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

Contenido

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.

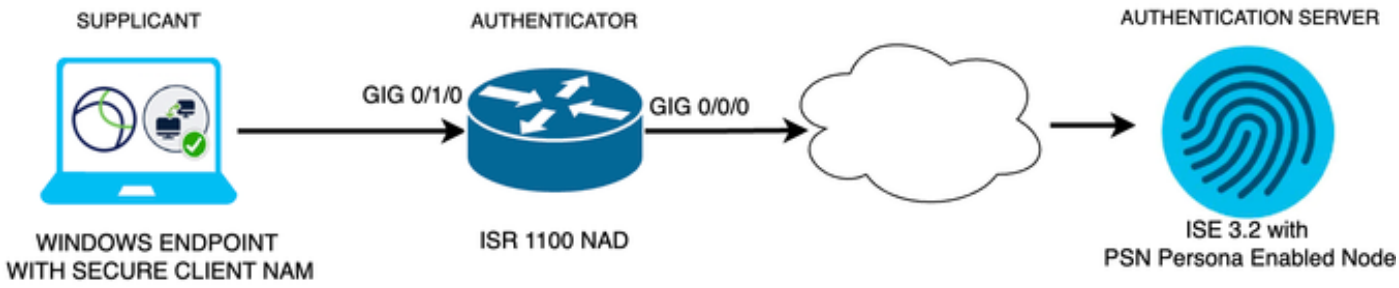


Diagrama de la red

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.

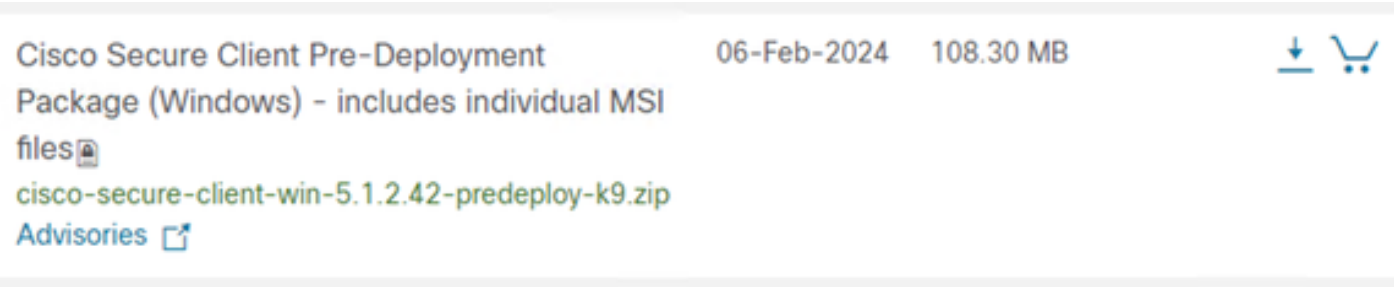
Inicio > Seguridad > VPN and Endpoint Security Clients > Secure Client (incluido AnyConnect) > Secure Client 5 > AnyConnect VPN Client Software.

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

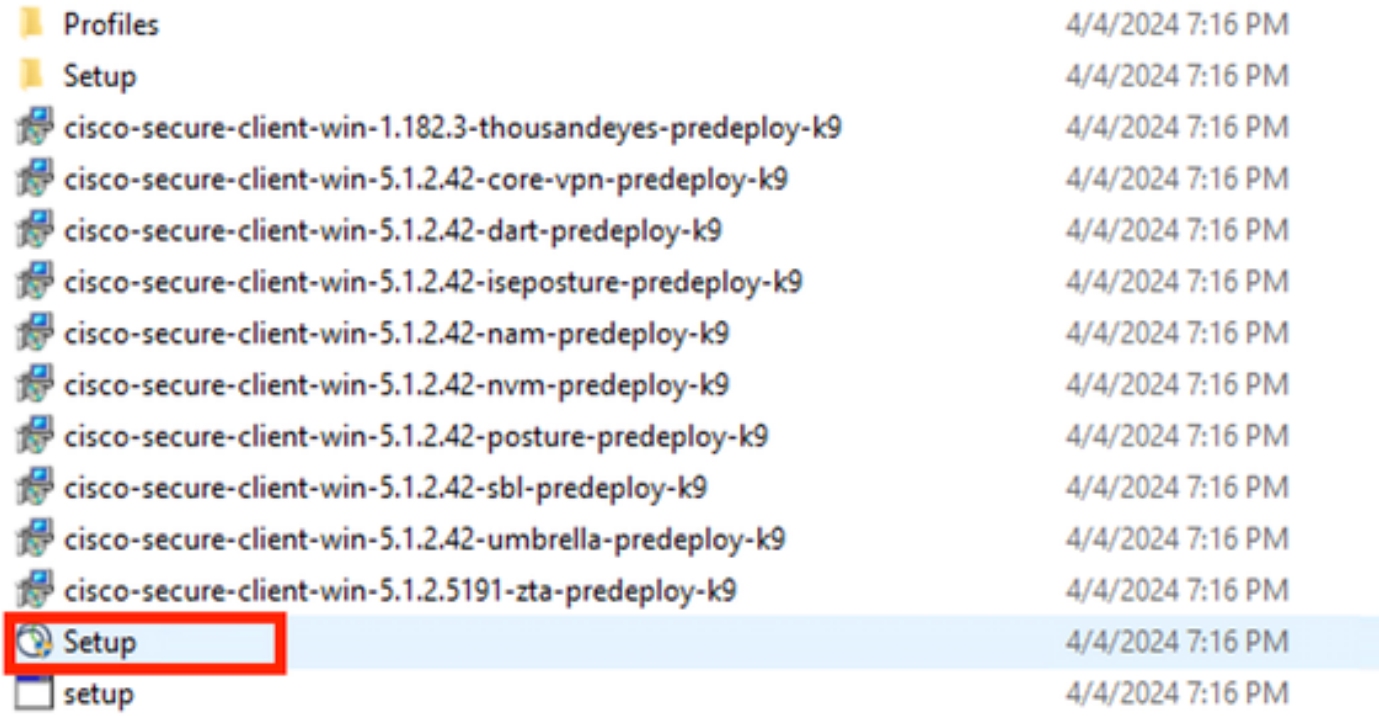
instalación utilizado es el método previo a la implementación.

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



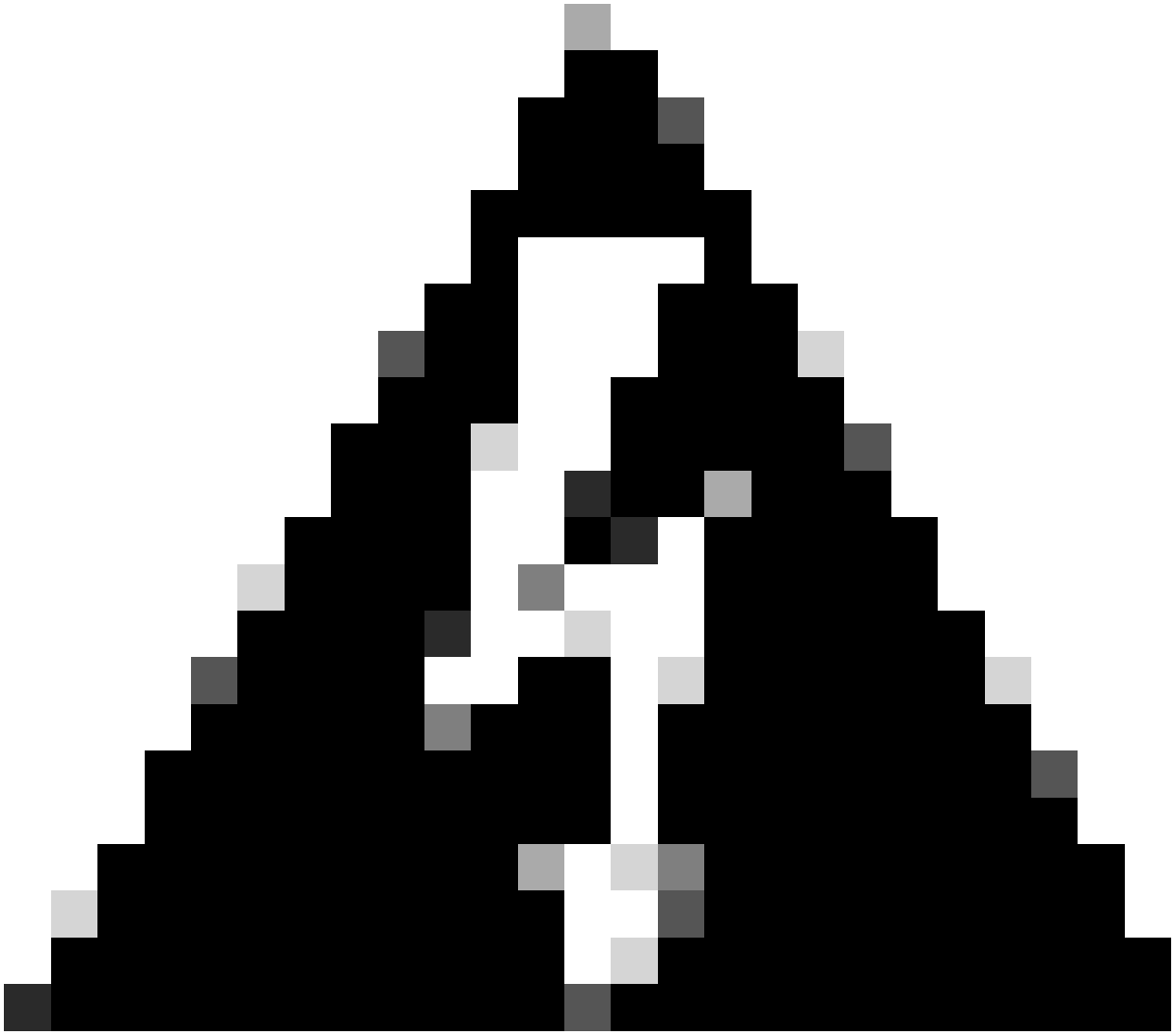
archivo zip Msi

Una vez descargado y extraído, haga clic en Setup.

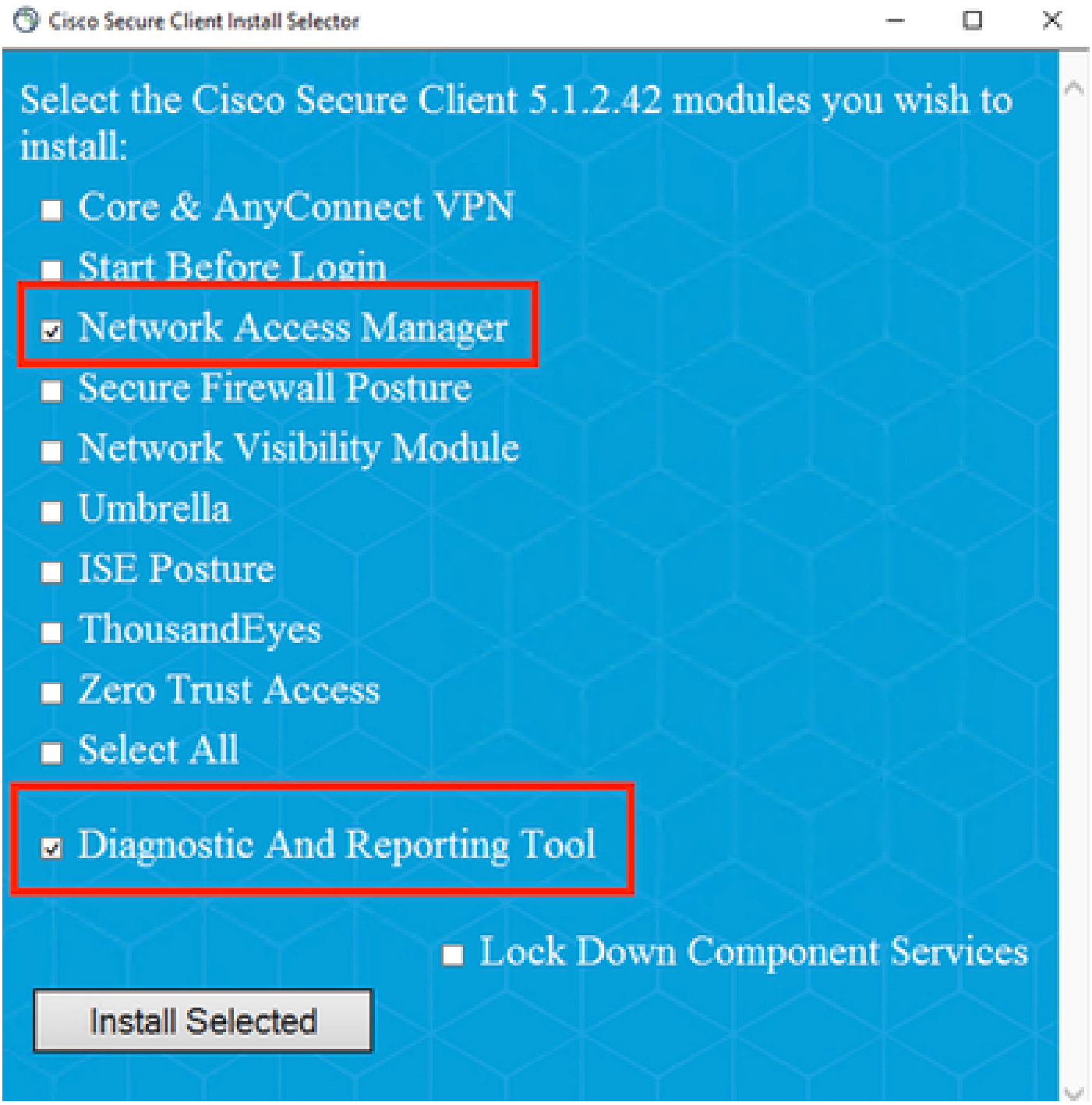


Archivos de Secure Client

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



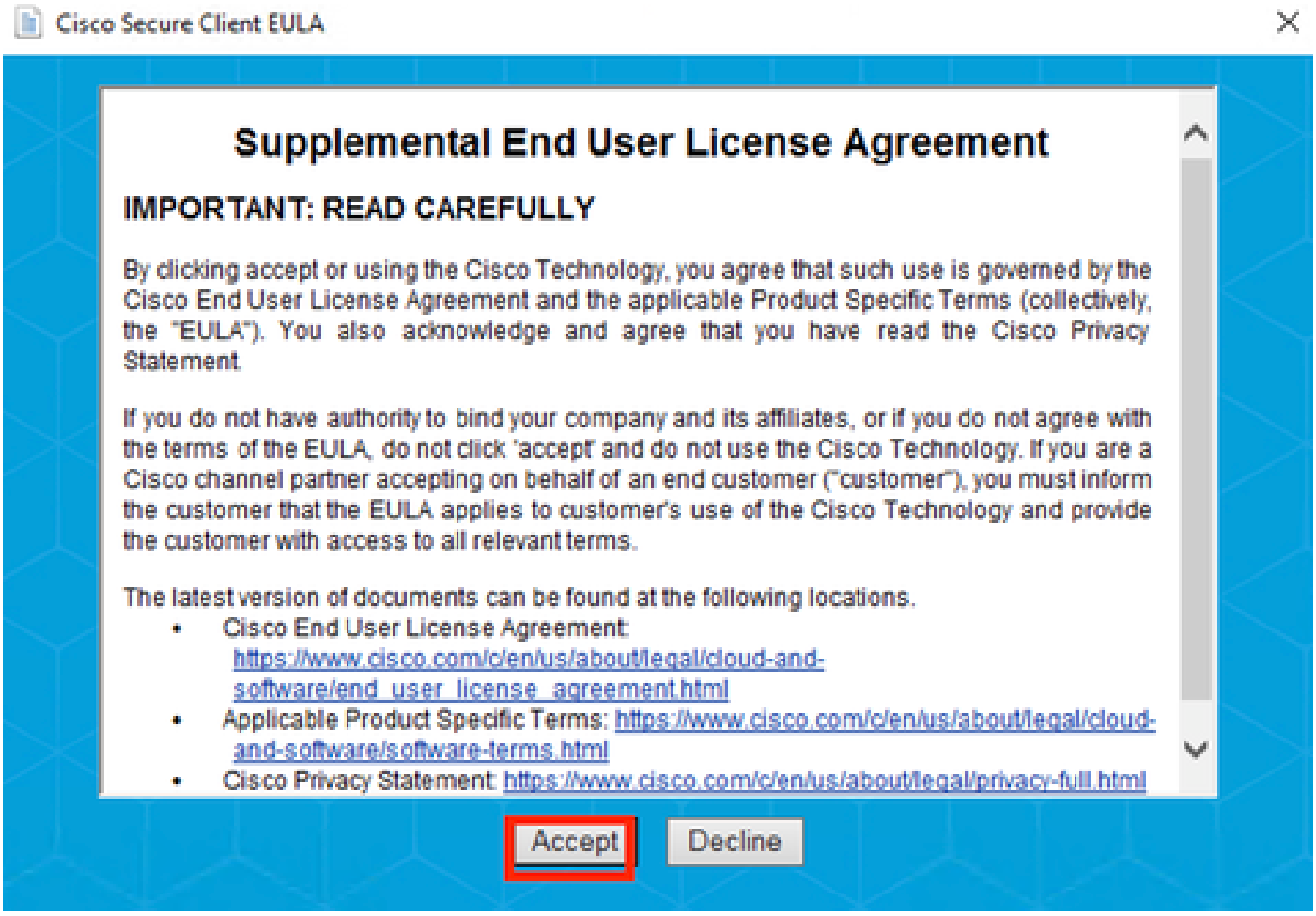
Advertencia: Si utiliza el Asistente de Cisco Secure Client, el módulo VPN se instala automáticamente y se oculta en la GUI. El NAM no funciona si el módulo VPN no está instalado. Si utiliza archivos MSI individuales o un método de instalación diferente, asegúrese de instalar el módulo VPN.



Selector de instalación

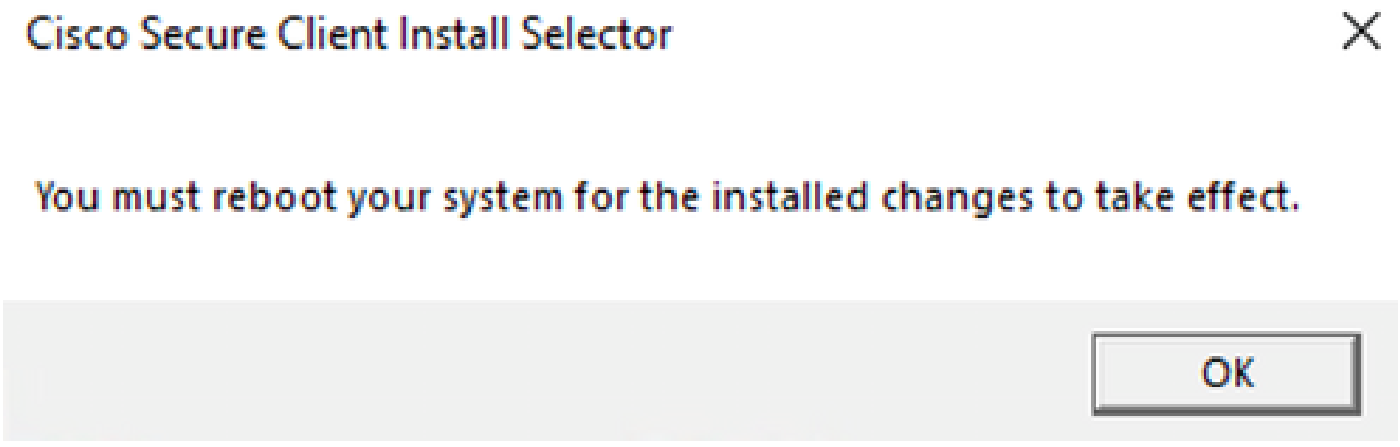
Haga clic en Instale la opción seleccionada.

Acepte el CLUF.



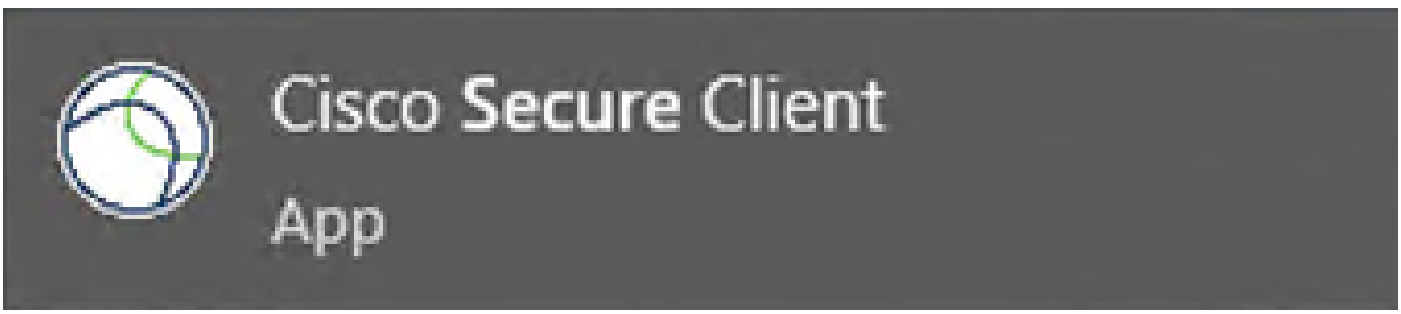
Ventana EULA

Es necesario reiniciar después de la instalación de NAM.



Ventana de requisitos de reinicio

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



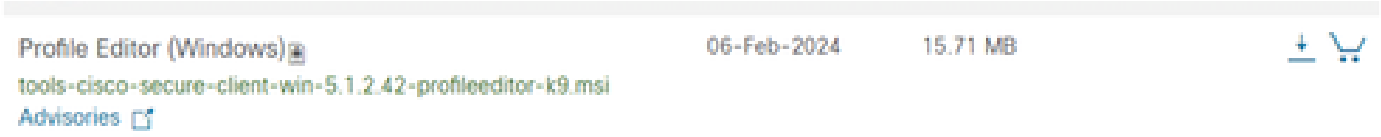
Programa Secure Client

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.



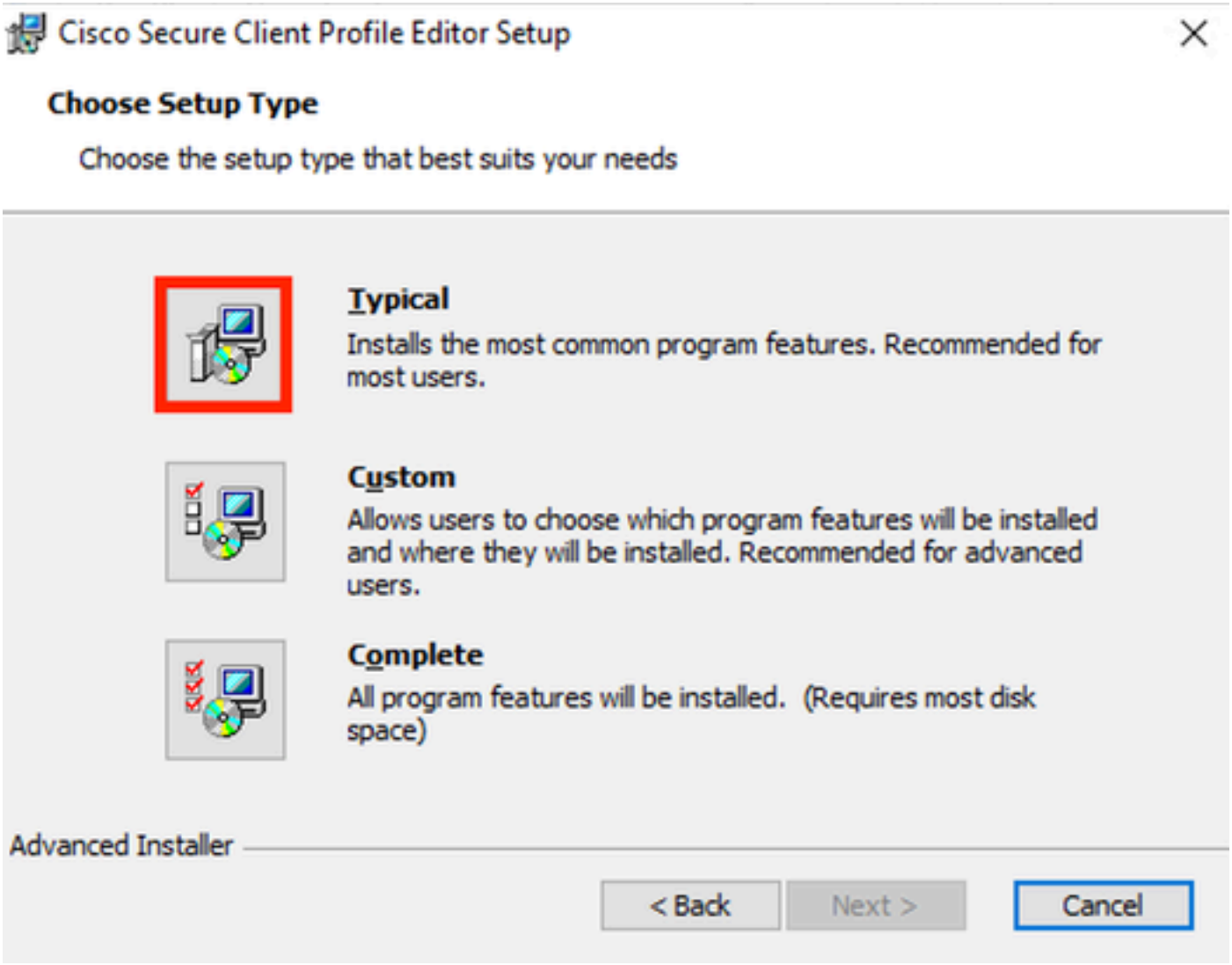
Editor de perfiles

Una vez descargado, continúe con la instalación.

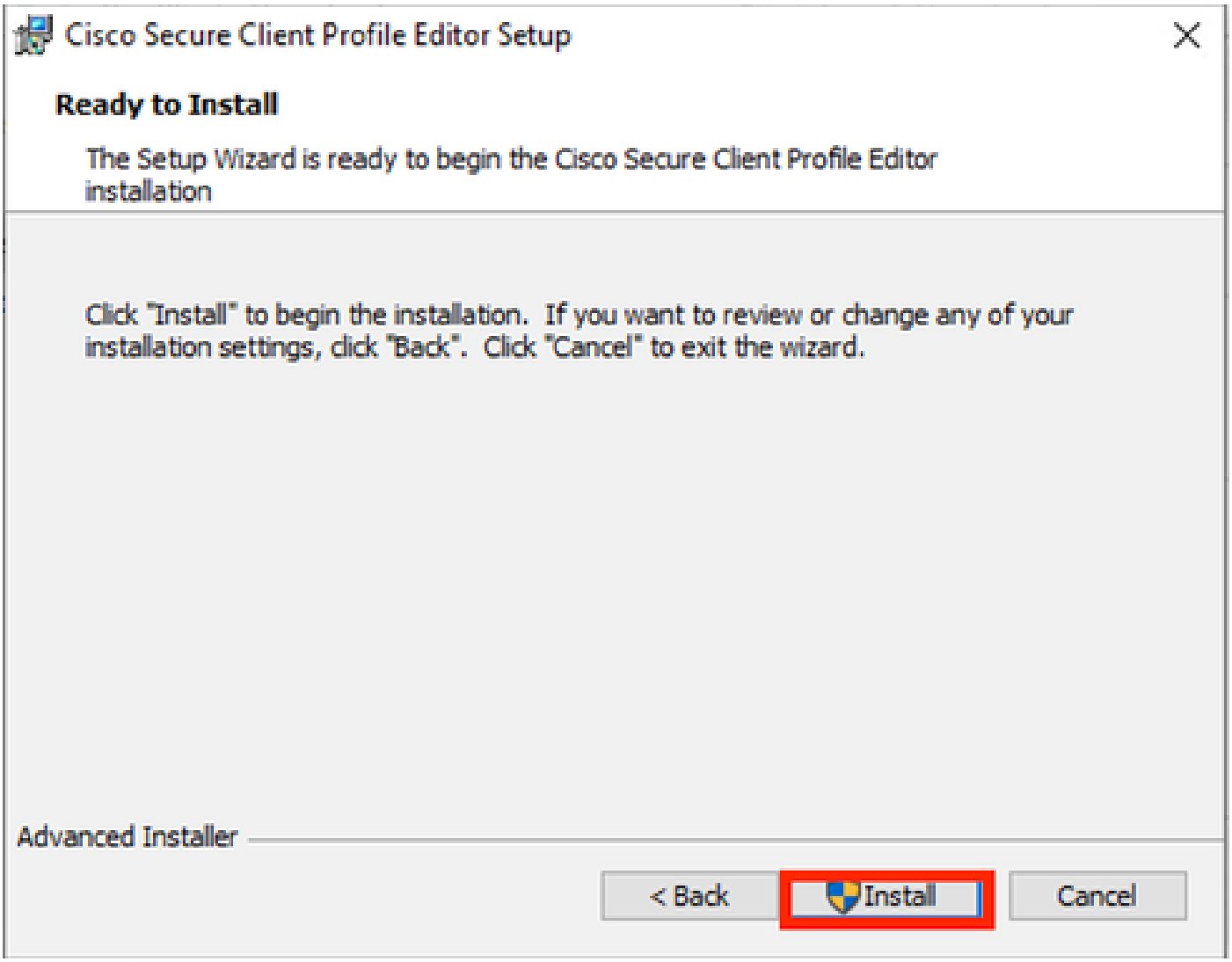
Ejecute el archivo msi.

Ventana de configuración del Editor de perfiles

Utilice la opción de configuración Típica.

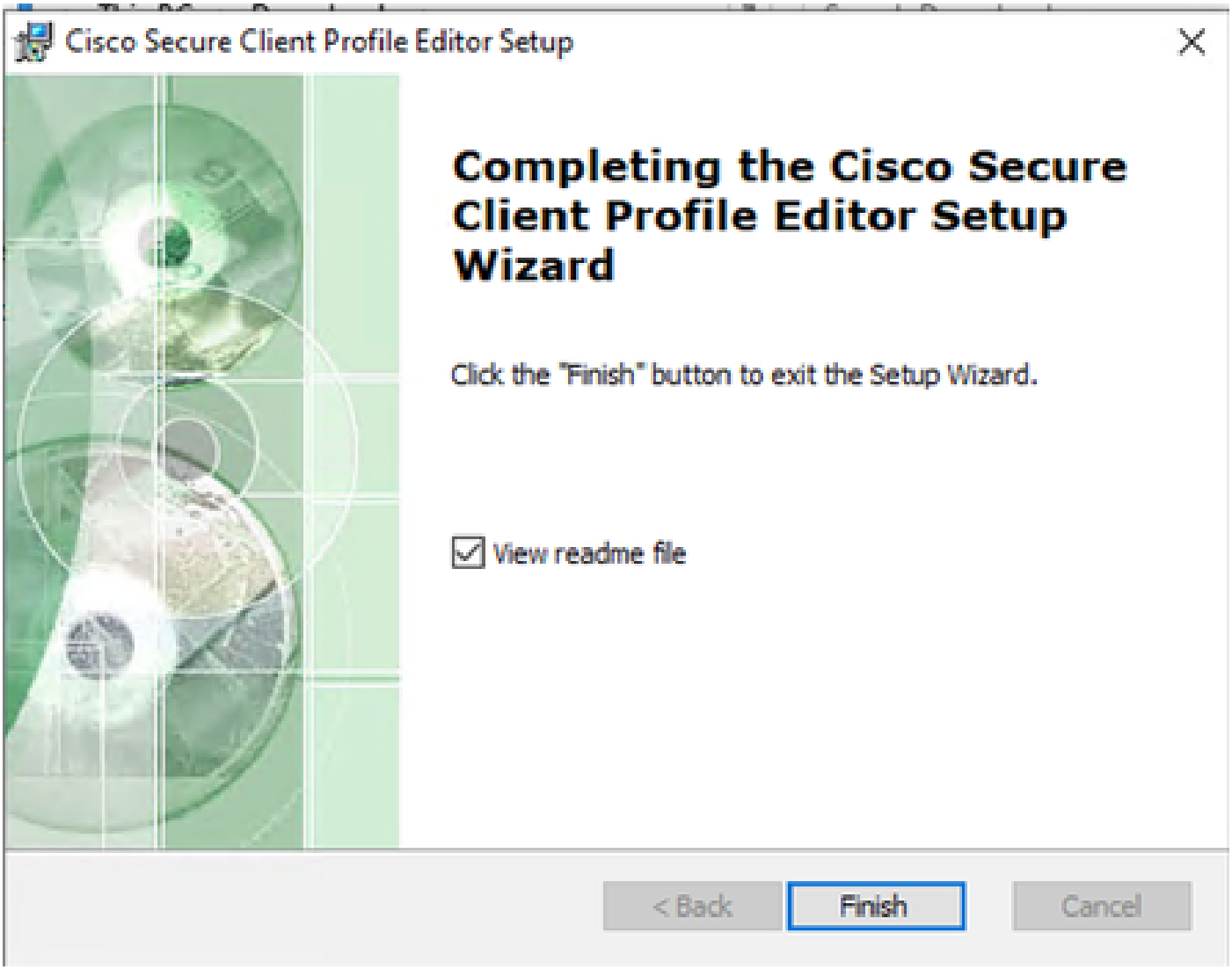


Configuración del Editor de perfiles



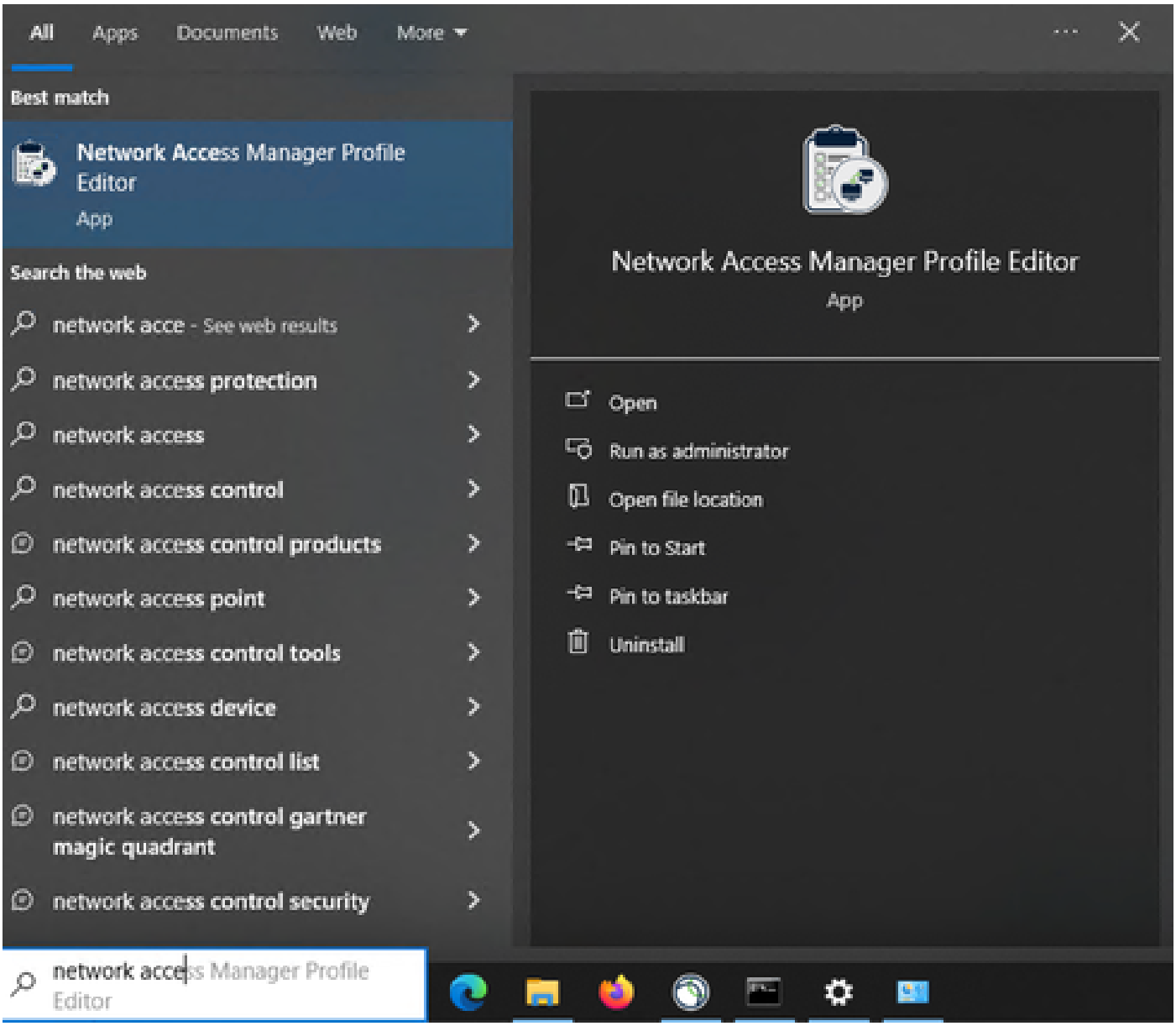
Ventana de instalación

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.



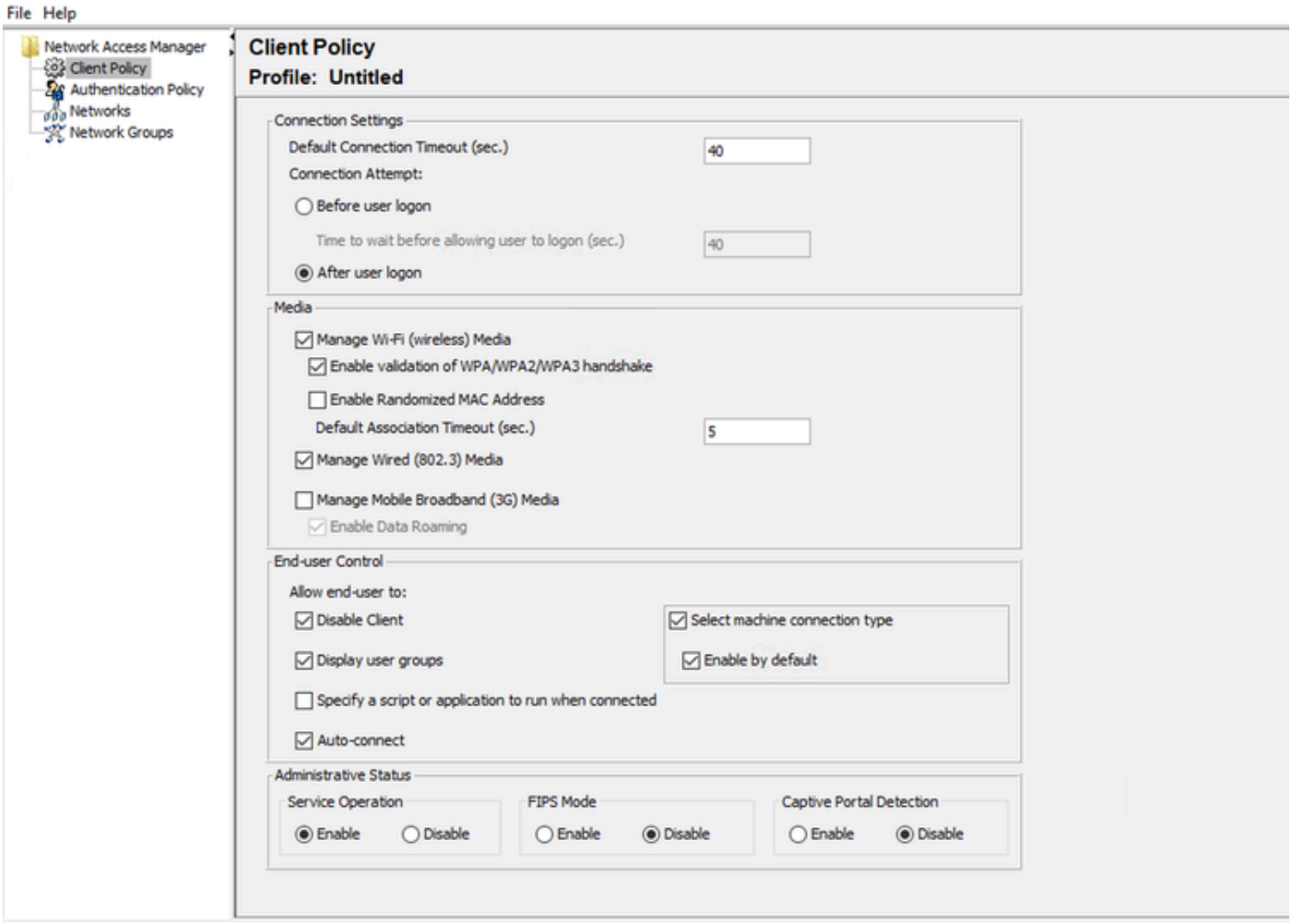
Editor de perfiles para NAM en la barra de búsqueda

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

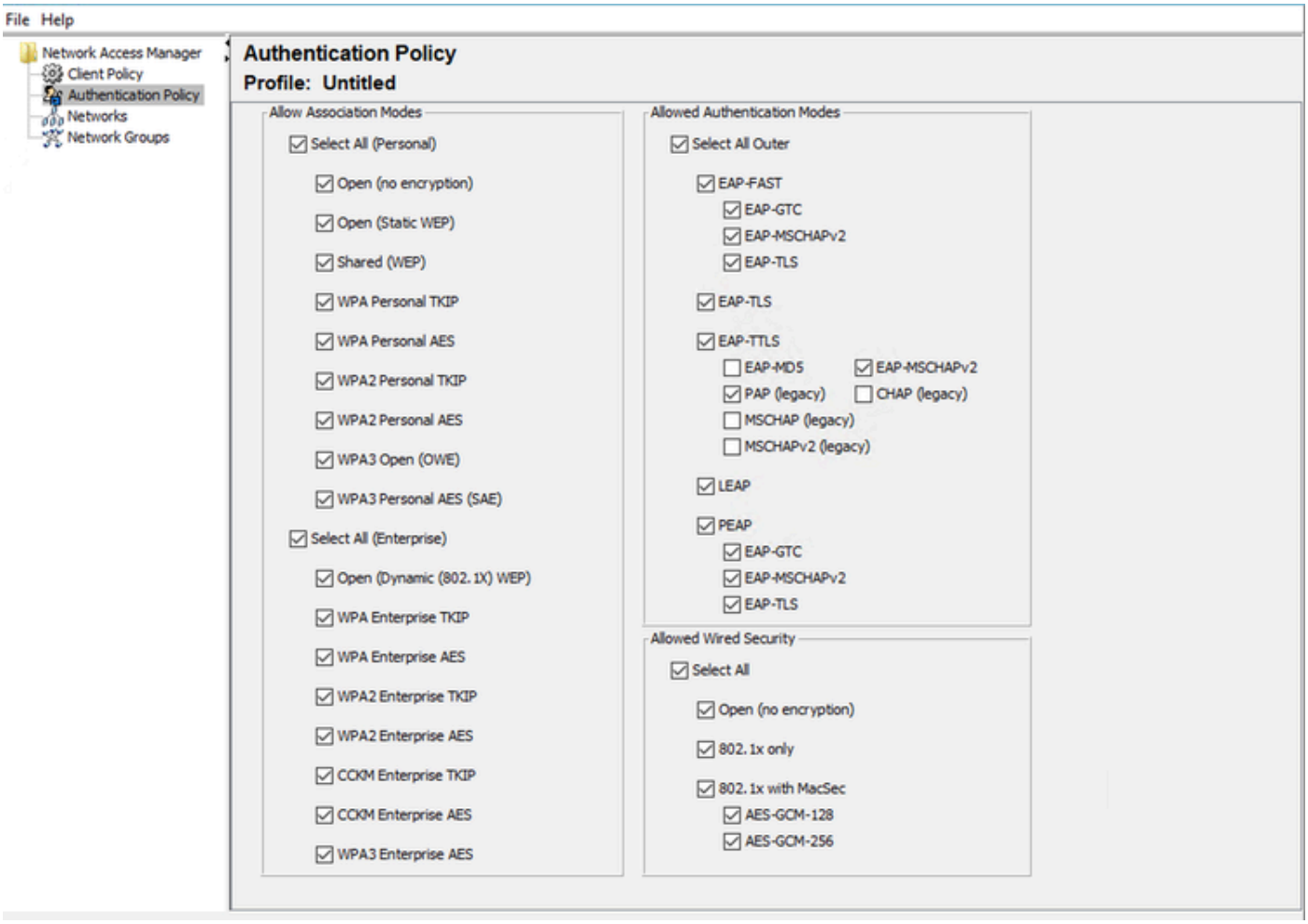
3. Configuraciones generales por defecto

Todos los escenarios presentados en este artículo contienen configuraciones para:

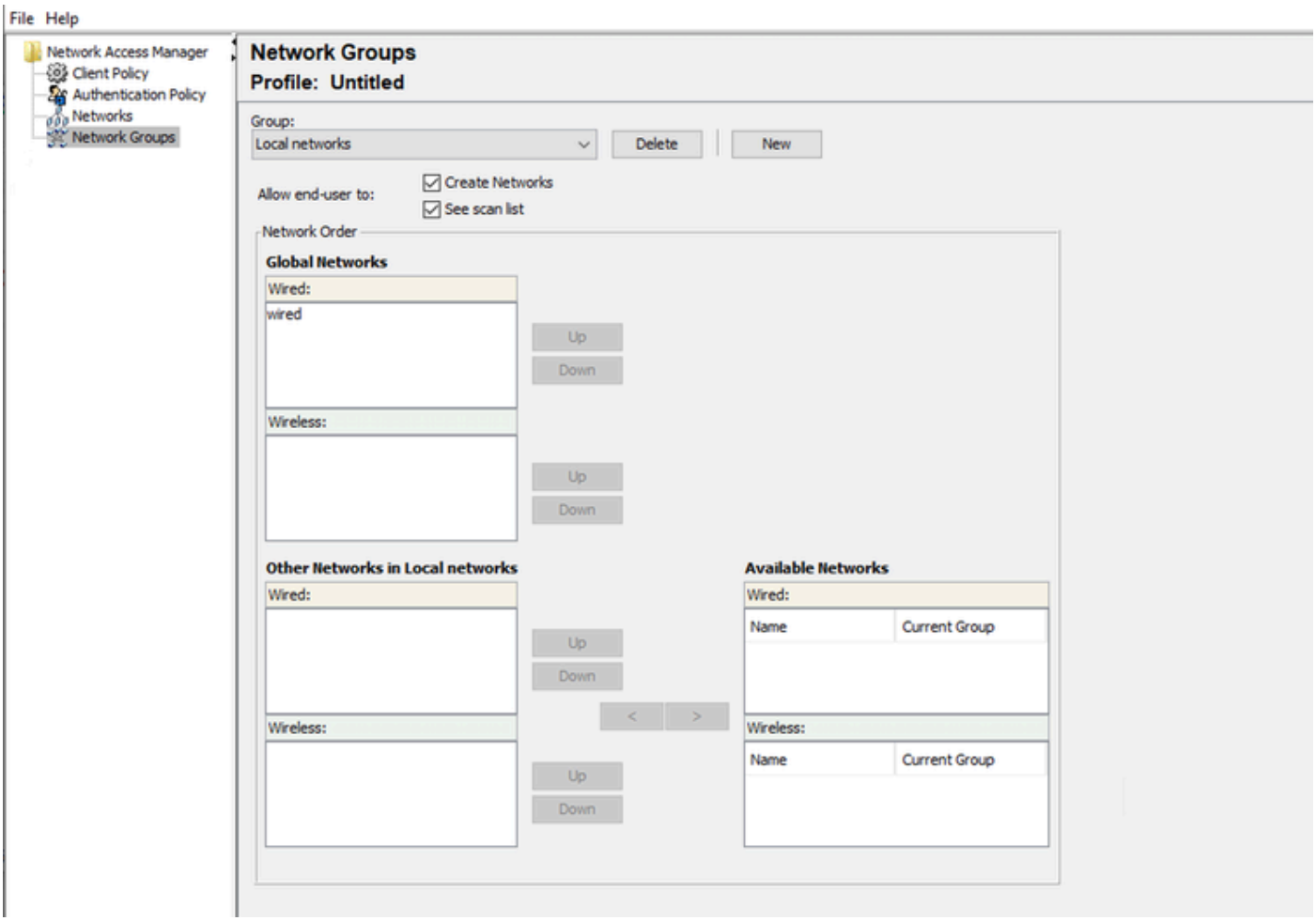
- Directiva de cliente
- Política de autenticación
- Grupos de red



Directiva de cliente del Editor de perfiles NAM



Política de autenticación del Editor de perfiles NAM



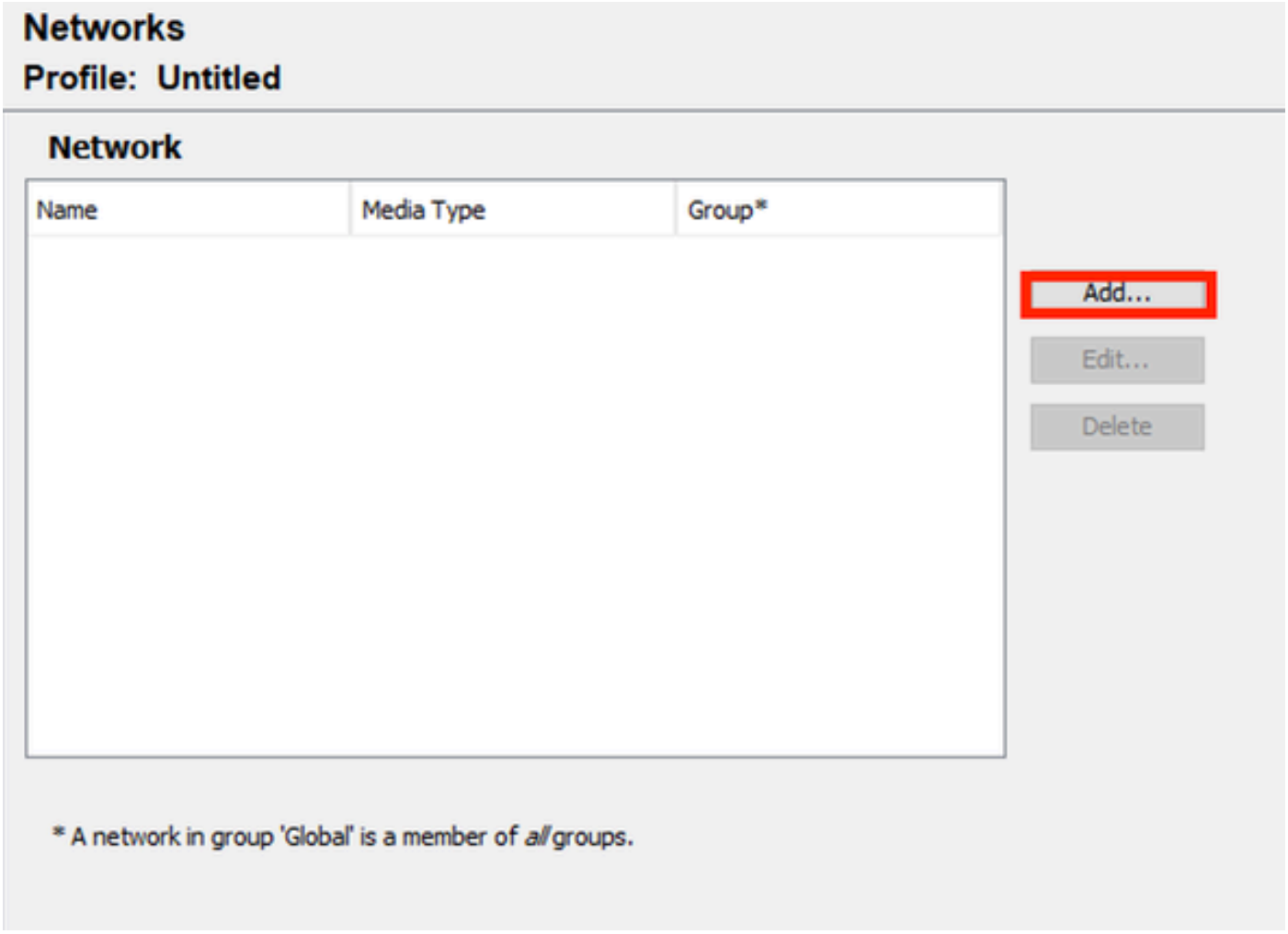
Ficha Grupos de red

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.

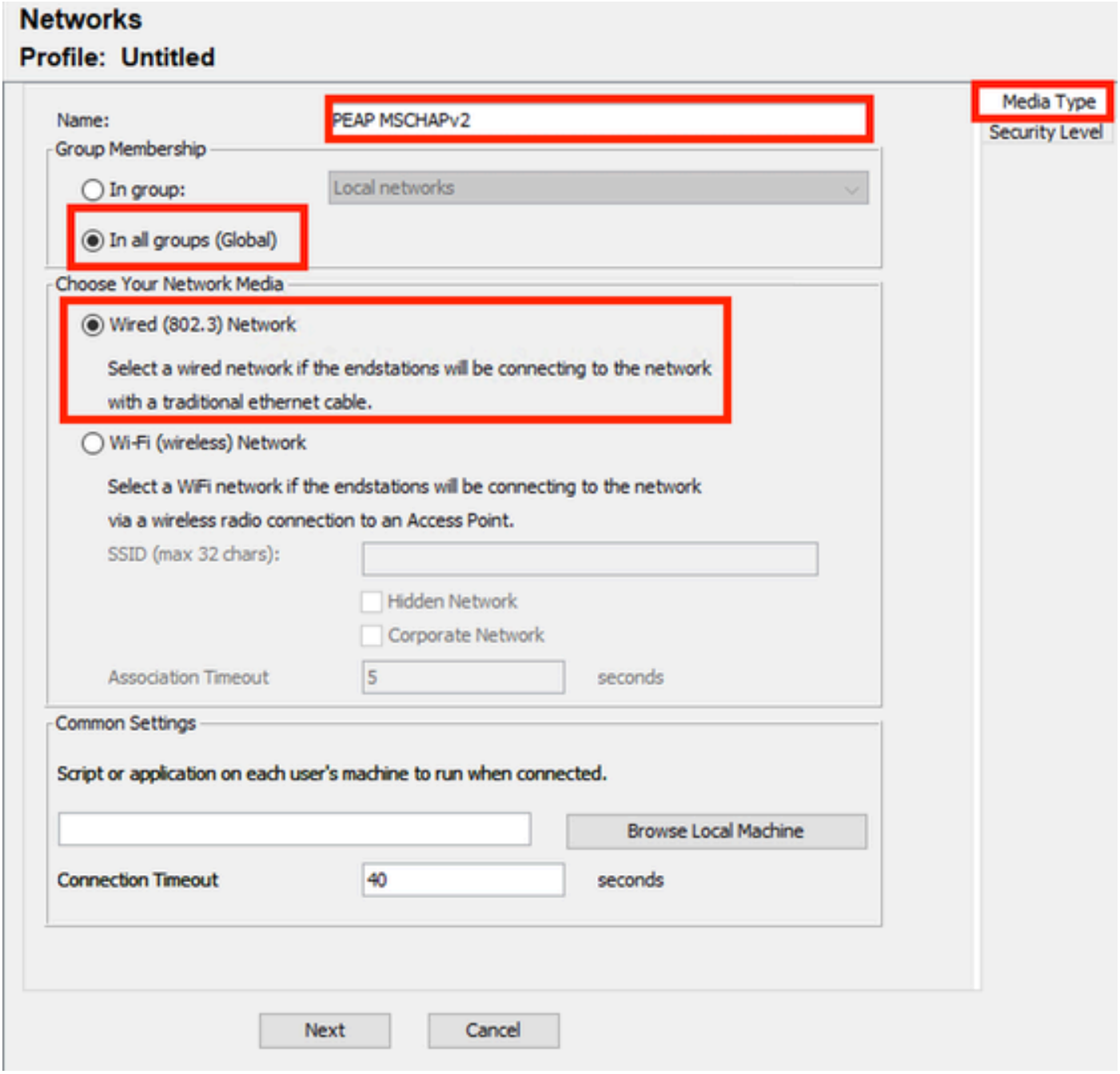
Haga clic en Add (Agregar).



Creación de perfiles de red

Asigne un nombre al perfil de red.

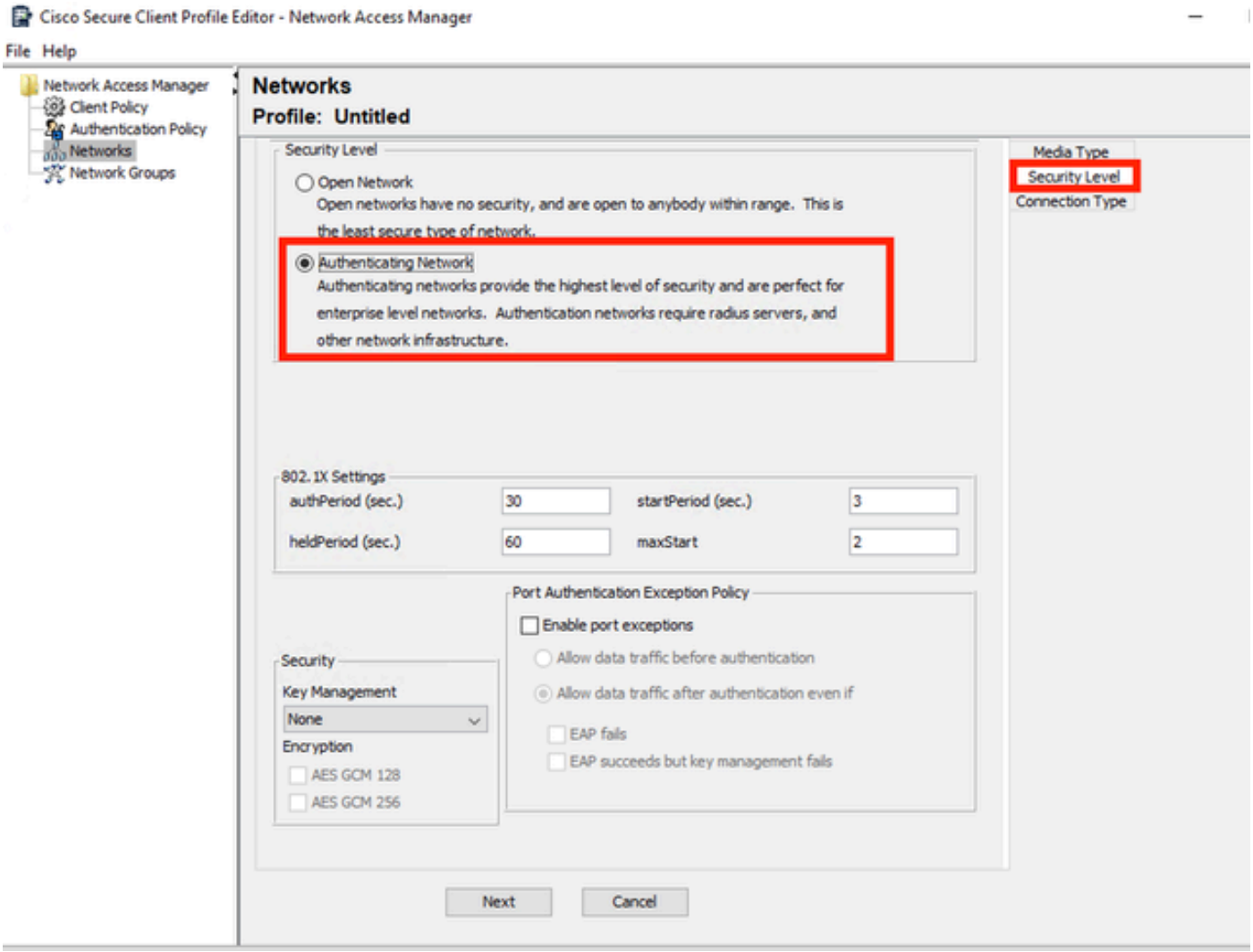
Seleccione Global para Membership Group. Seleccione medios de red con cables.



Sección Tipo de medio del perfil de red

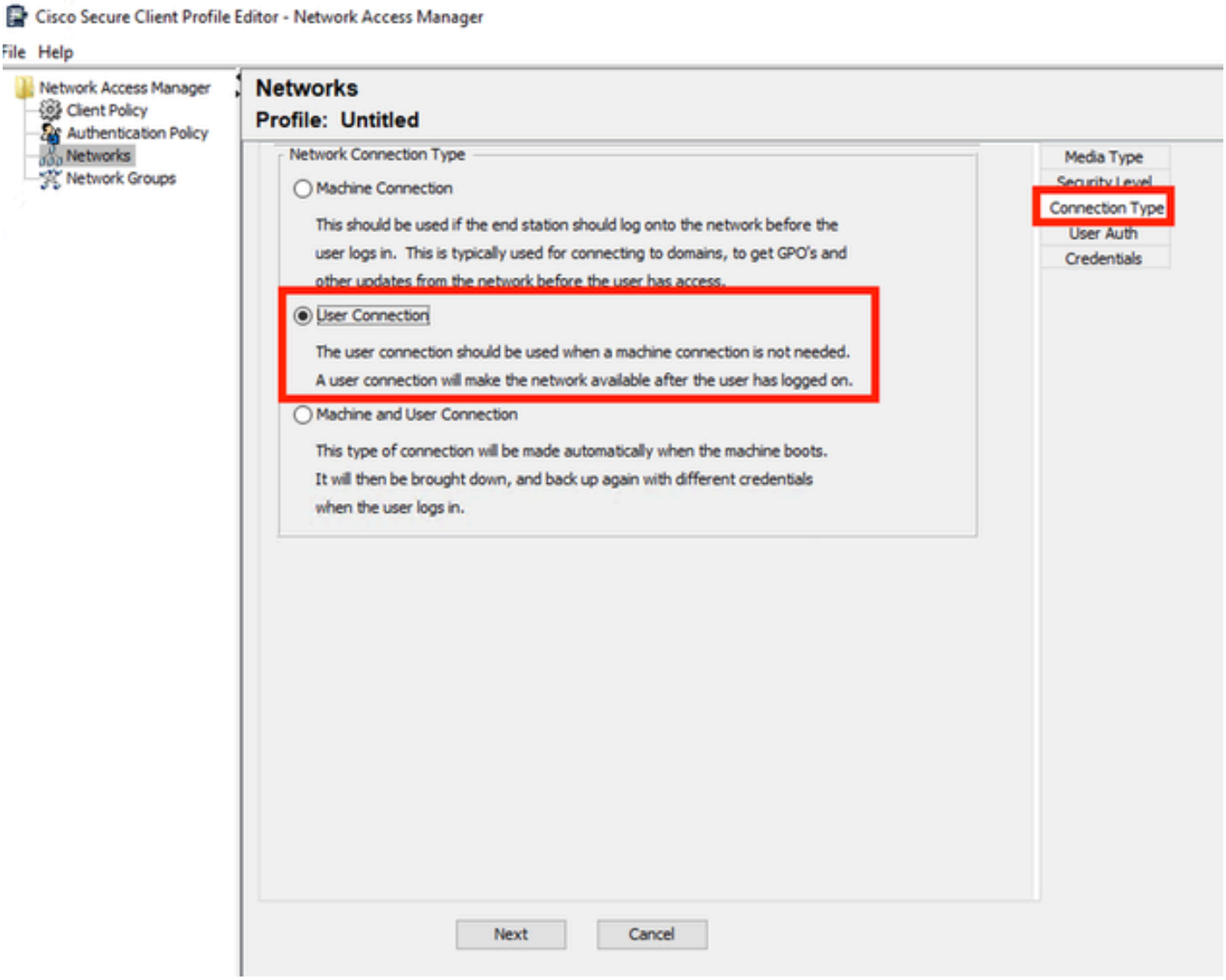
Haga clic en Next (Siguiente).

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



Nivel de seguridad del perfil de red

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

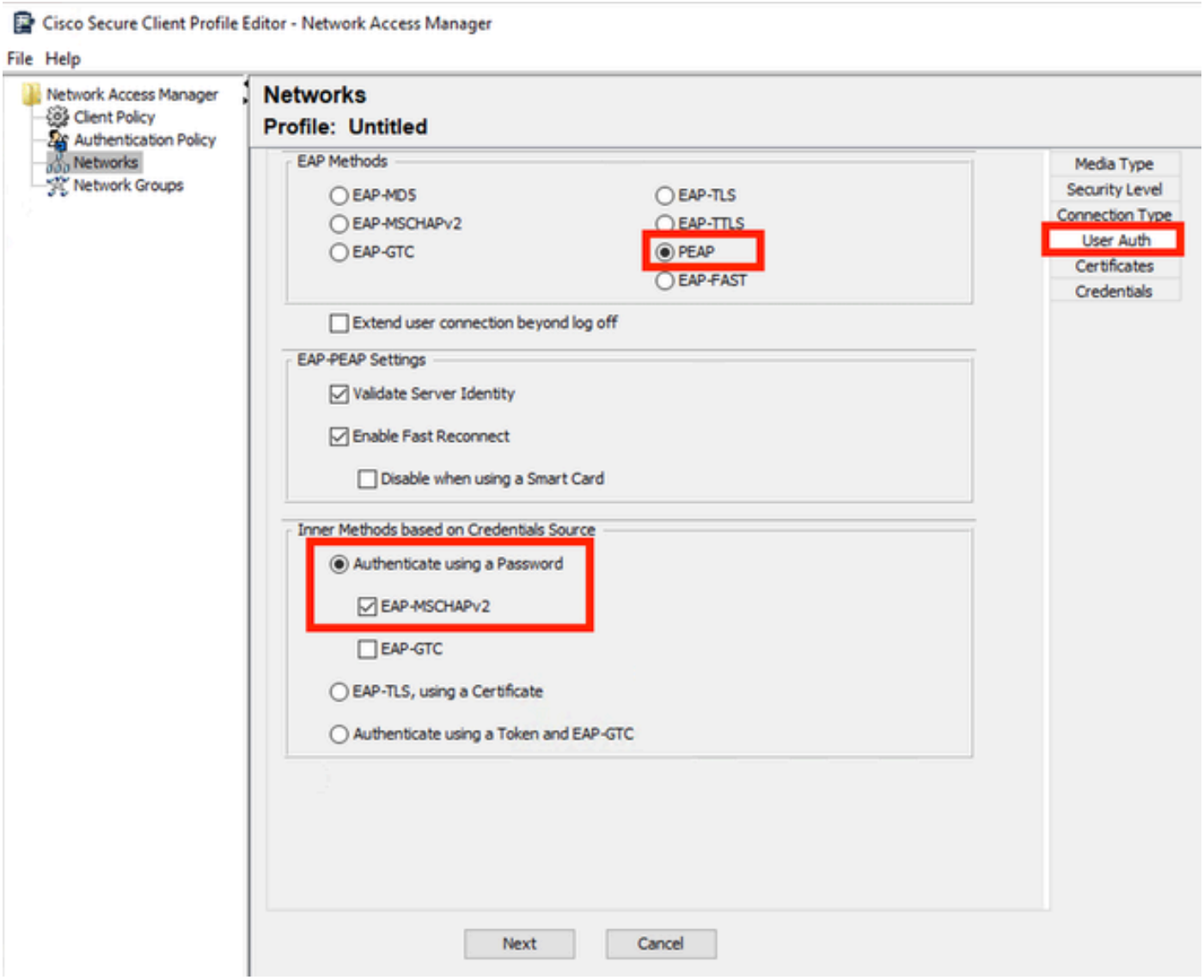


Tipo de conexión del perfil de red

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.



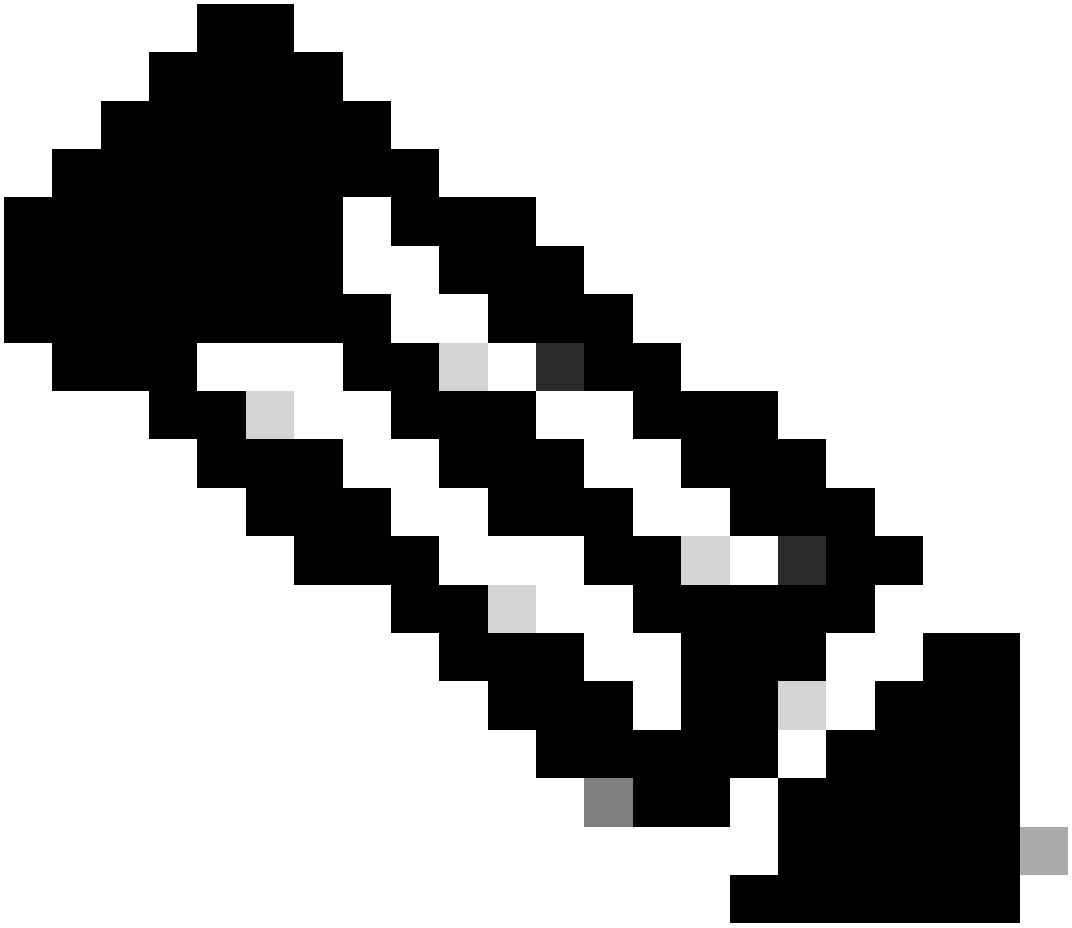
Autenticación de usuario de perfil de red

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

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

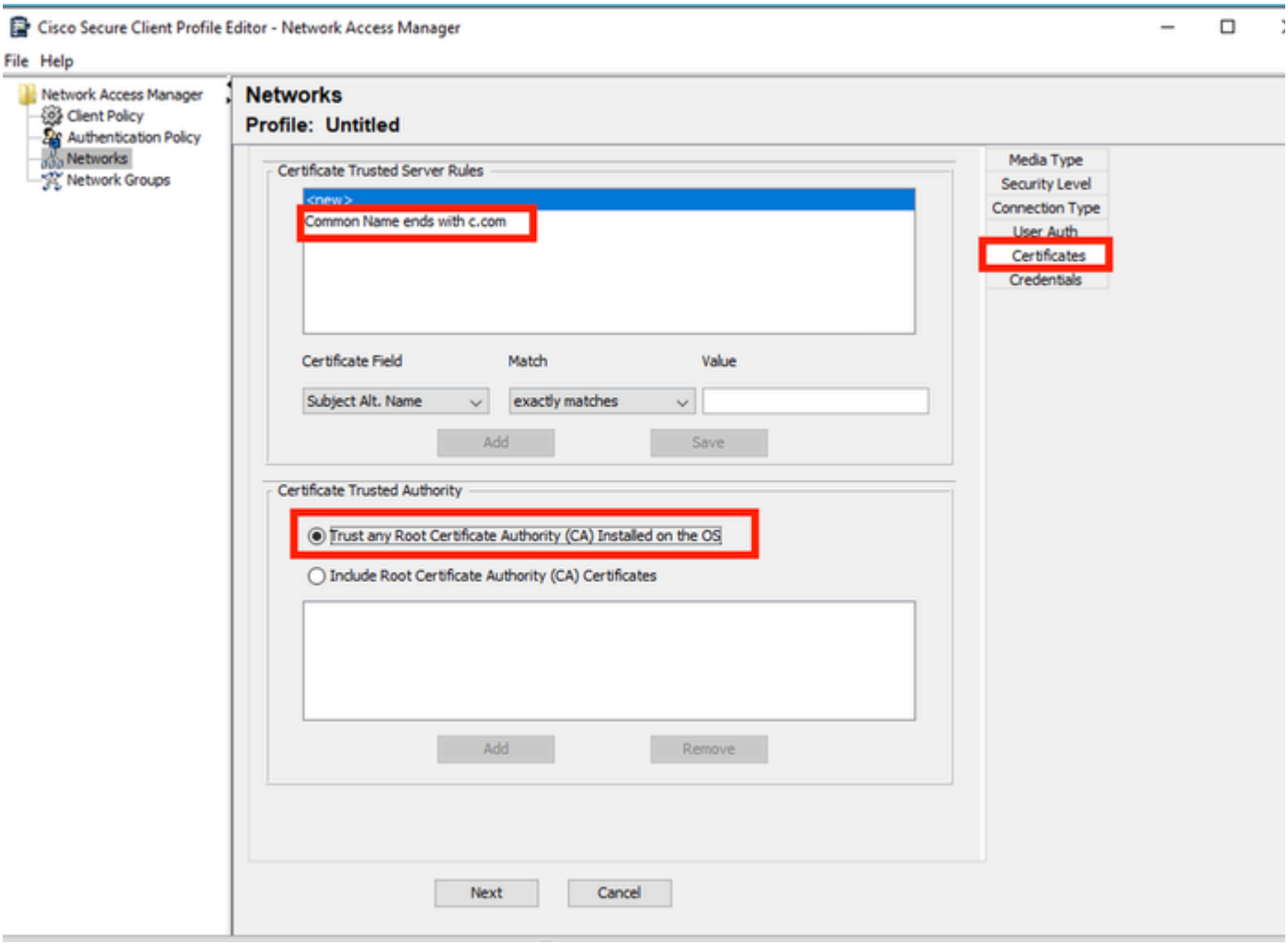
De los múltiples métodos internos que existen para EAP-PEAP, seleccione Authenticate using a Password y seleccione EAP-MSCHAPv2.

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.

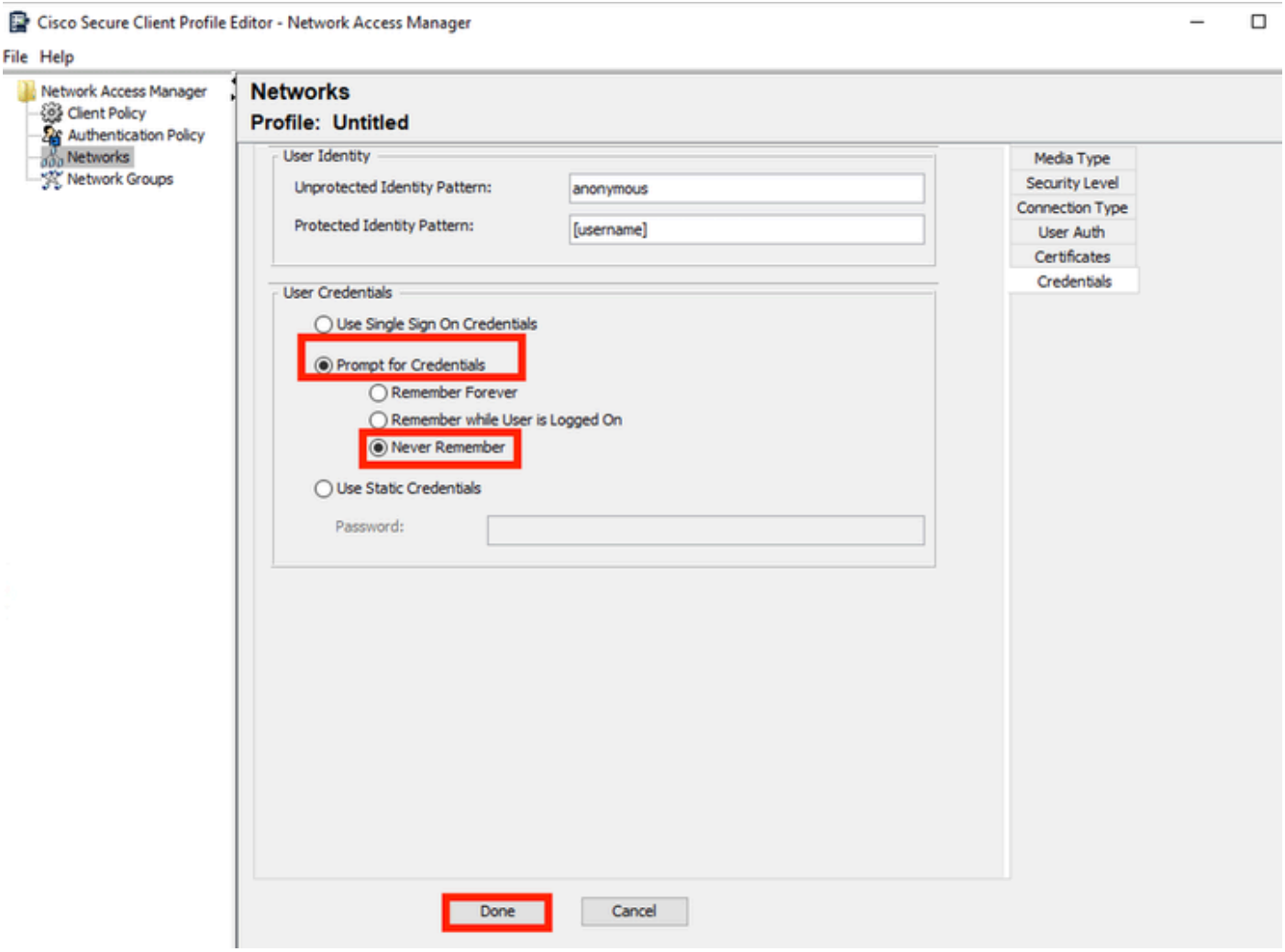


Sección Certificado de Perfil de Red

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 (Siguiente).



Sección Credenciales de Perfil de Red

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

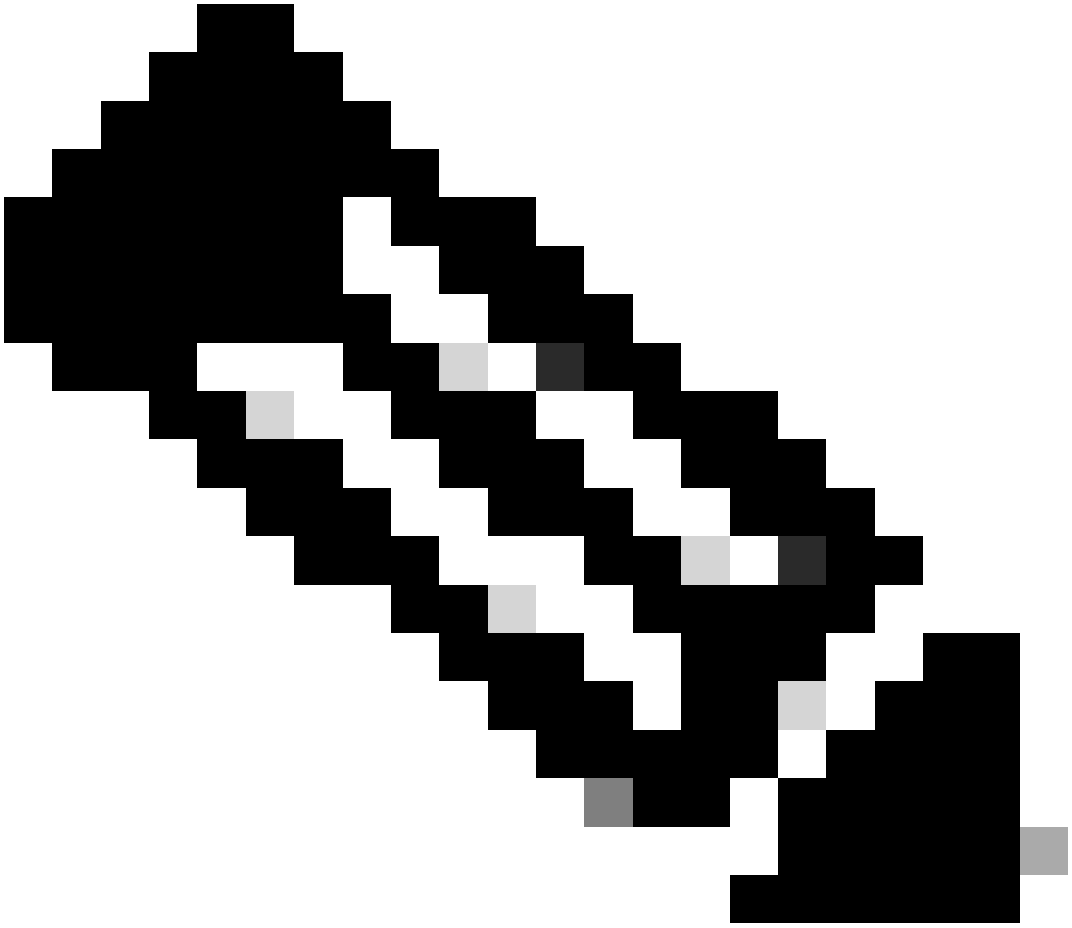
La opción Pedir credenciales > No recordar nunca está seleccionada, por lo que en cada autenticación, el usuario que realiza la autenticación debe introducir sus credenciales.

Haga clic en Done (Listo).

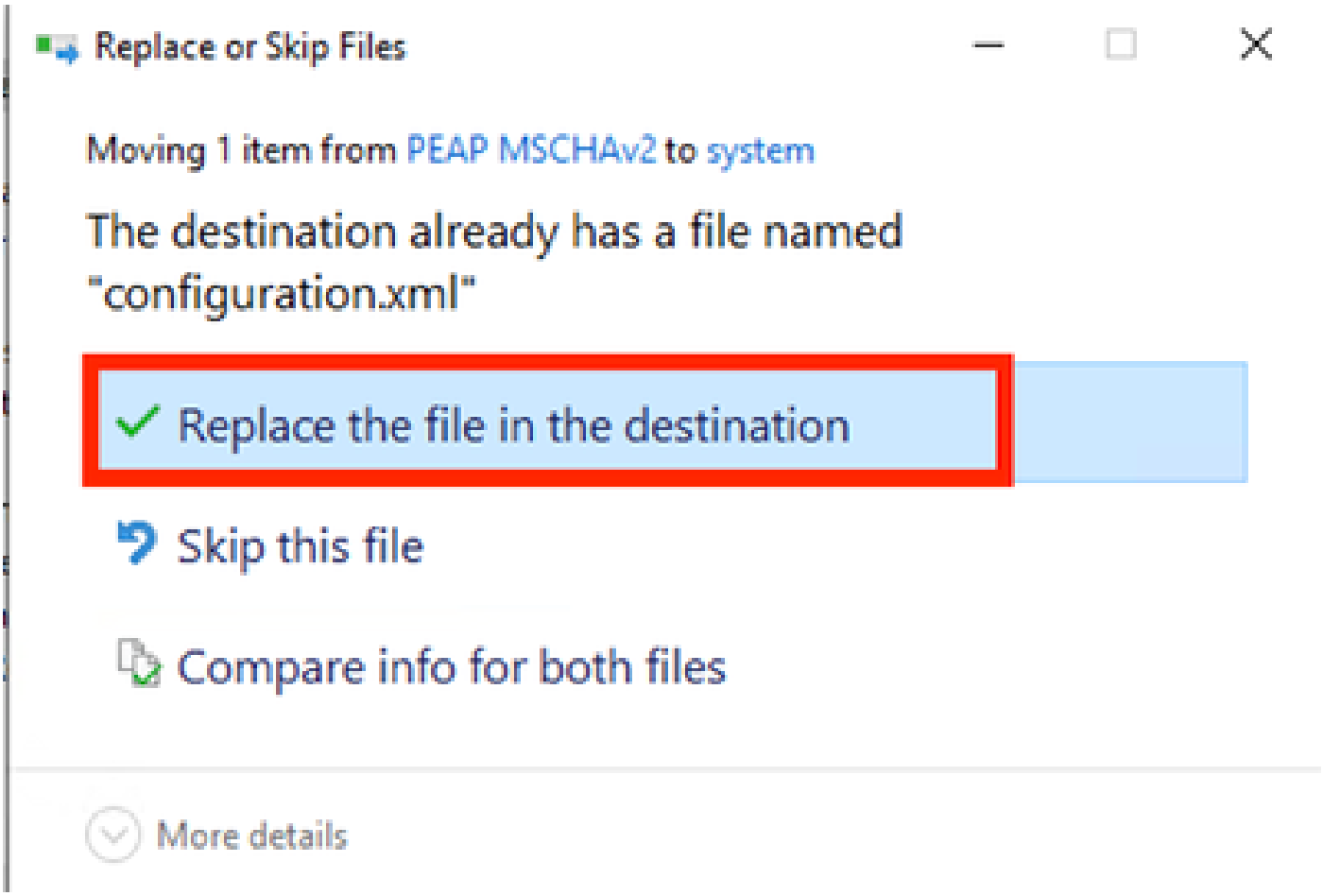
Guarde el perfil de Secure Client Network Access Manager, como configuration.xml con la opción File > Save As.

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.

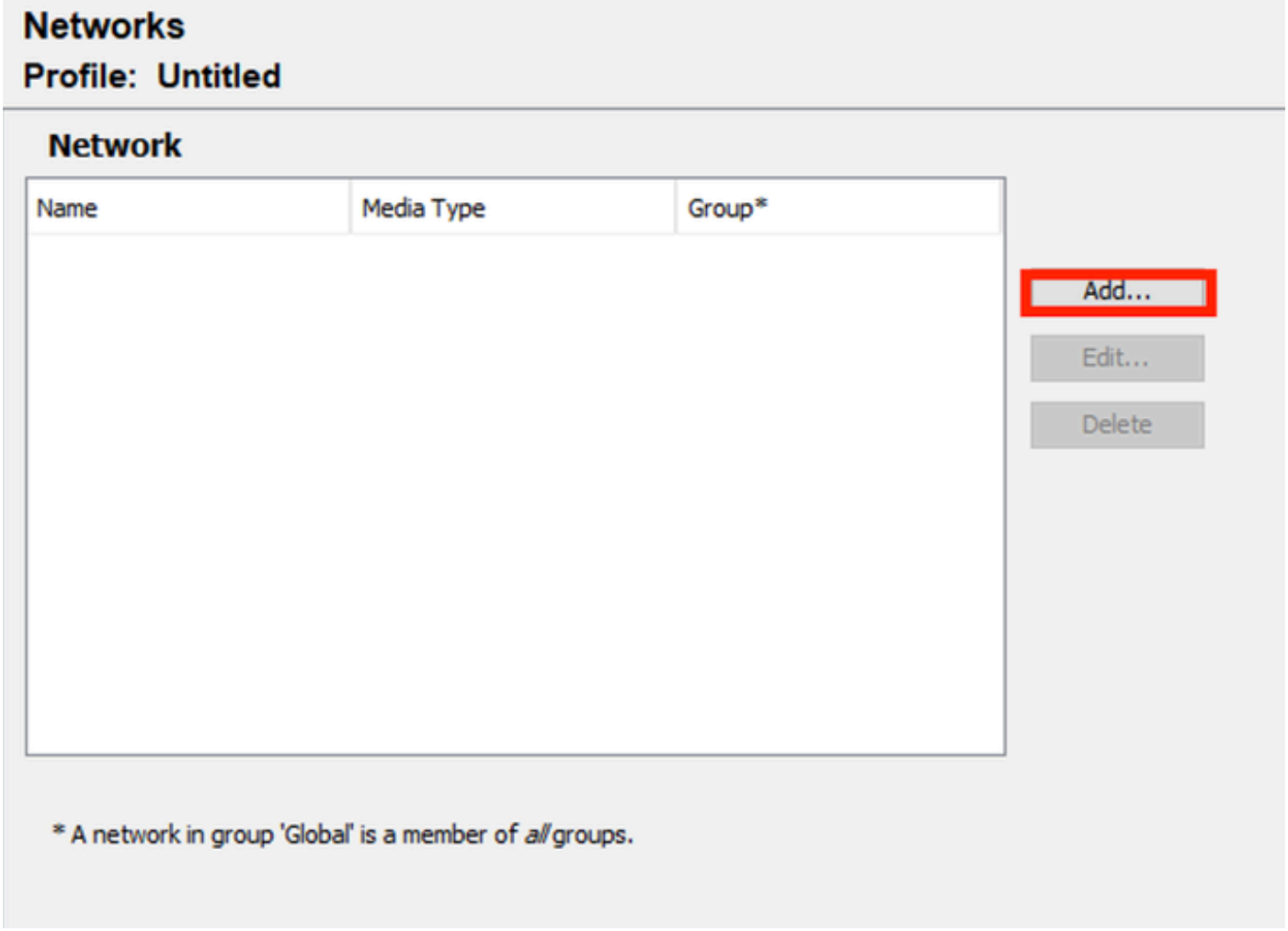


Sección Reemplazar archivo

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.

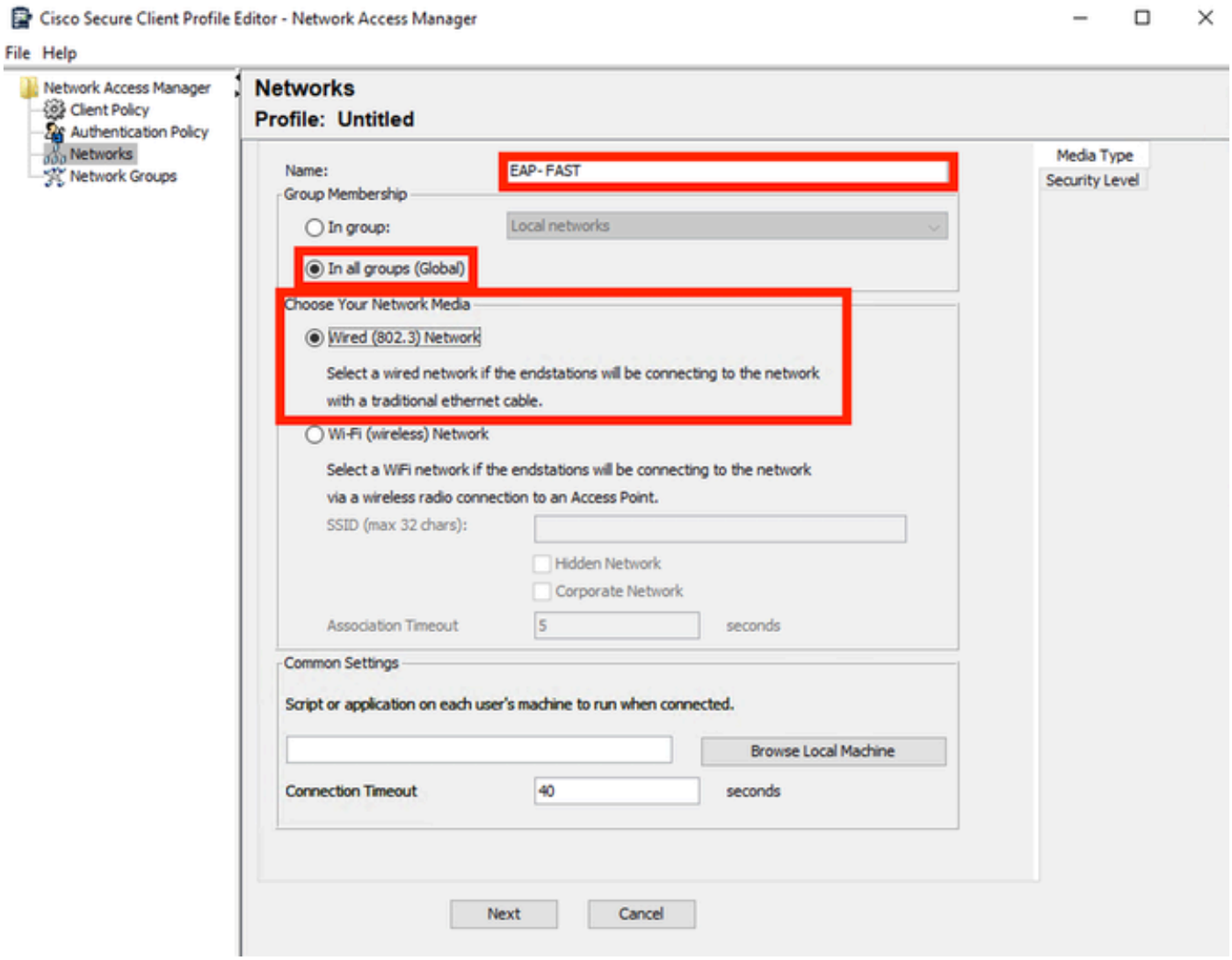
Haga clic en Add (Agregar).



Ficha Red del editor de perfiles NAM

Introduzca un nombre en el perfil de red.

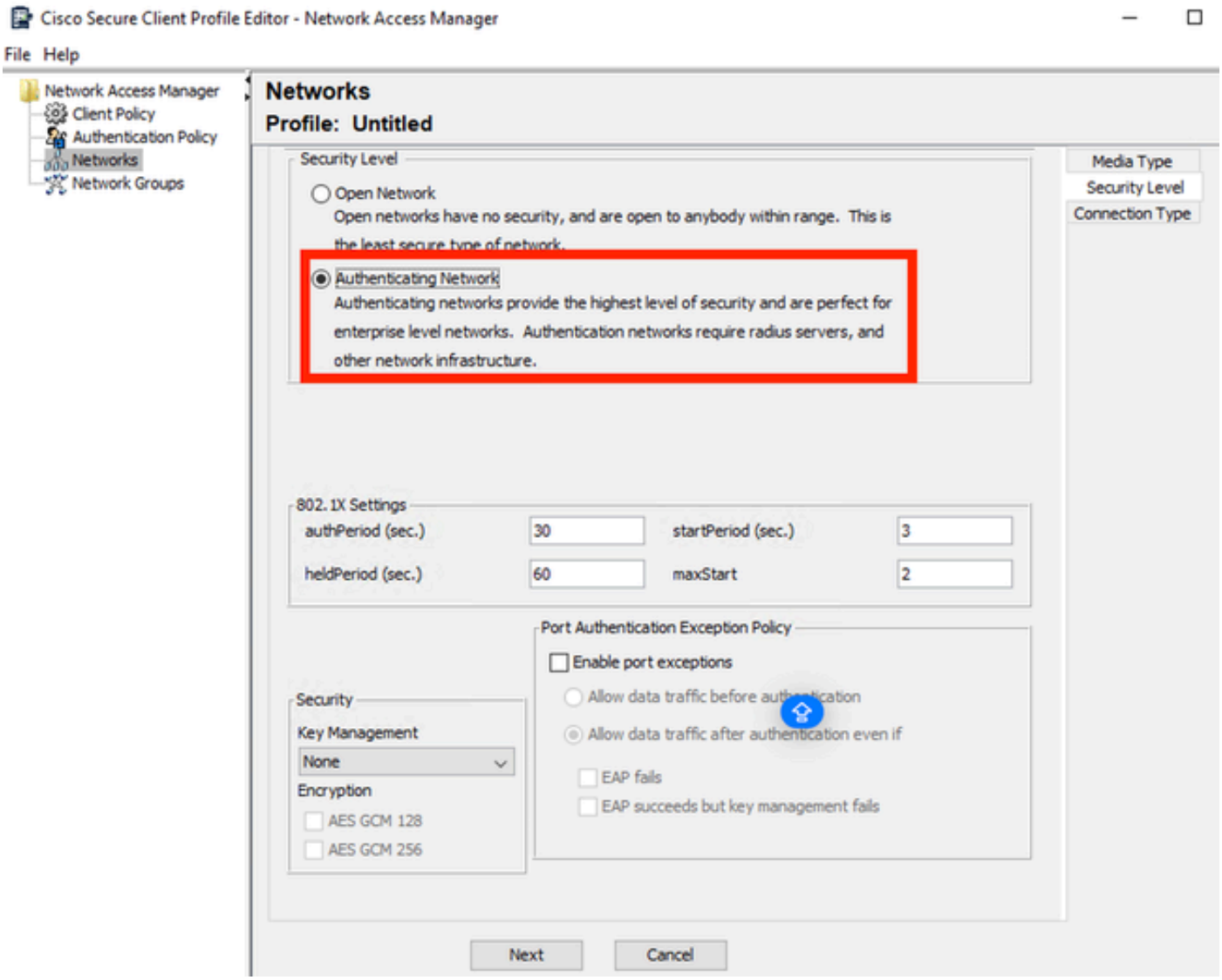
Seleccione Global para Membership Group. Seleccione WiredNetwork Media.



Sección Tipo de medio

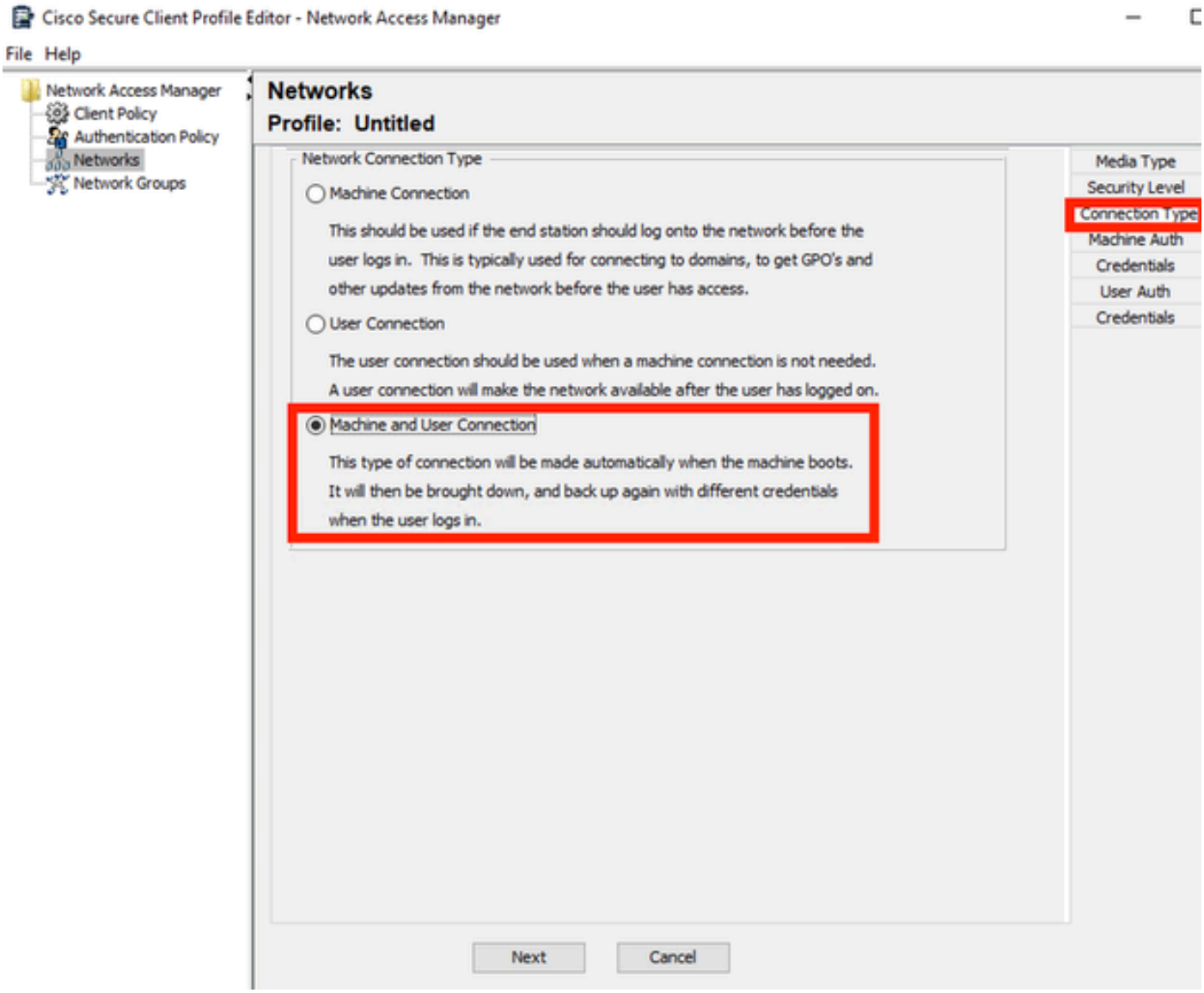
Haga clic en Next (Siguiente).

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



Sección Editor de perfiles de nivel de seguridad

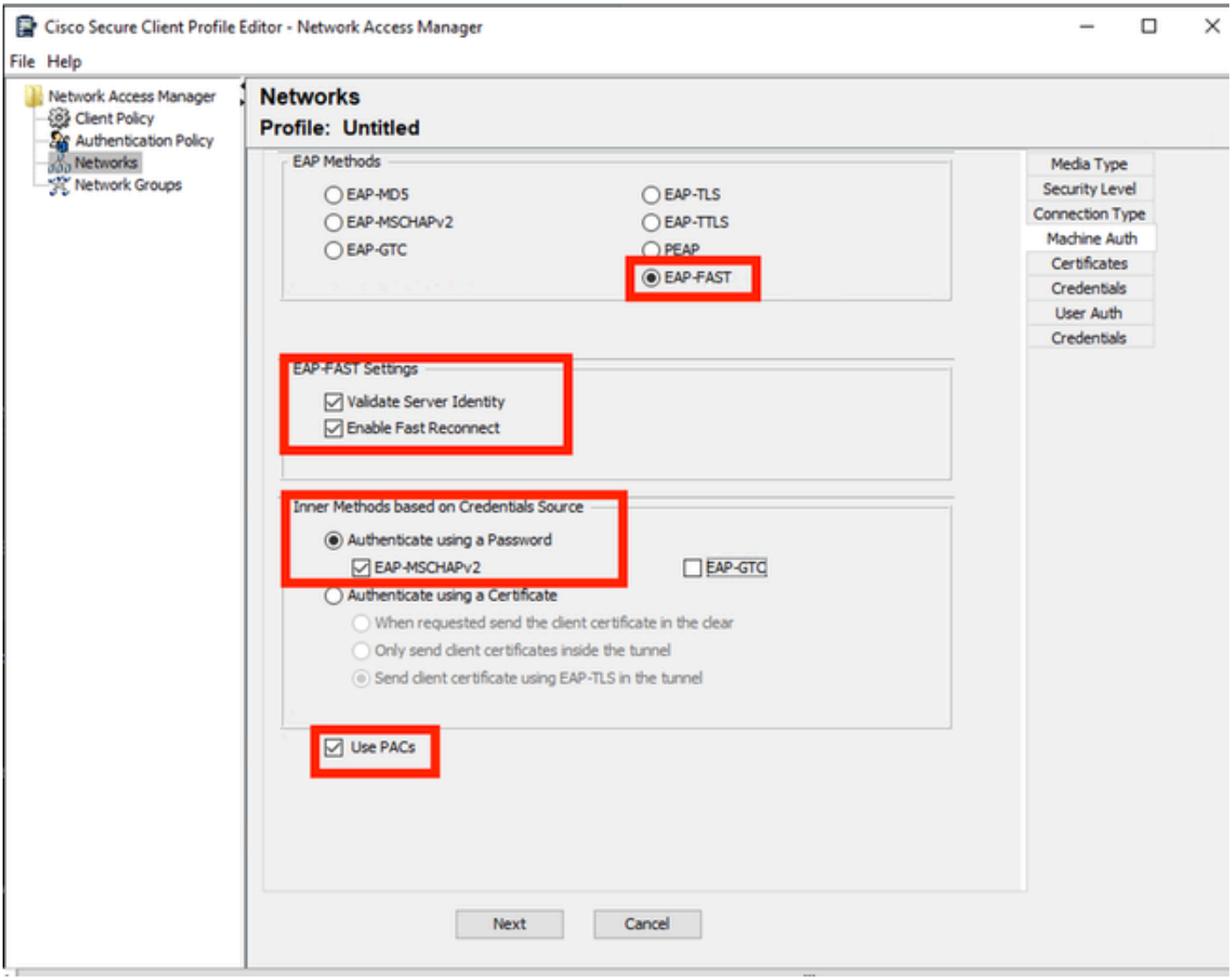
Haga clic en Siguiente para continuar con la sección Tipo de conexión.



Sección Tipo de conexión

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

Haga clic en Next (Siguiente).

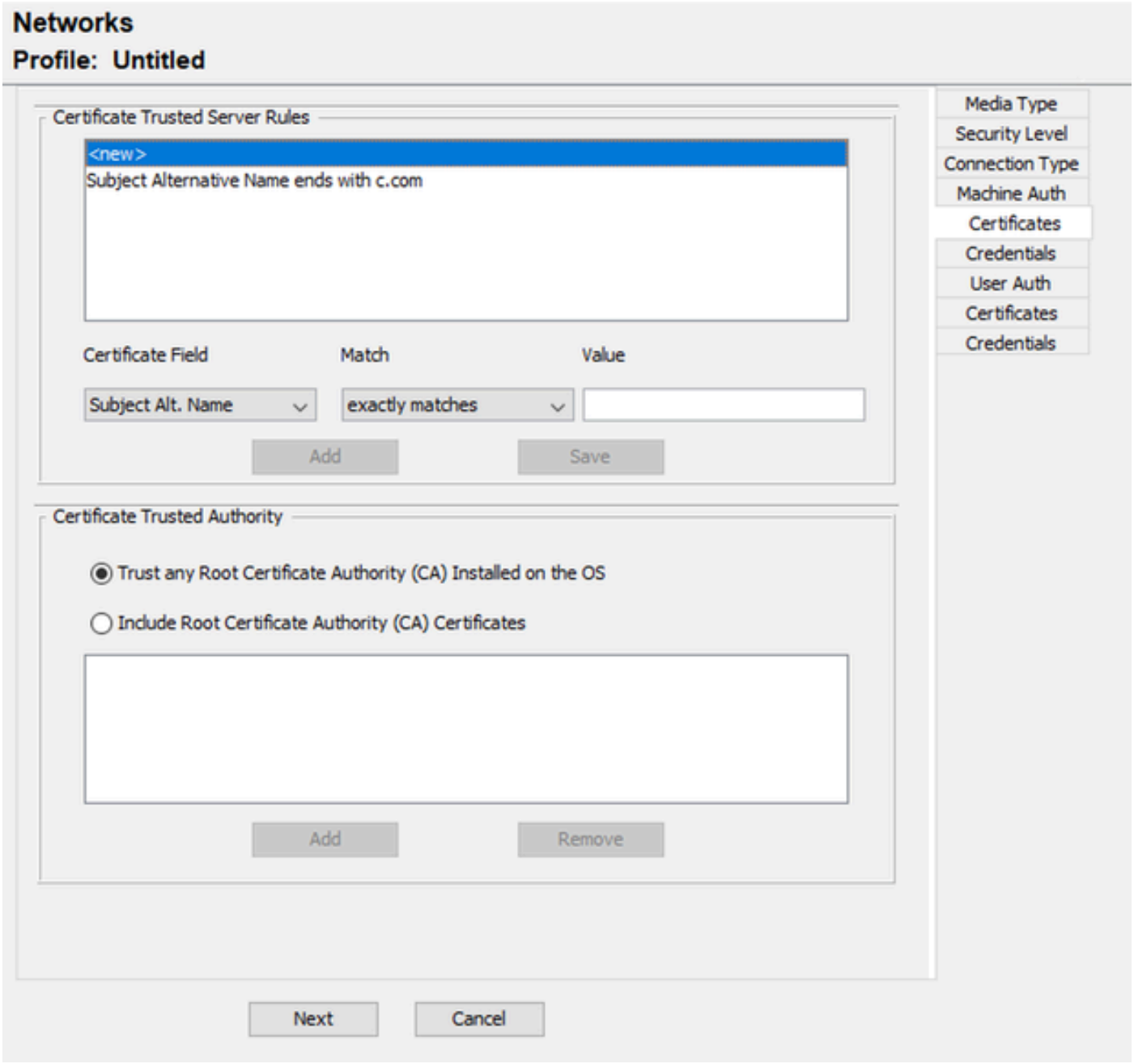


Sección de autenticación automática

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.

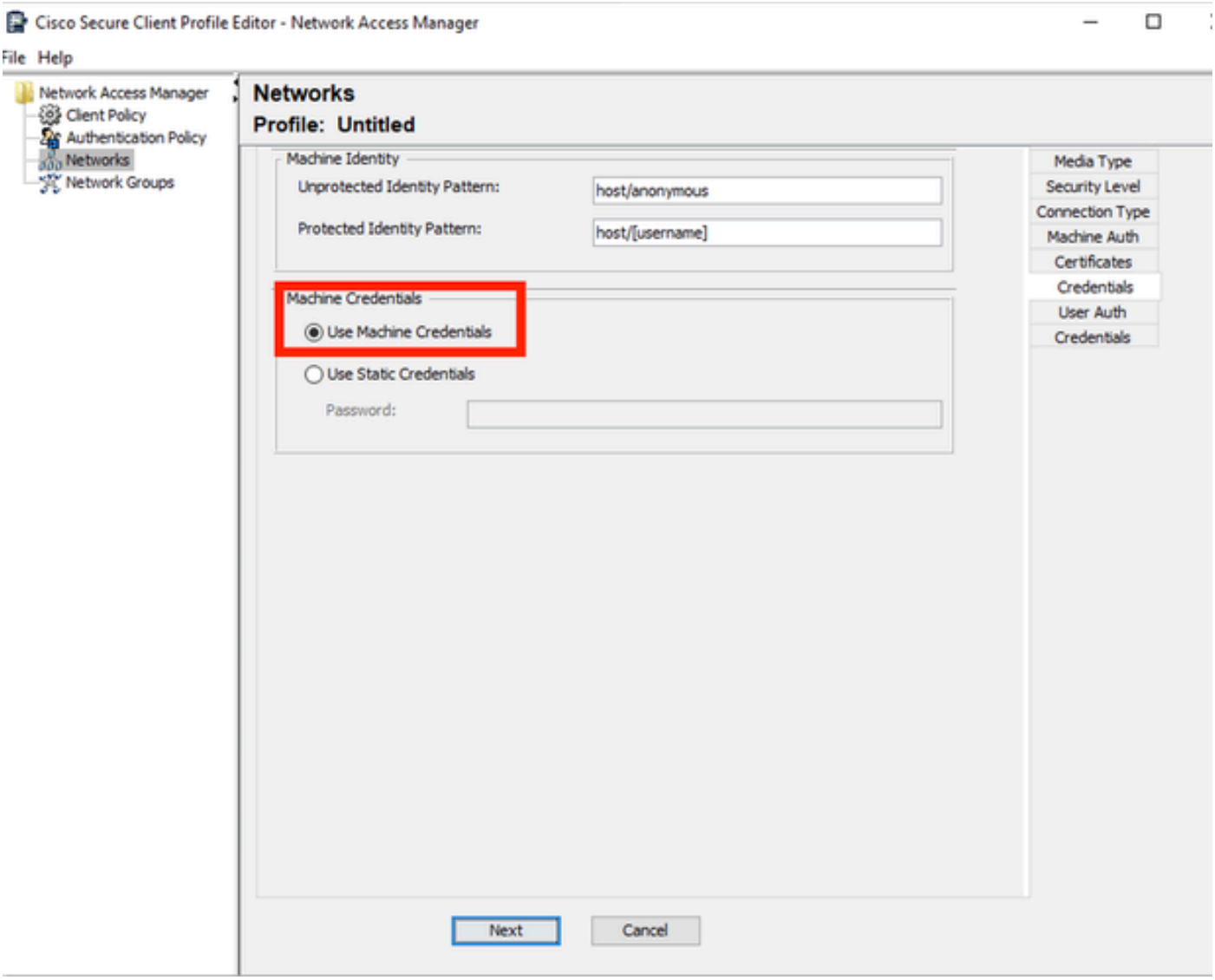


Sección Confianza del Certificado del Servidor de Autenticación de Máquina

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).

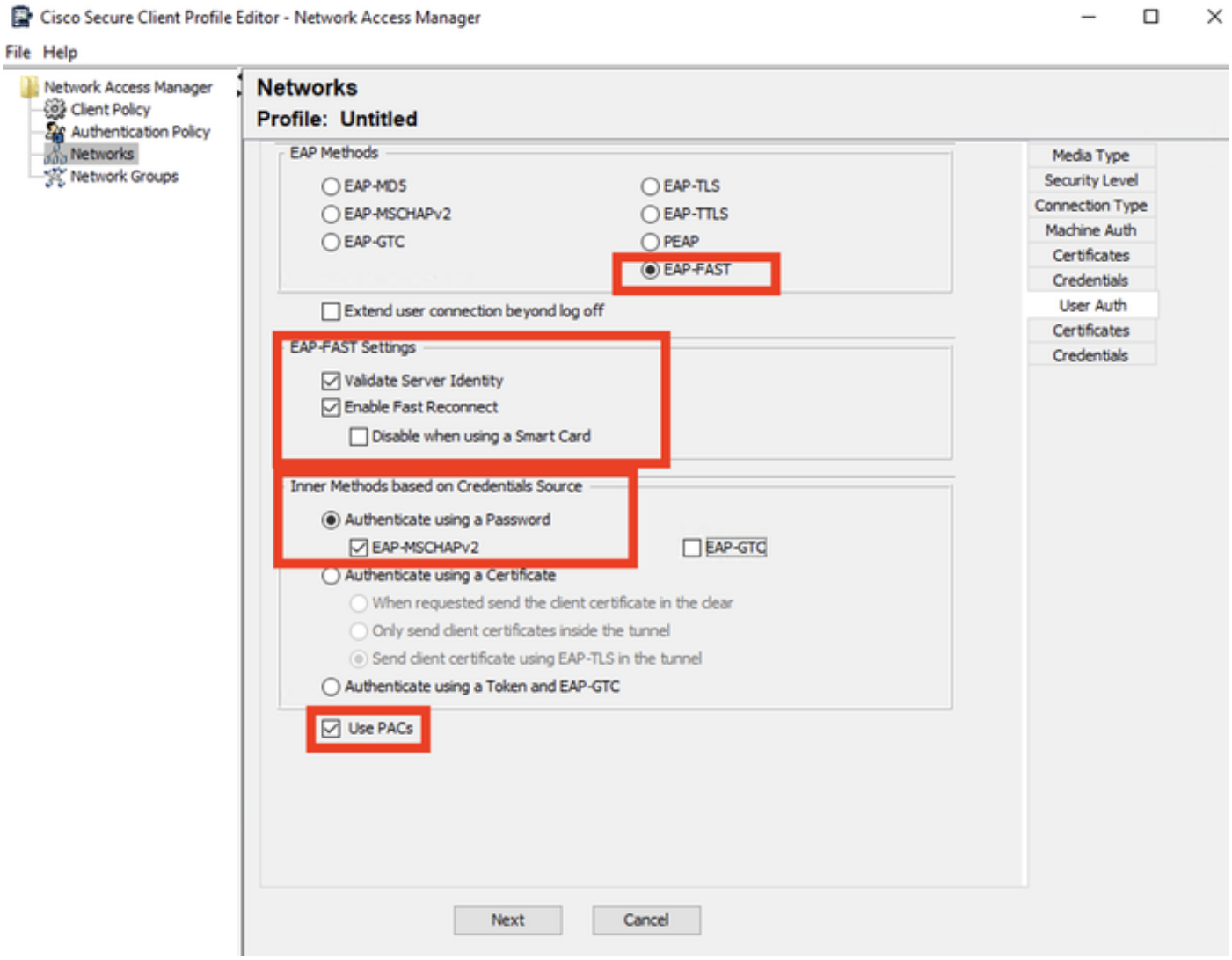
Haga clic en Next (Siguiente).



Sección de credenciales de autenticación de máquina

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

Haga clic en Next (Siguiente).



Sección Autenticación de usuario

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

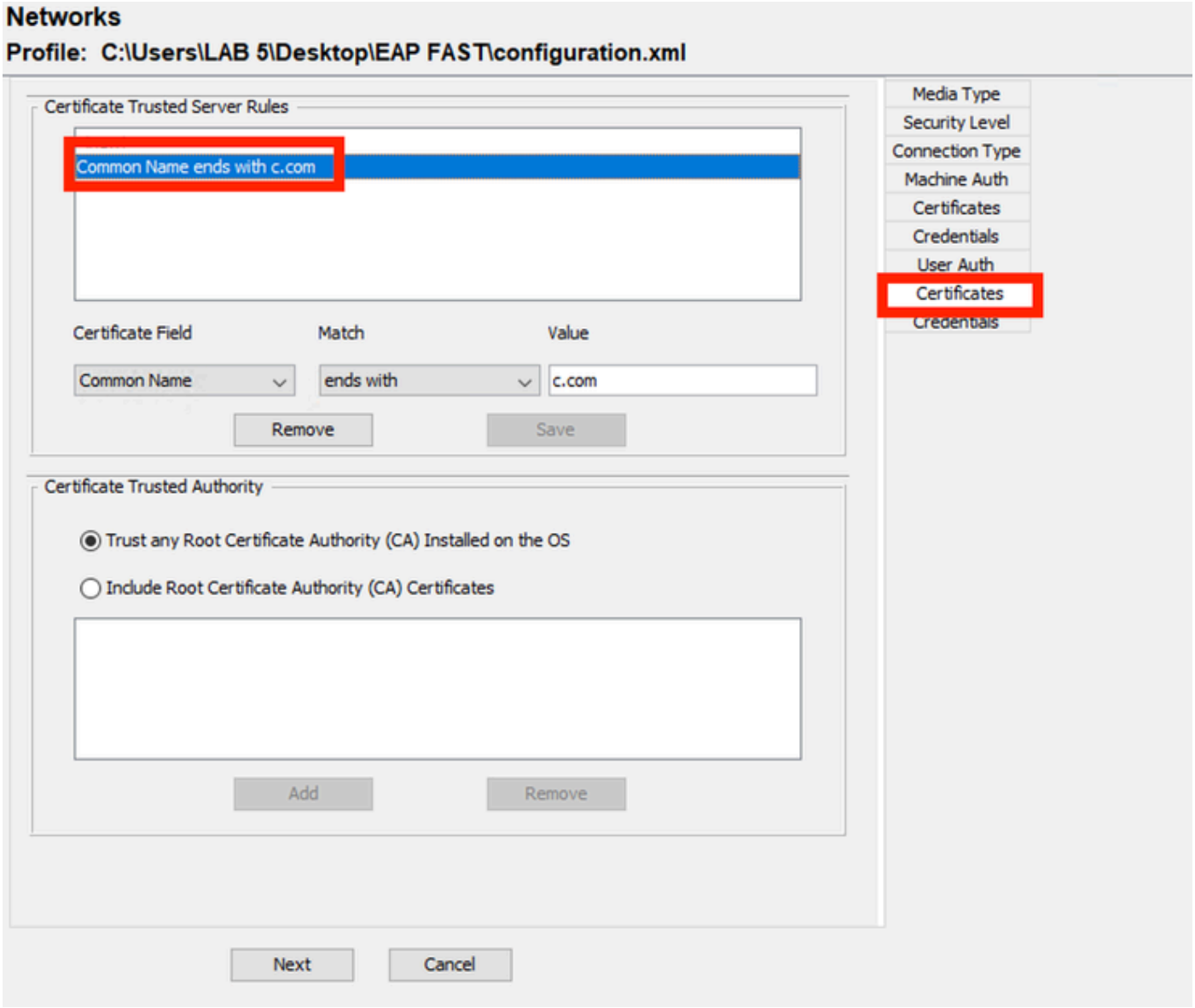
No cambie los valores predeterminados en la sección de configuración EAP-FAST.

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).

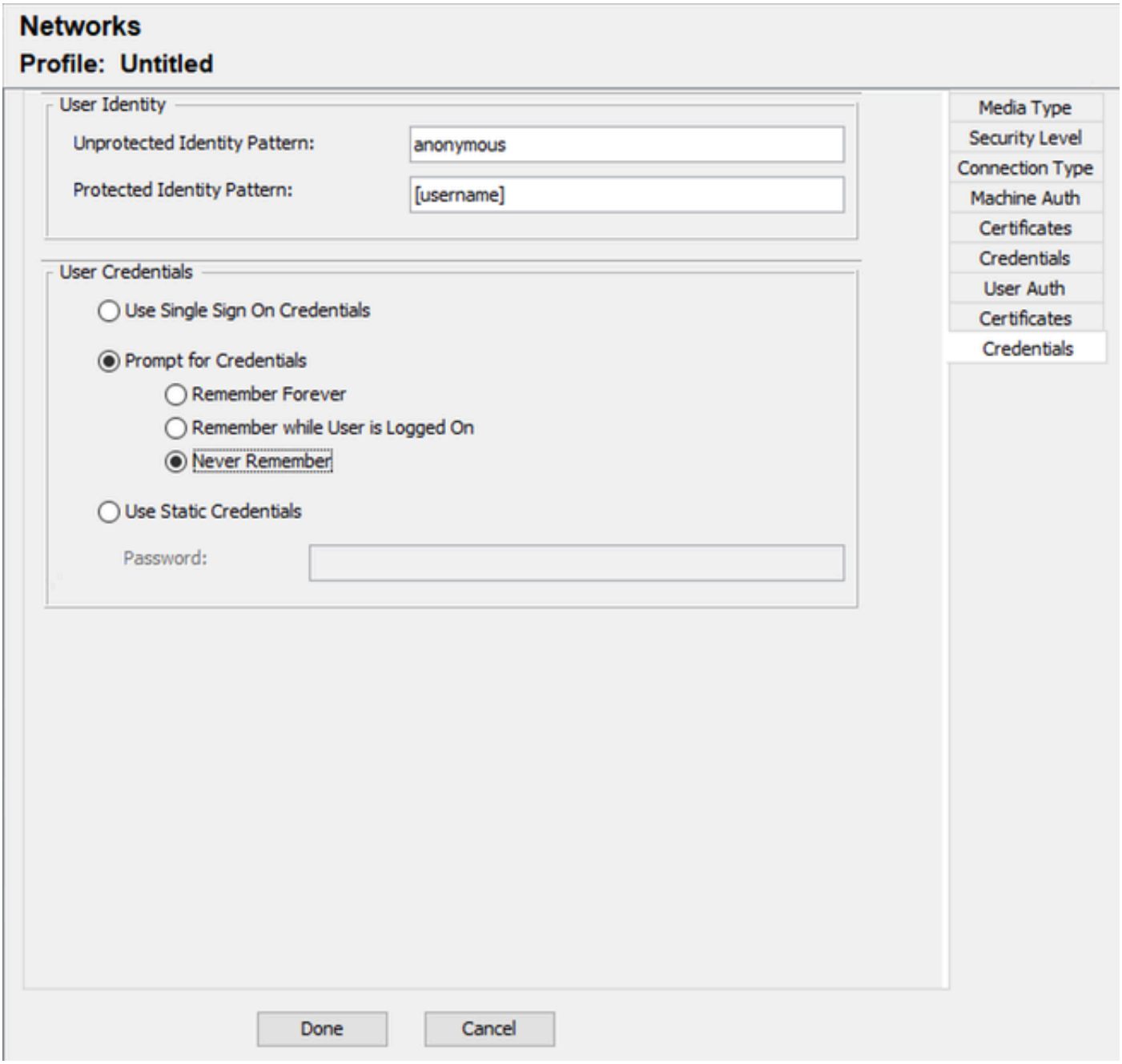
En la sección Certificados, en Reglas de servidor de confianza de certificados, la regla es Nombre común termina con c.com. Estas configuraciones son para el certificado que el servidor utiliza durante el flujo EAP PEAP. Si se utiliza ISE en su entorno, se puede utilizar el nombre común del certificado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



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).



Credenciales de autenticación de usuario

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

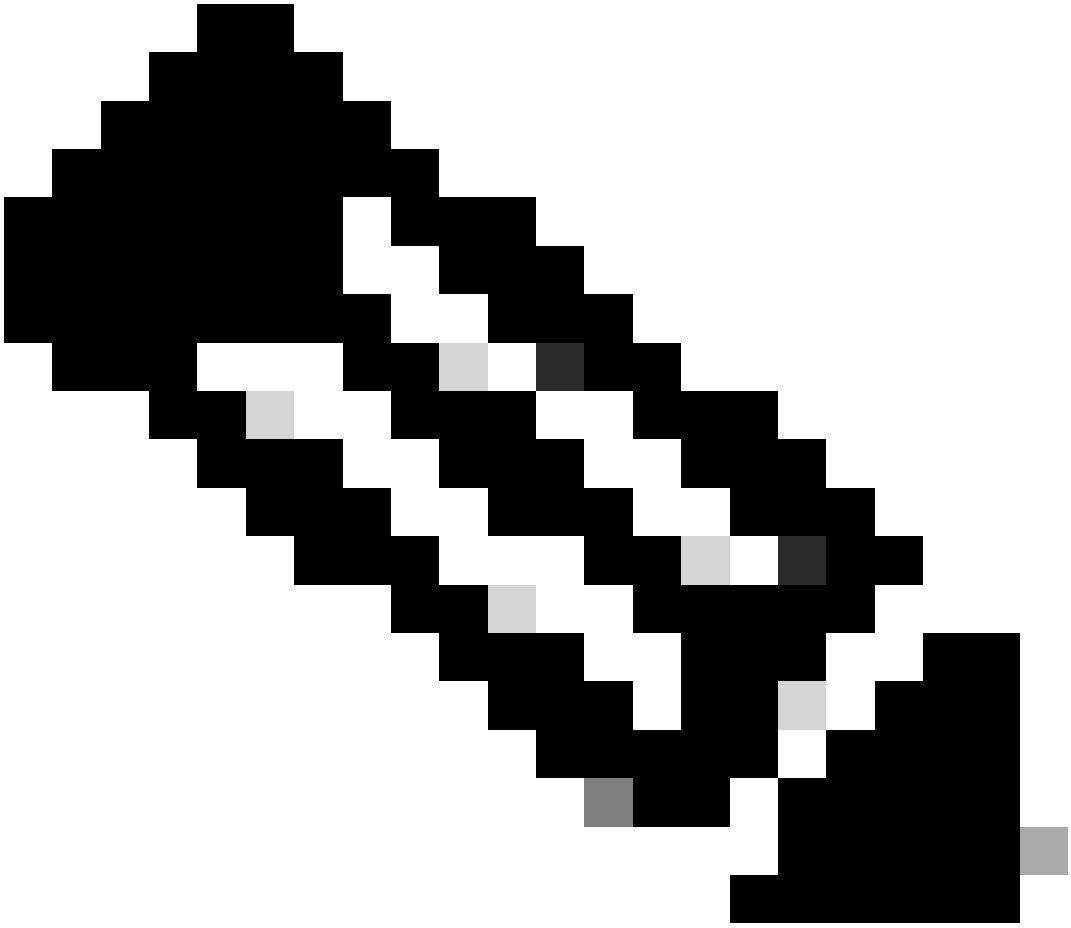
La opción Solicitar credenciales > No recordar nunca está seleccionada. Por lo tanto, en cada autenticación, el usuario que realiza la autenticación debe ingresar sus credenciales.

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

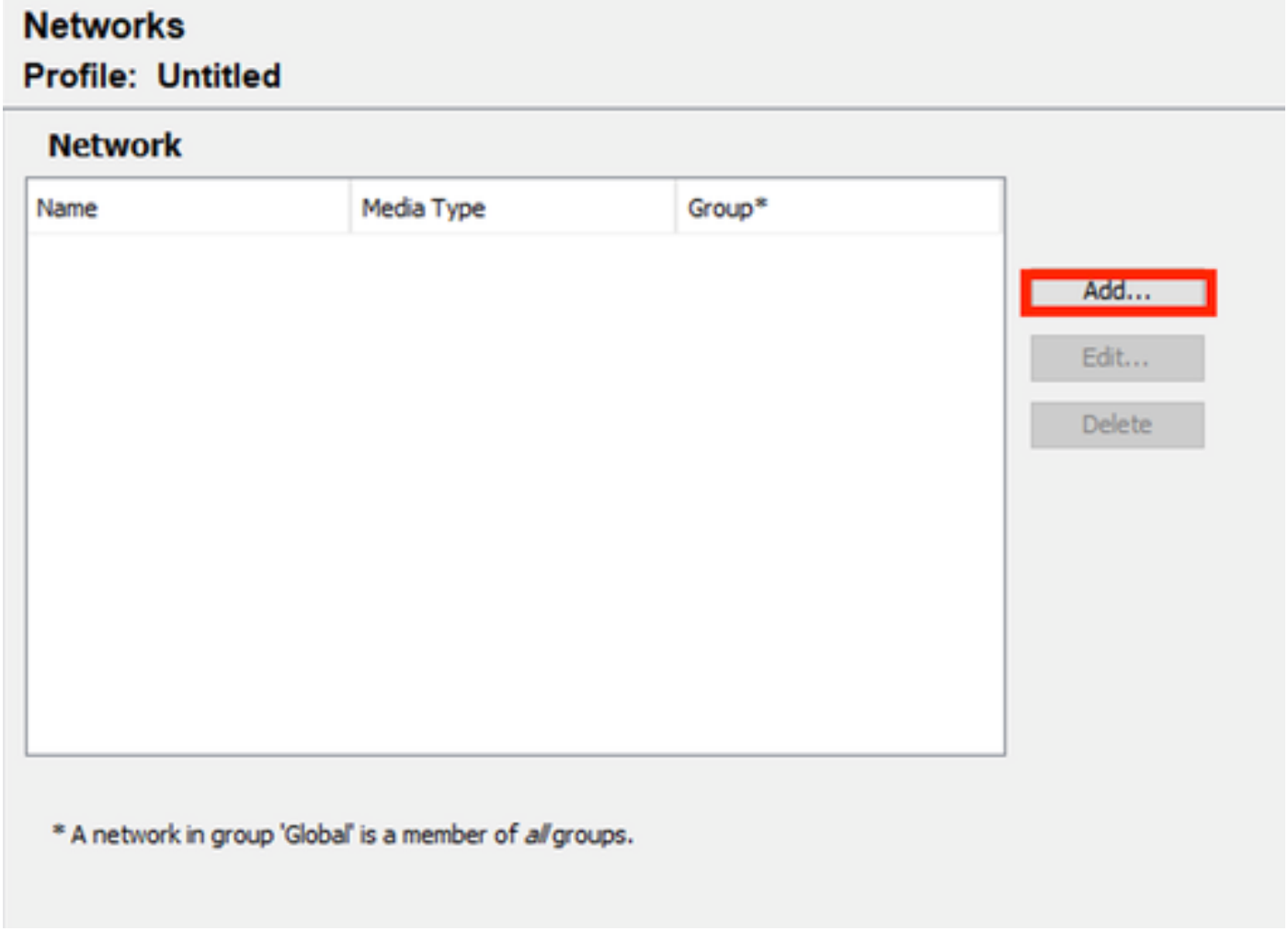


Nota: El archivo debe llamarse configuration.xml; de lo contrario, no funcionará.

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.

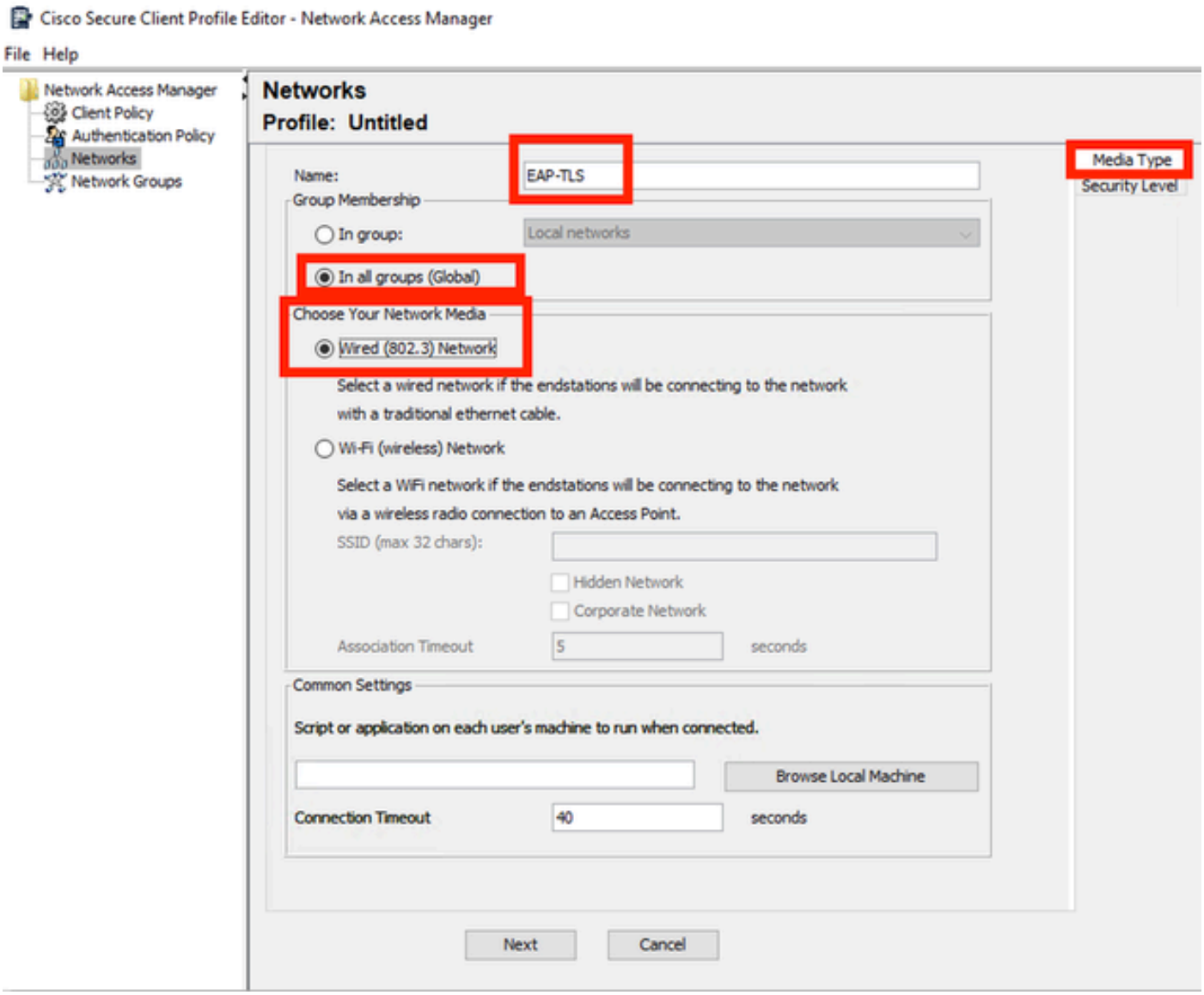
Haga clic en Add (Agregar).



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.

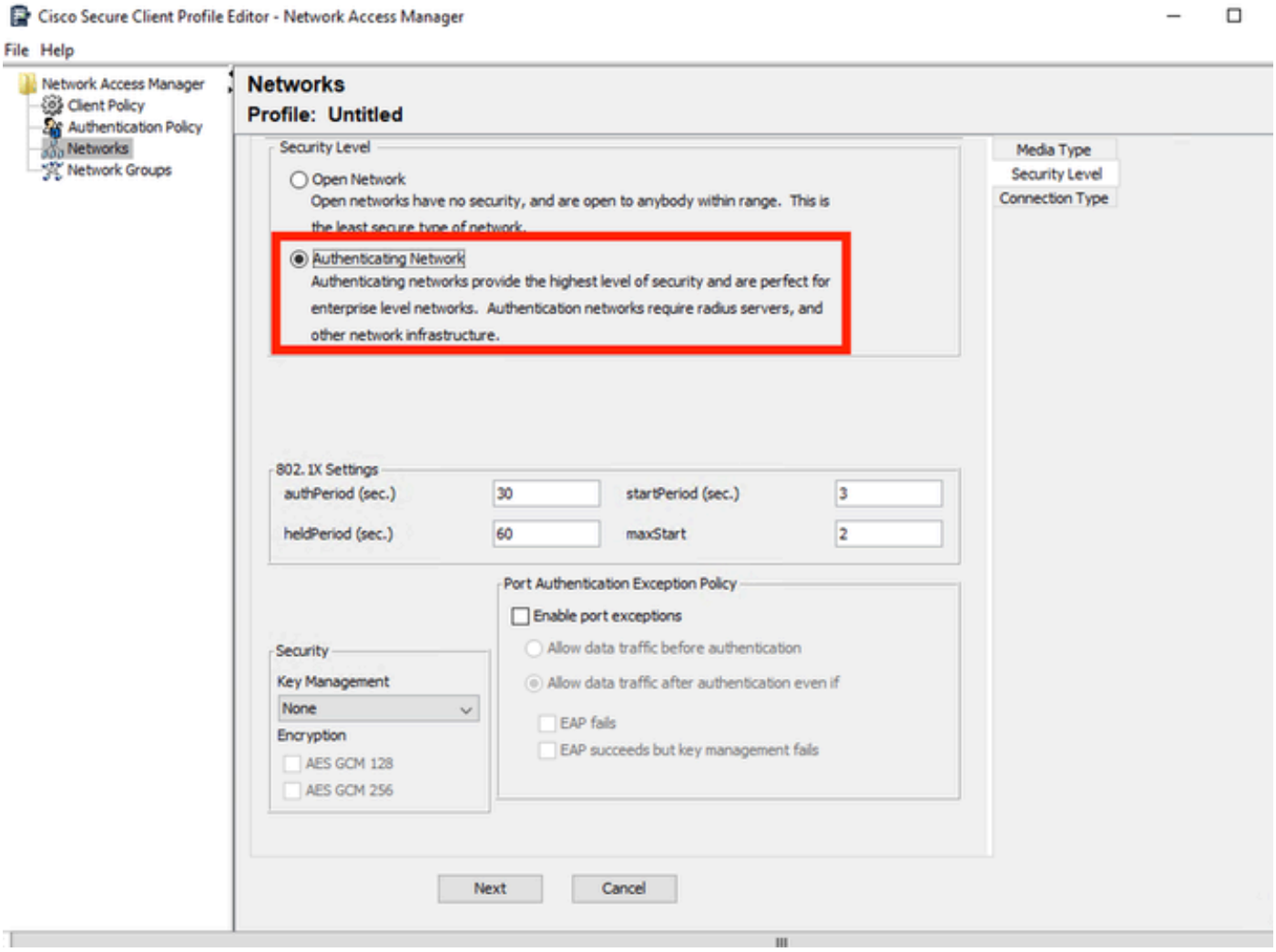
Seleccione Global para Membership Group. y medios de red por cable.



Sección Tipo de medio

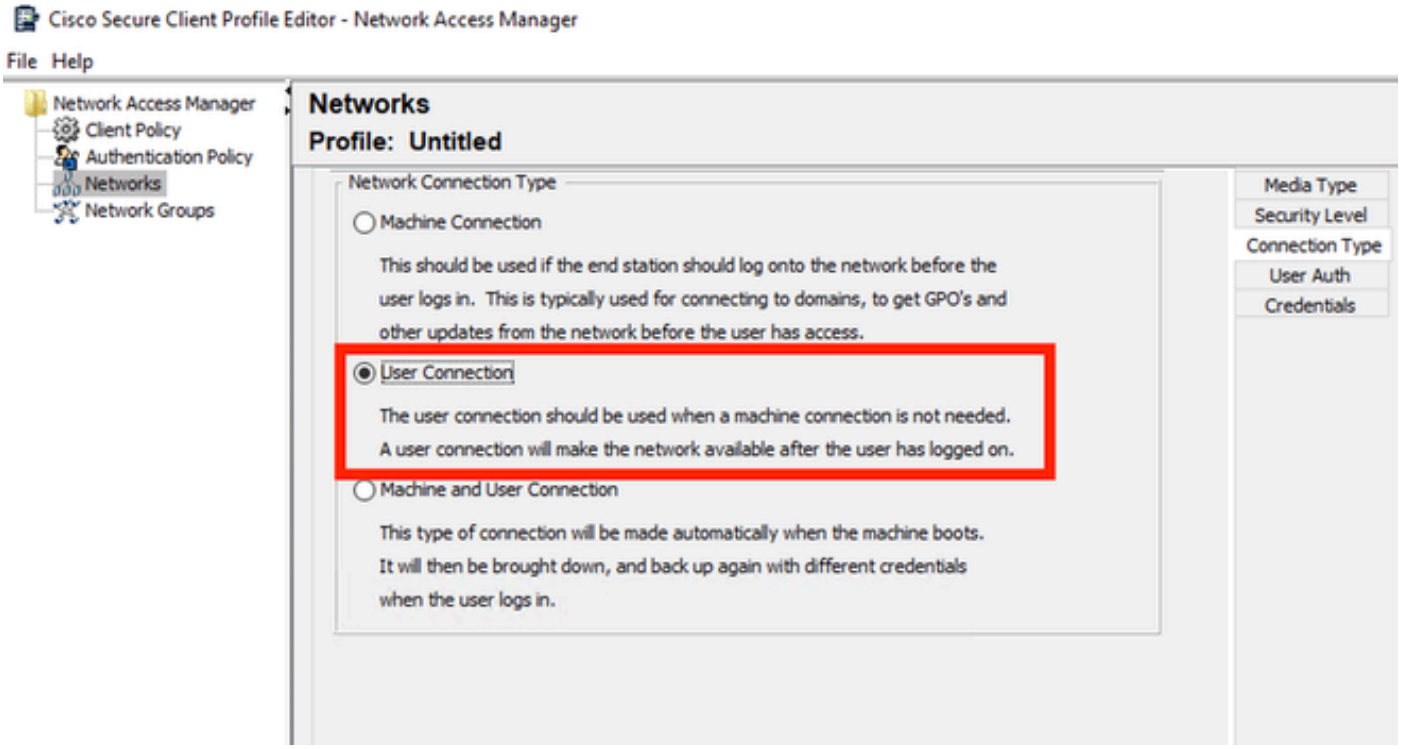
Haga clic en Next (Siguiente).

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



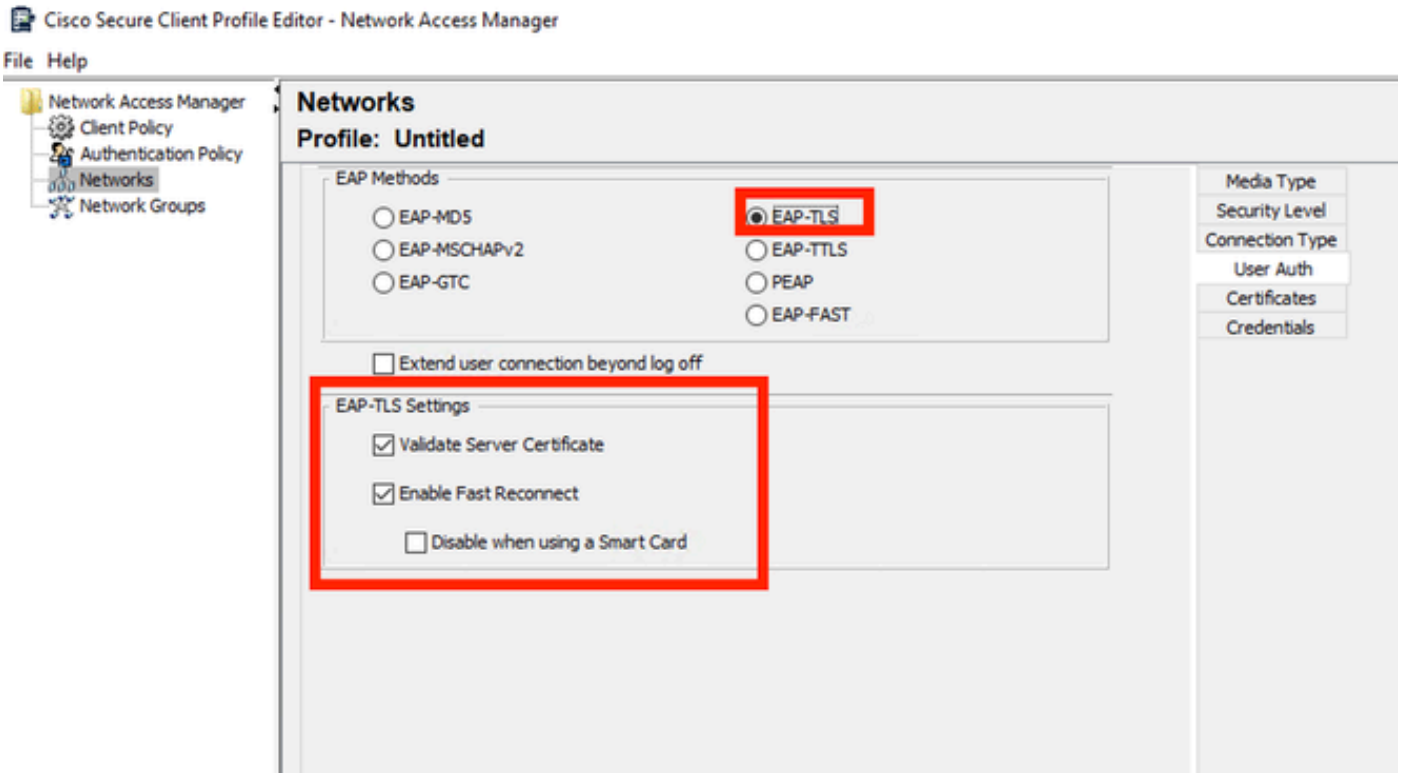
Nivel de seguridad

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



Tipo de conexión

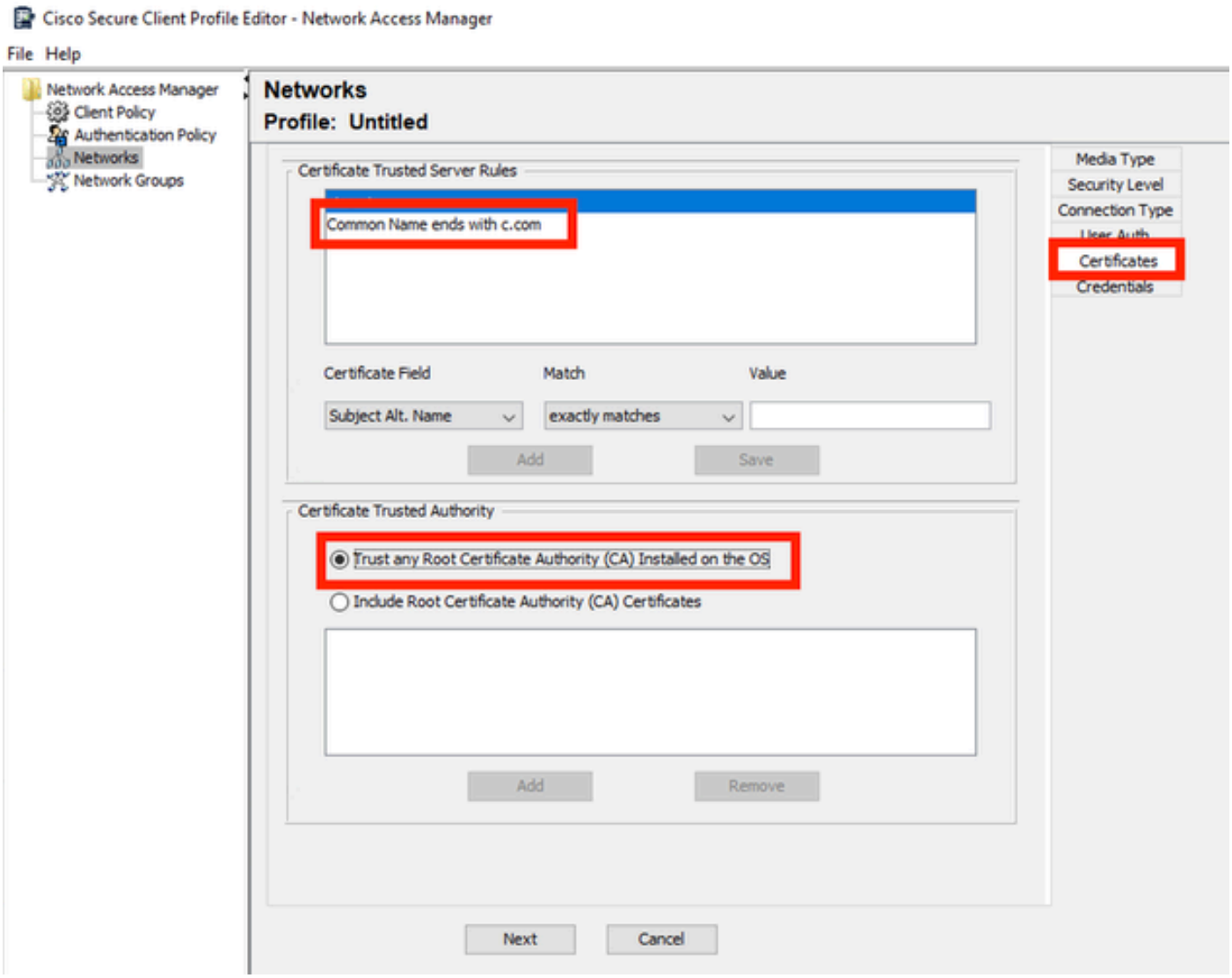
Configure EAP-TLS como el método EAP. No cambie los valores predeterminados en la sección Configuración de EAP-TLS.



Sección de autenticación de usuario

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.

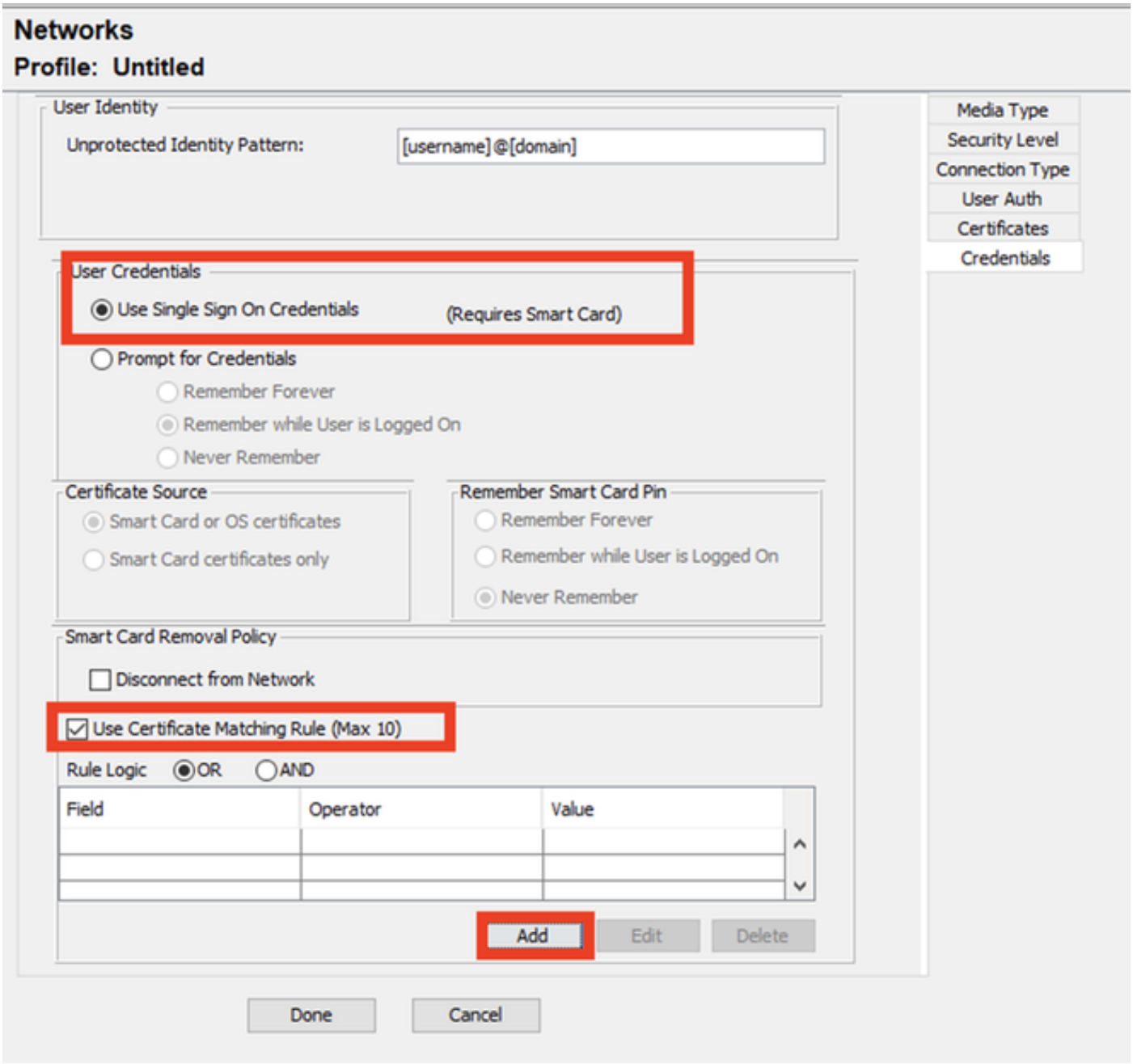
Para la sección Certificate Trusted Authority, seleccione Trust any Root Certificate Authority (CA) instalado en el sistema operativo.



Configuración de confianza del certificado del servidor de autenticación de usuario

Haga clic en Next (Siguiente).

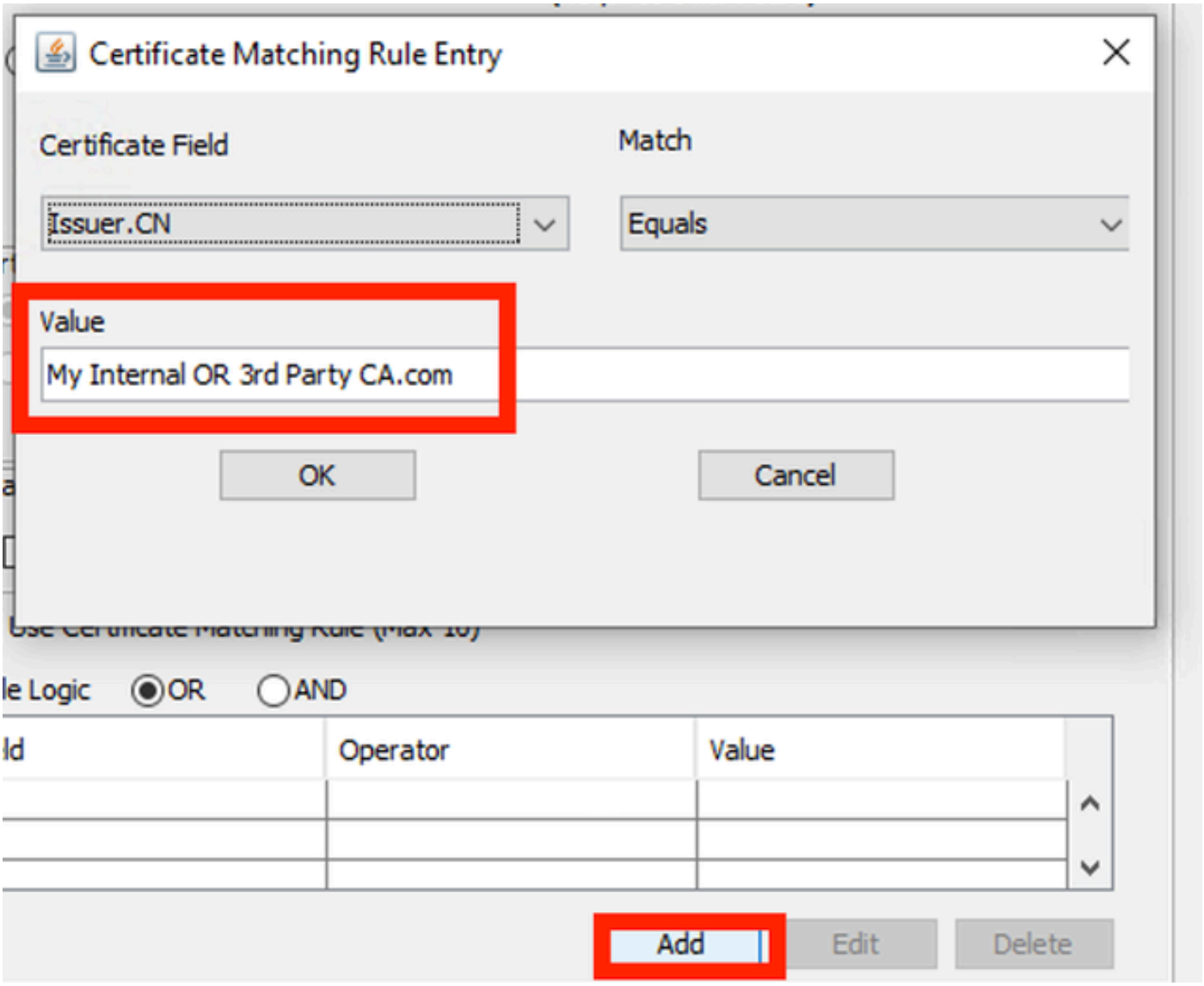
En la sección Credenciales de usuario, no cambie los valores predeterminados de la primera parte.



Sección Credenciales de Autenticación de Usuario

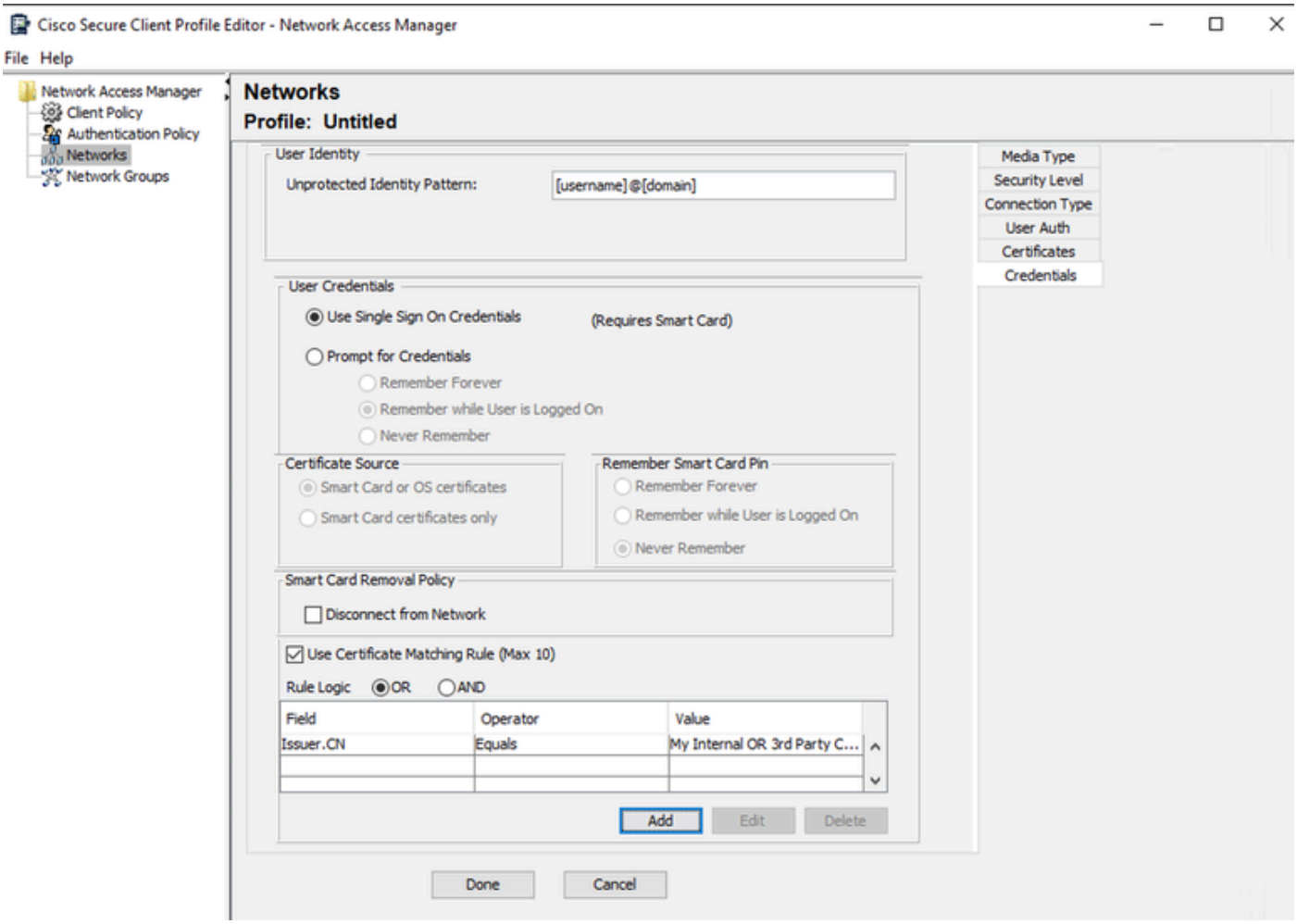
Es importante configurar una regla que coincida con el certificado de identidad que el usuario envía durante el proceso EAP-TLS. Para ello, haga clic en la casilla de verificación junto a Usar regla de asignación de certificados (máximo 10).

Haga clic en Add (Agregar).



Ventana Regla de coincidencia de certificados

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



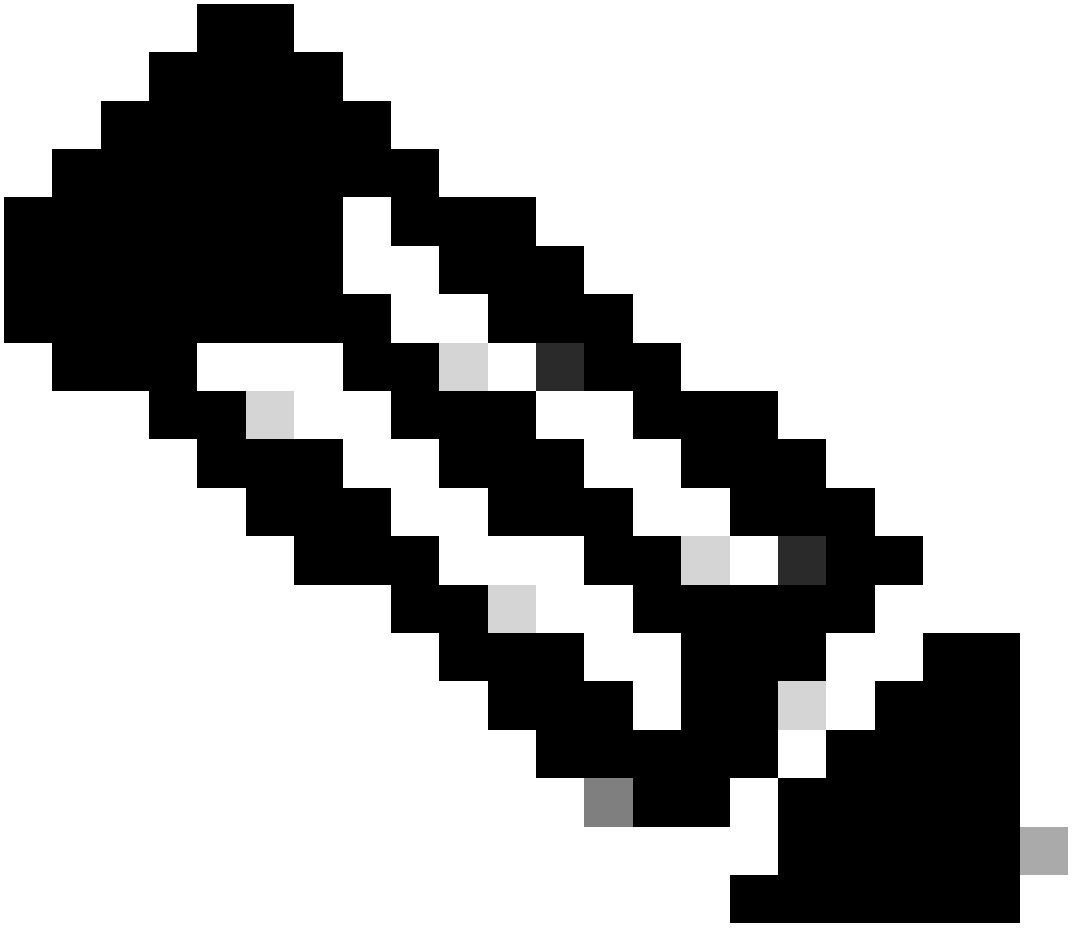
Sección Credenciales de Certificado de Autenticación de Usuario

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



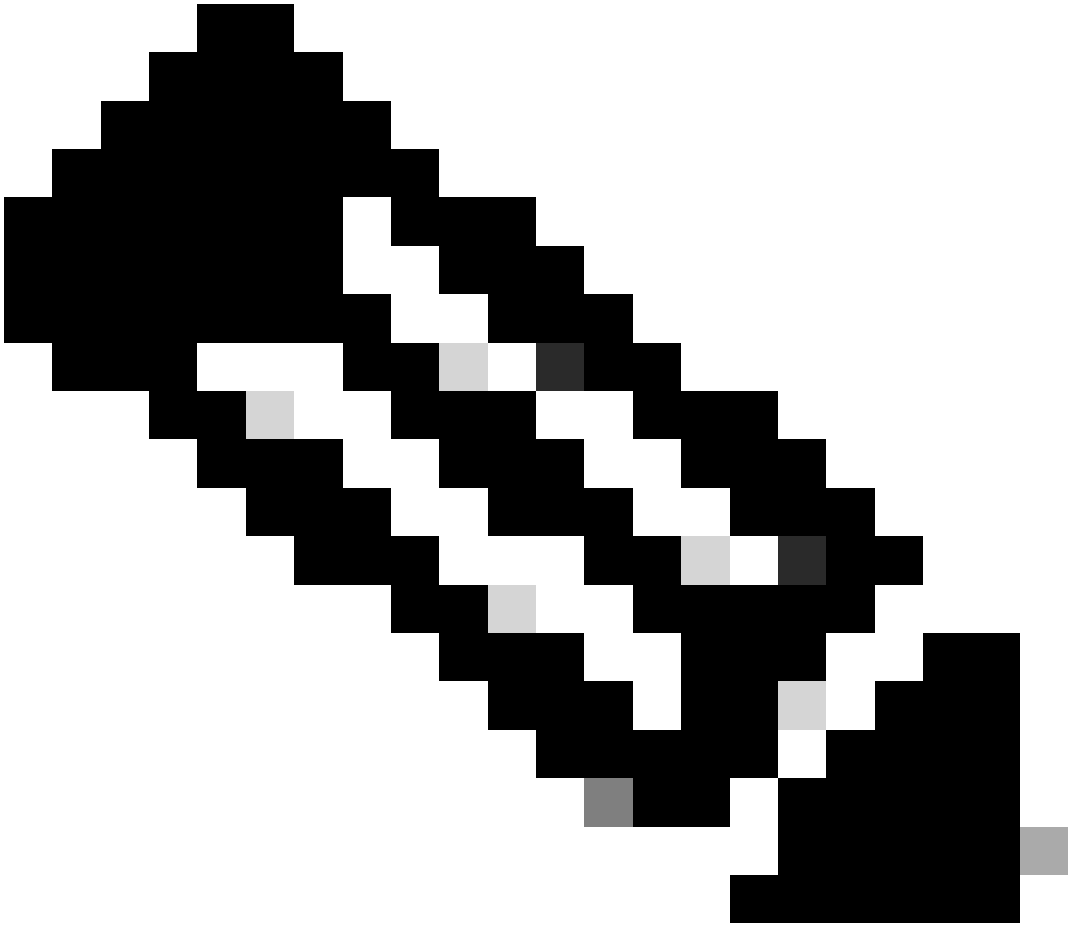
Nota: El archivo debe llamarse configuration.xml; de lo contrario, no funcionará.

---

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>
```

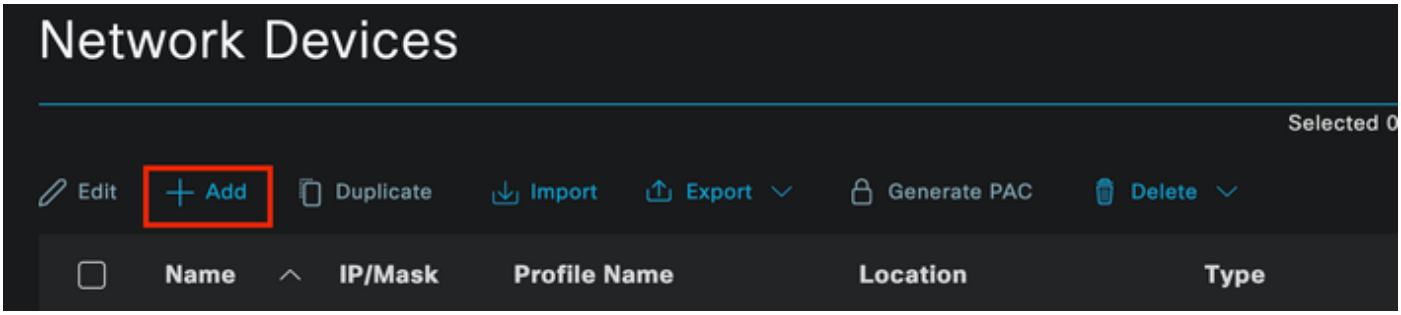
```
!
!
aaa group server radius ISE-CLUSTER
 server name ISE-PSN-1
!
interface GigabitEthernet0/1/0
 description "Endpoint that supports dot1x"
 switchport access vlan 15
 switchport mode access
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication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

Configuración de Identity Service Engine 3.2.

Configure el dispositivo de red.

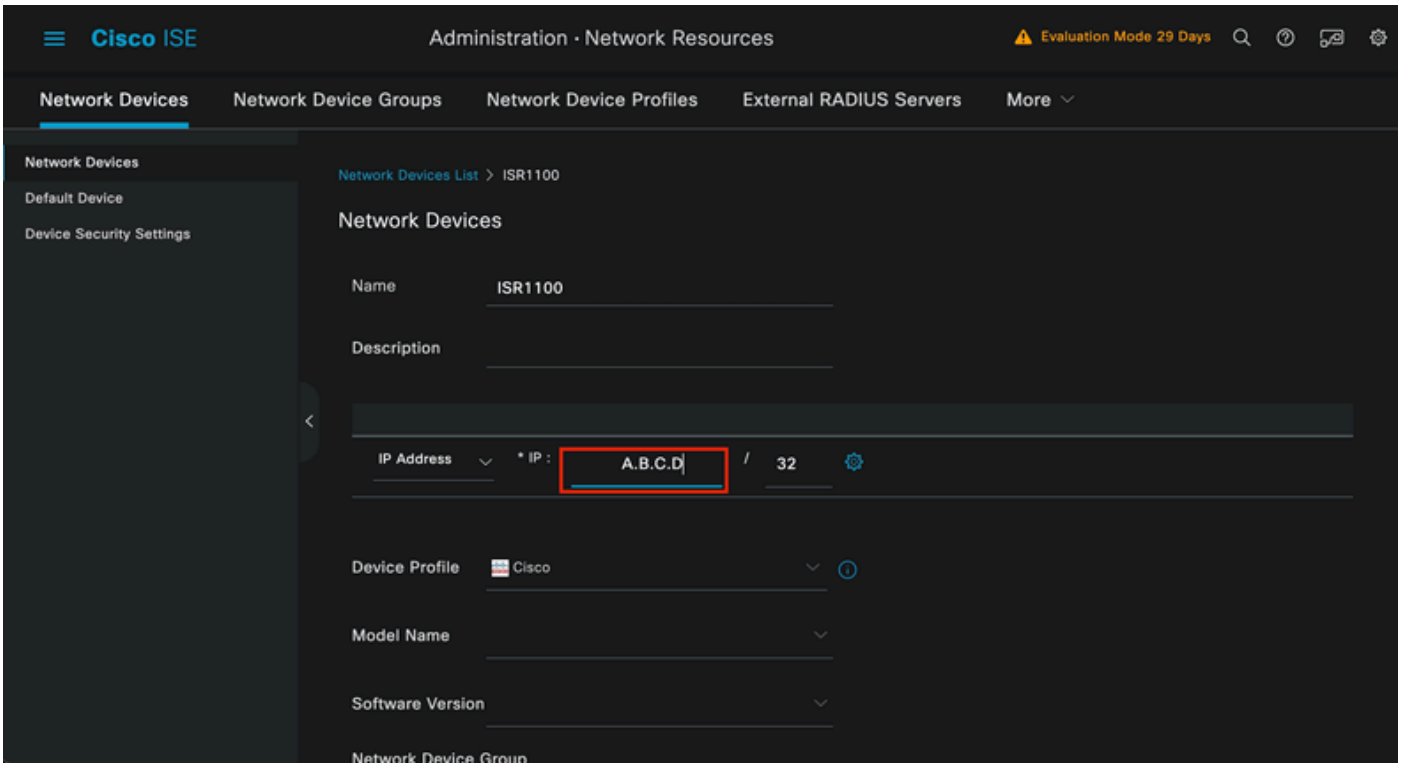
Agregue el ISR NAD a ISE Administration > Network Resources > Network Devices.

Haga clic en Add (Agregar).



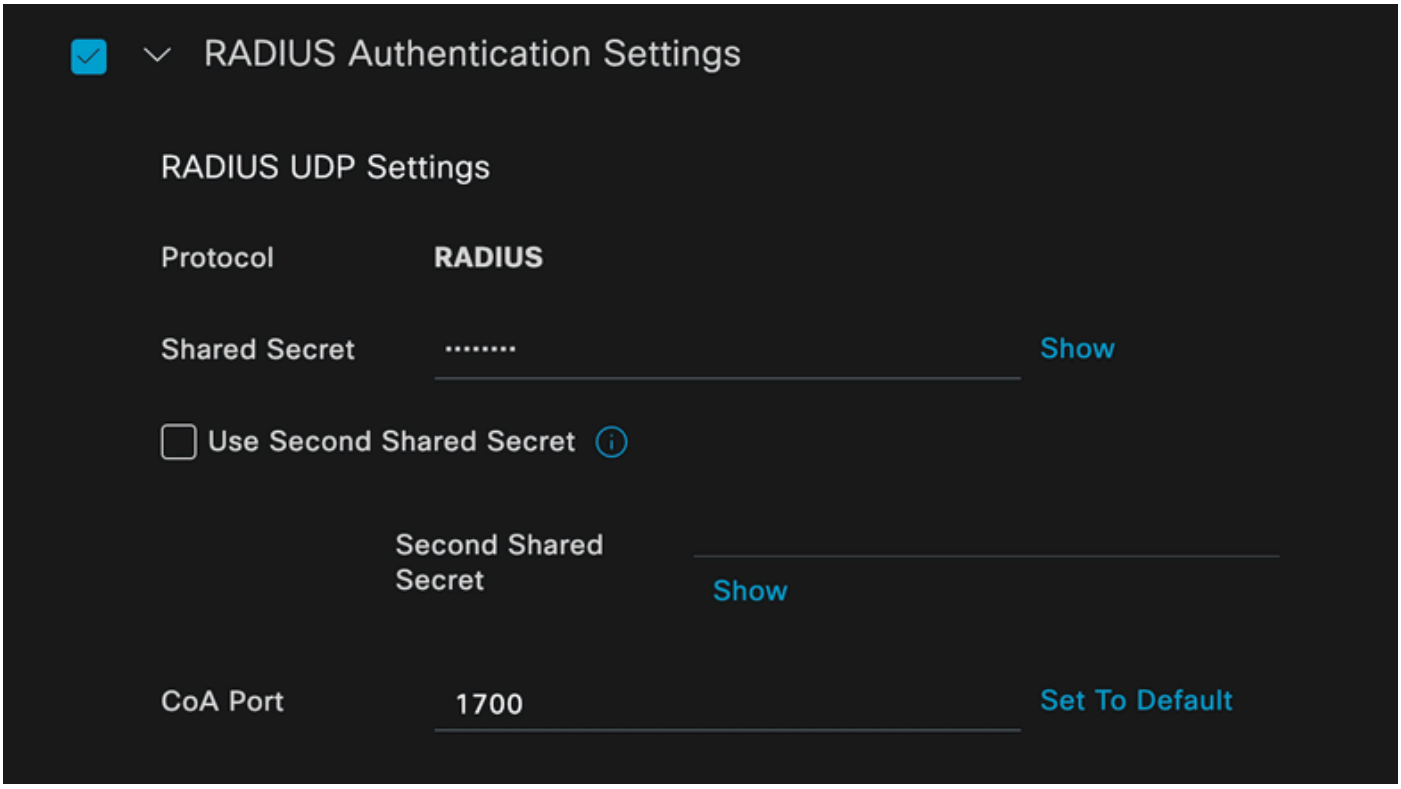
Sección Dispositivo de red

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.



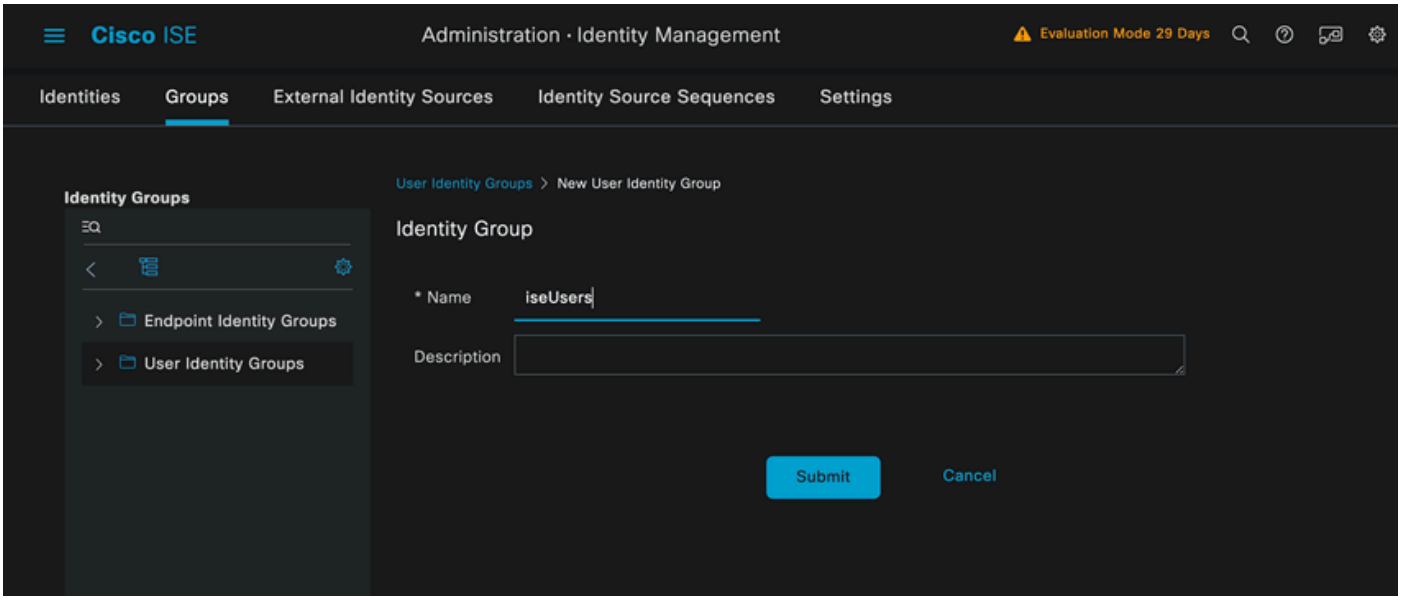
Configuración de RADIUS del dispositivo de red

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.

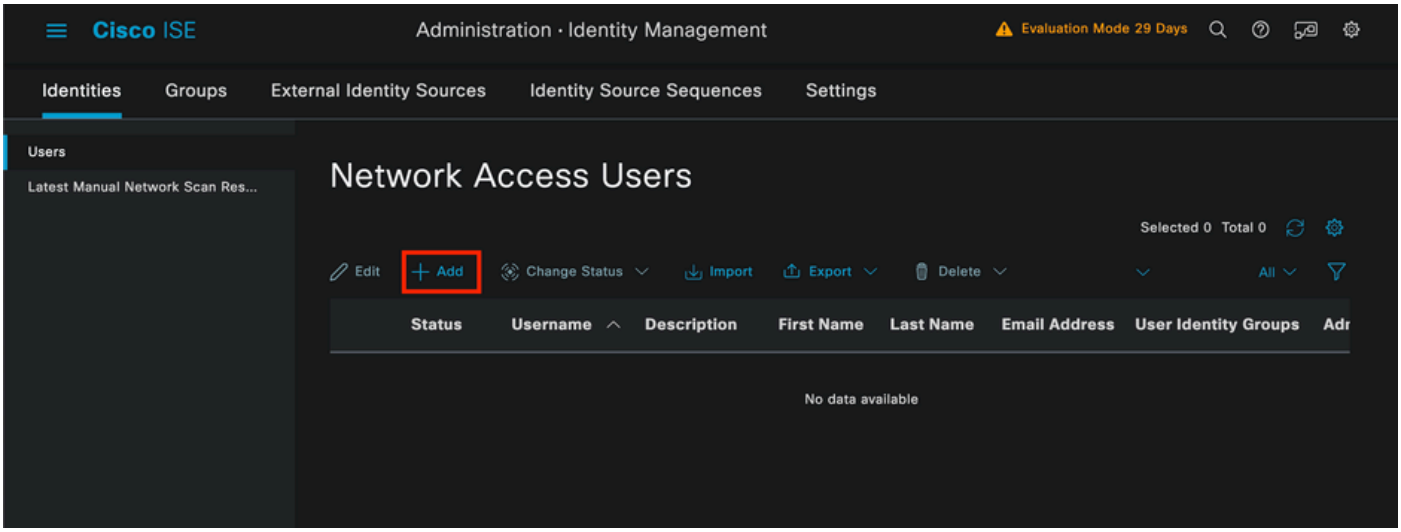


Creación de grupos de identidad

Haga clic en Submit (Enviar).

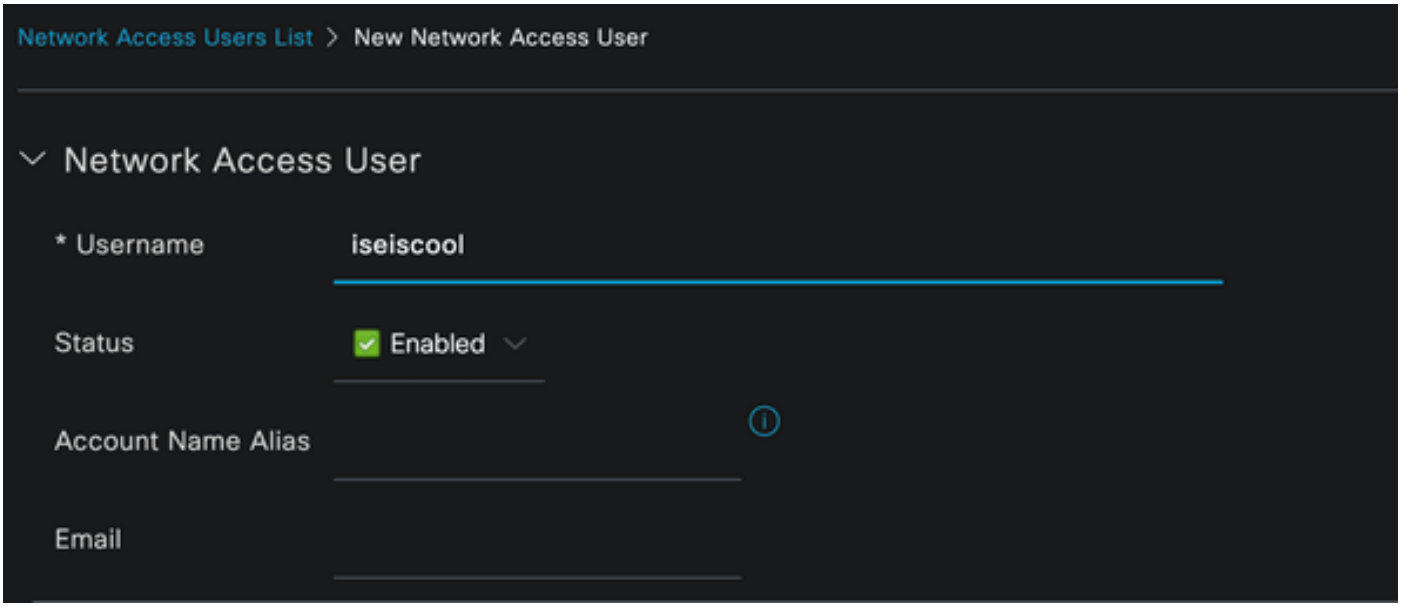
Vaya a Administration > Identity Management > Identity Tab.

Haga clic en Add (Agregar).



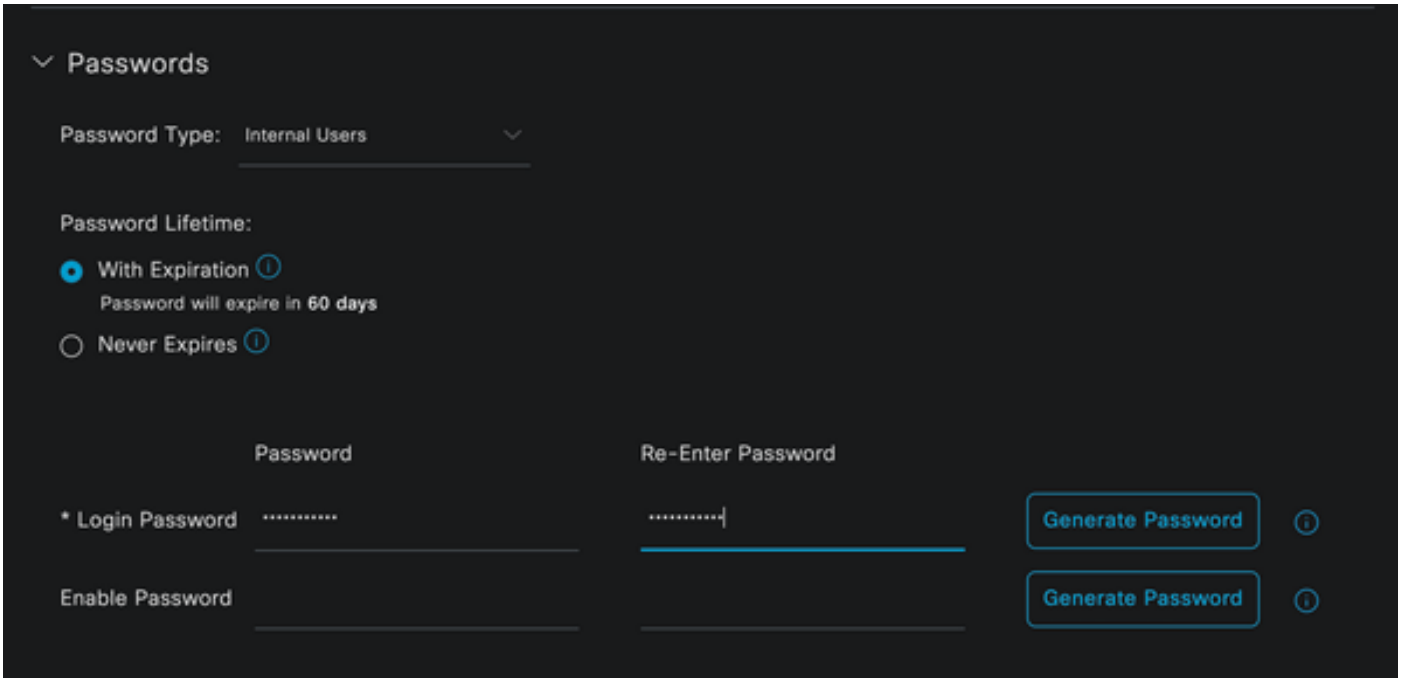
Sección Usuarios de Acceso a Red

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



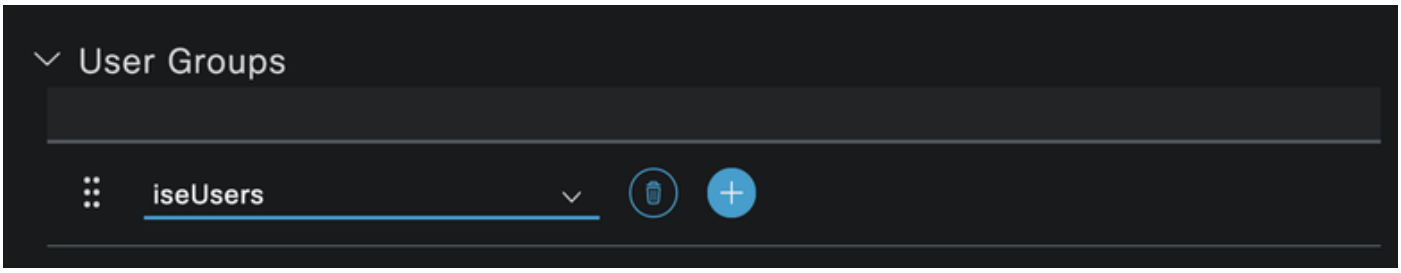
Creación de usuario de acceso a red

Asigne una contraseña al usuario. Se utiliza VainillaISE97.



Sección Contraseña de Creación de Usuario

Asigne el usuario al grupo iseUsers.

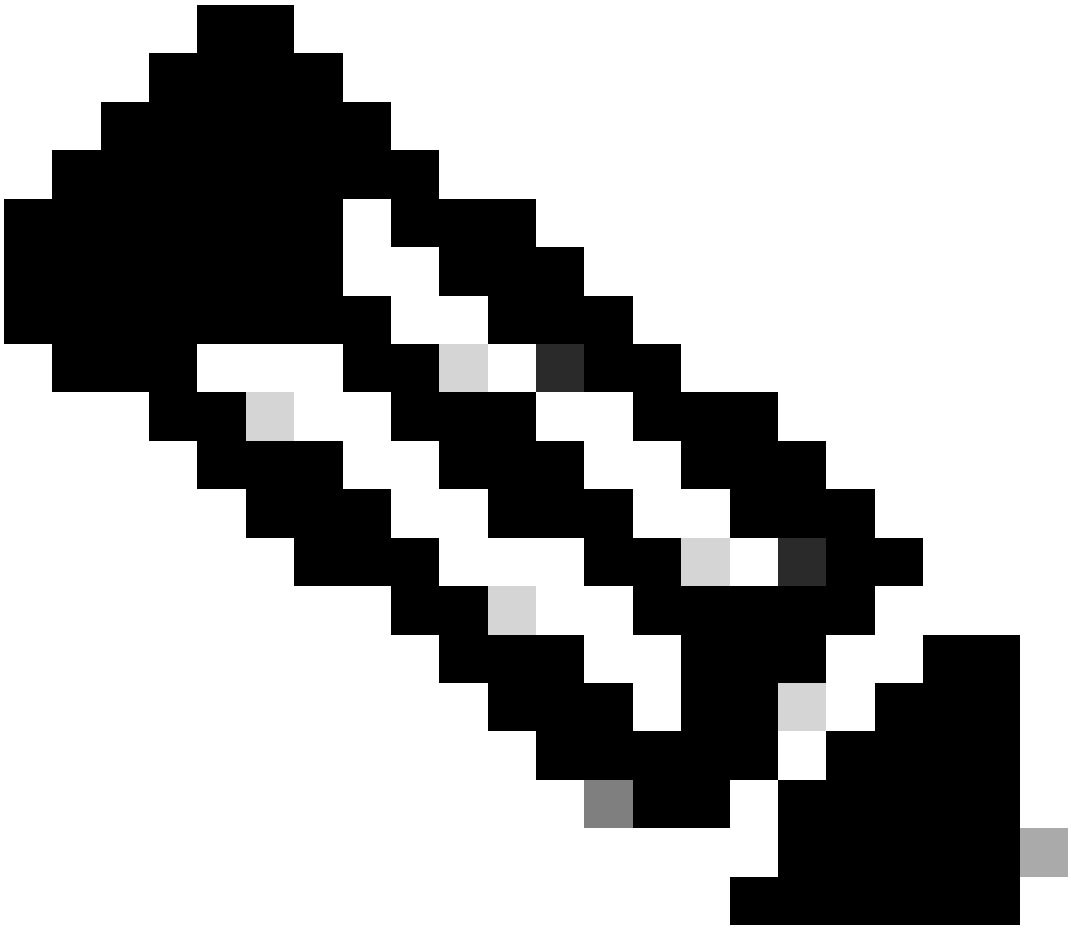


Asignación de grupo de usuarios

Configure el conjunto de directivas.

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

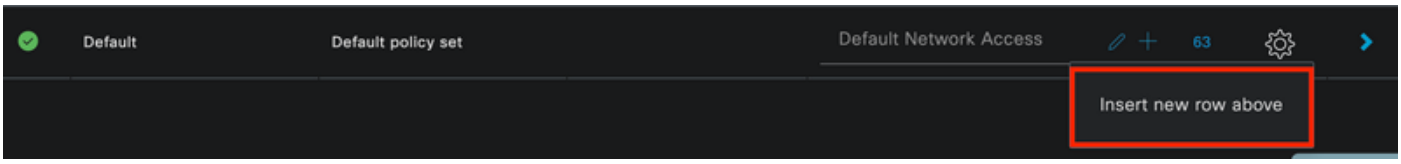
Se puede utilizar el conjunto de políticas predeterminado. Sin embargo, se crea una llamada Wired para este ejemplo.



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

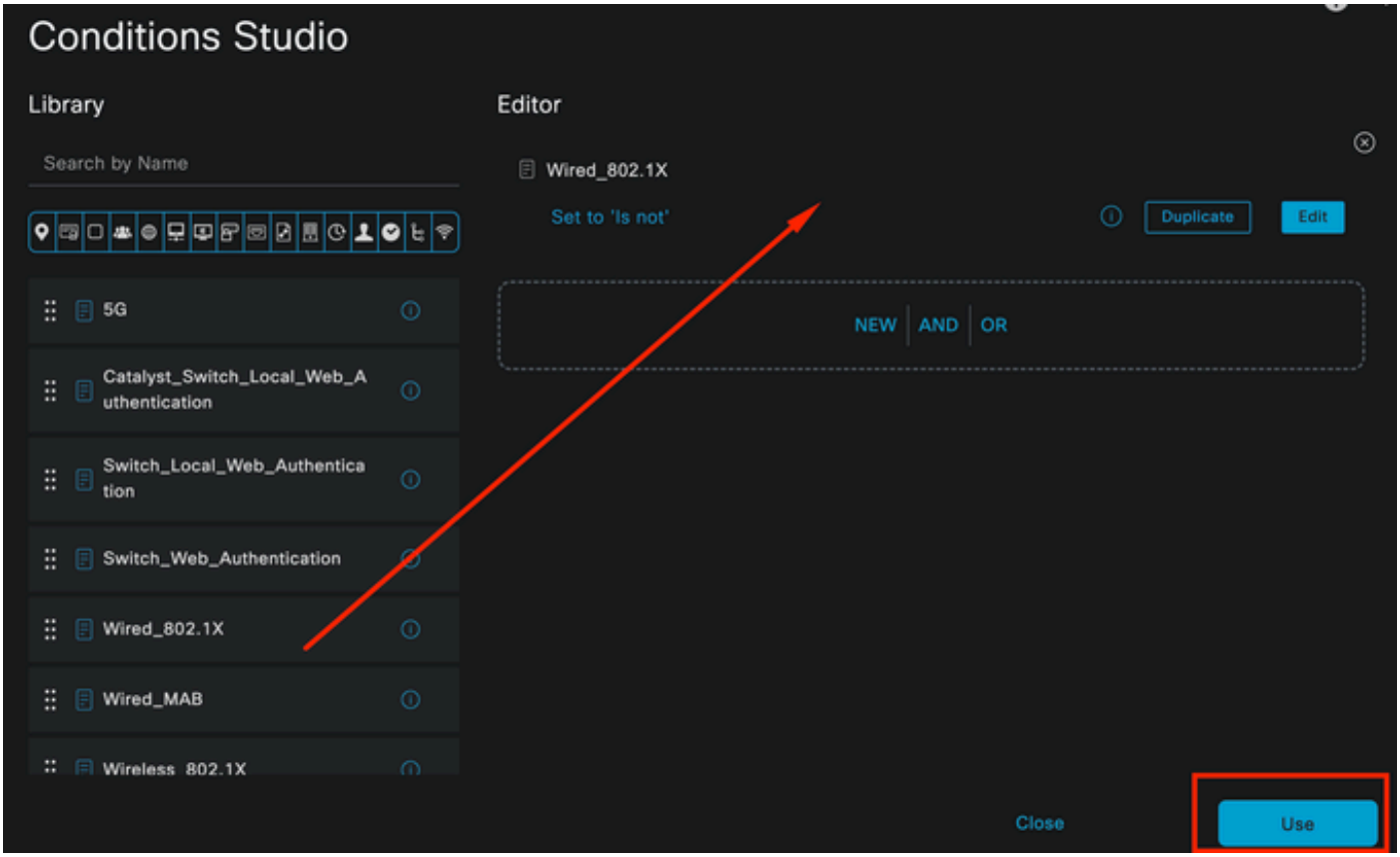
---

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.



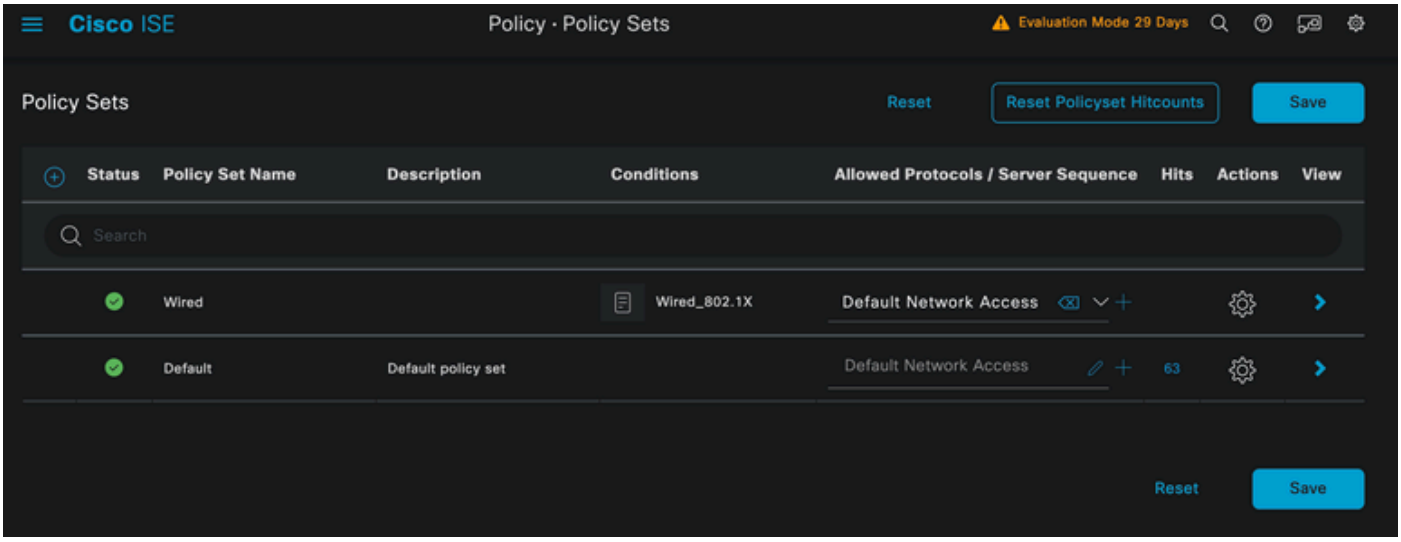
Opciones de iconos de engranajes

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.

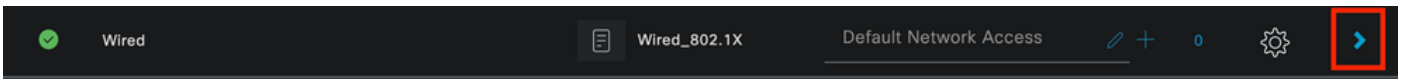


Vista general de conjuntos de políticas

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 +.

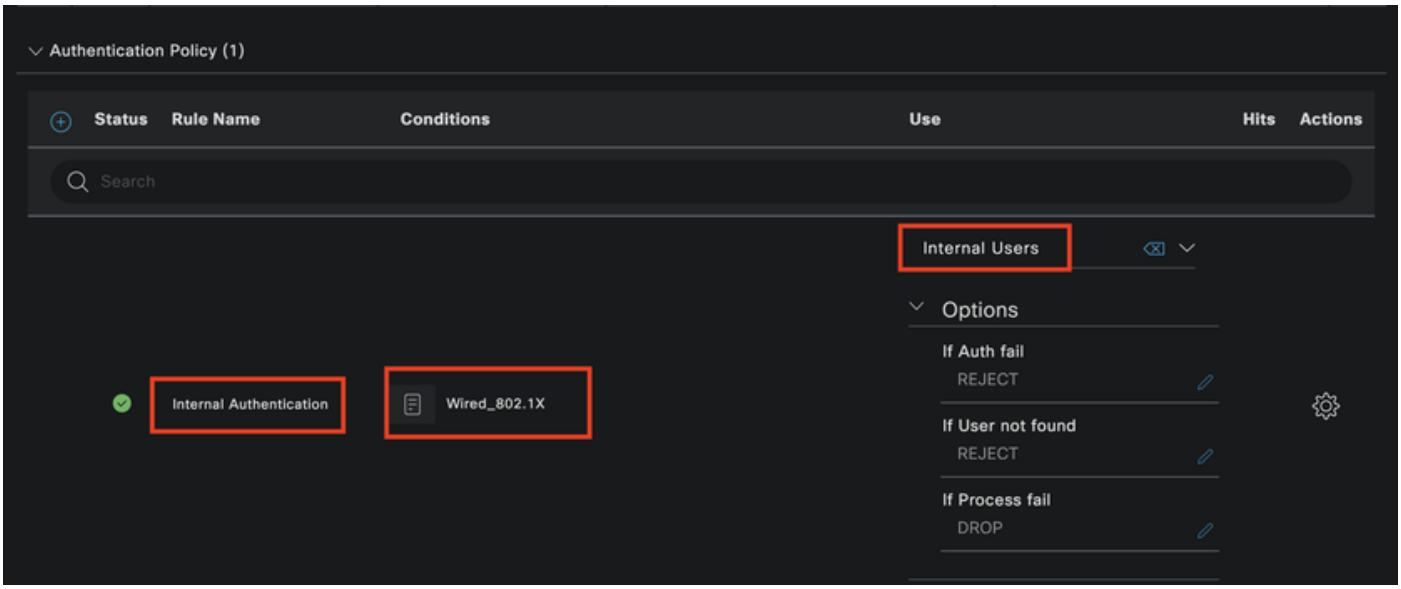
Política de autenticación

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.

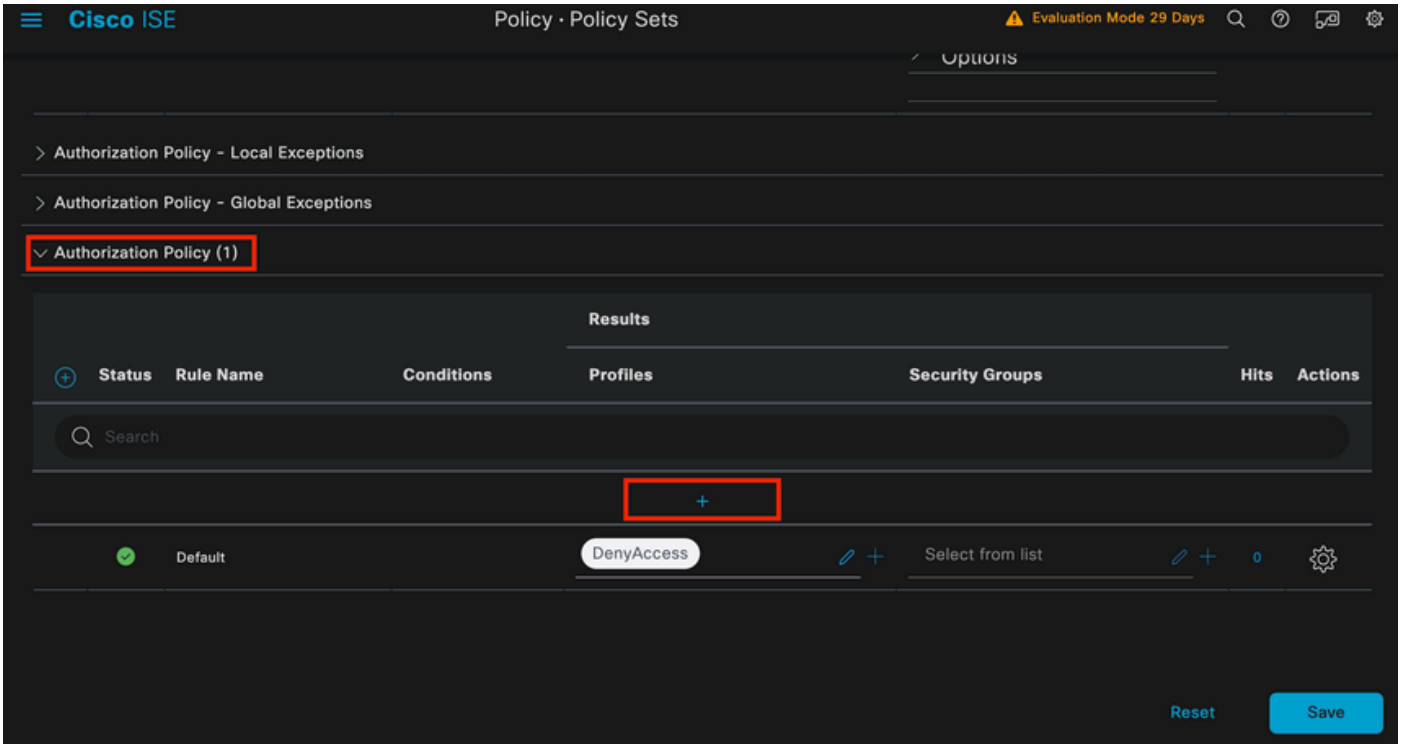
Por último, en la columna Use, seleccione Internal Users.



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.

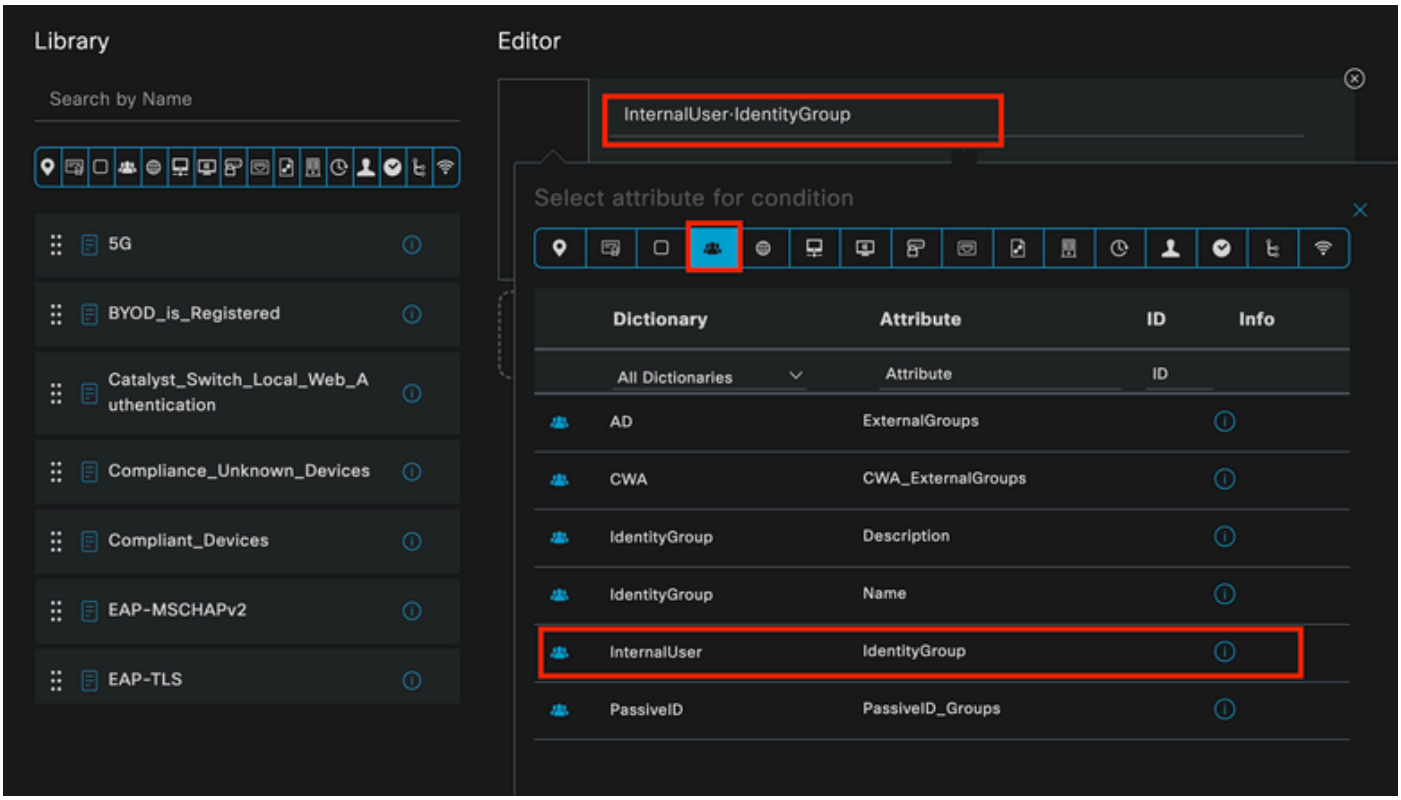
Para crear una condición para esta directiva de autorización, haga clic en el icono + de la columna Condiciones.

Se utiliza el grupo IseUsers.

Haga clic en la sección Atributo.

Seleccione el icono IdentityGroup.

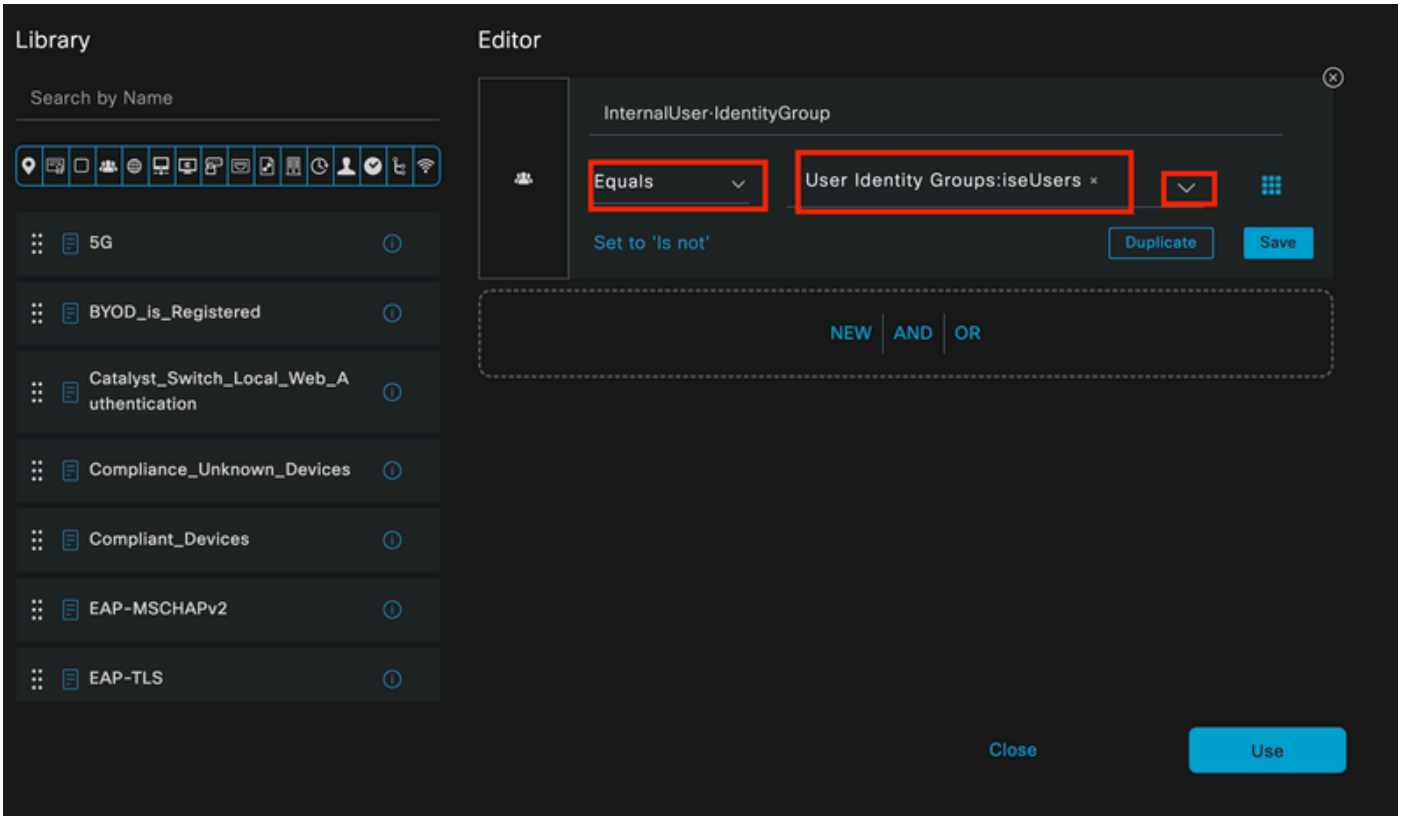
En el diccionario, seleccione el diccionario InternalUser que viene con el atributo IdentityGroup.



Creación de condiciones

Seleccione el operador Equals.

En User Identity Groups, seleccione el grupo IseUsers.

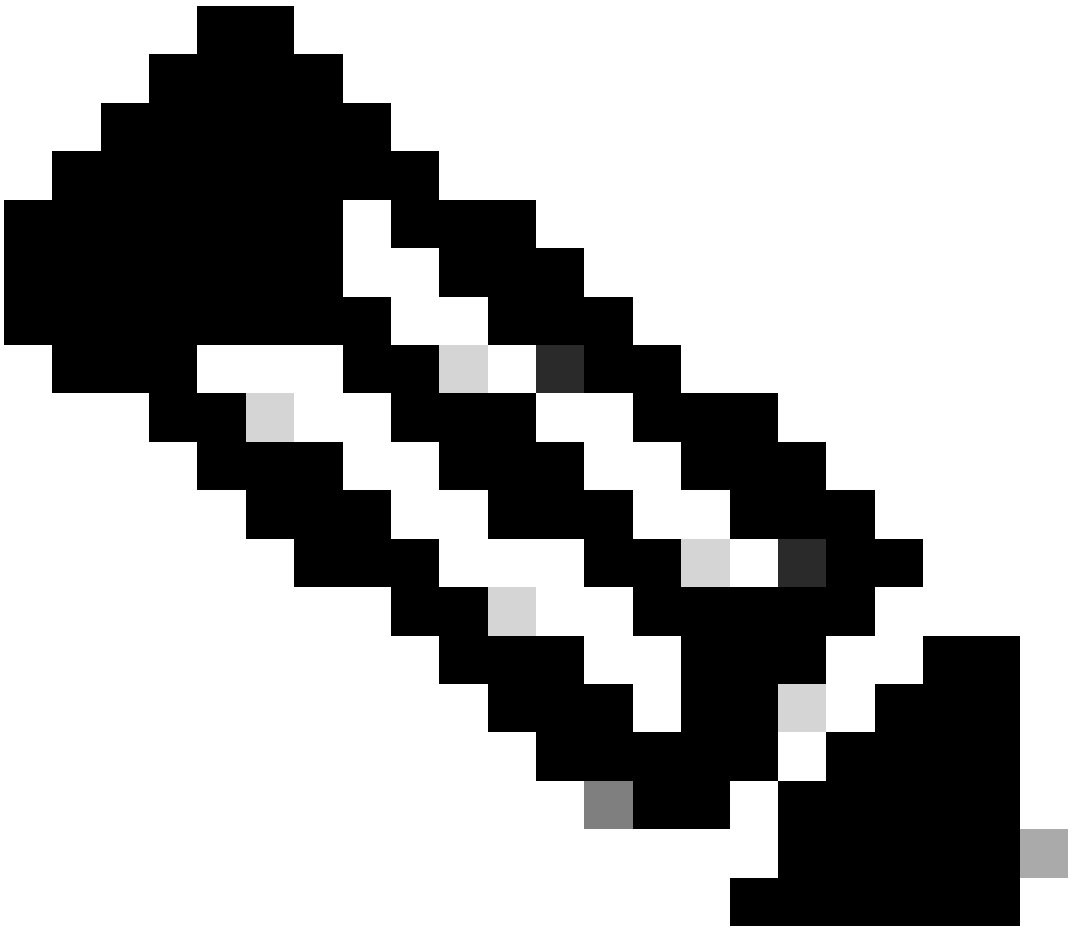


Creación de condiciones

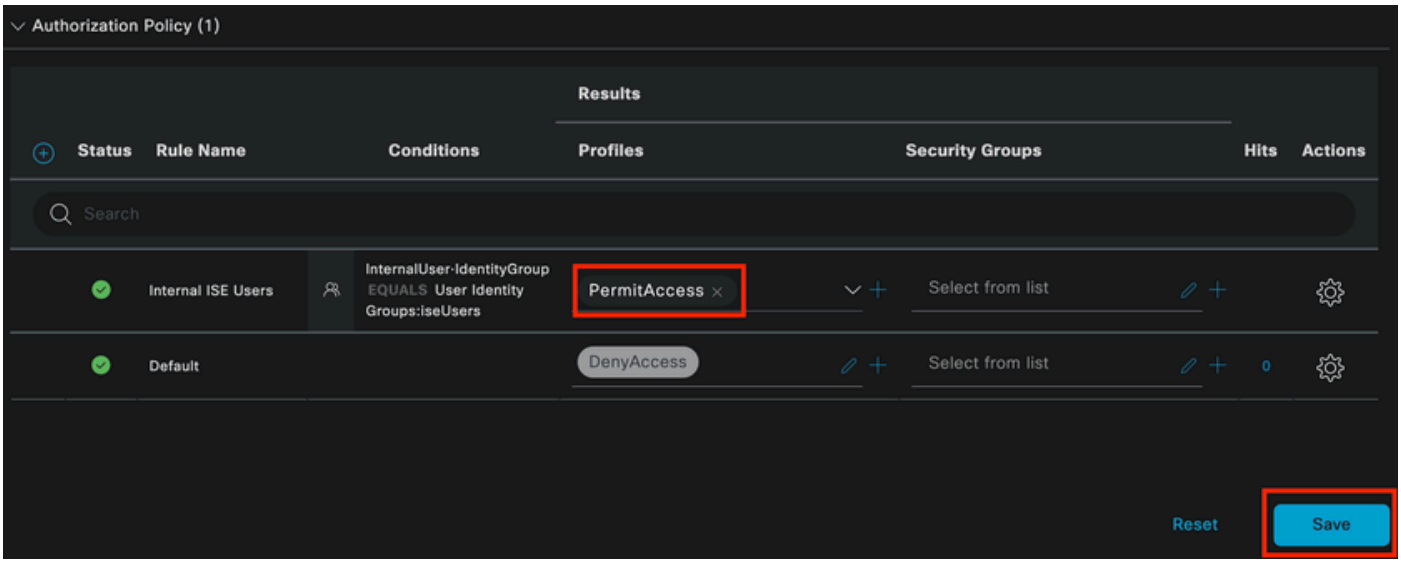
Haga clic en Usar.

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.



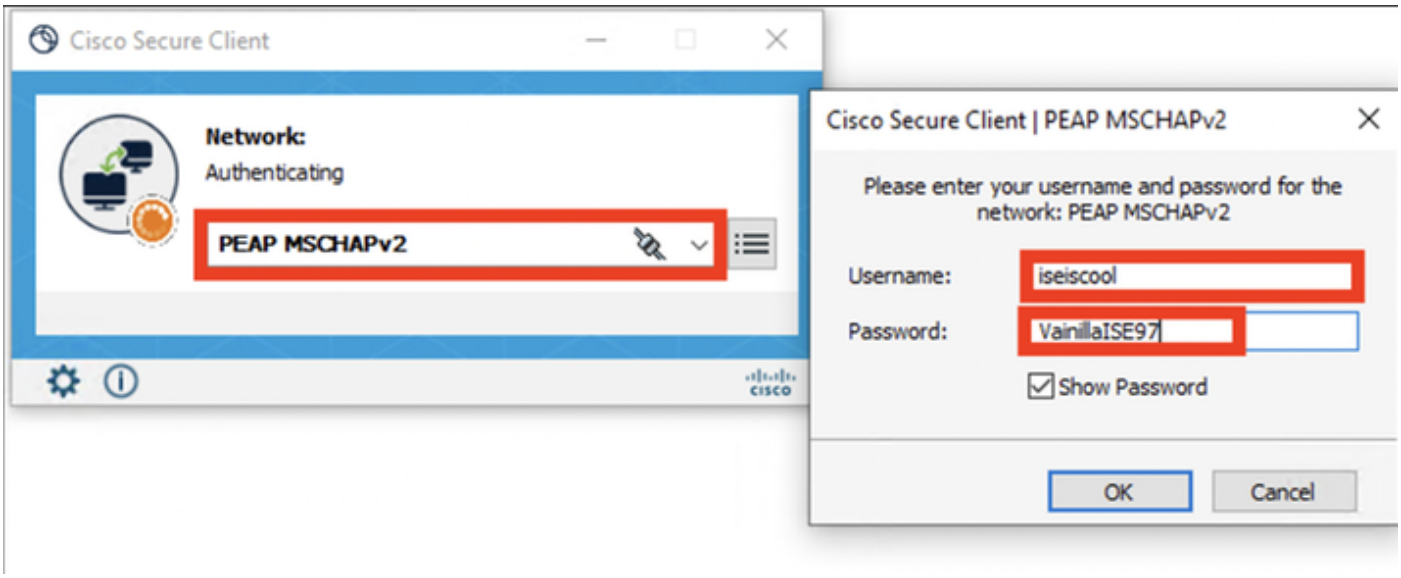
Política de autorización

Click Save.

Verificación

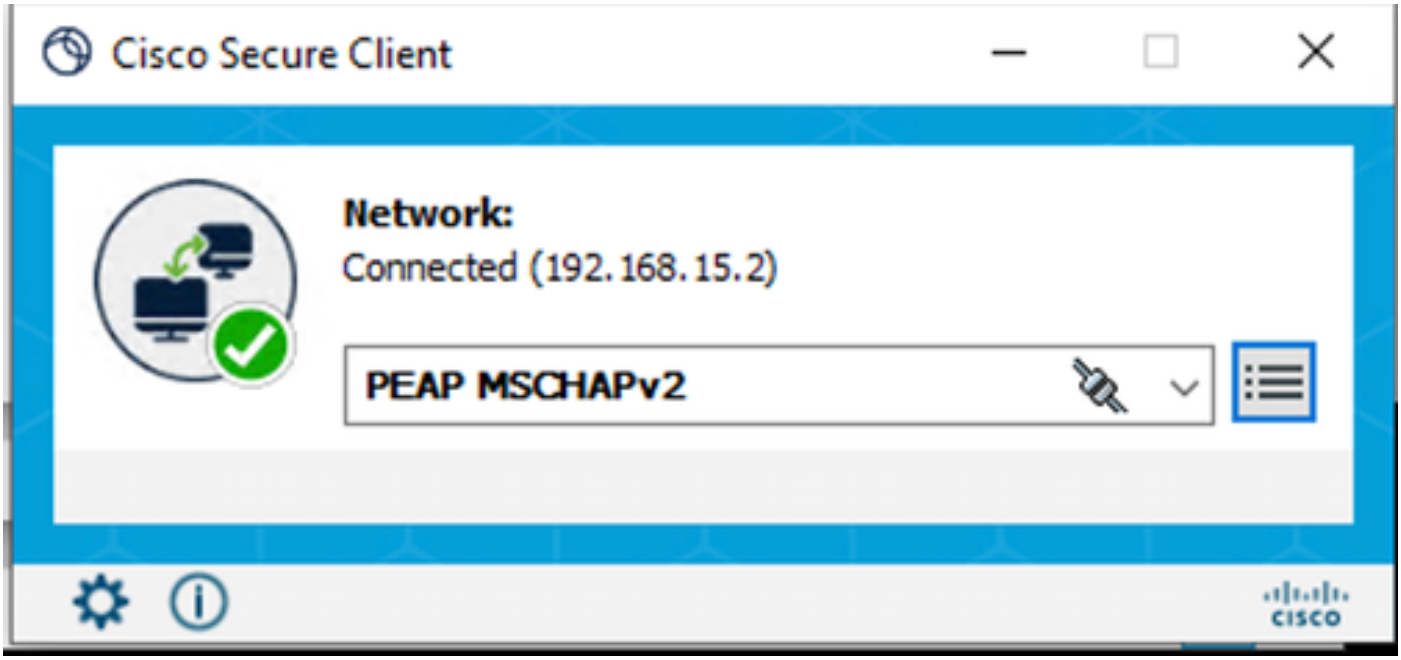
Una vez finalizada la configuración, Secure Client solicita las credenciales y especifica el uso del perfil PEAP MSCHAPv2.

Se introducen las credenciales creadas anteriormente.



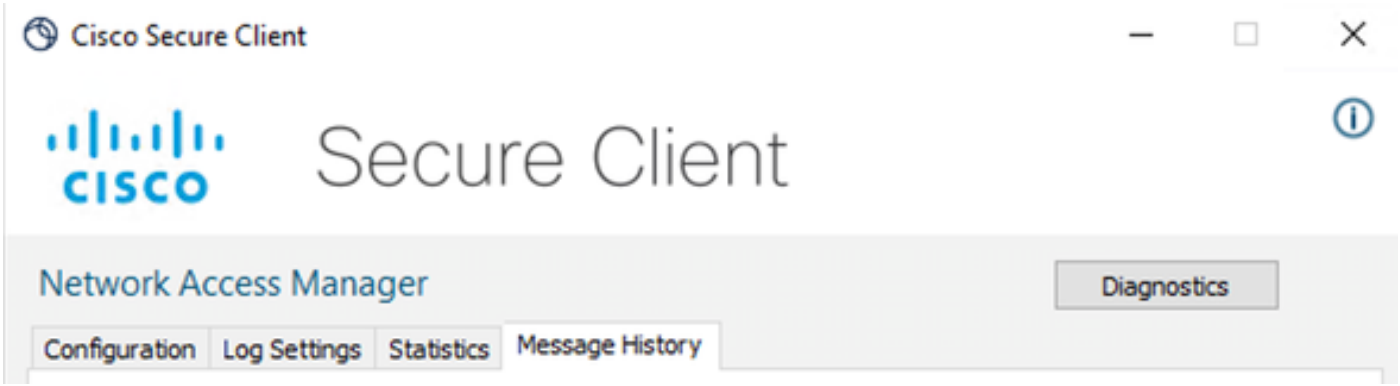
NAM de cliente seguro

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

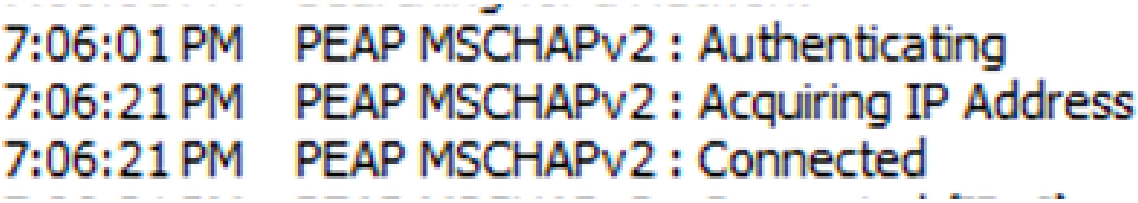


NAM de cliente seguro

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



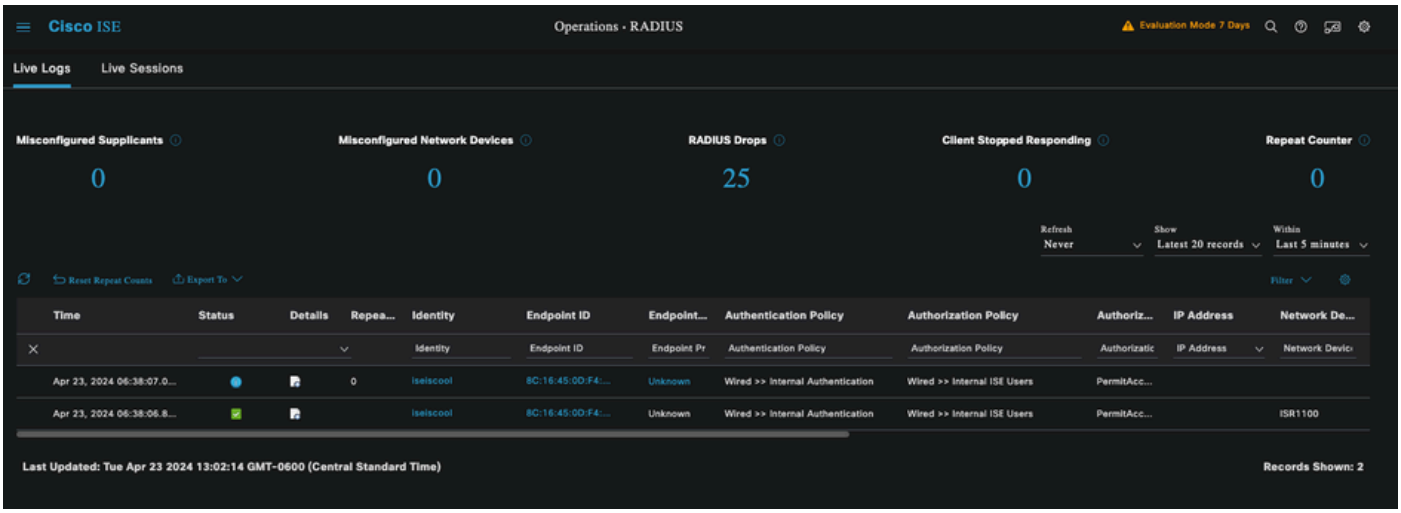
Historial de mensajes de Secure Client

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.



Registros en directo de ISE RADIUS

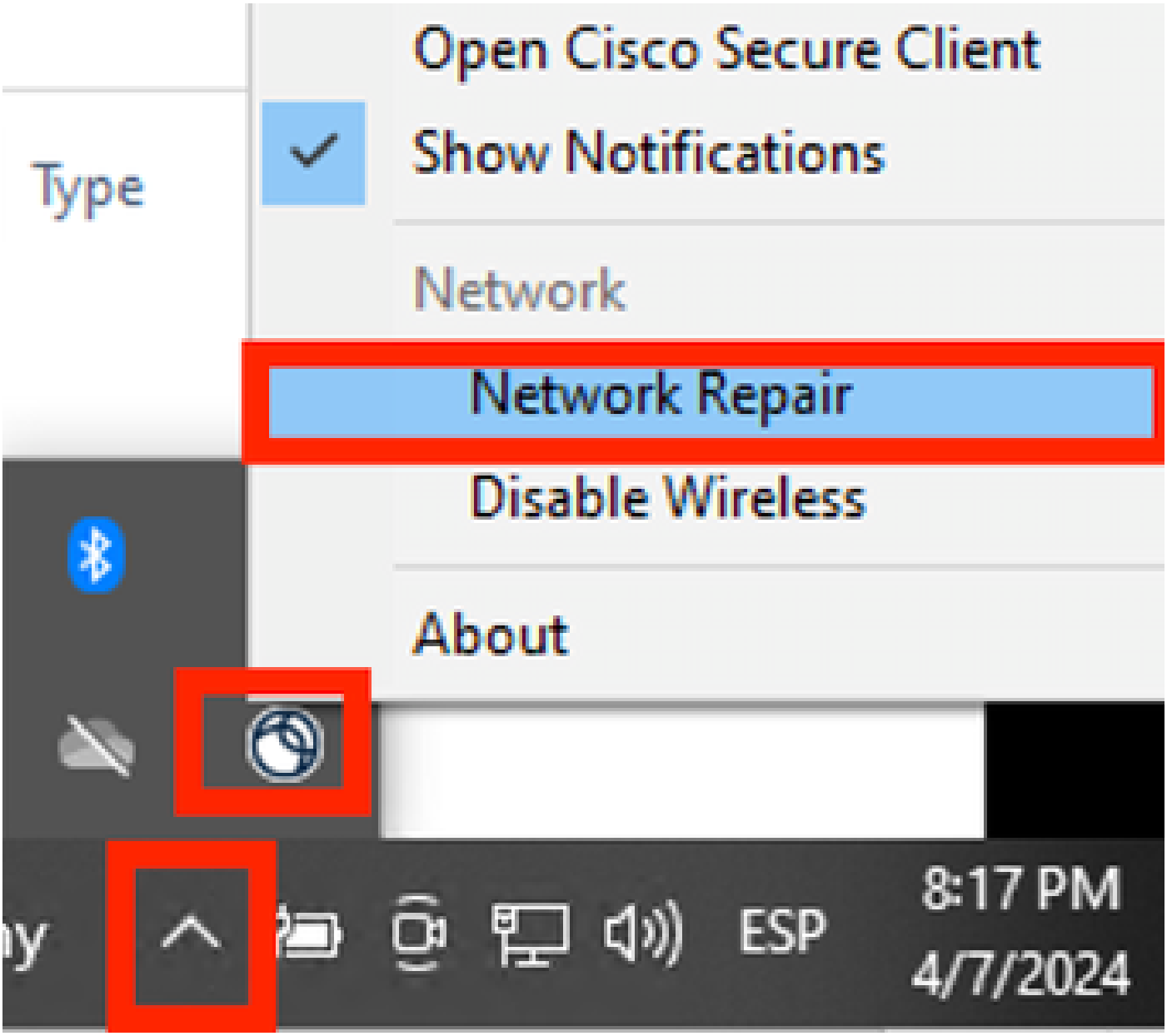
Como puede ver que llega a las políticas correctas, y el resultado es un estado de autenticación exitoso, se concluye que la configuración es correcta.

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.

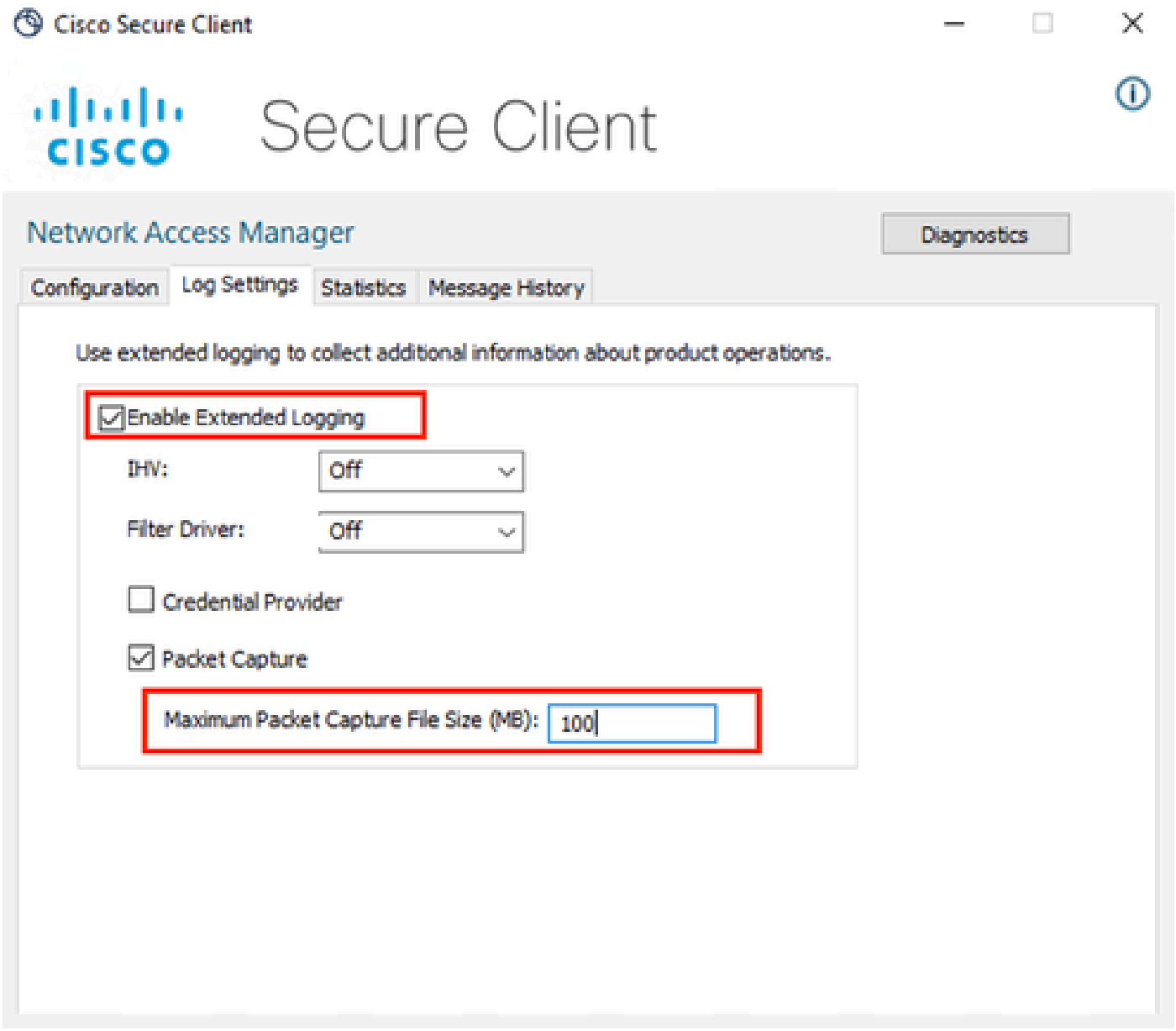
1. Activar registro extendido NAM

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.



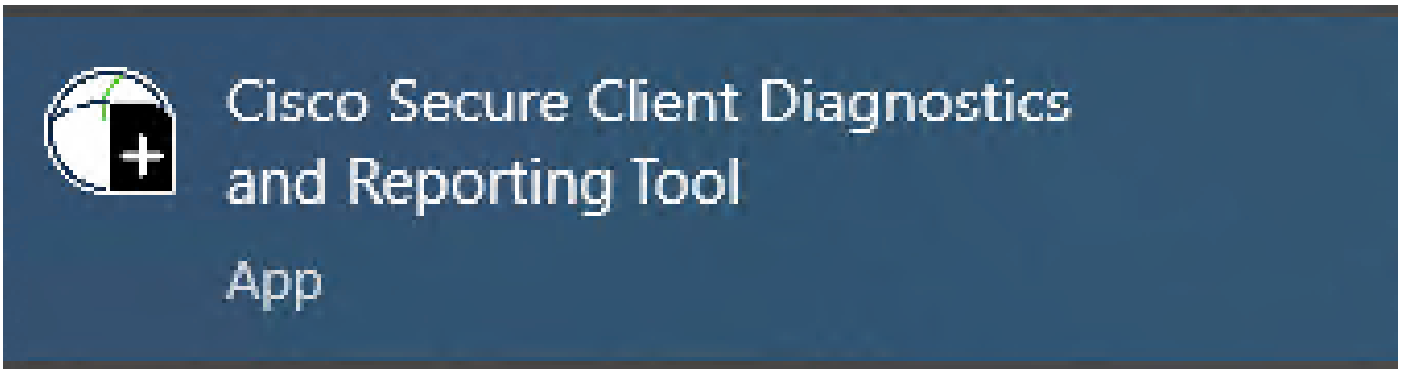
Configuración de registro de NAM de cliente seguro

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.

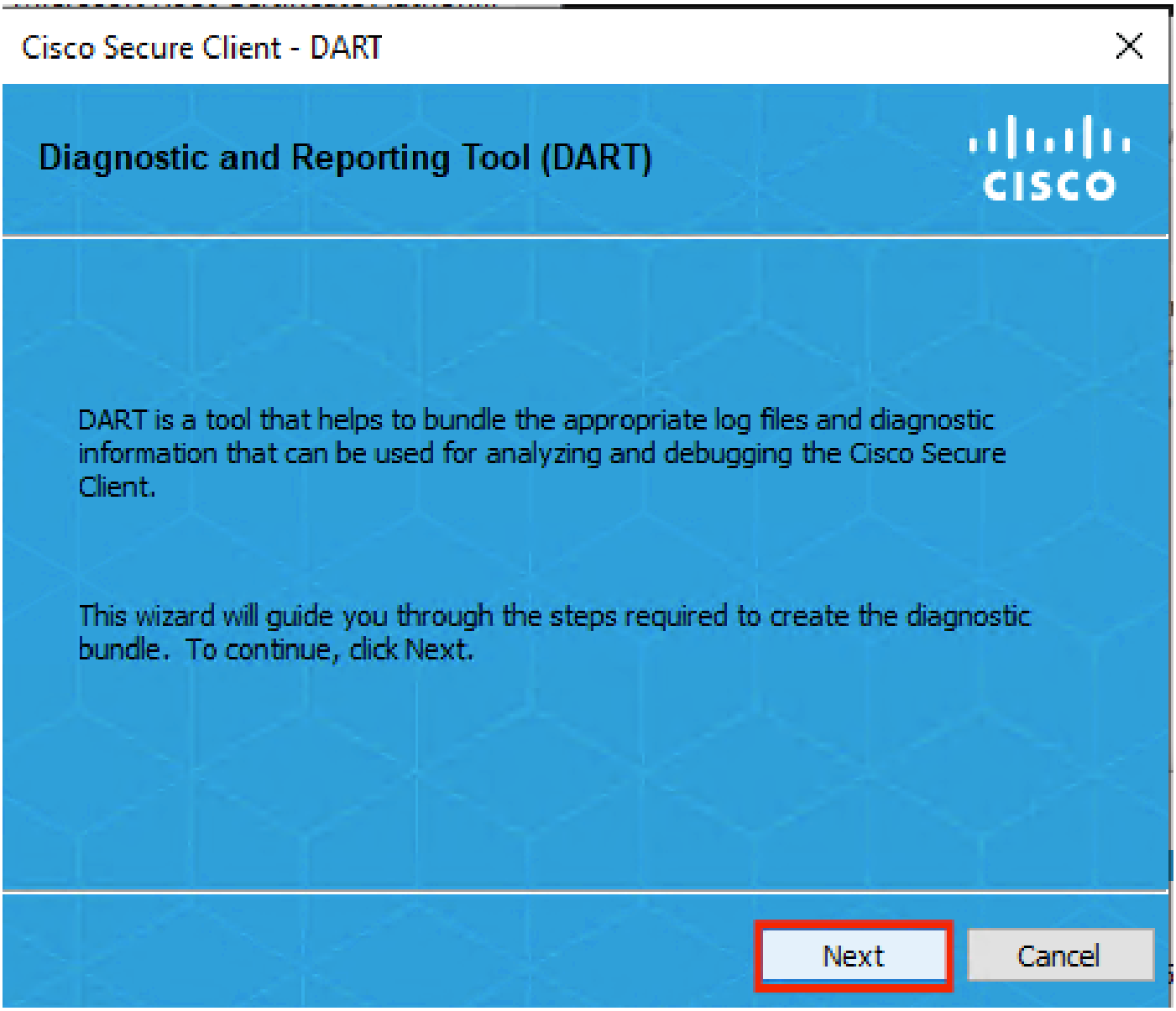
En Windows, vaya a la barra de búsqueda y escriba Cisco Secure Client Diagnostics and Reporting Tool.



Módulo DART

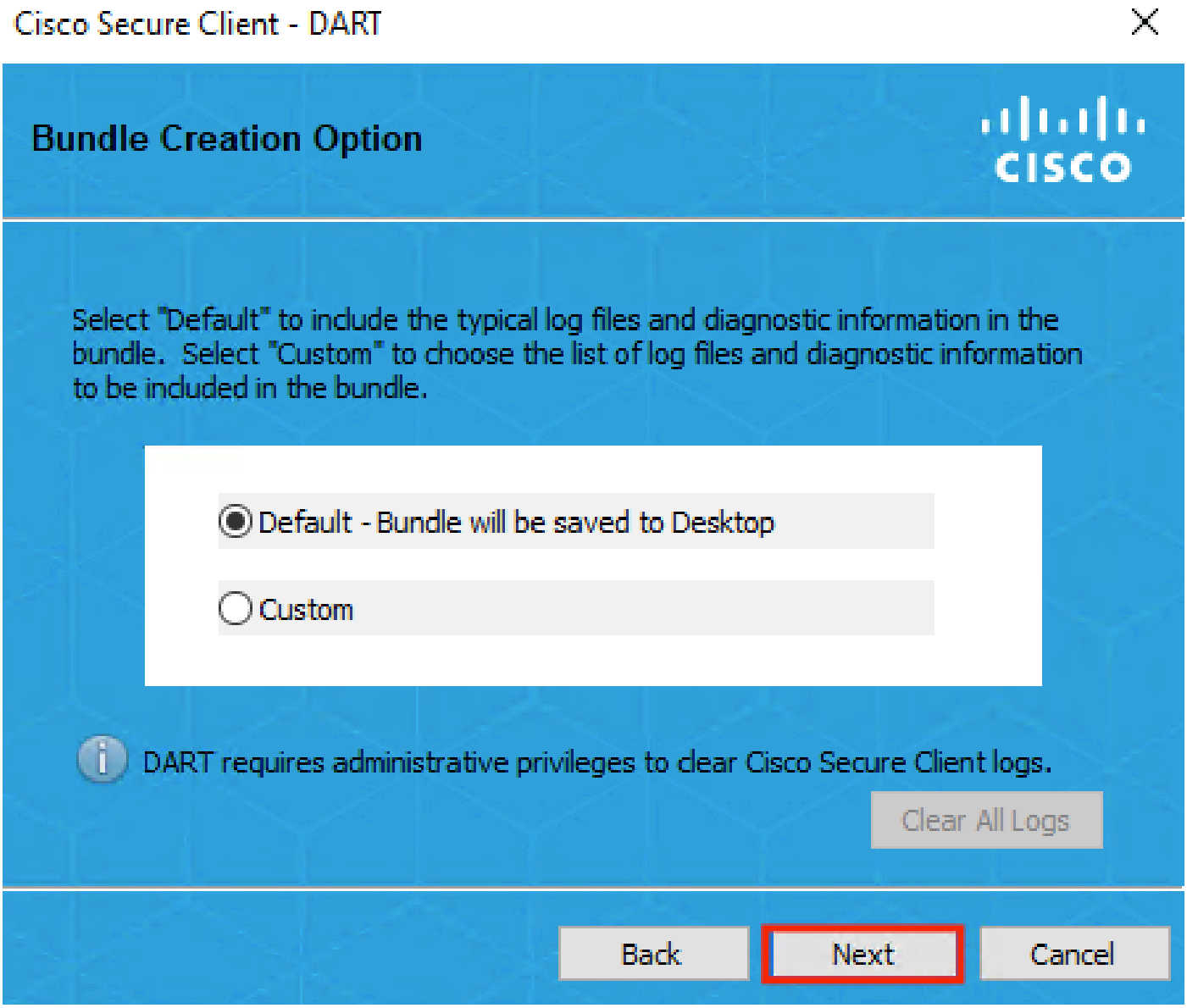
Durante el proceso de instalación, también instaló este módulo. Es una herramienta que ayuda durante el proceso de solución de problemas mediante la recopilación de registros e información de sesión dot1x relevante.

Haga clic en Next en la primera ventana.



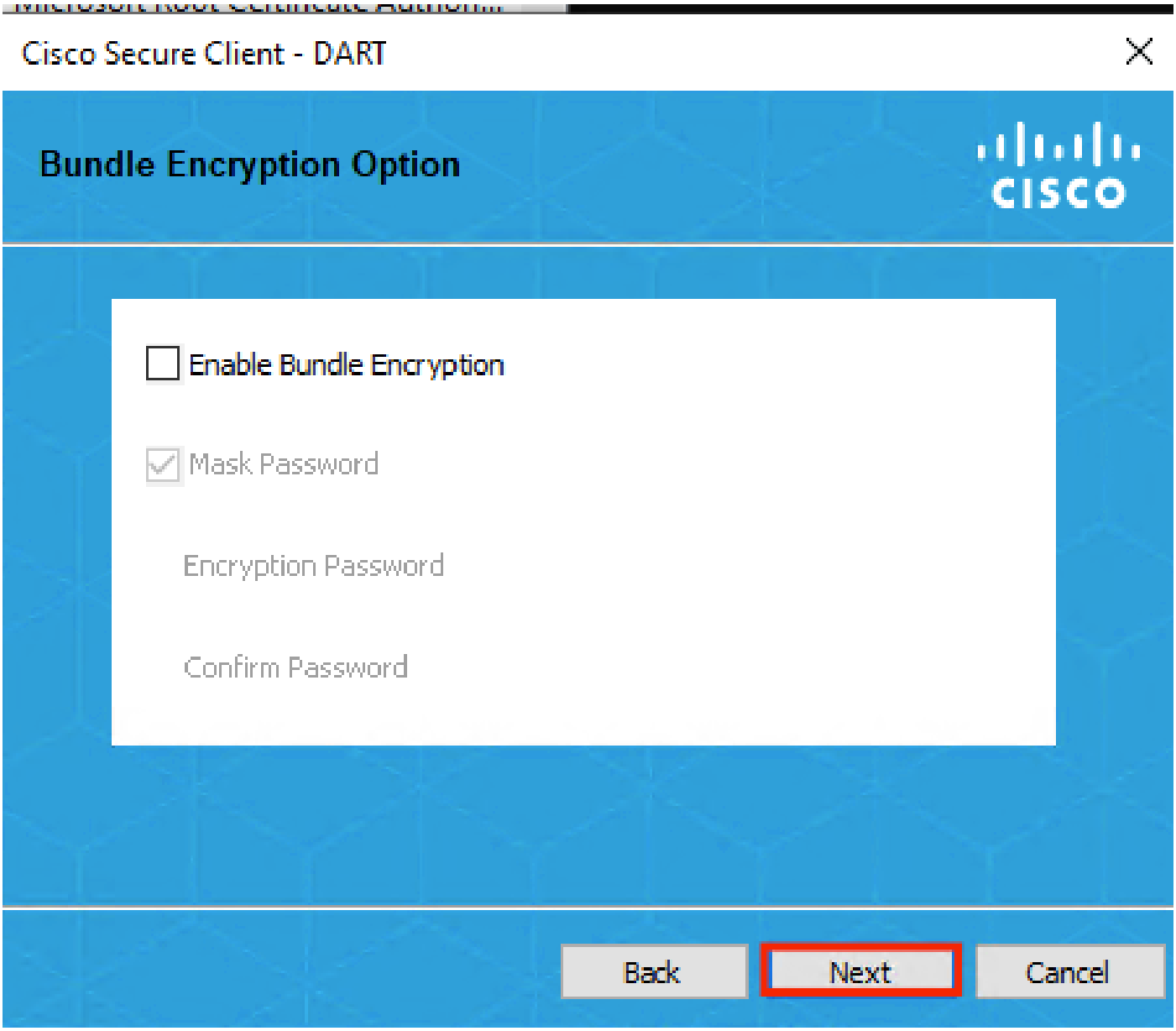
Módulo DART

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



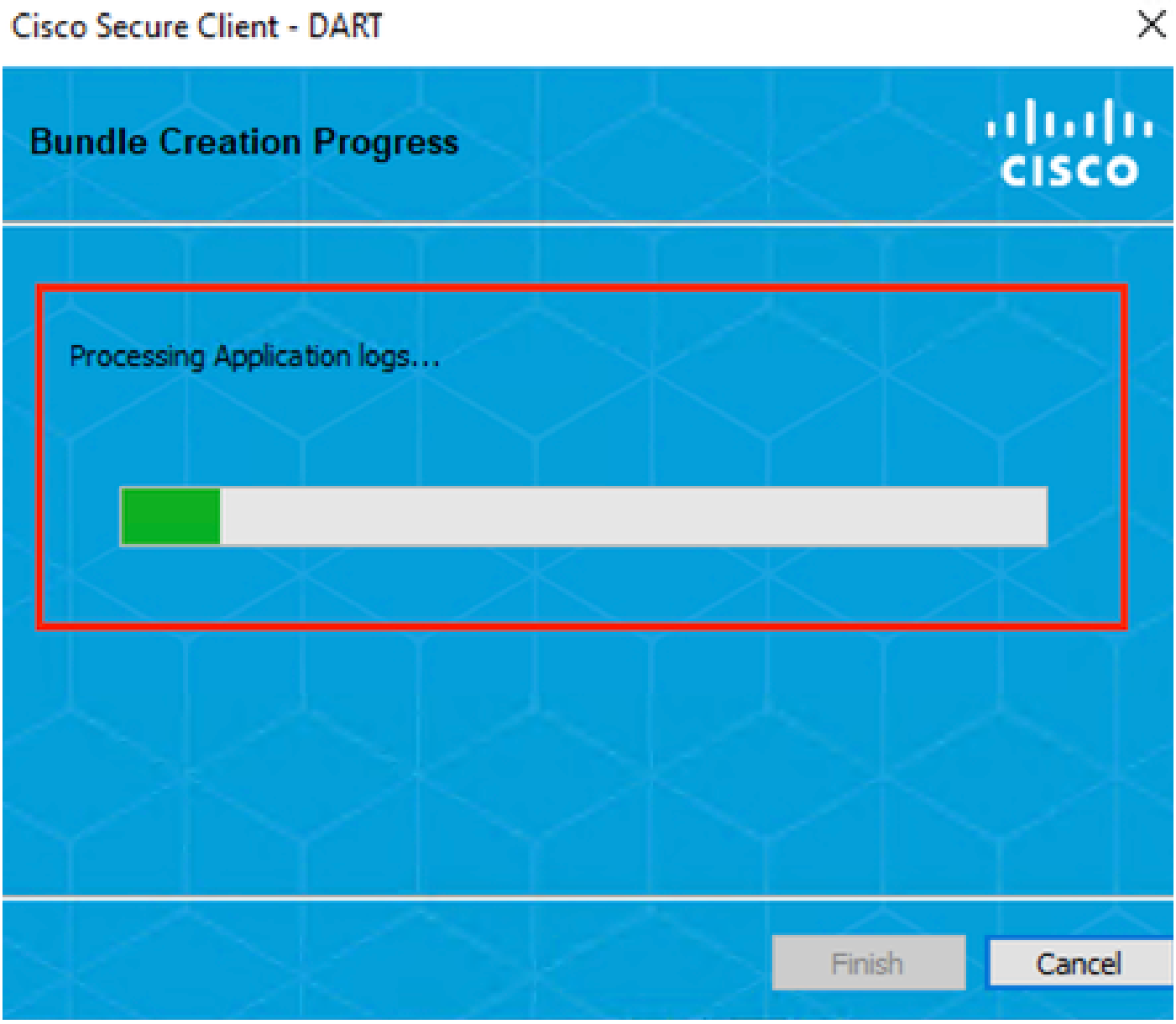
Módulo DART

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



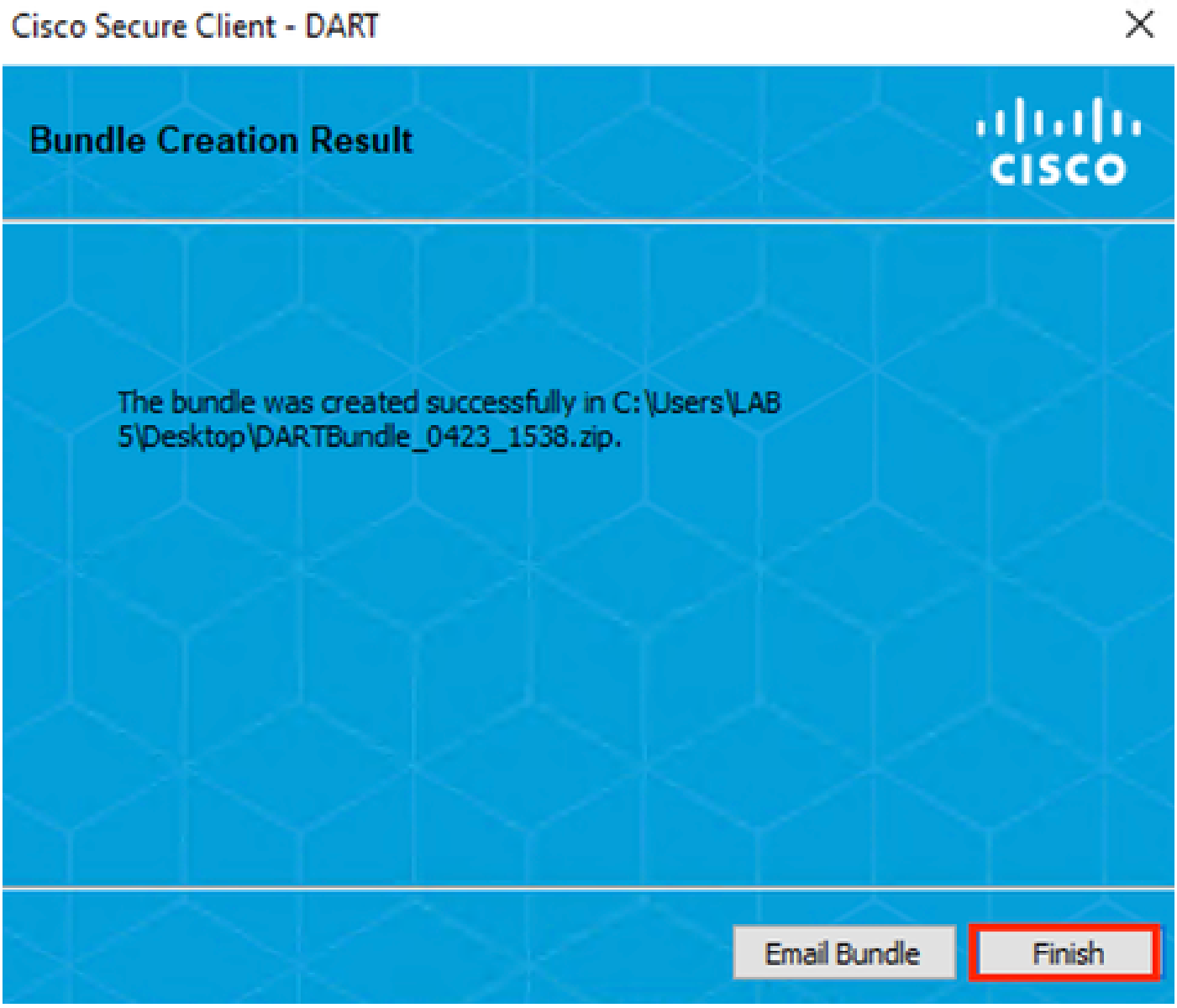
Módulo DART

Se inicia la recopilación de registros DART.



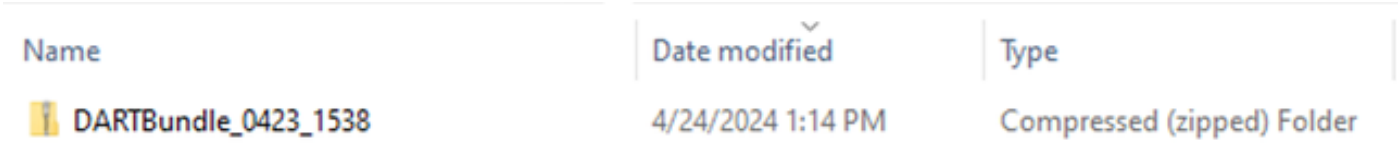
Recopilación de registros DART

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



Resultado de creación del paquete DART

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



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).