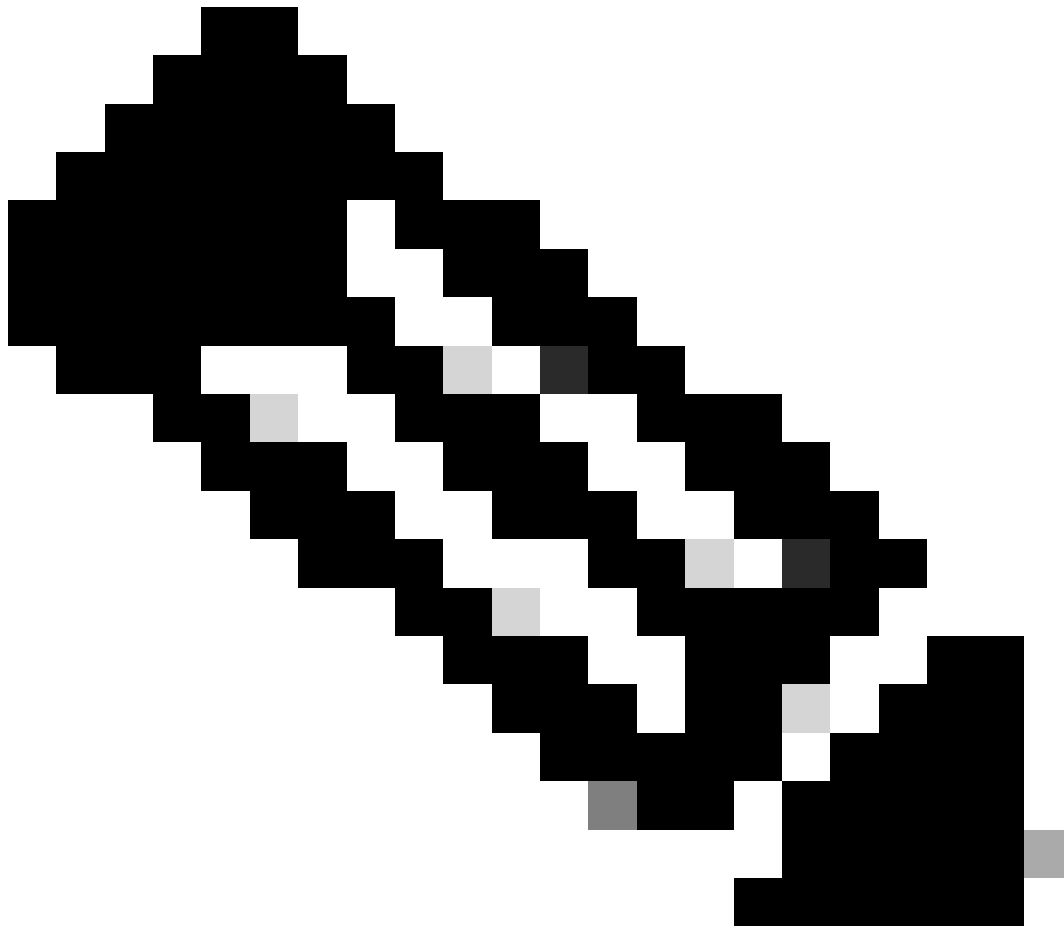
La opción Pedir credenciales > No recordar nunca está seleccionada, por lo que en cada autenticación, el usuario que realiza la autenticación debe introducir sus credenciales.

Haga clic en Done (Listo).

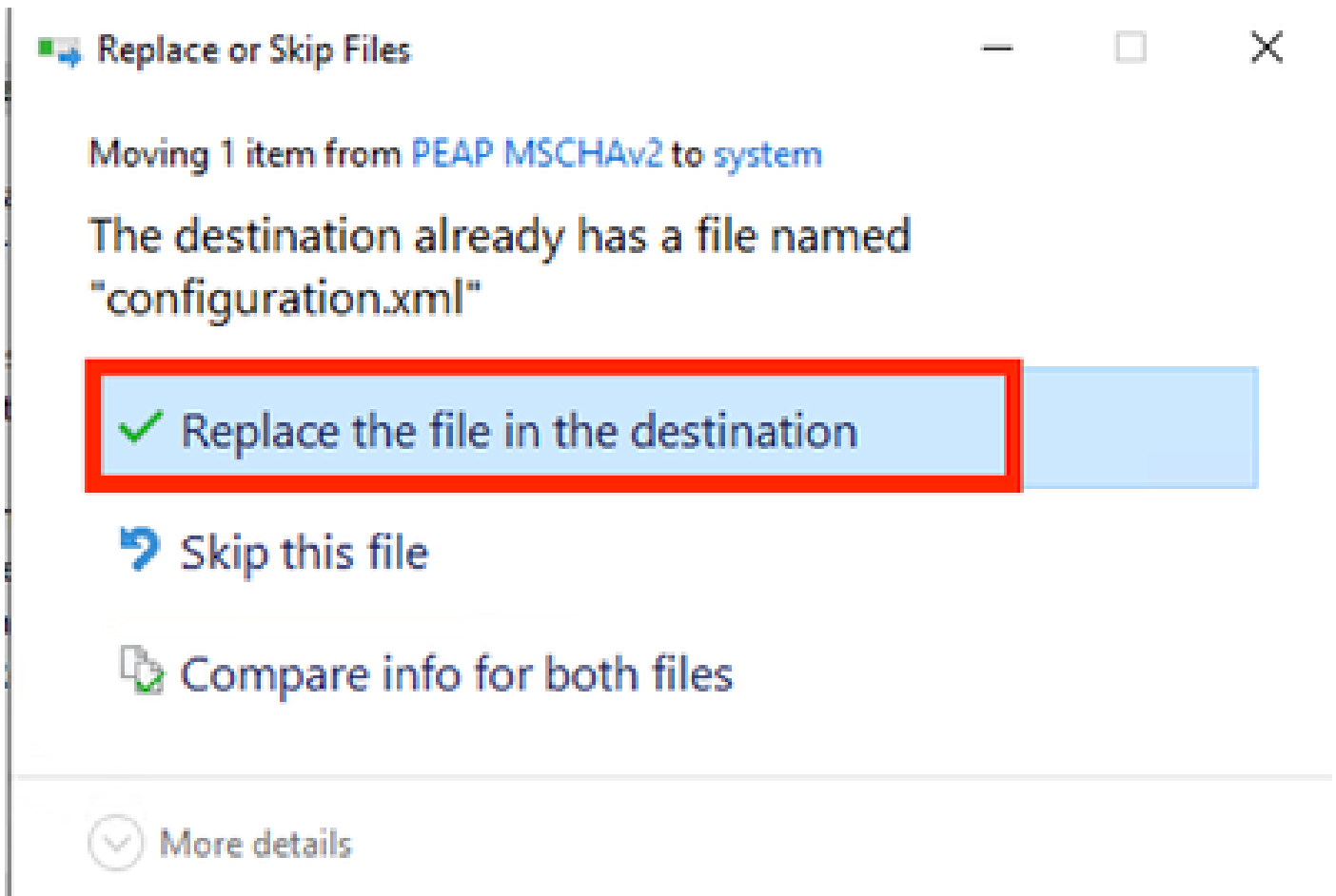
Guarde el perfil de Secure Client Network Access Manager, como configuration.xml con la opción File > Save As.

Para que Secure Client Network Access Manager utilice el perfil que se acaba de crear, sustituya el archivo configuration.xml del siguiente directorio por el nuevo:

C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system



Nota: El archivo debe llamarse configuration.xml; de lo contrario, no funcionará.



Sección Reemplazar archivo

5. Escenario 2: Configuración del Suplicante NAM de Secure Client para la Autenticación Simultánea de Usuario y Máquina EAP-FAST

Abra NAM Profile Editor y navegue hasta la sección Networks.

Haga clic en Add (Agregar).

Networks

Profile: Untitled

Network

Name	Media Type	Group*
------	------------	--------

Add...

Edit...

Delete

* A network in group 'Global' is a member of *all* groups.

Ficha Red del editor de perfiles NAM

Introduzca un nombre en el perfil de red.

Seleccione Global para Membership Group. Seleccione WiredNetwork Media.

File Help

Networks
Profile: Untitled

Name: **EAP-FAST**

Group Membership

In group: Local networks

In all groups (Global)

Choose Your Network Media

Wired (802.3) Network
Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.

Wi-Fi (wireless) Network
Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.

SSID (max 32 chars):

Hidden Network
 Corporate Network

Association Timeout: seconds

Common Settings

Script or application on each user's machine to run when connected.

Connection Timeout: seconds

Media Type
Security Level

Sección Tipo de medio

Haga clic en Next (Siguiete).

Seleccione Authenticating Network y no cambie los valores predeterminados para el resto de las opciones de esta sección.

File Help

Networks
Profile: Untitled

Security Level

Open Network
Open networks have no security, and are open to anybody within range. This is the least secure type of network.

Authenticating Network
Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

802.1X Settings

authPeriod (sec.)	30	startPeriod (sec.)	3
heldPeriod (sec.)	60	maxStart	2

Security

Key Management
None

Encryption

AES GCM 128
 AES GCM 256

Port Authentication Exception Policy

Enable port exceptions

Allow data traffic before authentication

Allow data traffic after authentication even if

EAP fails
 EAP succeeds but key management fails

Next Cancel

Sección Editor de perfiles de nivel de seguridad

Haga clic en Siguiente para continuar con la sección Tipo de conexión.

File Help

Networks
Profile: Untitled

Network Connection Type

Machine Connection

This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access.

User Connection

The user connection should be used when a machine connection is not needed. A user connection will make the network available after the user has logged on.

Machine and User Connection

This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.

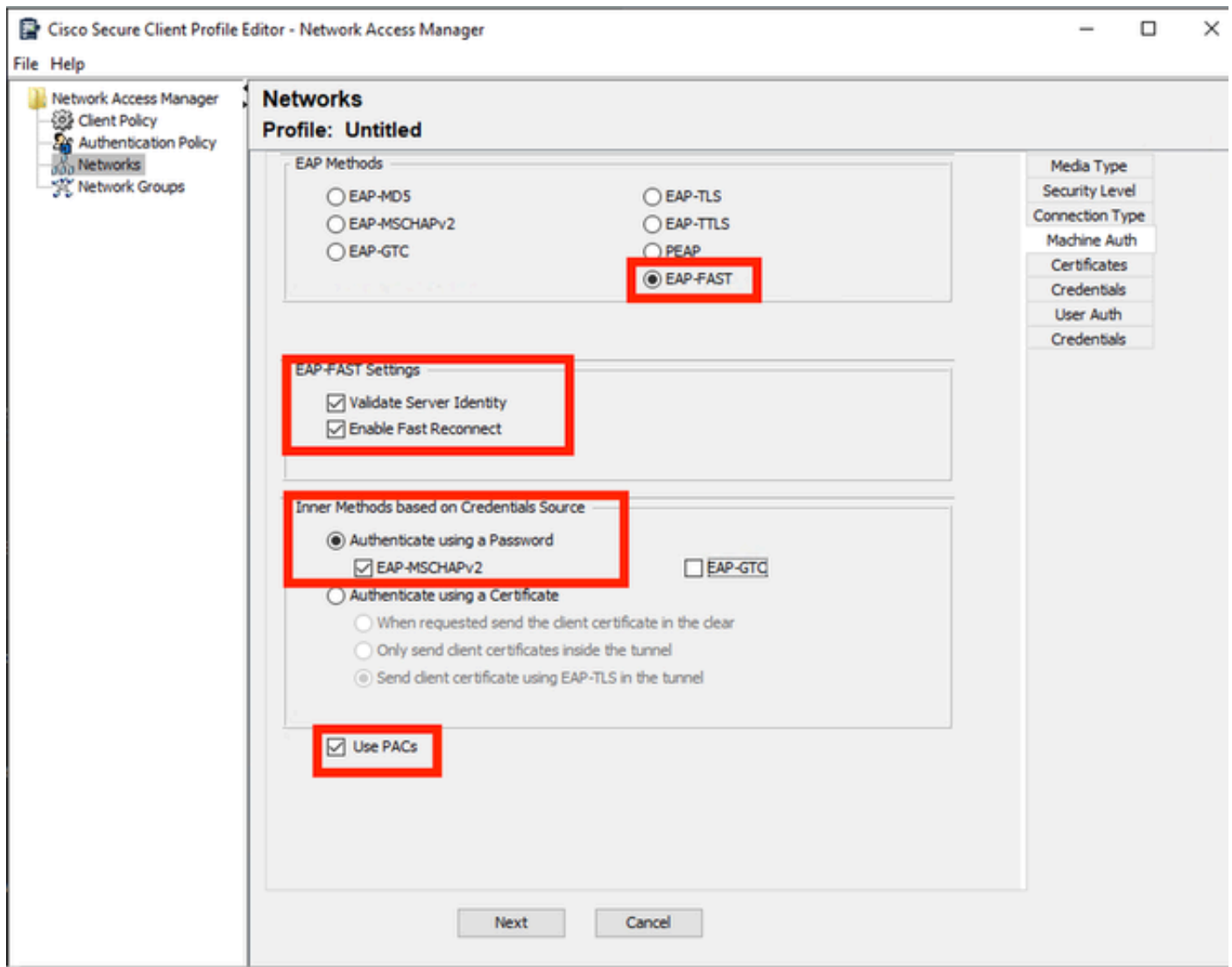
Media Type
Security Level
Connection Type
Machine Auth
Credentials
User Auth
Credentials

Next Cancel

Sección Tipo de conexión

Configure la autenticación de usuario y máquina simultáneamente seleccionando la tercera opción.

Haga clic en Next (Siguiente).



Sección de autenticación automática

En la sección Machine Auth, seleccione EAP-FAST como el método EAP. No cambie los valores predeterminados de Configuración de EAP FAST. En la sección Métodos internos basados en el origen de credenciales, seleccione Autenticar mediante una contraseña y EAP-MSCHAPv2 como método. A continuación, seleccione la opción Use PACs.

Haga clic en Next (Siguiente).

En la sección Certificados, en Reglas de servidor de confianza de certificados, el nombre común de la regla termina con c.com. Esta sección hace referencia al certificado que utiliza el servidor durante el flujo PEAP EAP. Si se utiliza Identity Service Engine (ISE) en su entorno, se puede utilizar el nombre común del certificado EAP del nodo del servidor de políticas.

Networks

Profile: Untitled

Certificate Trusted Server Rules

<new>
Subject Alternative Name ends with c.com

Certificate Field	Match	Value
Subject Alt. Name	exactly matches	

Add Save

Certificate Trusted Authority

Trust any Root Certificate Authority (CA) Installed on the OS

Include Root Certificate Authority (CA) Certificates

Add Remove

Next Cancel

Media Type

Security Level

Connection Type

Machine Auth

Certificates

Credentials

User Auth

Certificates

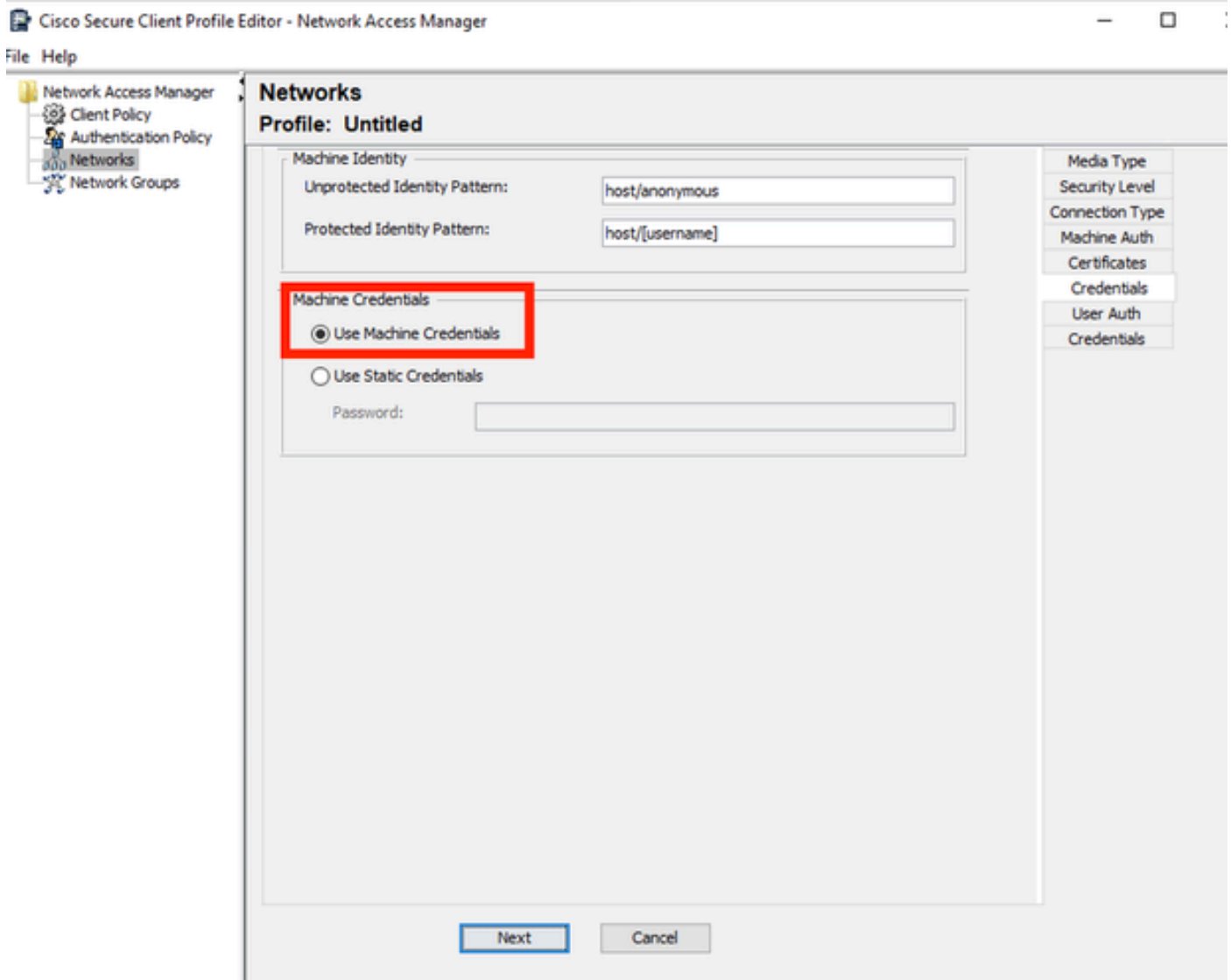
Credentials

Sección Confianza del Certificado del Servidor de Autenticación de Máquina

Se pueden seleccionar dos opciones en Certificate Trusted Authority. Para este escenario, en lugar de agregar un certificado de CA específico que firmó el certificado EAP RADIUS, utilice la opción Confiar en cualquier autoridad de certificados raíz (CA) instalada en el sistema operativo.

Con esta opción, Windows confía en cualquier certificado EAP firmado por un certificado incluido en el programa Administrar certificados de usuario (Usuario actual > Entidades de certificación raíz de confianza > Certificados).

Haga clic en Next (Siguiente).



Sección de credenciales de autenticación de máquina

Seleccione Usar credenciales de máquina en la sección Credenciales de máquina.

Haga clic en Next (Siguiente).

Networks
Profile: Untitled

EAP Methods

EAP-MD5 EAP-TLS
 EAP-MSCHAPv2 EAP-TTLS
 EAP-GTC PEAP
 EAP-FAST

Extend user connection beyond log off

EAP-FAST Settings

Validate Server Identity
 Enable Fast Reconnect
 Disable when using a Smart Card

Inner Methods based on Credentials Source

Authenticate using a Password
 EAP-MSCHAPv2 EAP-GTC
 Authenticate using a Certificate
 When requested send the client certificate in the clear
 Only send client certificates inside the tunnel
 Send client certificate using EAP-TLS in the tunnel
 Authenticate using a Token and EAP-GTC

Use PACs

Next Cancel

Media Type
Security Level
Connection Type
Machine Auth
Certificates
Credentials
User Auth
Certificates
Credentials

Sección Autenticación de usuario

Para User Auth, seleccione EAP-FAST como el método EAP.

No cambie los valores predeterminados en la sección de configuración EAP-FAST.

Para la sección Método interno basado en el origen de credenciales, seleccione Autenticar mediante una contraseña y EAP-MSCHAPv2 como método.

Seleccione Usar PACs.

Haga clic en Next (Siguiente).

En la sección Certificados, en Reglas de servidor de confianza de certificados, la regla es Nombre común termina con c.com. Estas configuraciones son para el certificado que el servidor utiliza durante el flujo EAP PEAP. Si se utiliza ISE en su entorno, se puede utilizar el nombre común del certificado EAP del nodo del servidor de políticas.

Networks

Profile: C:\Users\LAB 5\Desktop\EAP FAST\configuration.xml

The screenshot shows the 'Networks' configuration window for a profile named 'C:\Users\LAB 5\Desktop\EAP FAST\configuration.xml'. The window is divided into several sections:

- Certificate Trusted Server Rules:** A list box contains one rule: 'Common Name ends with c.com', which is highlighted in blue. Below the list box is a table with columns 'Certificate Field', 'Match', and 'Value'. The table contains one row: 'Common Name' (with a dropdown arrow), 'ends with' (with a dropdown arrow), and 'c.com'. Below the table are 'Remove' and 'Save' buttons.
- Certificate Trusted Authority:** Two radio button options are present: 'Trust any Root Certificate Authority (CA) Installed on the OS' (selected) and 'Include Root Certificate Authority (CA) Certificates'. Below these is an empty list box and 'Add' and 'Remove' buttons.
- Navigation:** 'Next' and 'Cancel' buttons are located at the bottom of the window.
- Right Panel:** A vertical list of tabs includes 'Media Type', 'Security Level', 'Connection Type', 'Machine Auth', 'Certificates', 'Credentials', 'User Auth', and 'Certificates' (highlighted with a red box), and 'Credentials'.

Sección de Confianza del Certificado del Servidor de Autenticación de Usuario

Se pueden seleccionar dos opciones en Certificate Trusted Authority. Para este escenario, en lugar de agregar un certificado de CA específico que firmó el certificado EAP RADIUS, se utiliza la opción Confiar en cualquier autoridad de certificación raíz (CA) instalada en el sistema operativo.

Haga clic en Next (Siguiente).

Networks

Profile: Untitled

User Identity

Unprotected Identity Pattern:

Protected Identity Pattern:

User Credentials

Use Single Sign On Credentials

Prompt for Credentials

- Remember Forever
- Remember while User is Logged On
- Never Remember

Use Static Credentials

Password:

Media Type

Security Level

Connection Type

Machine Auth

Certificates

Credentials

User Auth

Certificates

Credentials

Done Cancel

Credenciales de autenticación de usuario

En la sección Credenciales, sólo se cambia la sección Credenciales de Usuario.

La opción Solicitar credenciales > No recordar nunca está seleccionada. Por lo tanto, en cada autenticación, el usuario que realiza la autenticación debe ingresar sus credenciales.

Haga clic en el botón Finalizado.

Seleccione File > Save as y guarde el perfil de Secure Client Network Access Manager como configuration.xml.

Para hacer que el Secure Client Network Access Manager utilice el perfil que se acaba de crear, reemplace el archivo configuration.xml en el siguiente directorio por el nuevo:

C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system



Nota: El archivo debe llamarse configuration.xml; de lo contrario, no funcionará.

6. Escenario 3: Configuración del Suplicante NAM de Secure Client para la Autenticación de Certificado de Usuario EAP TLS

Abra NAM Profile Editor y navegue hasta la sección Networks.

Haga clic en Add (Agregar).

Networks

Profile: Untitled

Network

Name	Media Type	Group*
------	------------	--------

Add...

Edit...

Delete

* A network in group 'Global' is a member of *all* groups.

Sección Creación de Red

Asigne un nombre al perfil de red; en este caso, el nombre se asigna al protocolo EAP utilizado para este escenario.

Seleccione Global para Membership Group. y medios de red por cable.

Networks
Profile: Untitled

Name:

Group Membership

In group:

In all groups (Global)

Choose Your Network Media

Wired (802.3) Network

Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.

Wi-Fi (wireless) Network

Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.

SSID (max 32 chars):

Hidden Network

Corporate Network

Association Timeout: seconds

Common Settings

Script or application on each user's machine to run when connected.

Connection Timeout: seconds

Media Type
Security Level

Sección Tipo de medio

Haga clic en Next (Siguiete).

Seleccione Authenticating Network y no cambie los valores predeterminados para el resto de las opciones de la sección Security Level.

Networks
Profile: Untitled

Security Level

Open Network
Open networks have no security, and are open to anybody within range. This is the least secure type of network.

Authenticating Network
Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

802.1X Settings

authPeriod (sec.) startPeriod (sec.)

heldPeriod (sec.) maxStart

Port Authentication Exception Policy

Enable port exceptions

Allow data traffic before authentication

Allow data traffic after authentication even if

EAP fails

EAP succeeds but key management fails

Security

Key Management
None

Encryption

AES GCM 128

AES GCM 256

Media Type

Security Level

Connection Type

Next Cancel

Nivel de seguridad

Este escenario es para la autenticación de usuario mediante un certificado. Por esta razón se utiliza la opción User Connection.

Networks
Profile: Untitled

Network Connection Type

Machine Connection
This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access.

User Connection
The user connection should be used when a machine connection is not needed. A user connection will make the network available after the user has logged on.

Machine and User Connection
This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.

Media Type

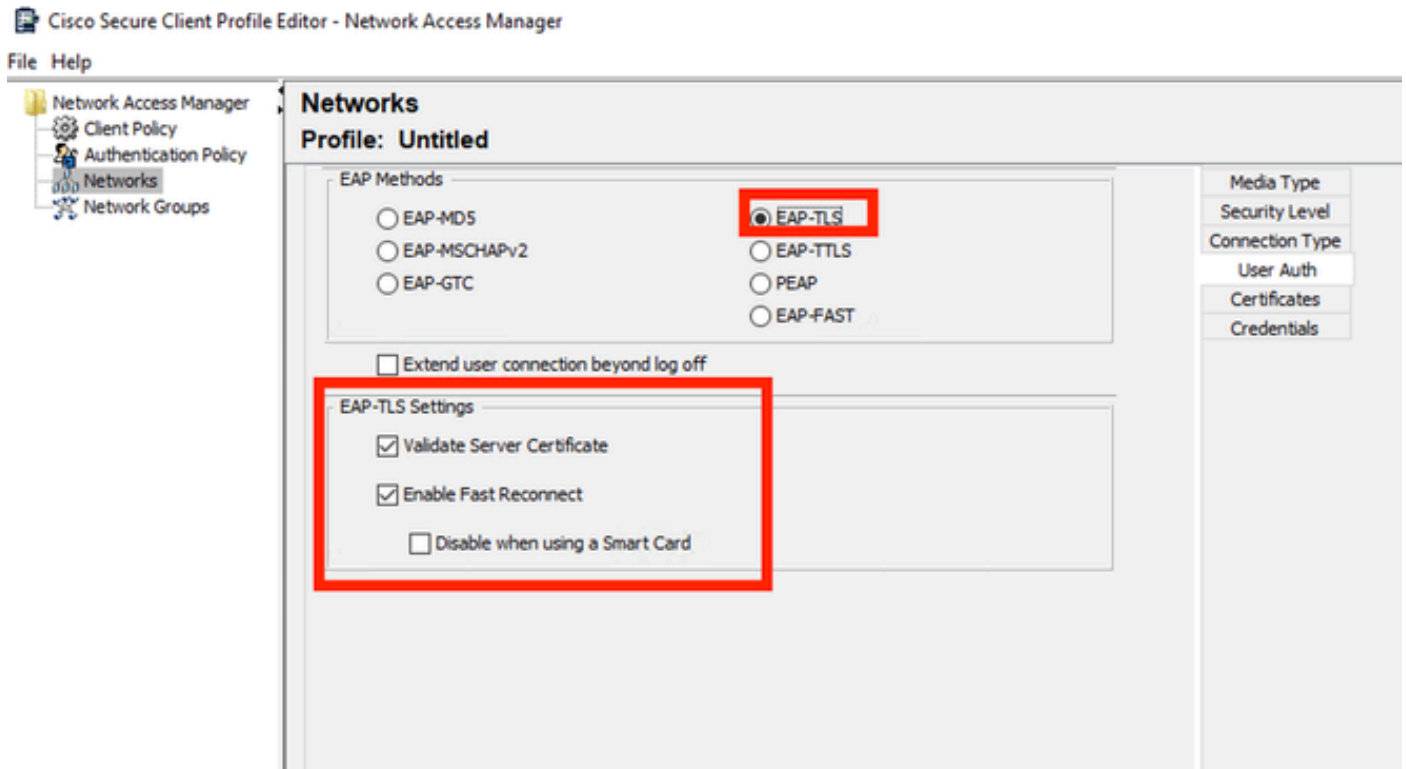
Security Level

Connection Type

User Auth

Credentials

Configure EAP-TLS como el método EAP. No cambie los valores predeterminados en la sección Configuración de EAP-TLS.



Para la sección Certificados, cree una regla que coincida con el certificado EAP-TLS de AAA. Si utiliza ISE, busque esta regla en la sección Administración > Sistema > Certificados.

Para la sección Certificate Trusted Authority, seleccione Trust any Root Certificate Authority (CA) instalado en el sistema operativo.

Networks
Profile: Untitled

Certificate Trusted Server Rules

Common Name ends with c.com

Certificate Field	Match	Value
Subject Alt. Name	exactly matches	

Add Save

Certificate Trusted Authority

Trust any Root Certificate Authority (CA) Installed on the OS

Include Root Certificate Authority (CA) Certificates

Add Remove

Next Cancel

Media Type
Security Level
Connection Type
User Auth
Certificates
Credentials

Configuración de confianza del certificado del servidor de autenticación de usuario

Haga clic en Next (Siguiente).

En la sección Credenciales de usuario, no cambie los valores predeterminados de la primera parte.

Networks

Profile: Untitled

User Identity

Unprotected Identity Pattern:

User Credentials

Use Single Sign On Credentials (Requires Smart Card)

Prompt for Credentials

- Remember Forever
- Remember while User is Logged On
- Never Remember

Certificate Source

Smart Card or OS certificates

Smart Card certificates only

Remember Smart Card Pin

Remember Forever

Remember while User is Logged On

Never Remember

Smart Card Removal Policy

Disconnect from Network

Use Certificate Matching Rule (Max 10)

Rule Logic OR AND

Field	Operator	Value

Media Type

Security Level

Connection Type

User Auth

Certificates

Credentials

Sección Credenciales de Autenticación de Usuario

Es importante configurar una regla que coincida con el certificado de identidad que el usuario envía durante el proceso EAP-TLS. Para ello, haga clic en la casilla de verificación junto a Usar regla de asignación de certificados (máximo 10).

Haga clic en Add (Agregar).

Certificate Matching Rule Entry [X]

Certificate Field: Issuer.CN Match: Equals

Value: My Internal OR 3rd Party CA.com

OK Cancel

Use Certificate Matching Rule (Max 10)

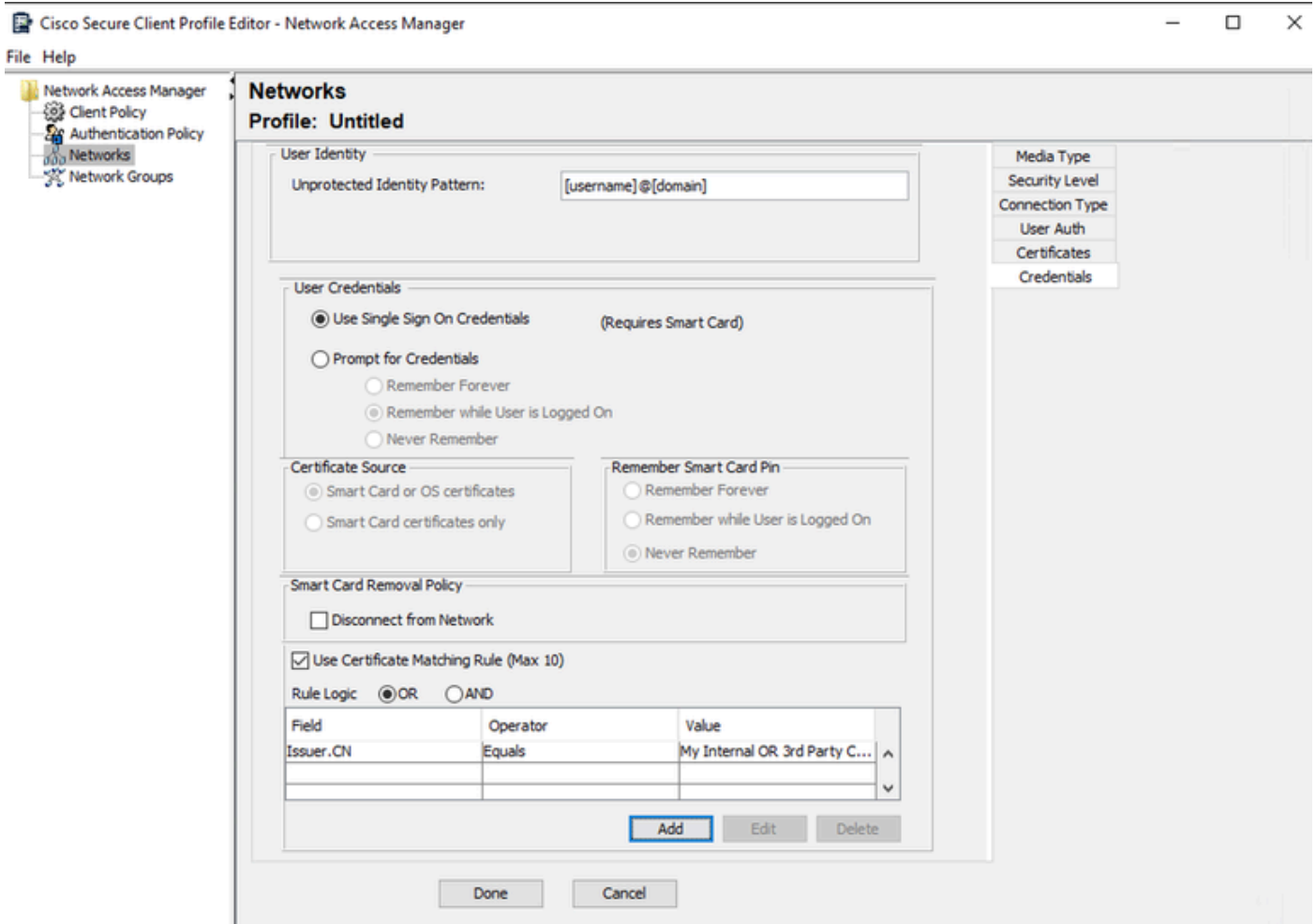
Logic: OR AND

Id	Operator	Value

Add Edit Delete

Ventana Regla de coincidencia de certificados

Reemplace el valor My Internal OR 3rd Party CA.com por el CN del certificado de usuario.



Sección Credenciales de Certificado de Autenticación de Usuario

Haga clic en Finalizado para finalizar la configuración.

Seleccione File > Save as para guardar el perfil de Secure Client Network Access Manager como configuration.xml.

Para hacer que el Secure Client Network Access Manager utilice el perfil que se acaba de crear, reemplace el archivo configuration.xml en el siguiente directorio por el nuevo:

C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system



Nota: El archivo debe llamarse configuration.xml; de lo contrario, no funcionará.

7. Configure ISR 1100 e ISE para permitir las autenticaciones basadas en el escenario 1 PEAP MSCHAPv2

Configuración del router ISR 1100.

Esta sección trata sobre la configuración básica que debe tener el NAD para que funcione dot1x.

Nota: Para la implementación de ISE de varios nodos, apunte a cualquier nodo que tenga activada la persona del nodo del servidor de políticas. Para comprobarlo, vaya a ISE en la pestaña Administration > System > Deployment.

```
aaa new-model
aaa session-id common
!
aaa authentication dot1x default group ISE-CLUSTER
aaa authorization network default group ISE-CLUSTER
aaa accounting system default start-stop group ISE-CLUSTER
aaa accounting dot1x default start-stop group ISE-CLUSTER
!
aaa server radius dynamic-author
  client A.B.C.D server-key <Your shared secret>
!
!
radius server ISE-PSN-1
  address ipv4 A.B.C.D auth-port 1645 acct-port 1646
  timeout 15
  key <Your shared secret>
```

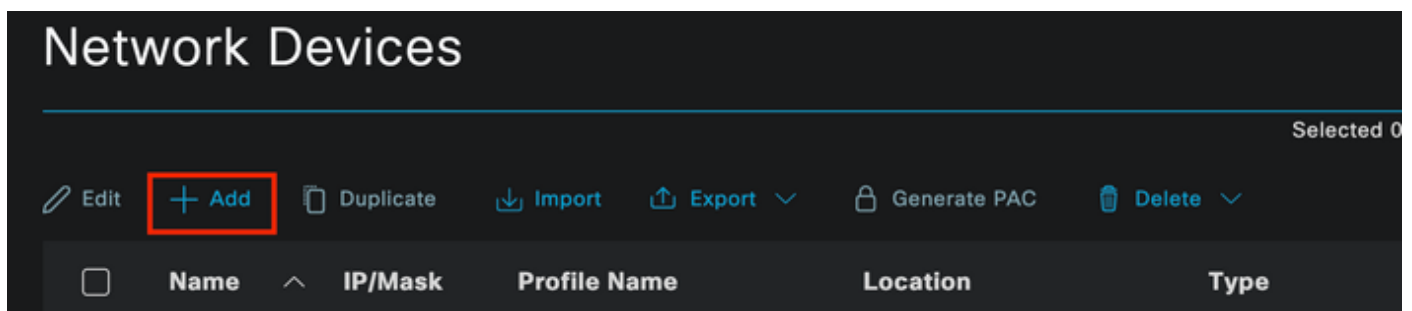
```
!  
!  
aaa group server radius ISE-CLUSTER  
  server name ISE-PSN-1  
!  
interface GigabitEthernet0/1/0  
  description "Endpoint that supports dot1x"  
  switchport access vlan 15  
  switchport mode access  
  authentication host-mode multi-auth  
  authentication order dot1x mab  
  authentication priority dot1x mab  
  authentication port-control auto  
  dot1x pae authenticator  
  spanning-tree portfast
```

Configuración de Identity Service Engine 3.2.

Configure el dispositivo de red.

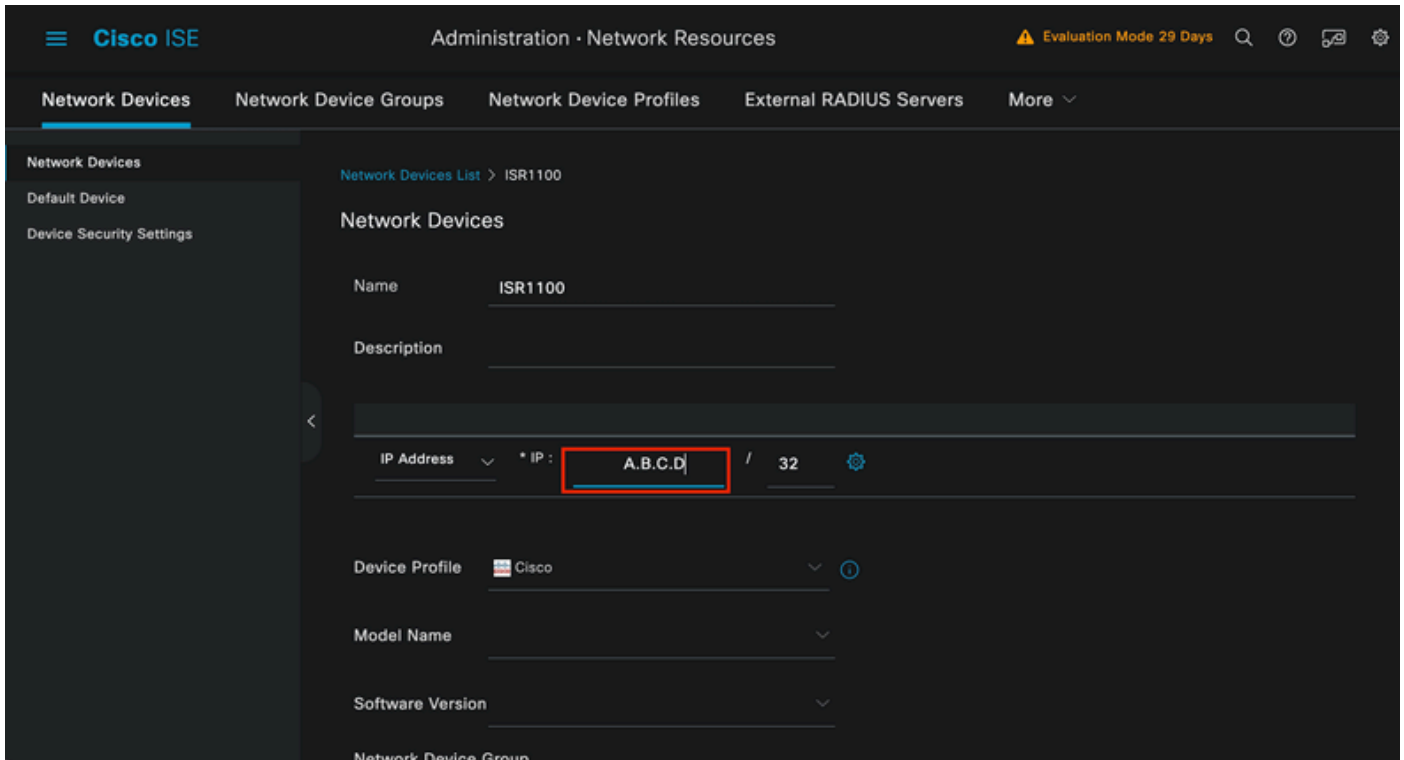
Agregue el ISR NAD a ISE Administration > Network Resources > Network Devices.

Haga clic en Add (Agregar).



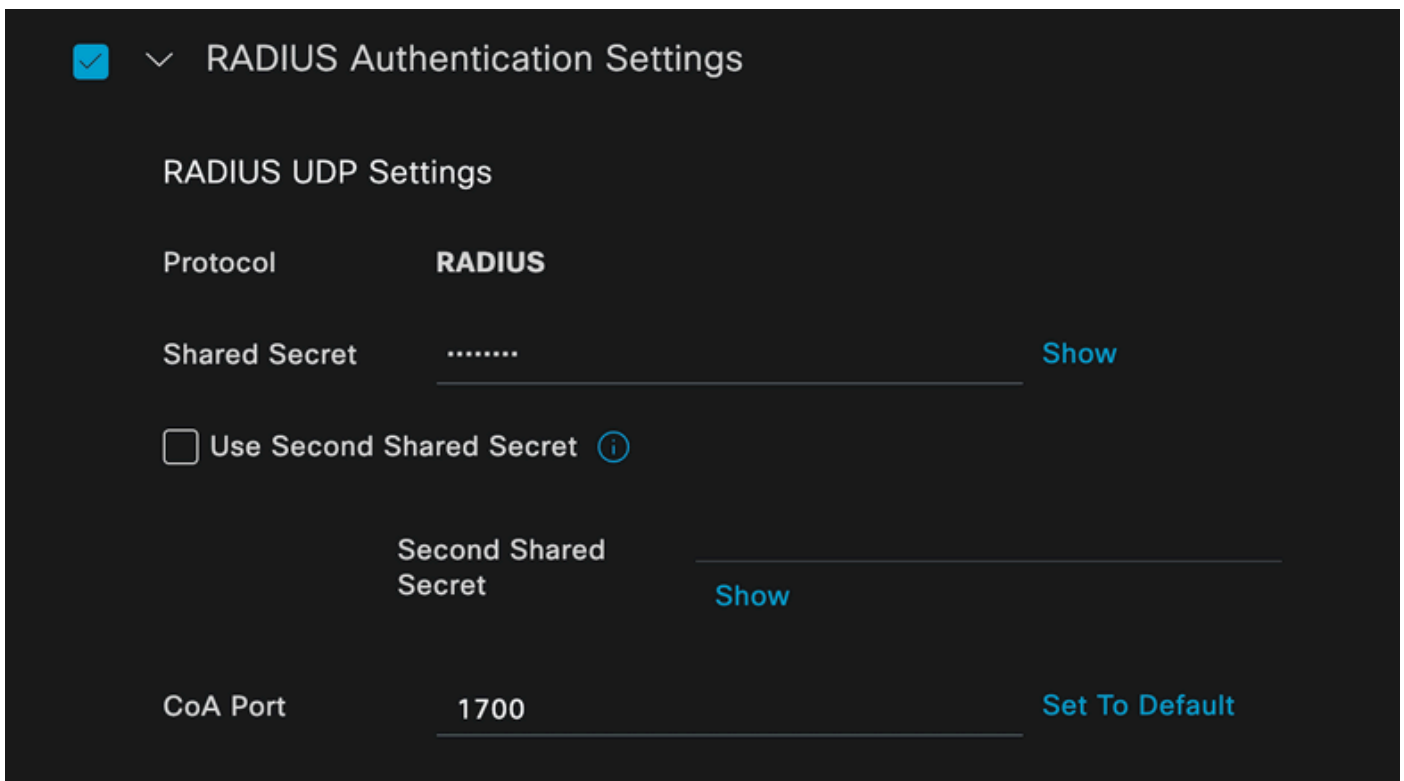
Sección Dispositivo de red

Asigne un nombre al NAD que está creando. Agregue la IP del dispositivo de red.



Creación de dispositivos de red

En la parte inferior de la misma página, agregue la misma clave secreta compartida que utilizó en la configuración del dispositivo de red.



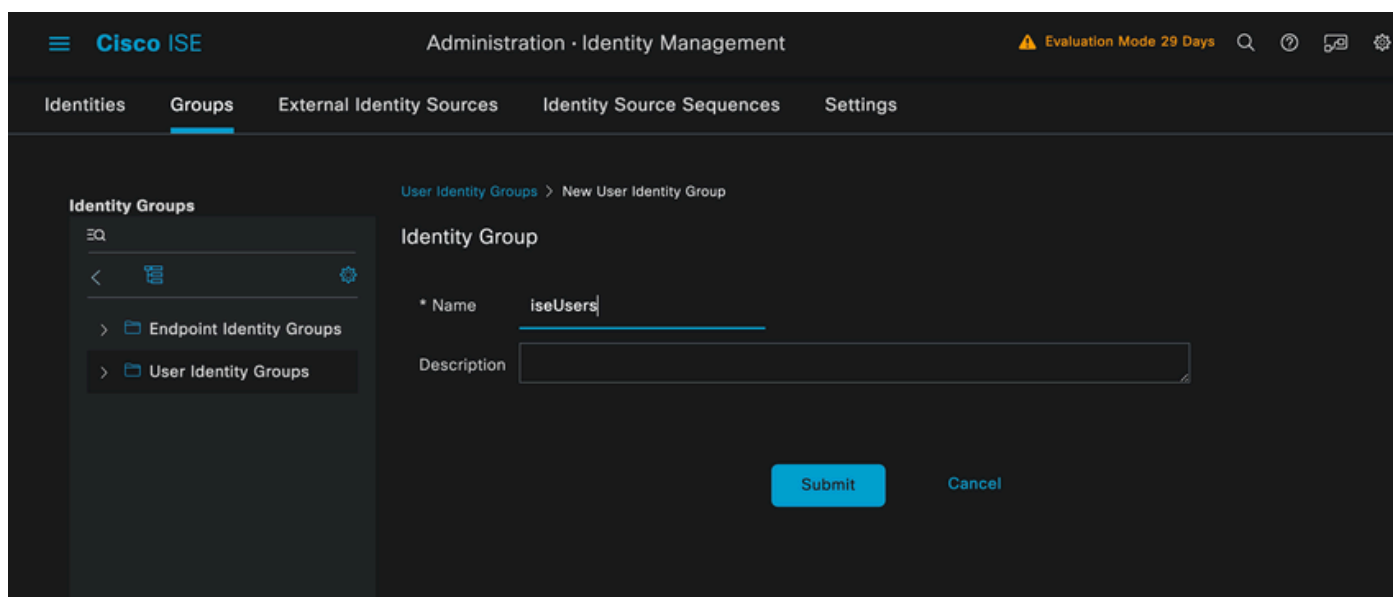
Configuración de RADIUS del dispositivo de red

Guarde los cambios.

Configure la identidad que se utiliza para autenticar el extremo.

Se utiliza la autenticación local de ISE. La autenticación externa de ISE no se explica en este artículo.

Vaya a la pestaña Administration > Identity Management > Groups y cree el grupo del que el usuario forma parte. El grupo de identidad creado para esta demostración es iseUsers.



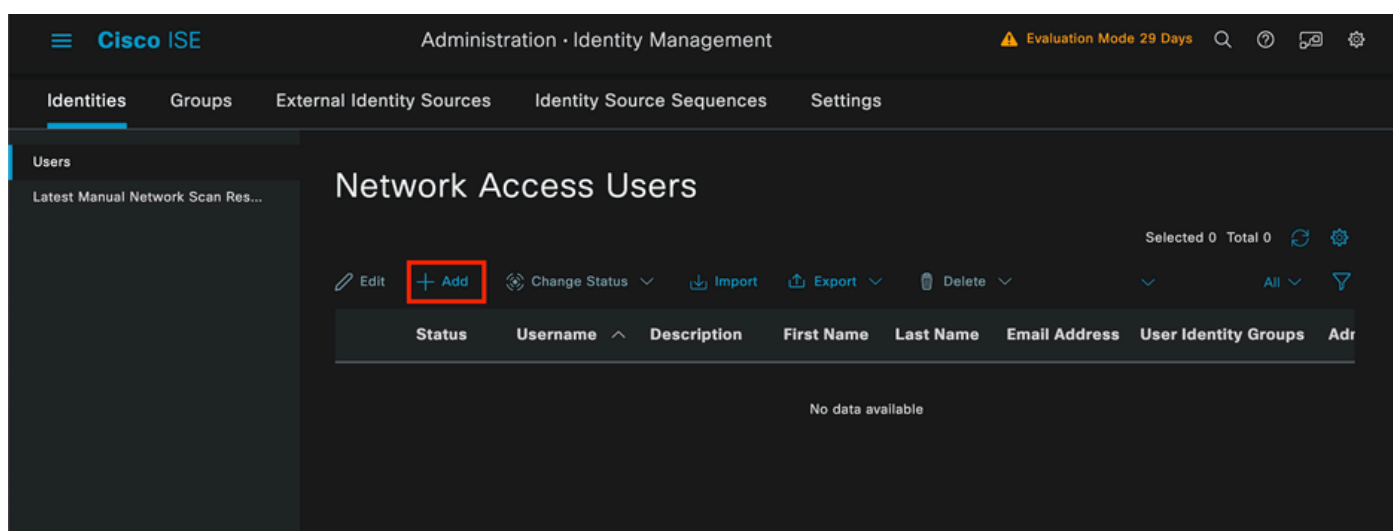
The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE', 'Administration · Identity Management', and 'Evaluation Mode 29 Days'. The main navigation tabs are 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'Groups' tab is selected. On the left, there is a sidebar for 'Identity Groups' with a search bar and a tree view showing 'Endpoint Identity Groups' and 'User Identity Groups'. The main content area is titled 'User Identity Groups > New User Identity Group' and 'Identity Group'. It contains a form with two fields: '* Name' (filled with 'iseUsers') and 'Description' (empty). At the bottom right of the form are 'Submit' and 'Cancel' buttons.

Creación de grupos de identidad

Haga clic en Submit (Enviar).

Vaya a Administration > Identity Management > Identity Tab.

Haga clic en Add (Agregar).



The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE', 'Administration · Identity Management', and 'Evaluation Mode 29 Days'. The main navigation tabs are 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'Identities' tab is selected. On the left, there is a sidebar for 'Users' with a search bar and a list of users. The main content area is titled 'Network Access Users'. It contains a toolbar with buttons for 'Edit', '+ Add', 'Change Status', 'Import', 'Export', and 'Delete'. Below the toolbar is a table with columns: 'Status', 'Username', 'Description', 'First Name', 'Last Name', 'Email Address', 'User Identity Groups', and 'Adr'. The table is currently empty, with the text 'No data available' displayed below it.

Sección Usuarios de Acceso a Red

Como parte de los campos obligatorios, empiece por el nombre del usuario. En este ejemplo se utiliza el nombre de usuario iseiscool.

Network Access User

* Username

Status Enabled ▼

Account Name Alias ⓘ

Email

Creación de usuario de acceso a red

Asigne una contraseña al usuario. Se utiliza VainillaISE97.

Passwords

Password Type: ▼

Password Lifetime:

- With Expiration ⓘ
Password will expire in 60 days
- Never Expires ⓘ

Password

Re-Enter Password

* Login Password

Generate Password ⓘ

Enable Password

Generate Password ⓘ

Sección Contraseña de Creación de Usuario

Asigne el usuario al grupo iseUsers.

User Groups

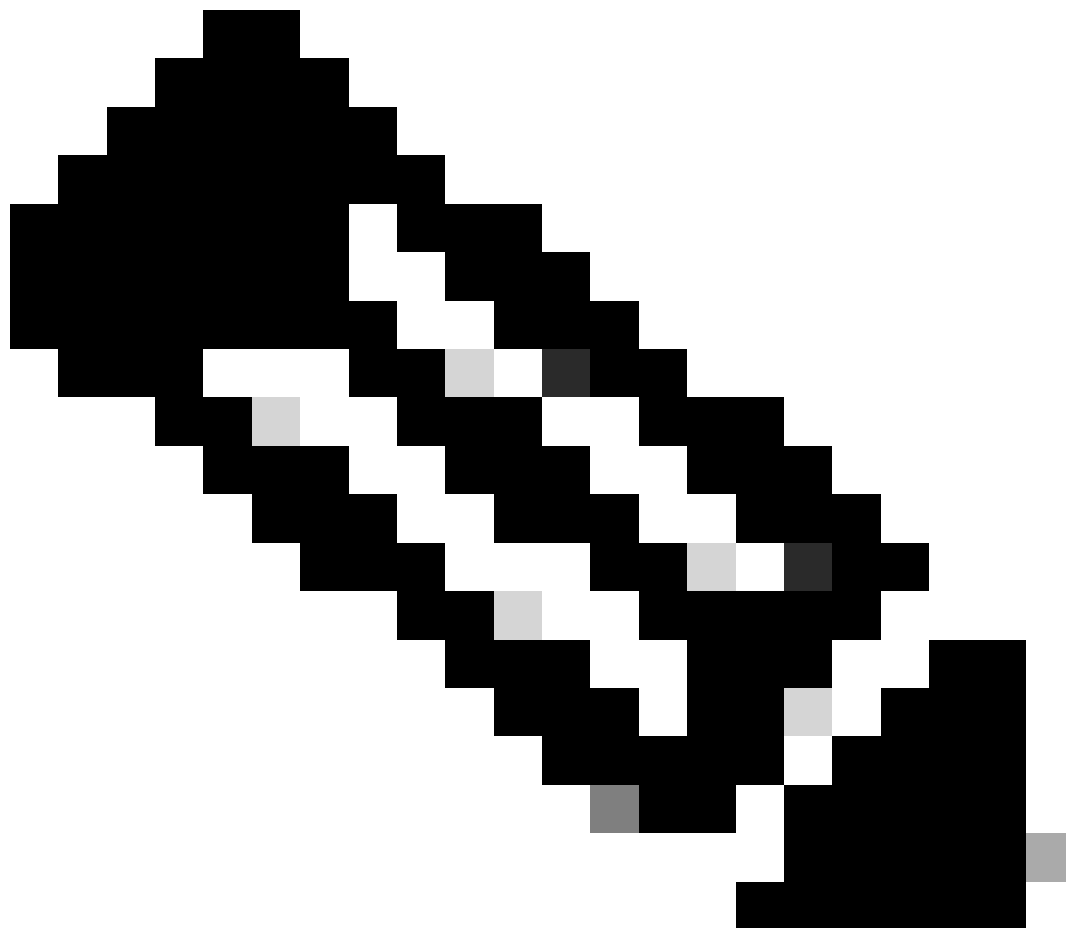
ⓘ +

Asignación de grupo de usuarios

Configure el conjunto de directivas.

Vaya al menú de ISE > Política > Conjuntos de políticas.

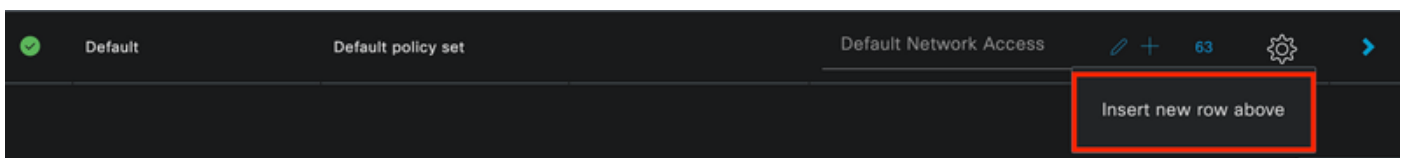
Se puede utilizar el conjunto de políticas predeterminado. Sin embargo, se crea una llamada Wired para este ejemplo.



Nota: la clasificación y diferenciación de los conjuntos de políticas ayuda a la hora de solucionar problemas,

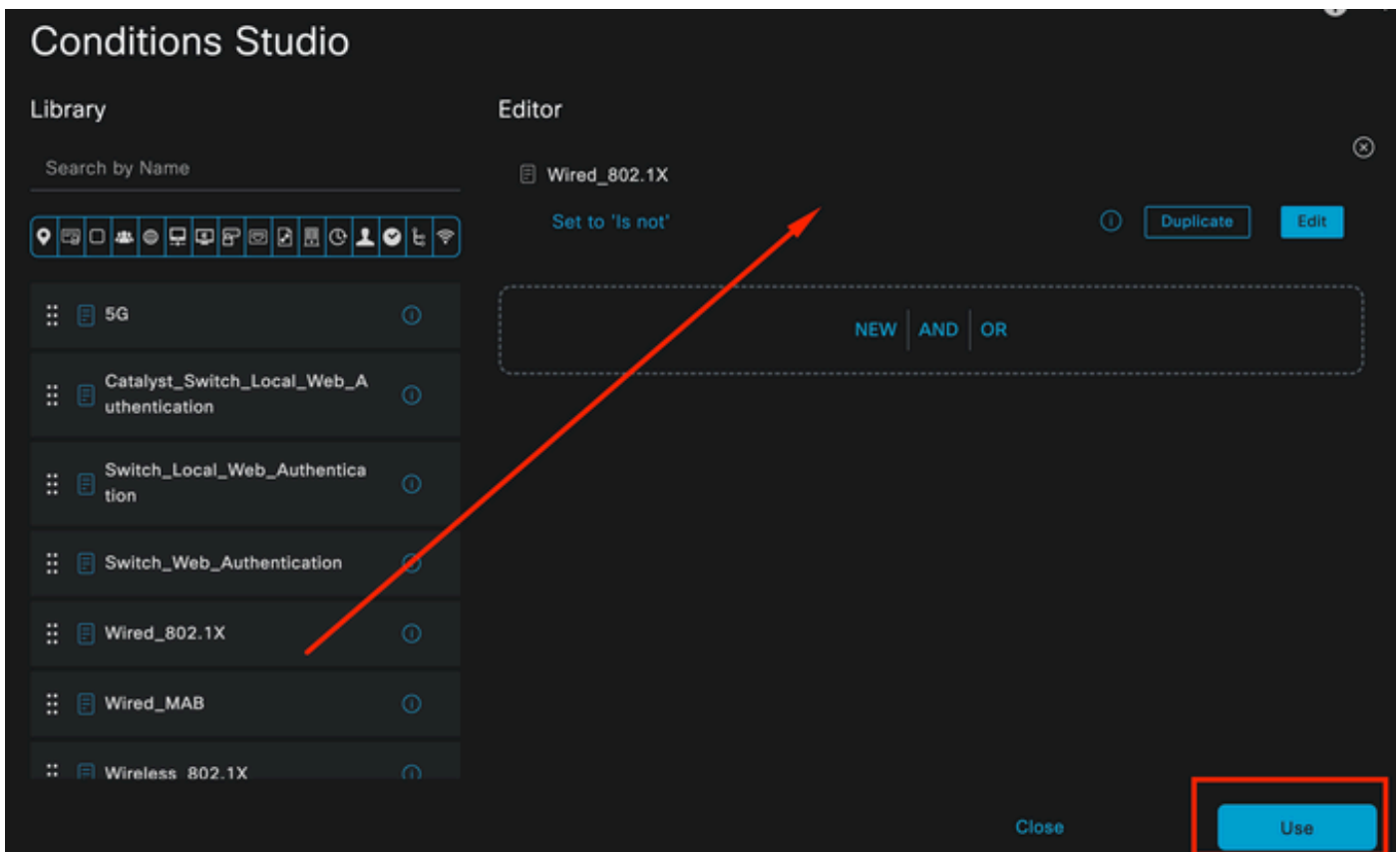


Nota: Si el icono de añadir o más no está visible, se puede hacer clic en el icono de engranaje de cualquier conjunto de directivas y, a continuación, seleccionar Insertar nueva fila encima.



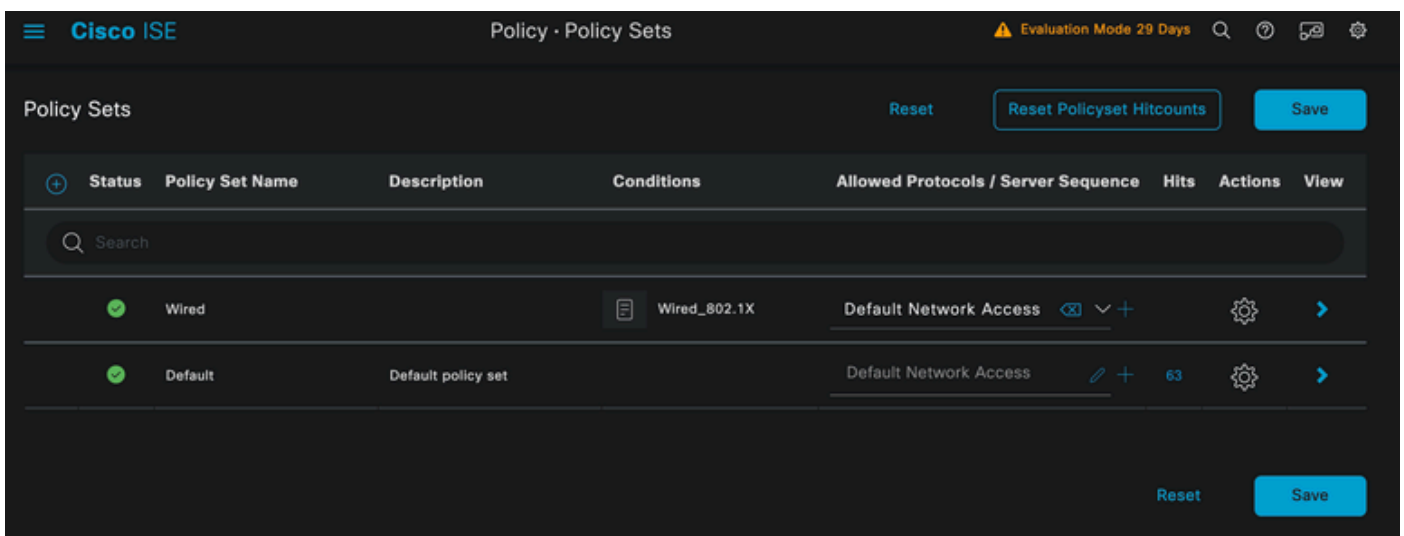
Opciones de iconos de engranajes

La condición utilizada es Wired 8021x. Arrástrelo y, a continuación, haga clic en Usar.



Authentication Policy Condition Studio

Seleccione Default Network Access en la sección Allowed Protocols.



Vista general de conjuntos de políticas

Click Save.

2.d. Configure las directivas de autenticación y autorización.

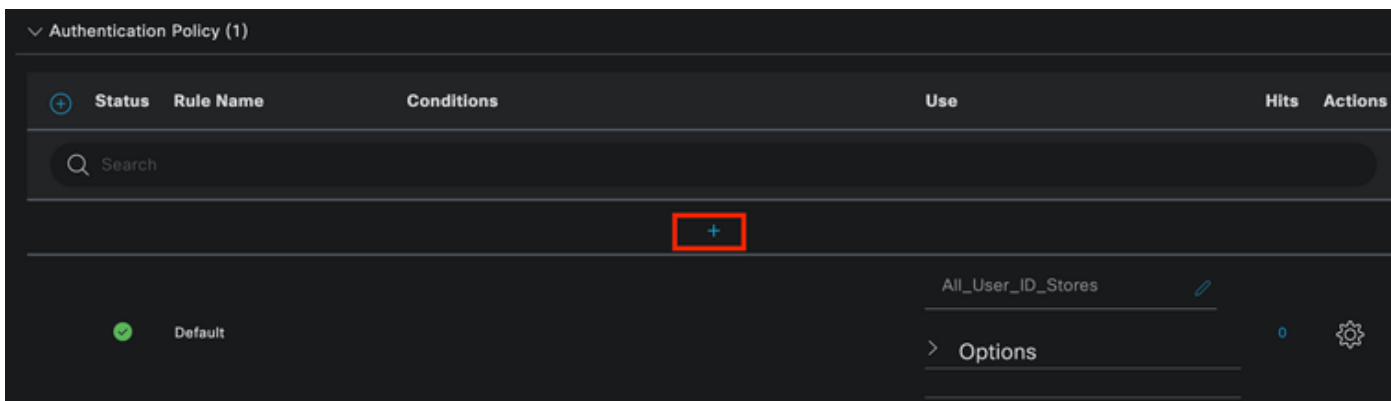
Haga clic en el icono >.



Conjunto de políticas por cable

Expanda la sección Política de autenticación.

Haga clic en el icono +.



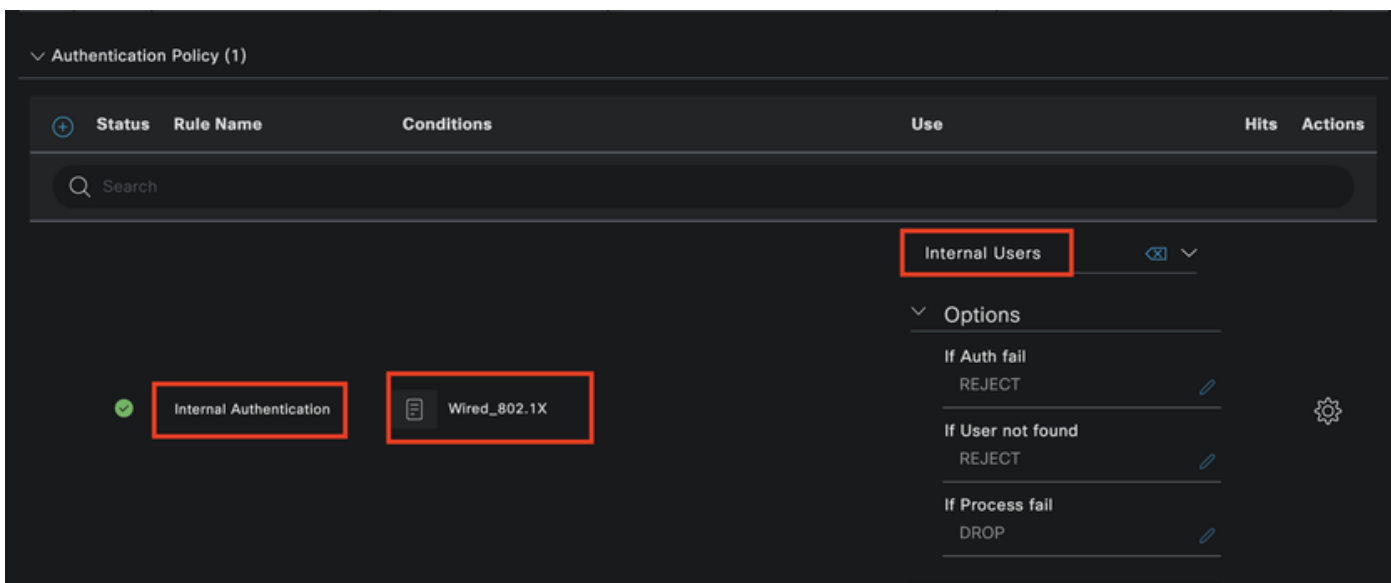
Política de autenticación

Asigne un nombre a la política de autenticación. La autenticación interna se utiliza en este ejemplo.

Haga clic en el icono + en la columna de condiciones para esta nueva política de autenticación.

Se utiliza la condición preconfigurada Wired Dot1x.

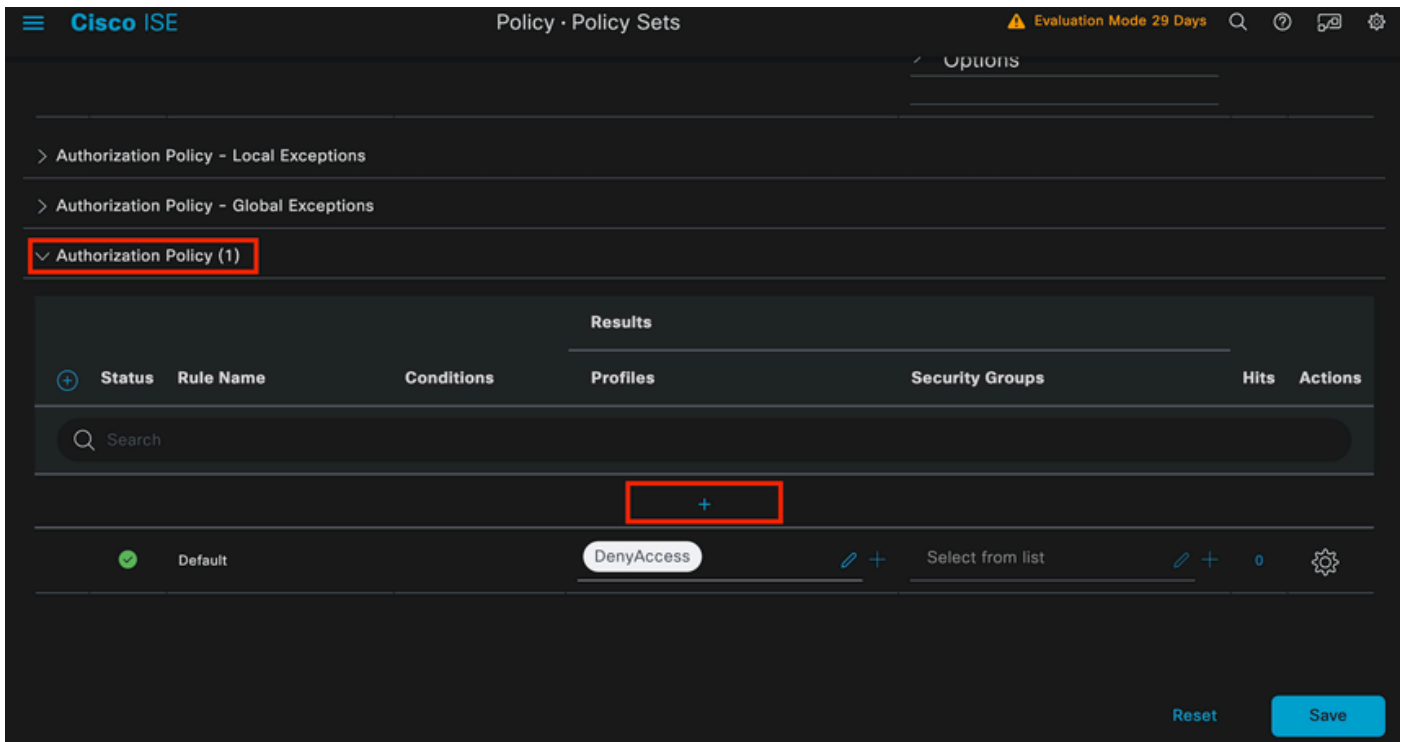
Por último, en la columna Use, seleccione Internal Users.



Política de autenticación

Directiva de autorización.

La sección Política de autorización se encuentra en la parte inferior de la página. Expanda el icono y haga clic en el icono +.



Política de autorización

Asigne un nombre a la directiva de autorización creada recientemente. En este ejemplo de configuración se utiliza el nombre Internal ISE Users.

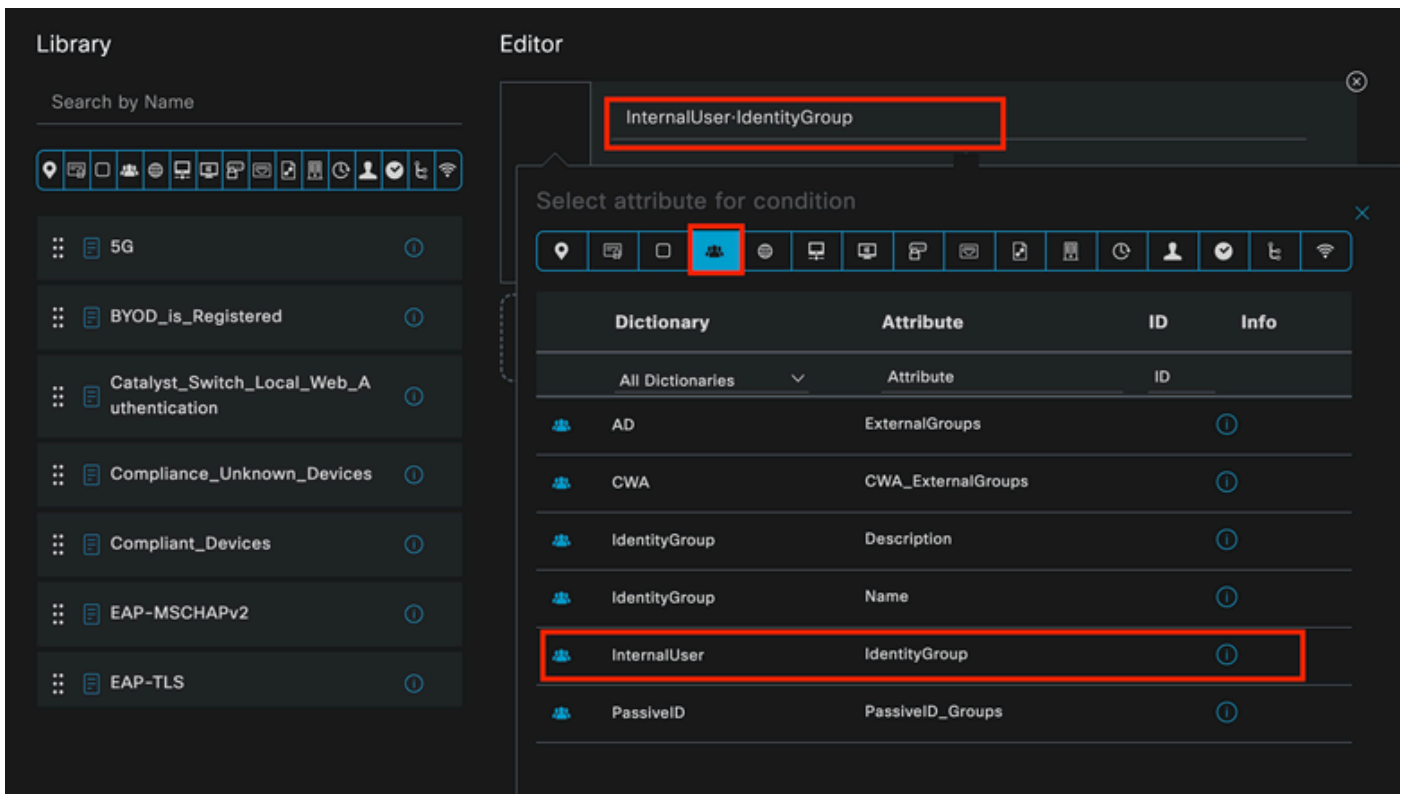
Para crear una condición para esta directiva de autorización, haga clic en el icono + de la columna Condiciones.

Se utiliza el grupo IseUsers.

Haga clic en la sección Atributo.

Seleccione el icono IdentityGroup.

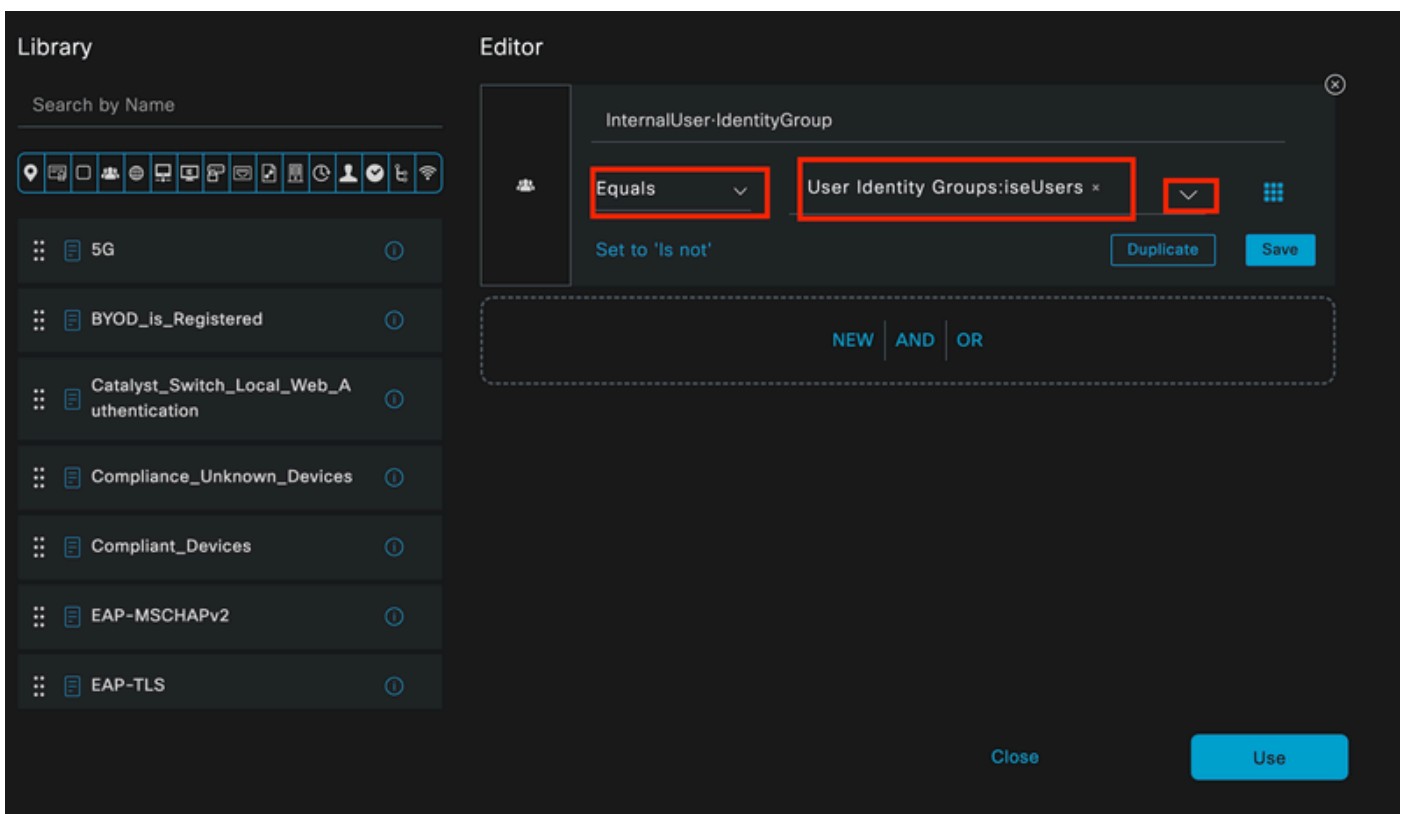
En el diccionario, seleccione el diccionario InternalUser que viene con el atributo IdentityGroup.



Creación de condiciones

Seleccione el operador Equals.

En User Identity Groups, seleccione el grupo IseUsers.

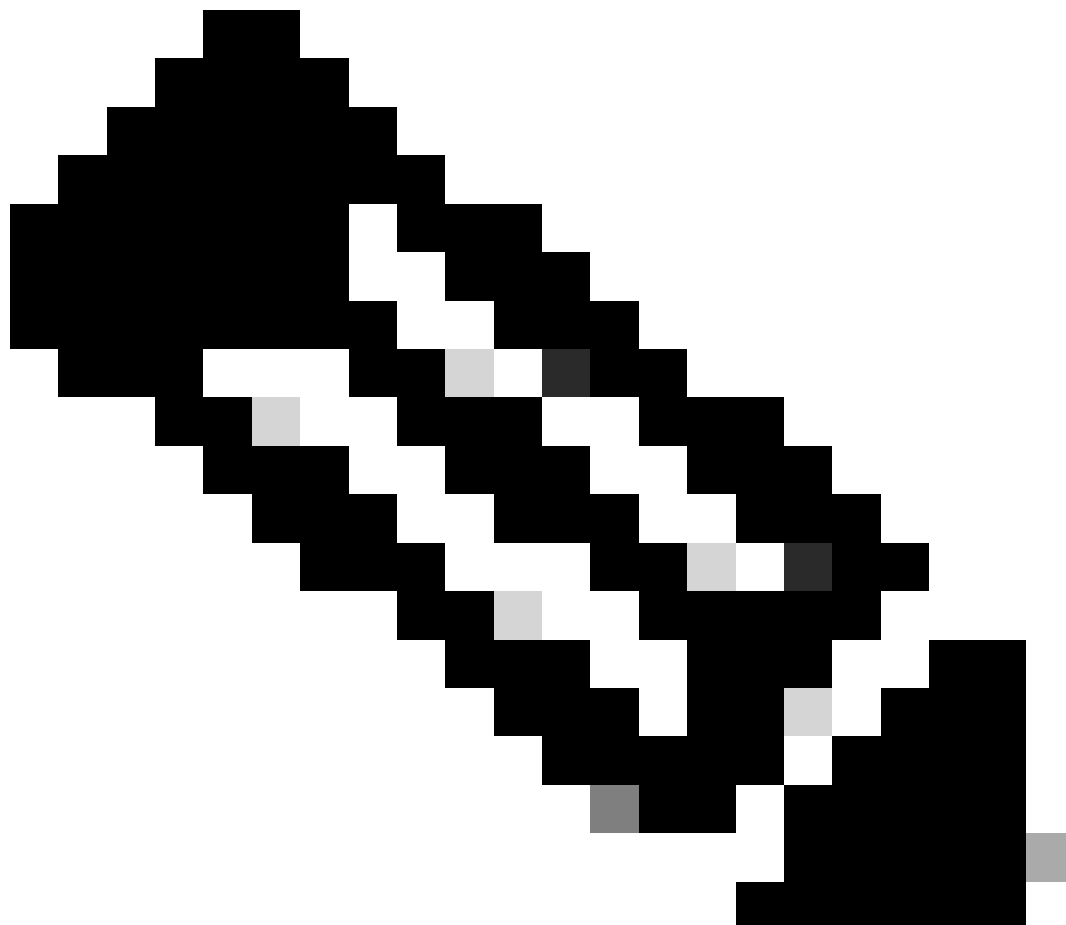


Creación de condiciones

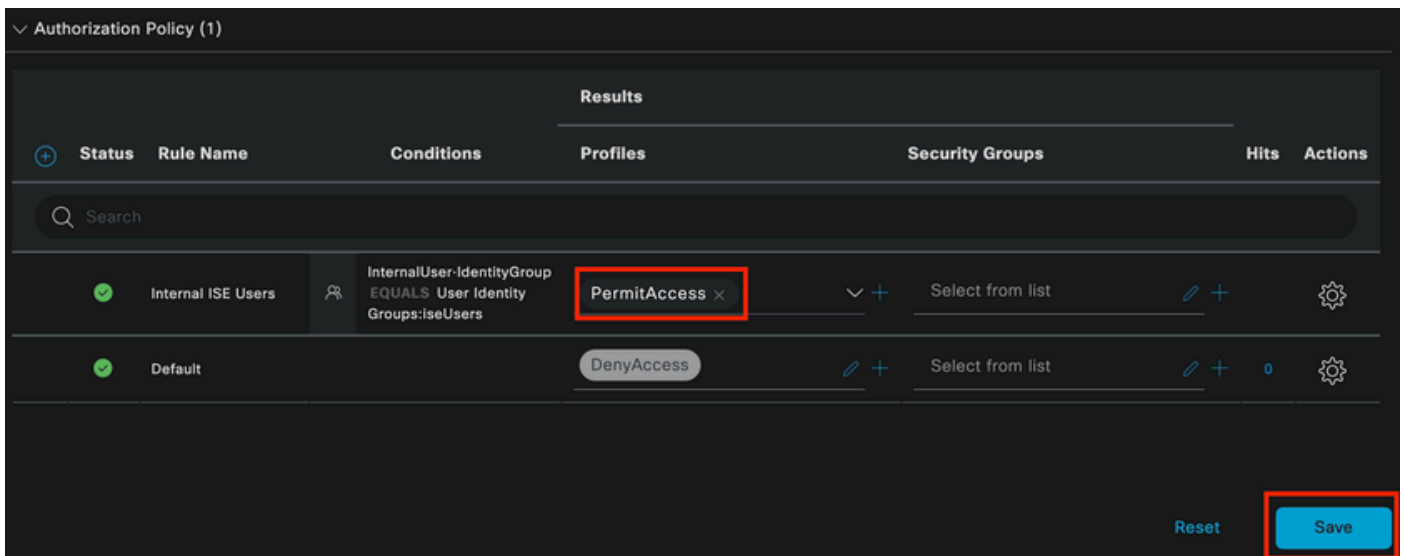
Haga clic en Usar.

Agregue el perfil de autorización de resultados.

Se utiliza el perfil preconfigurado Permit Access.



Nota: Tenga en cuenta que las autenticaciones que llegan a ISE y que llegan a este conjunto de políticas de punto 1x cableado que no forman parte de los usuarios ISEU del grupo de identidad de usuarios, llegan a la política de autorización predeterminada, que tiene como resultado DenyAccess.



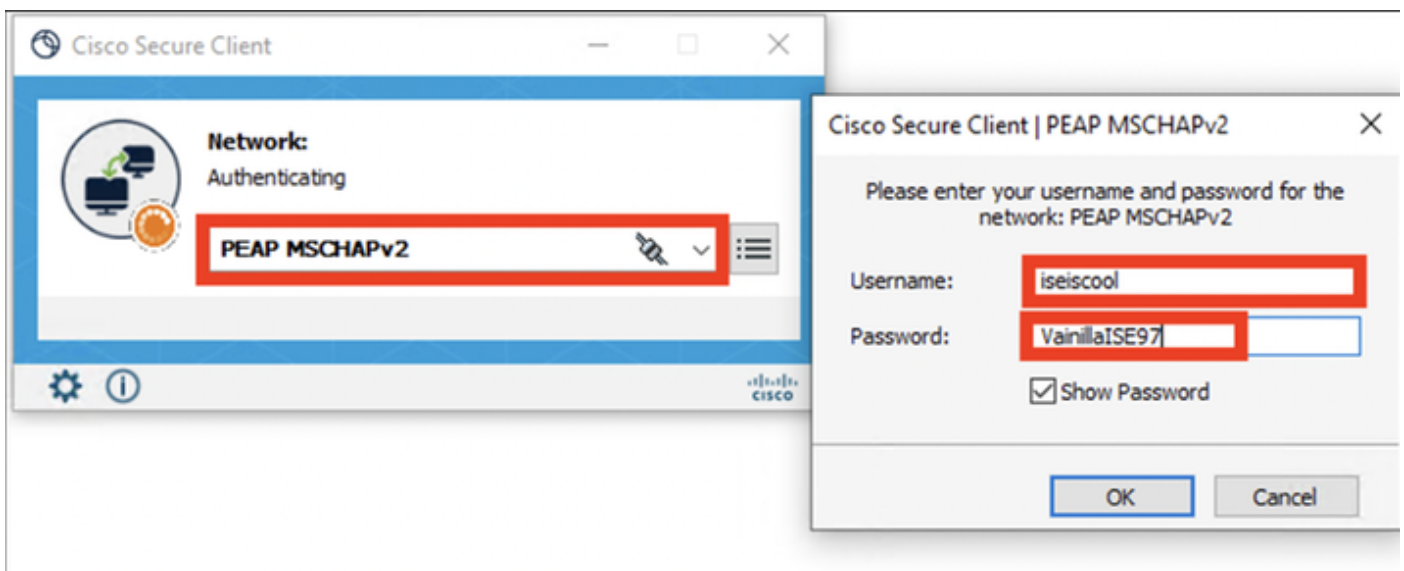
Política de autorización

Click Save.

Verificación

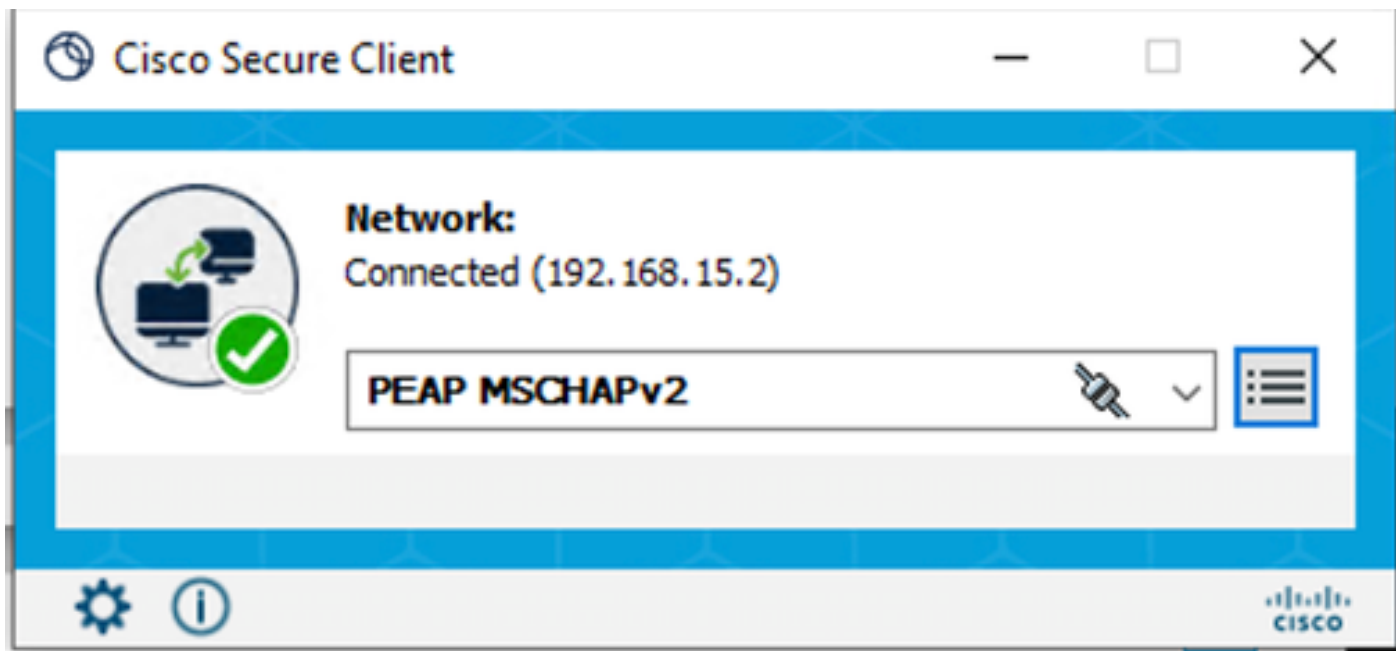
Una vez finalizada la configuración, Secure Client solicita las credenciales y especifica el uso del perfil PEAP MSCHAPv2.

Se introducen las credenciales creadas anteriormente.



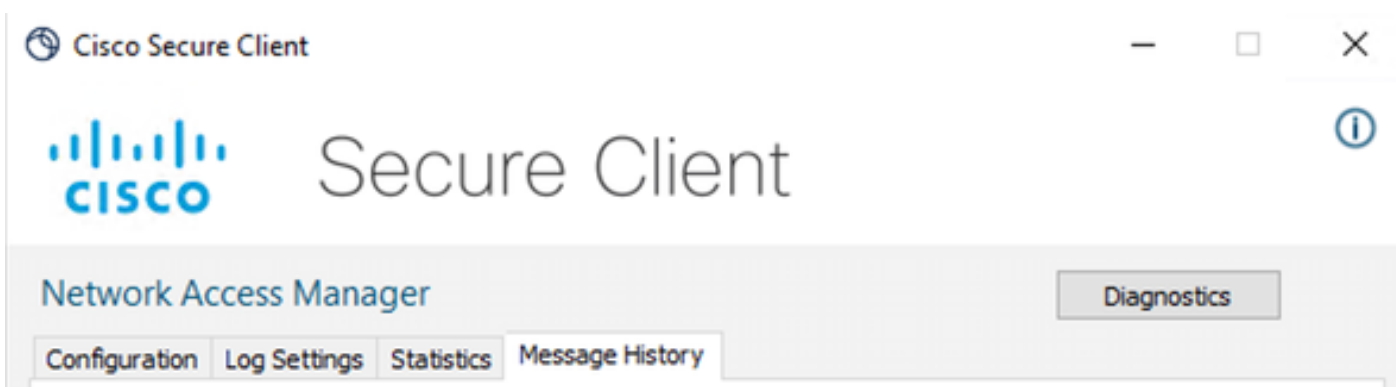
NAM de cliente seguro

Si el punto final se autentica correctamente,. NAM muestra que está conectado.



NAM de cliente seguro

Al hacer clic en el icono de información y navegar a la sección Historial de Mensajes, se muestran los detalles de cada paso que NAM realizó.



Historial de mensajes de Secure Client

```
7:06:01 PM PEAP MSCHAPv2 : Authenticating
7:06:21 PM PEAP MSCHAPv2 : Acquiring IP Address
7:06:21 PM PEAP MSCHAPv2 : Connected
```

Historial de mensajes de Secure Client

En ISE, vaya a Operations > Radius LiveLogs para ver los detalles de la autenticación. Como se ve en la siguiente imagen, se muestra el nombre de usuario que se utilizó.

También otros detalles como:

- Grupo fecha/hora.
- Dirección MAC.
- Conjunto de políticas utilizado.
- Política de autenticación.

- Directiva de autorización.
- Otra información pertinente.

The screenshot shows the Cisco ISE Operations - RADIUS interface. At the top, there are five summary cards: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (25), Client Stopped Responding (0), and Repeat Counter (0). Below these cards is a table with columns: Time, Status, Details, Repea..., Identity, Endpoint ID, Endpoint..., Authentication Policy, Authorization Policy, Authoriz..., IP Address, and Network De... The table contains two rows of log entries. The first row shows a status of 'Success' (blue dot) and the second row shows a status of 'Success' (green checkmark). The table is updated as of Tue Apr 23 2024 13:02:14 GMT-0600 (Central Standard Time) and shows 2 records.

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication Policy	Authorization Policy	Authoriz...	IP Address	Network De...
Apr 23, 2024 06:38:07.0...	Success		0	iselscool	8C:16:45:00:F4...	Unknown	Wired >> Internal Authentication	Wired >> Internal ISE Users	PermitAcc...		
Apr 23, 2024 06:38:06.8...	Success			iselscool	8C:16:45:00:F4...	Unknown	Wired >> Internal Authentication	Wired >> Internal ISE Users	PermitAcc...		ISR1100

Registros en directo de ISE RADIUS

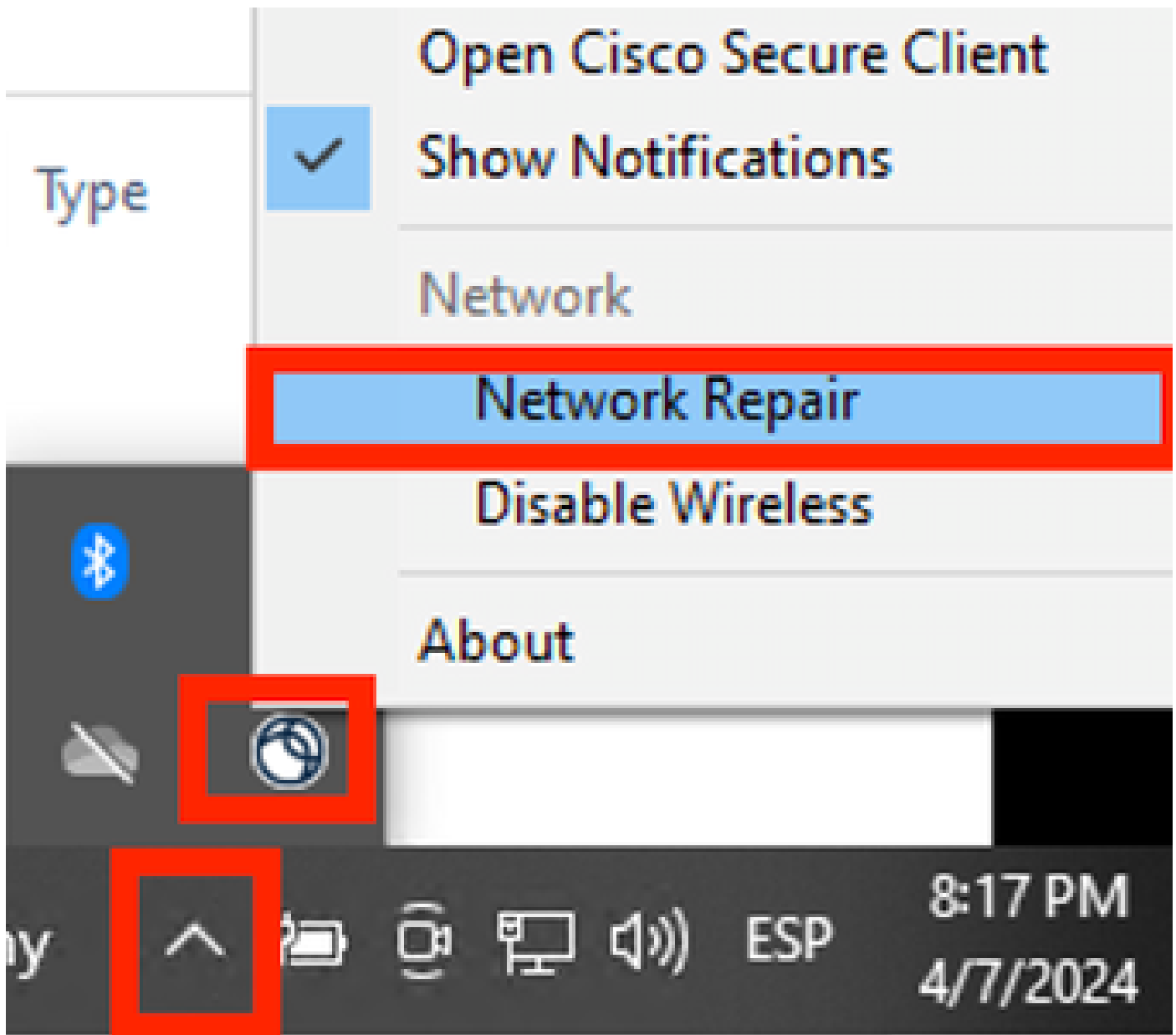
Como puede ver que llega a las políticas correctas, y el resultado es un estado de autenticación exitoso, se concluye que la configuración es correcta.

Troubleshoot

Problema: Secure Client no utiliza el perfil NAM.

Si el NAM no utiliza el nuevo perfil que se creó en el editor de perfiles, utilice la opción Network Repair para Secure Client.

Puede encontrar esta opción navegando hasta la Barra de Windows > Haciendo clic en el icono circumflex > Haga clic con el botón derecho en el icono Secure Client > Haga clic en Reparación de red.



Sección de reparación de red

Problema 2: Los registros deben recopilarse para realizar análisis adicionales.

1. Activar registro extendido NAM

Abra NAM y haga clic en el icono del engranaje.



Interfaz NAM

Vaya a la pestaña Log Settings. Marque la casilla de verificación Enable Extended Logging.

Establezca el tamaño del archivo de captura de paquetes en 100 MB.



Network Access Manager Diagnostics

Configuration Log Settings Statistics Message History

Use extended logging to collect additional information about product operations.

Enable Extended Logging

IHV:

Filter Driver:

Credential Provider

Packet Capture

Maximum Packet Capture File Size (MB):

Configuración de registro de NAM de cliente seguro

2. Reproduzca el problema.

Una vez habilitado el registro extendido, reproduzca el problema varias veces para asegurarse de que se generen los registros y se capture el tráfico.

3. Recopile el paquete DART de Secure Client.

En Windows, vaya a la barra de búsqueda y escriba Cisco Secure Client Diagnostics and Reporting Tool.



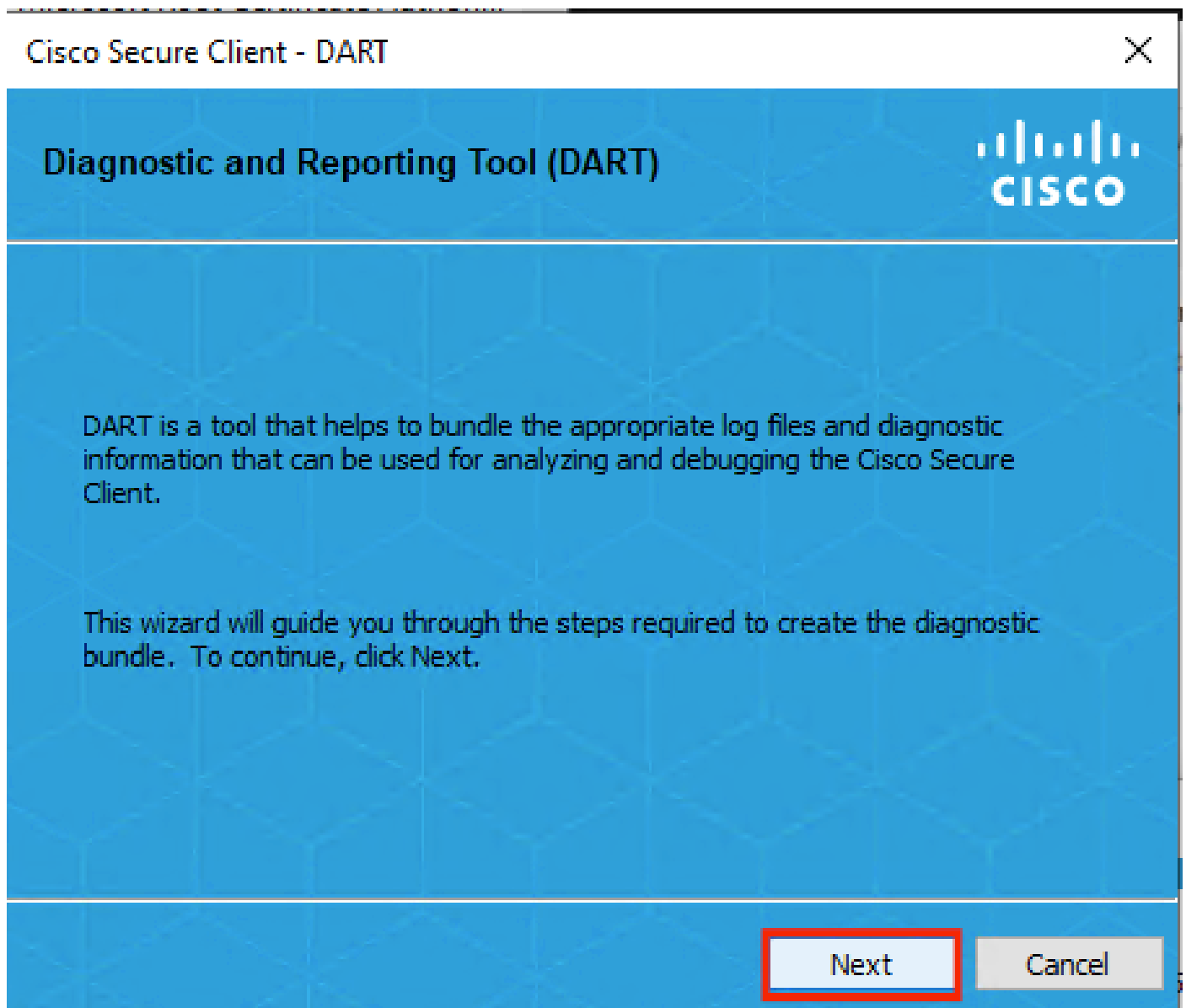
Cisco Secure Client Diagnostics and Reporting Tool

App

Módulo DART

Durante el proceso de instalación, también instaló este módulo. Es una herramienta que ayuda durante el proceso de solución de problemas mediante la recopilación de registros e información de sesión dot1x relevante.

Haga clic en Next en la primera ventana.




Módulo DART

Una vez más, haga clic en Next para guardar el paquete de registro en el escritorio.

Cisco Secure Client - DART




Bundle Creation Option 

Select "Default" to include the typical log files and diagnostic information in the bundle. Select "Custom" to choose the list of log files and diagnostic information to be included in the bundle.

Default - Bundle will be saved to Desktop

Custom

 DART requires administrative privileges to clear Cisco Secure Client logs.

[Clear All Logs](#)

[Back](#) [Next](#) [Cancel](#)

Módulo DART

Si es necesario, marque la casilla de verificación Enable Bundle Encryption.



Bundle Encryption Option



Enable Bundle Encryption

Mask Password

Encryption Password

Confirm Password

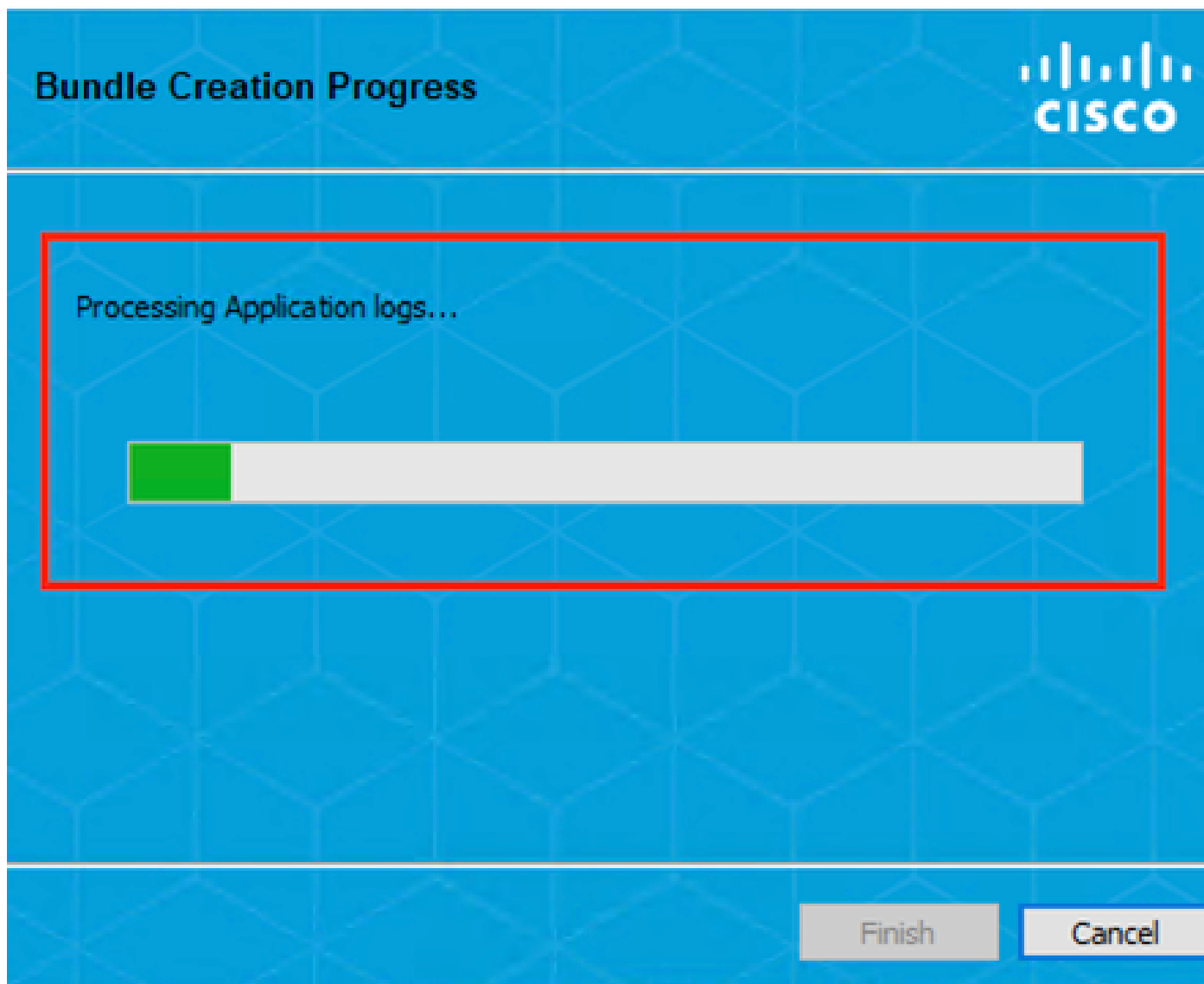
Back

Next

Cancel

Módulo DART

Se inicia la recopilación de registros DART.



Recopilación de registros DART

Puede tardar 10 minutos o más hasta que el proceso finalice.

Bundle Creation Result




The bundle was created successfully in C:\Users\LAB5\Desktop\DARTBundle_0423_1538.zip.

[Email Bundle](#)[Finish](#)

Resultado de creación del paquete DART

El archivo de resultados DART se encuentra en el directorio de escritorio.

Name	Date modified	Type
 DARTBundle_0423_1538	4/24/2024 1:14 PM	Compressed (zipped) Folder

Archivo de resultados DART

Información Relacionada

- [Soporte técnico y descargas de Cisco](#)

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).