Configuración de la autenticación de equipo y usuario con EAP-TTLS

Contenido

Introducción

Este documento describe cómo configurar la autenticación de equipo y usuario con EAP-TTLS (EAP-MSCHAPv2) en Secure Client NAM y Cisco ISE.

Prerequisites

Requirements

Cisco recomienda conocer estos temas antes de continuar con esta implementación:

- Cisco Identity Services Engine (ISE)
- Módulo Secure Client Network Analysis (NAM)
- Protocolos EAP

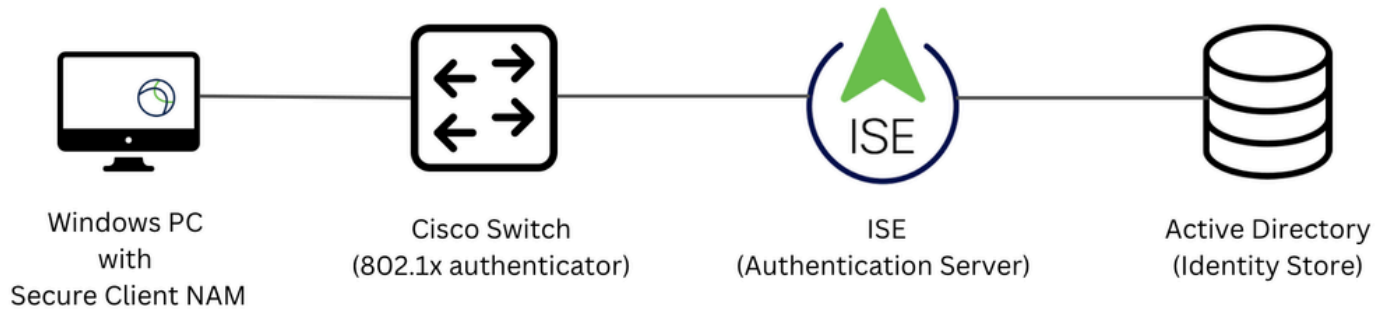
Componentes Utilizados

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

- Identity Services Engine (ISE) versión 3.4
- Switch C9300 con software Cisco IOS® XE, versión 16.12.01
- Windows 10 Pro Versión 22H2 Construido 19045.3930

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.

Topología de red



Topología de red

Configurar

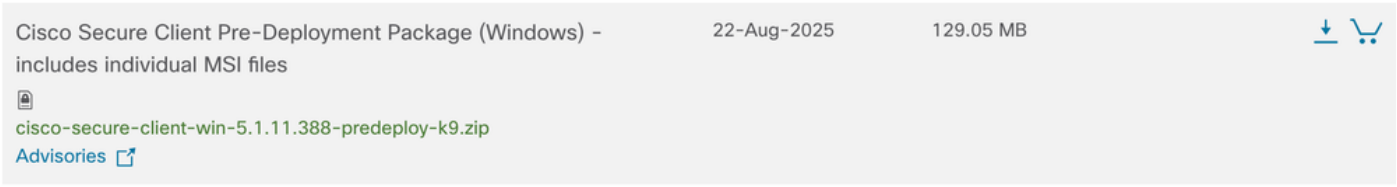
Configuraciones

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

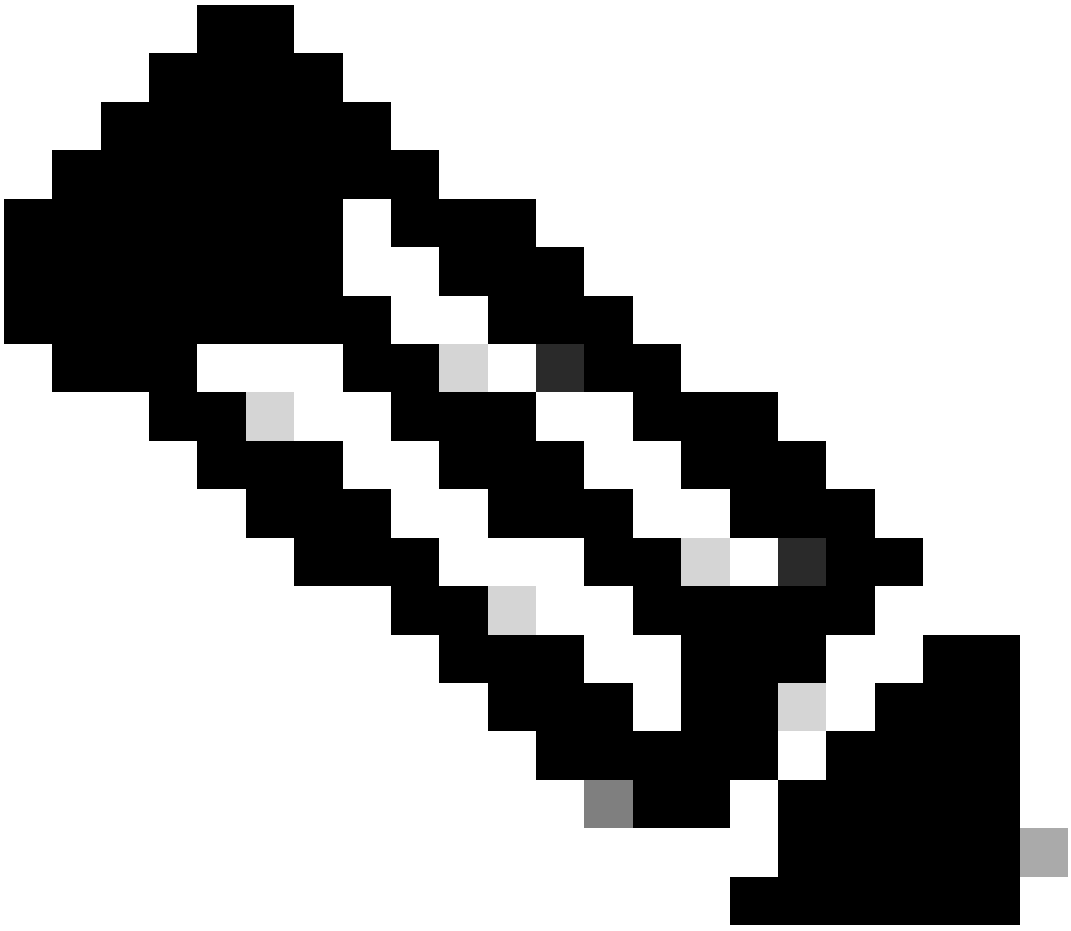
Paso 1. Vaya a Descarga de software de Cisco. En la barra de búsqueda de productos, introduzca Secure Client 5.

En este ejemplo de configuración se utiliza la versión 5.1.11.388. La instalación se realiza mediante el método previo a la implementación.

En la página de descarga, localice y descargue el paquete de implementación previa de Cisco Secure Client (Windows).

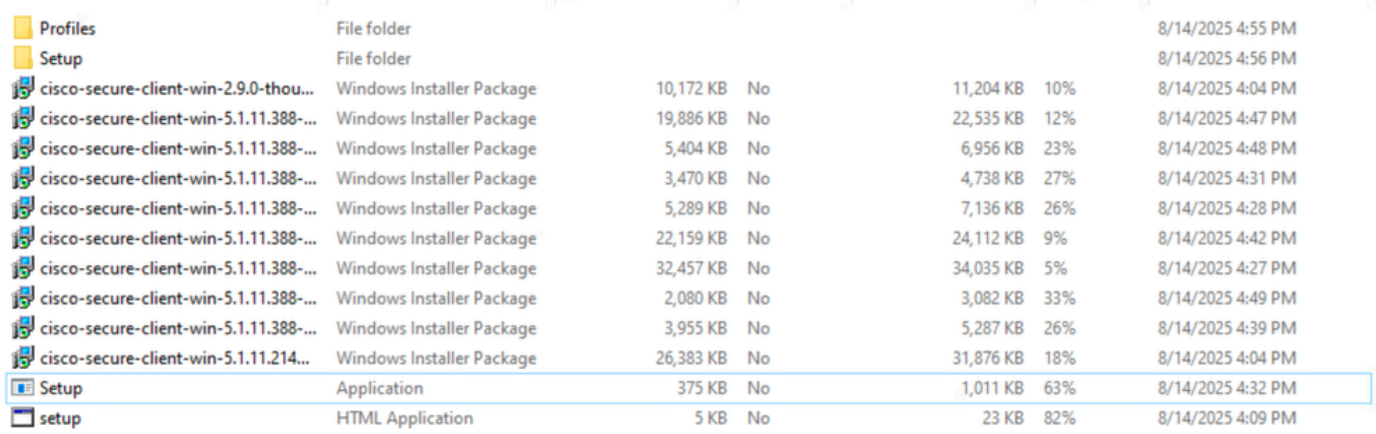


Archivo zip de preimplementación



> Nota: Cisco AnyConnect ha quedado obsoleto y ya no está disponible en el sitio de descarga de software de Cisco.

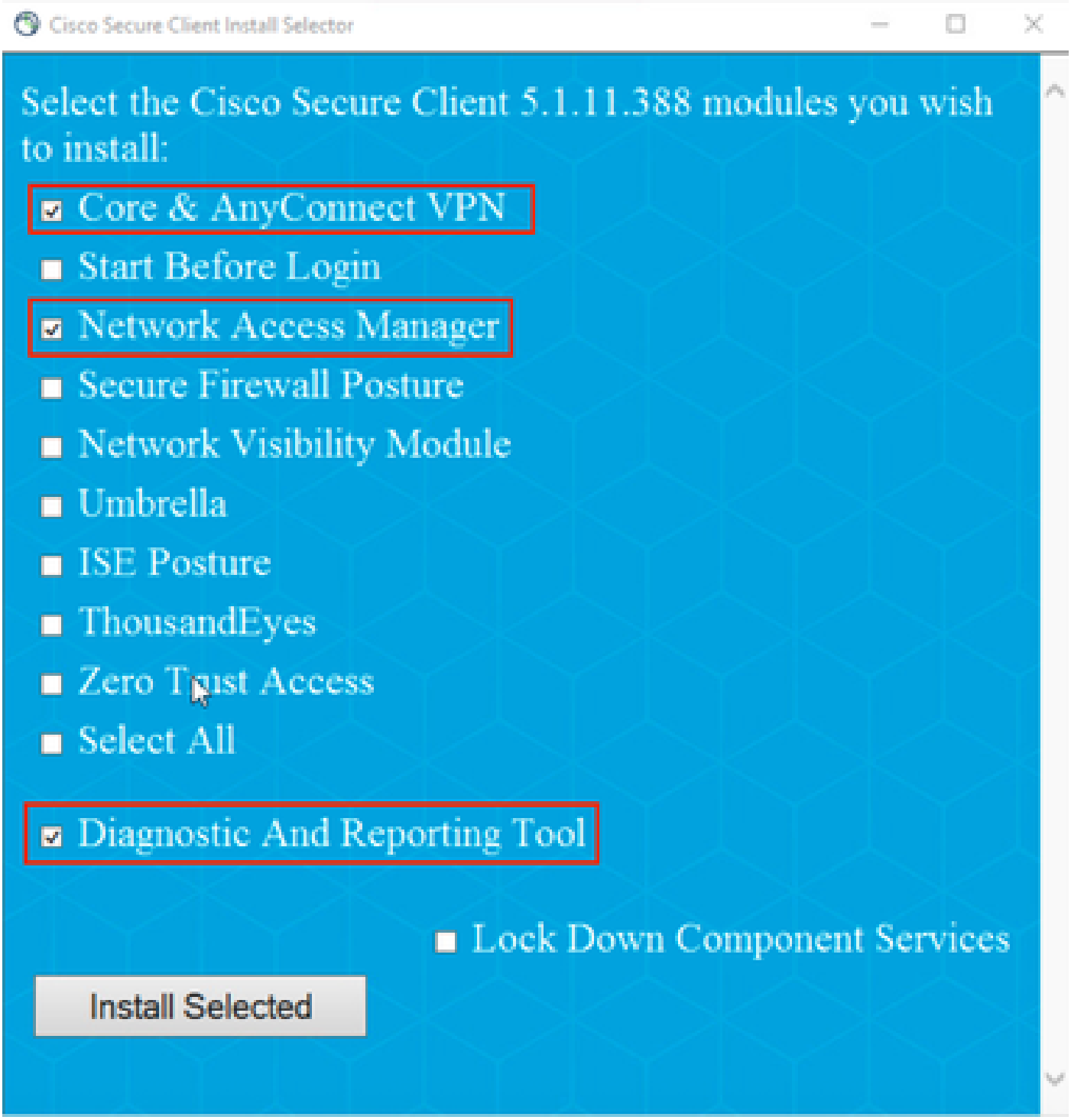
Paso 2. Una vez descargado y extraído, haga clic en Setup.



Profiles	File folder					8/14/2025 4:55 PM
Setup	File folder					8/14/2025 4:56 PM
cisco-secure-client-win-2.9.0-thou...	Windows Installer Package	10,172 KB	No	11,204 KB	10%	8/14/2025 4:04 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	19,886 KB	No	22,535 KB	12%	8/14/2025 4:47 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	5,404 KB	No	6,956 KB	23%	8/14/2025 4:48 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	3,470 KB	No	4,738 KB	27%	8/14/2025 4:31 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	5,289 KB	No	7,136 KB	26%	8/14/2025 4:28 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	22,159 KB	No	24,112 KB	9%	8/14/2025 4:42 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	32,457 KB	No	34,035 KB	5%	8/14/2025 4:27 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	2,080 KB	No	3,082 KB	33%	8/14/2025 4:49 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	3,955 KB	No	5,287 KB	26%	8/14/2025 4:39 PM
cisco-secure-client-win-5.1.11.214...	Windows Installer Package	26,383 KB	No	31,876 KB	18%	8/14/2025 4:04 PM
Setup	Application	375 KB	No	1,011 KB	63%	8/14/2025 4:32 PM
setup	HTML Application	5 KB	No	23 KB	82%	8/14/2025 4:09 PM

Archivo Zip De Preimplementación

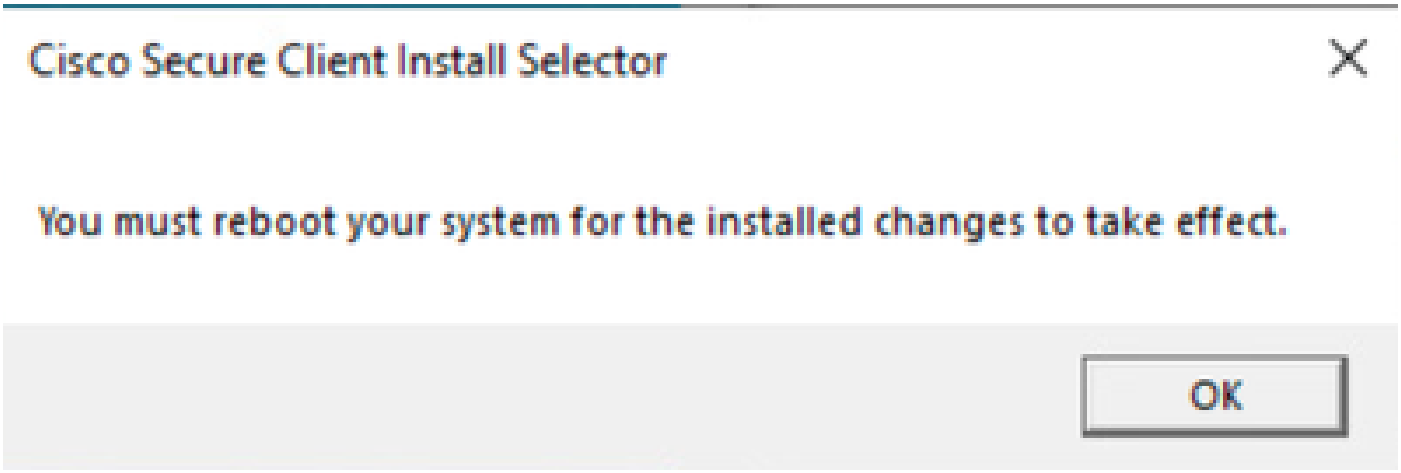
Paso 3. Instale la VPN de Core y AnyConnect, el Administrador de acceso de red y los módulos de las herramientas de diagnóstico e informes.



Instalador de Secure Client

Haga clic en Instale la opción seleccionada.

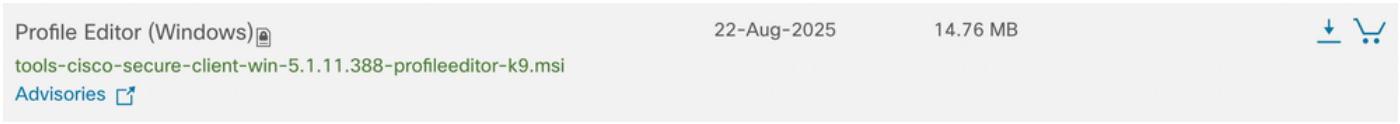
Paso 4. Es necesario reiniciar después de la instalación. Haga clic en Aceptar y reinicie el dispositivo.



Elemento emergente Reboot Required (Reiniciar)

Parte 2: Descargue e instale Secure Client NAM Profile Editor

Paso 1. El Editor de perfiles se puede encontrar en la misma página de descargas que Secure Client. En este ejemplo de configuración se utiliza la versión 5.1.11.388.



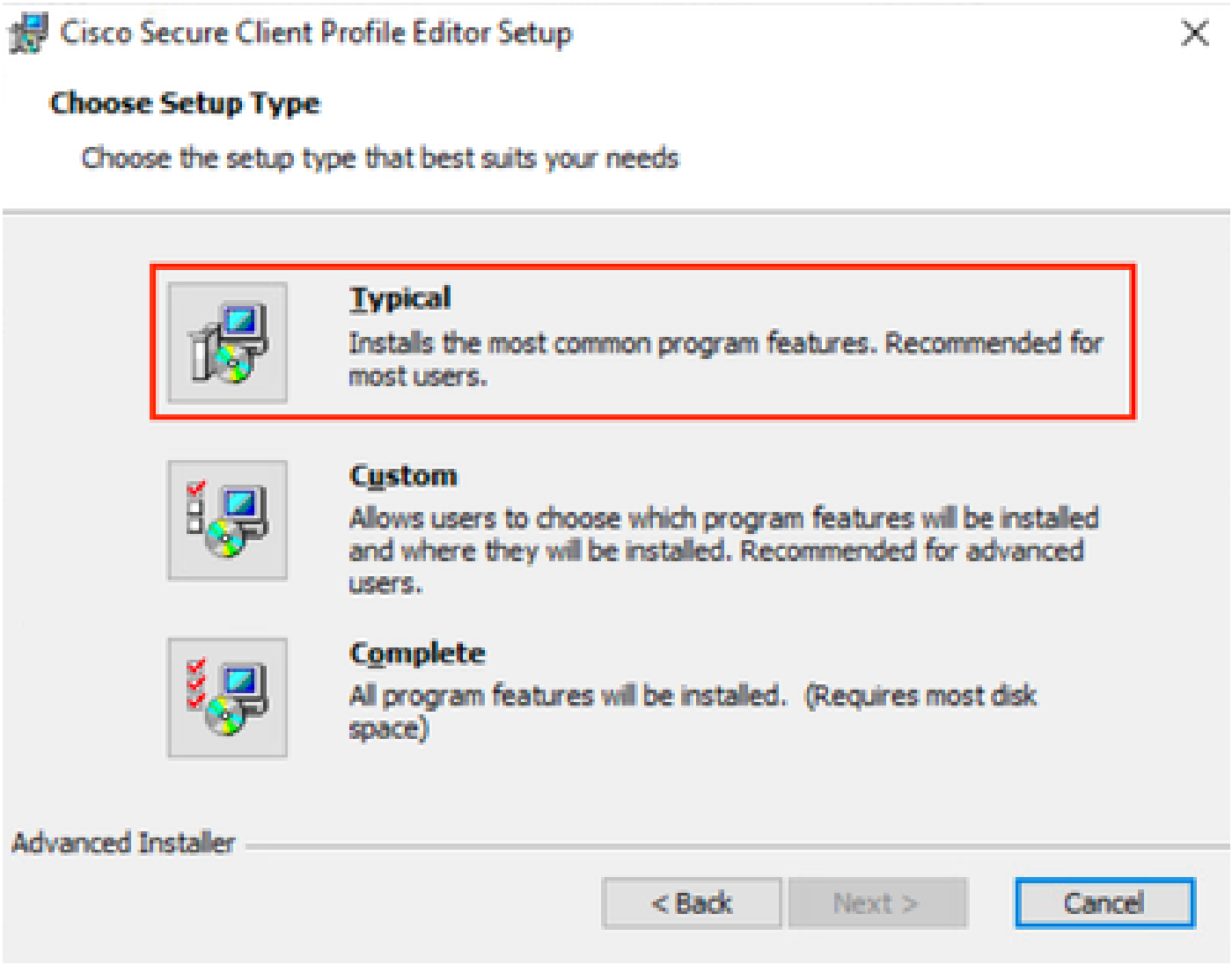
Editor de perfiles

Descargue e instale el Editor de perfiles.

Paso 2. Ejecute el archivo MSI.

Inicio de configuración del Editor de perfiles

Paso 3. Use la opción de configuración Typical e instale el Editor de perfiles NAM.

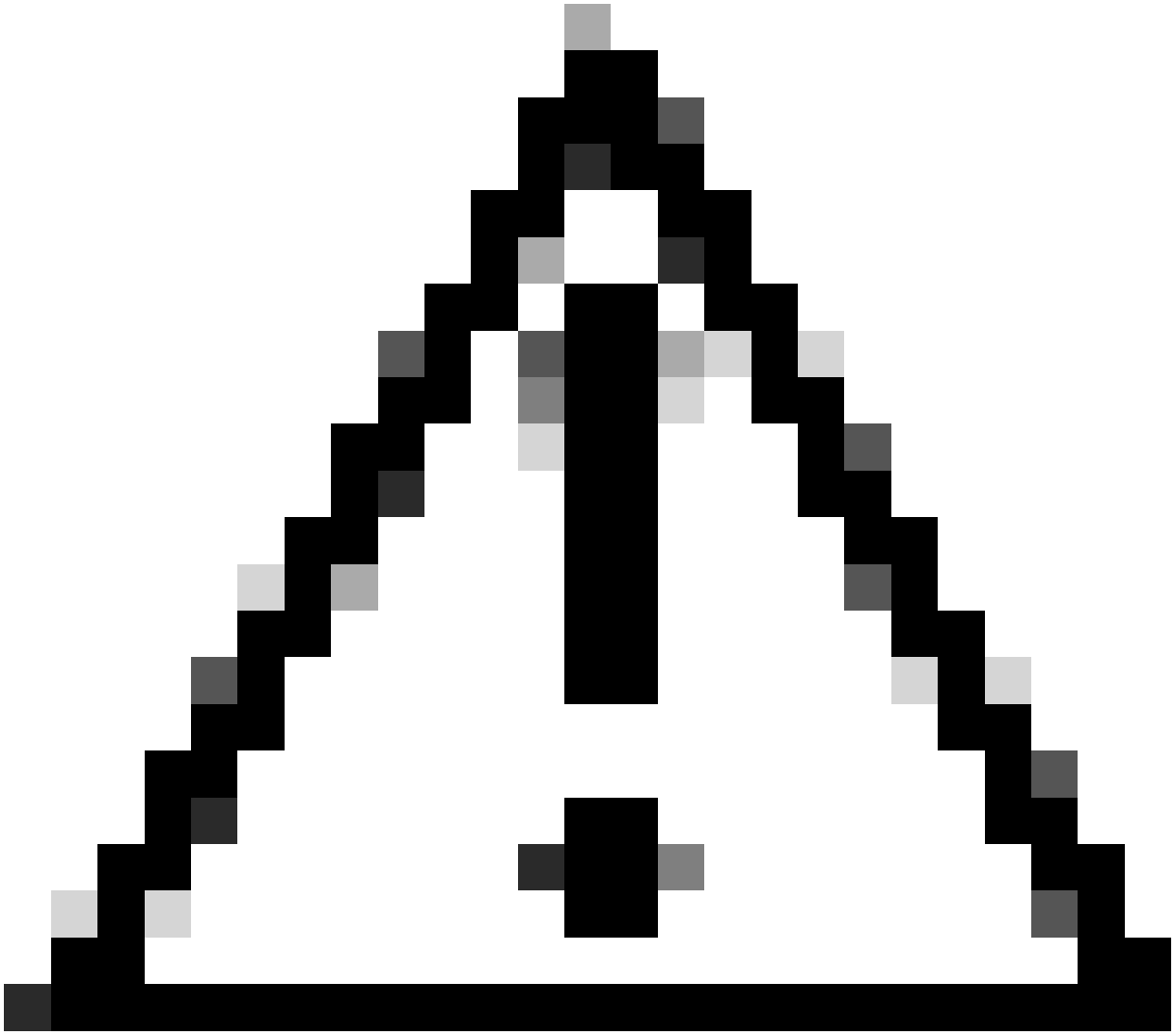


Configuración del Editor de perfiles

Parte 3: Permitir el acceso de NAM a las credenciales de caché de Windows

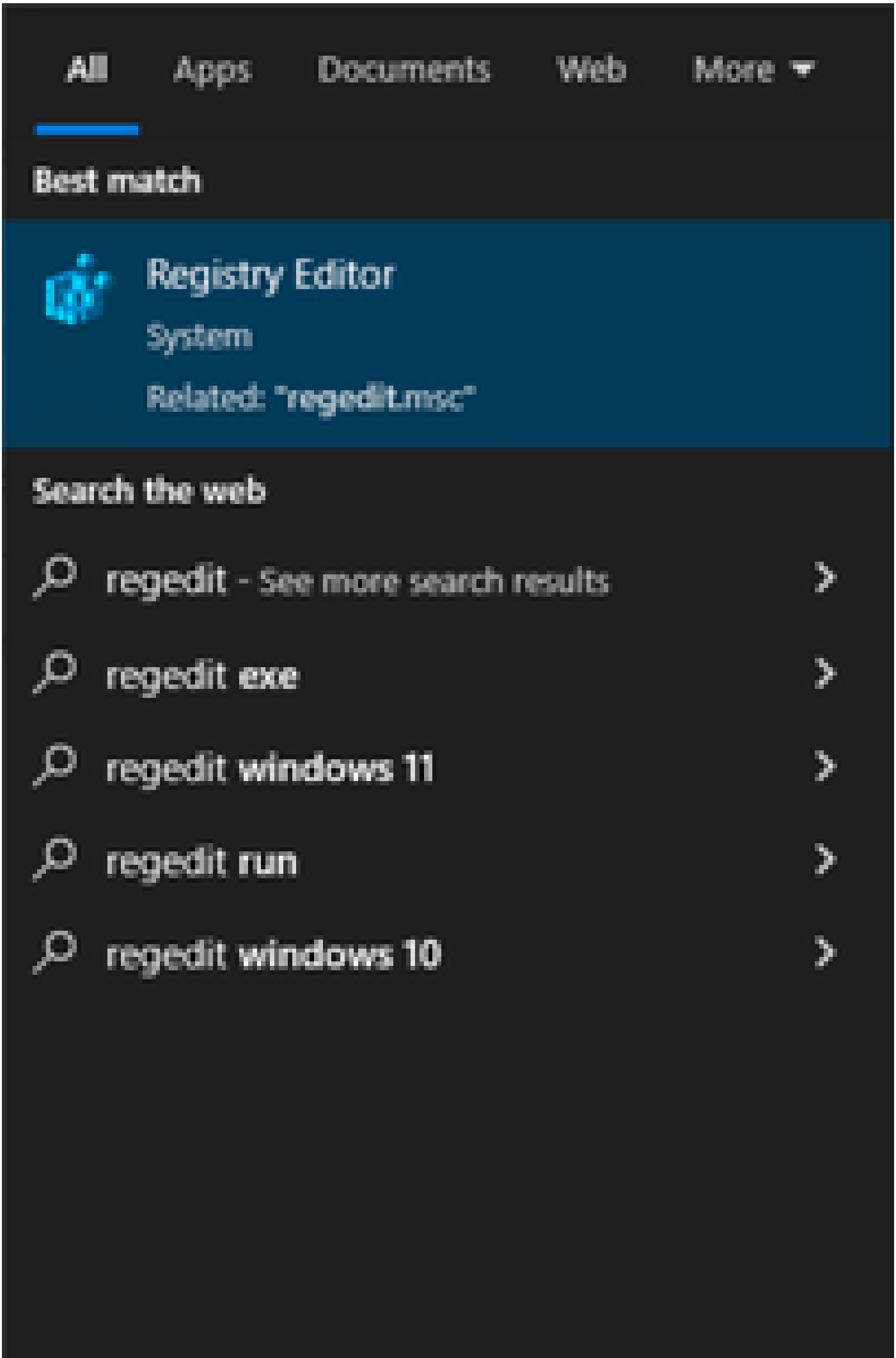
De forma predeterminada, en Windows 10, Windows 11 y Windows Server 2012, el sistema operativo impide que el Administrador de acceso de red (NAM) recupere la contraseña del equipo necesaria para la autenticación del equipo. Como resultado, la autenticación de la máquina mediante la contraseña de la máquina no funciona a menos que se aplique una corrección del Registro.

Para permitir que NAM acceda a las credenciales de la máquina, aplique la corrección de Microsoft KB 2743127 en el escritorio del cliente.



Precaución: La edición incorrecta del Registro de Windows puede causar graves problemas. Asegúrese de realizar una copia de seguridad del Registro antes de realizar cambios.

Paso 1. En la barra de búsqueda de Windows, ingrese regedit, y luego haga clic en Editor del Registro.

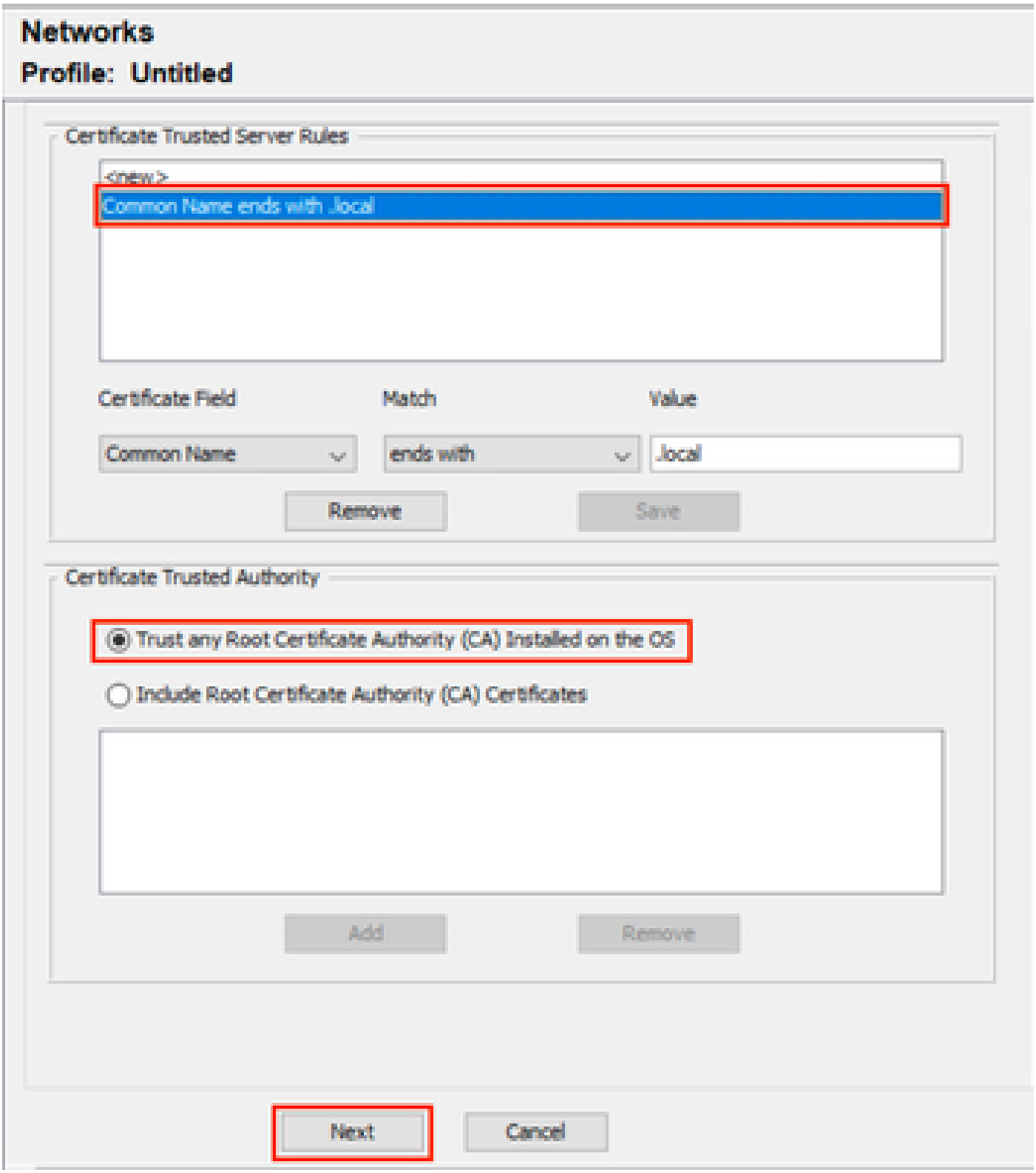

All
Apps
Documents
Web
More
Best match
Registry Editor
System
Related: "regedit.msc"
Search the web
regedit - See more search results
regedit exe
regedit windows 11
regedit run
regedit windows 10

En este ejemplo, el certificado de nodo PSN es emitido por varshaah.varshaah.local. Por lo tanto, se utiliza la regla Common Name termina con .local. Esta regla valida el certificado que el servidor presenta durante el flujo EAP-TTLS.

También puede especificar el nombre común del certificado de autenticación EAP del nodo de servicios de directivas (PSN).

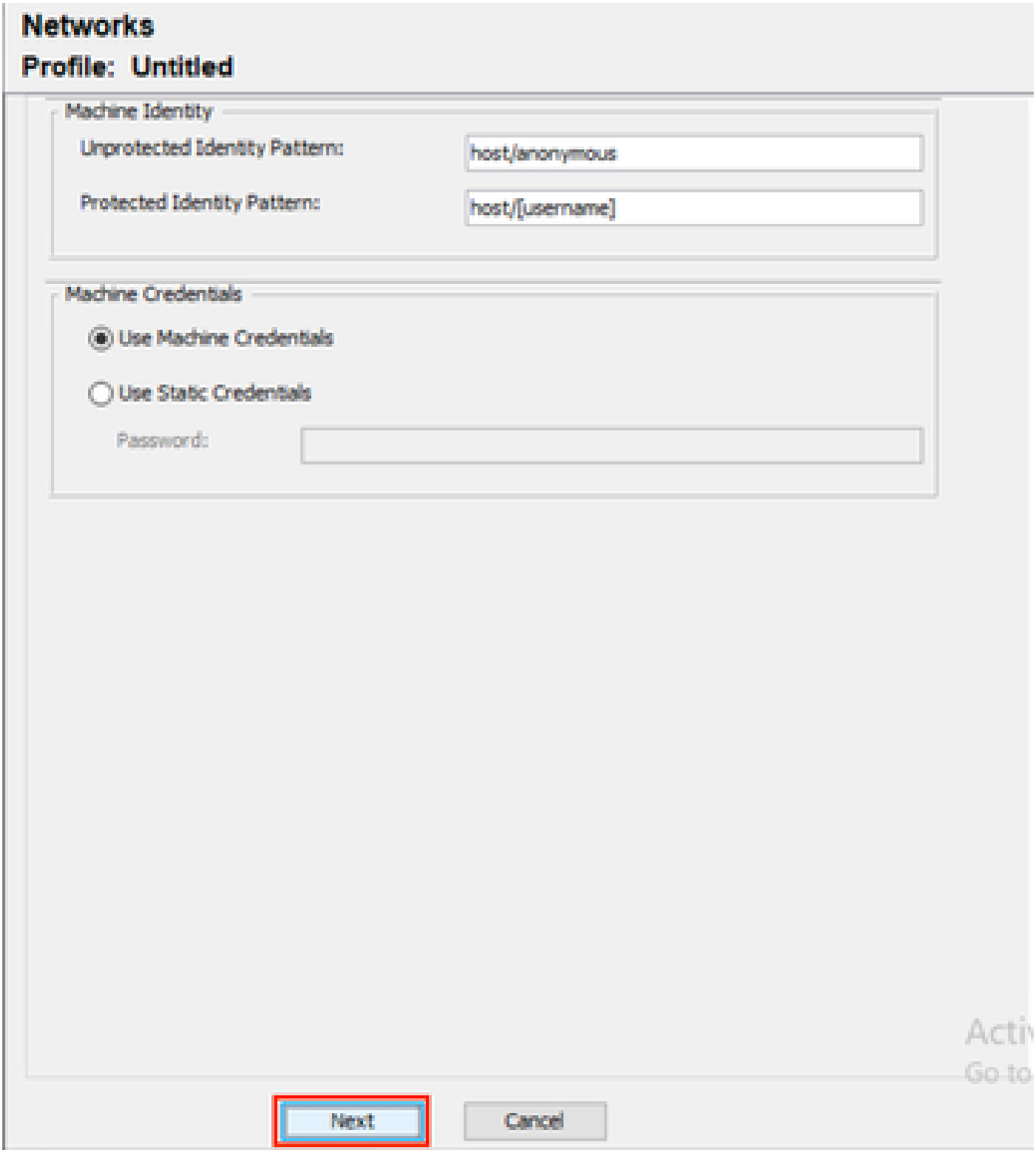
- En Certificate Trusted Authority, hay dos opciones disponibles.
  En este escenario, se utiliza la opción Confiar en cualquier autoridad de certificación raíz (CA) instalada en el sistema operativo en lugar de agregar un certificado de CA específico.

  Con esta opción, el dispositivo Windows confía en cualquier certificado EAP firmado por un certificado incluido en Certificados - Usuario actual > Entidades de certificación raíz de confianza > Certificados (administrado por el sistema operativo).
- Para continuar, haga clic en Next (Siguiente).



Certificados del editor de perfiles NAM

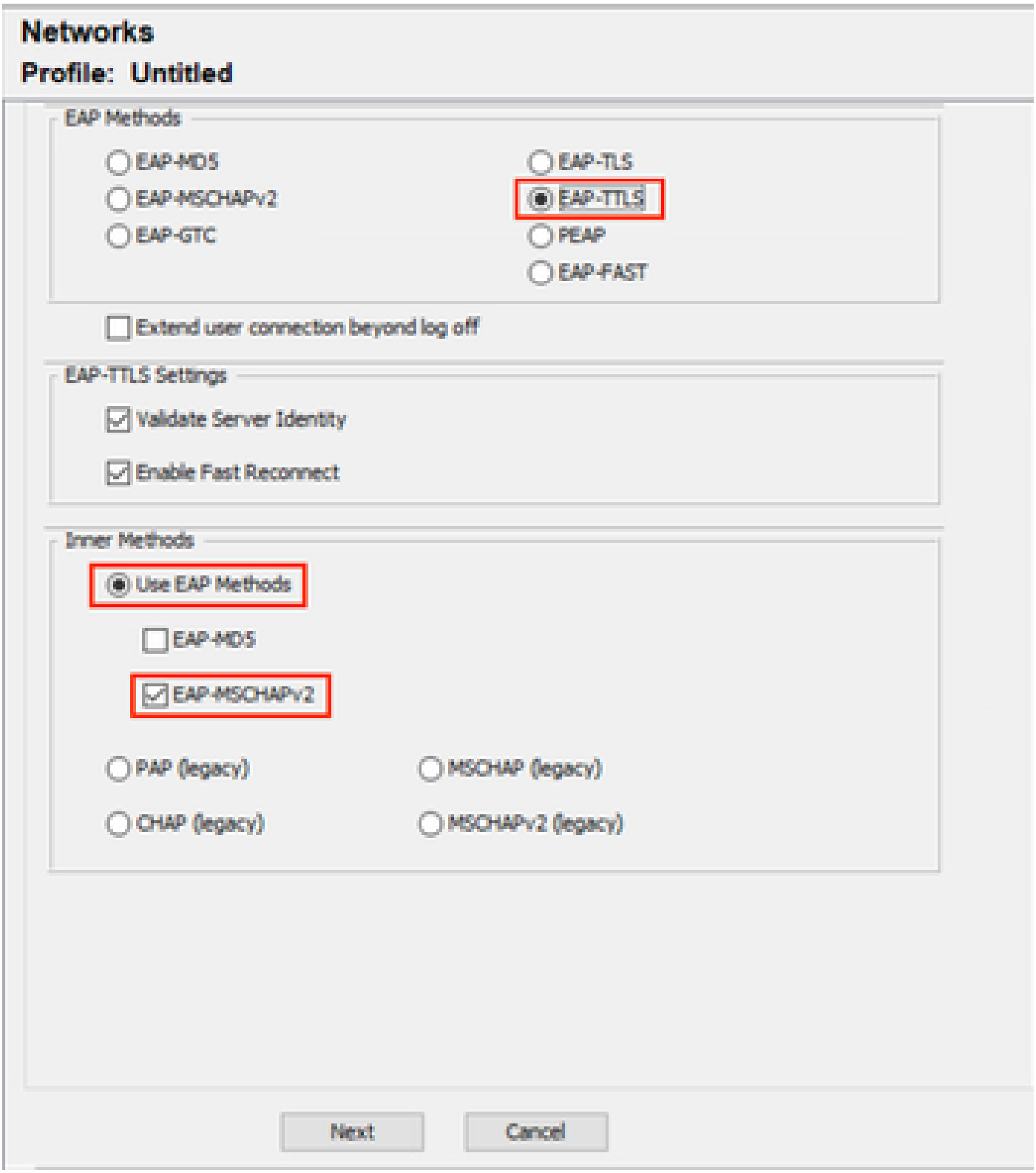
Paso 6. En la sección Credenciales de Máquina, seleccione Usar Credenciales de Máquina, y luego haga clic en Siguiente.



Credenciales del Editor de Perfiles NAM

Paso 7. Sección Configure User Auth.

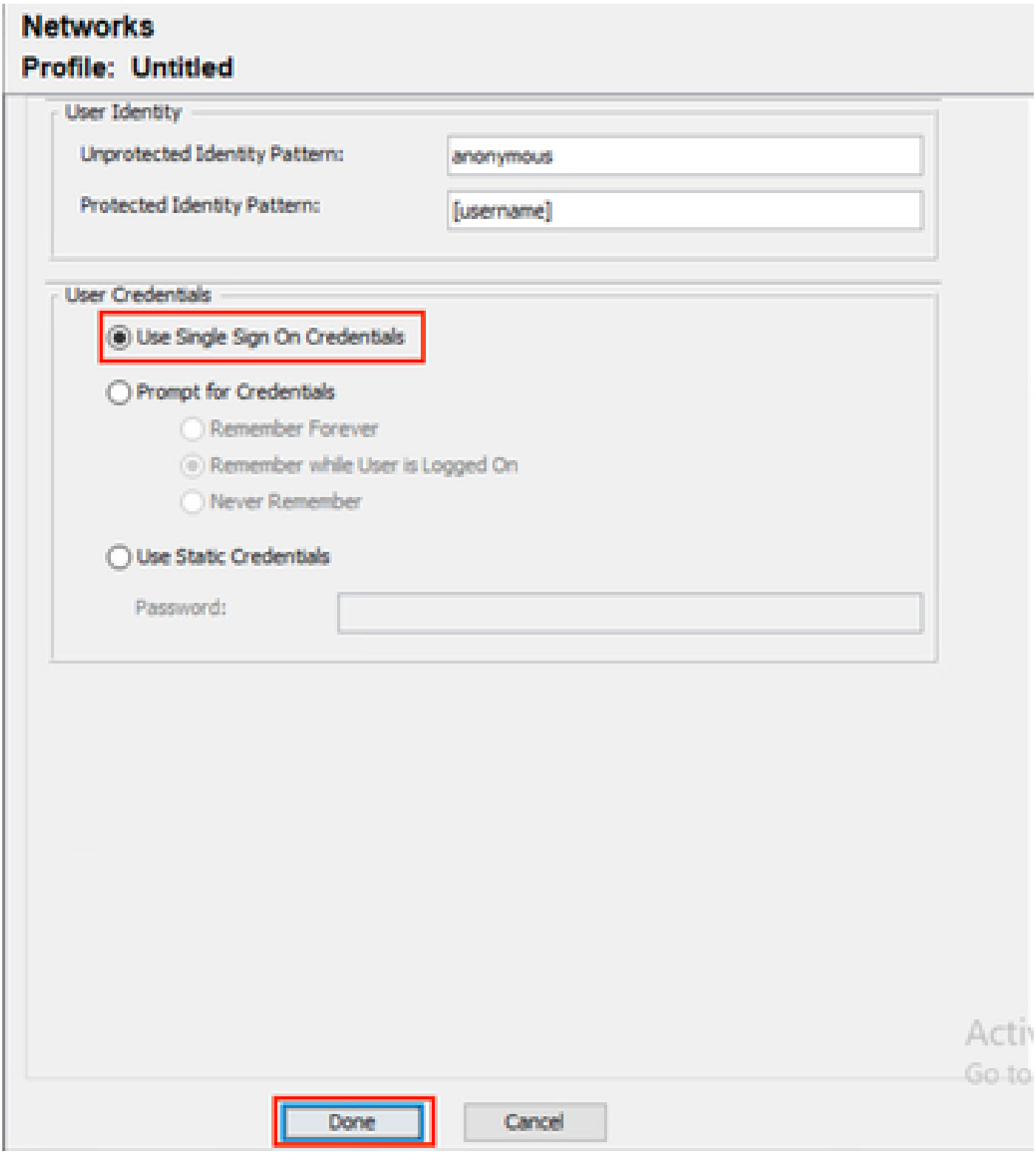
- Seleccione EAP-TTLS en Métodos EAP.
- En Métodos internos, seleccione Usar métodos EAP y seleccione EAP-MSCHAPv2.
- Haga clic en Next (Siguiente).



Autenticación de usuario del Editor de perfiles NAM

Paso 8. En Certificados, configure las mismas reglas de validación de certificados que se describen en el Paso 5.

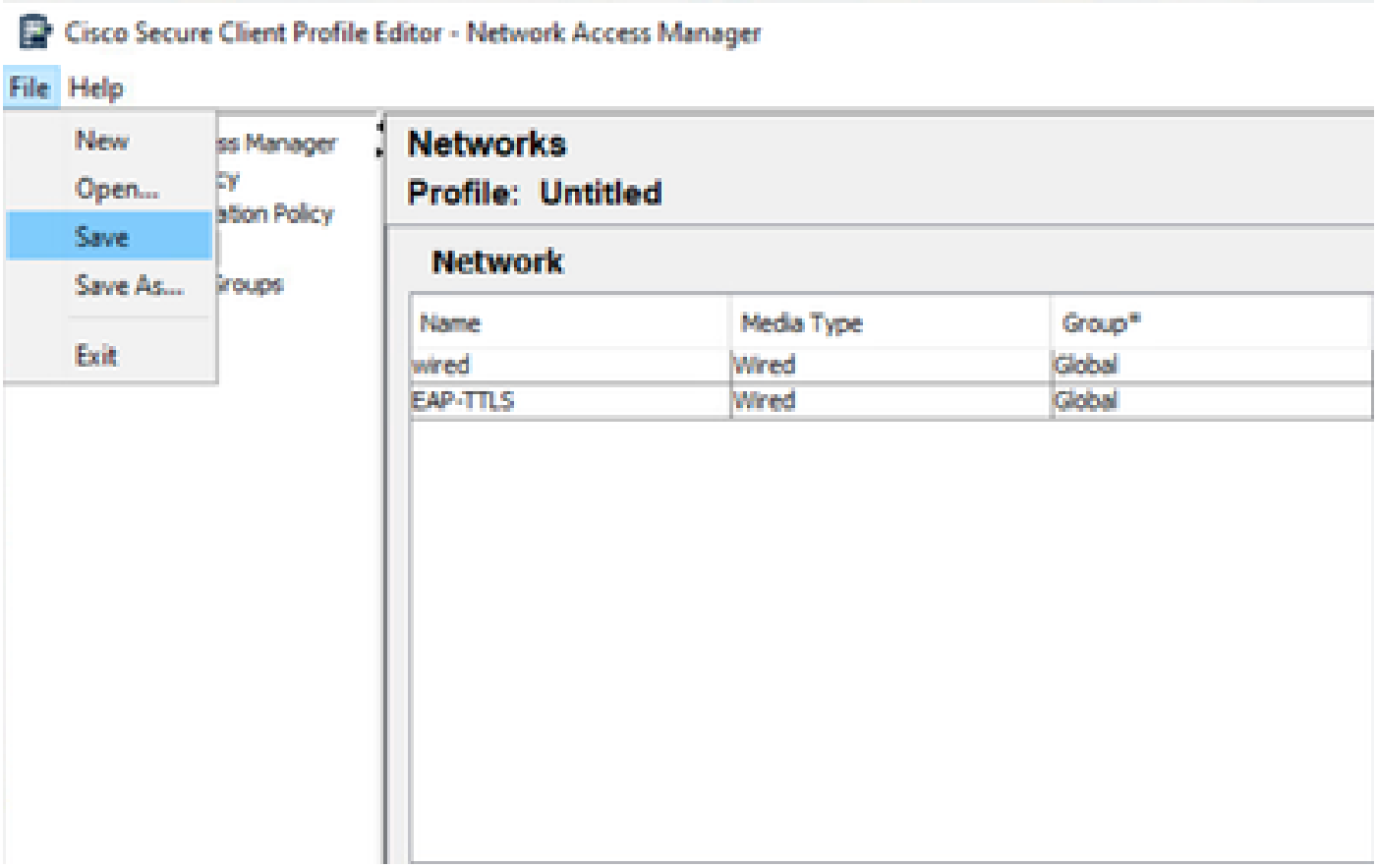
Paso 9. En Credenciales de usuario, seleccione Usar credenciales de inicio de sesión único y, a continuación, haga clic en Finalizado.



Credenciales de usuario del Editor de perfiles NAM

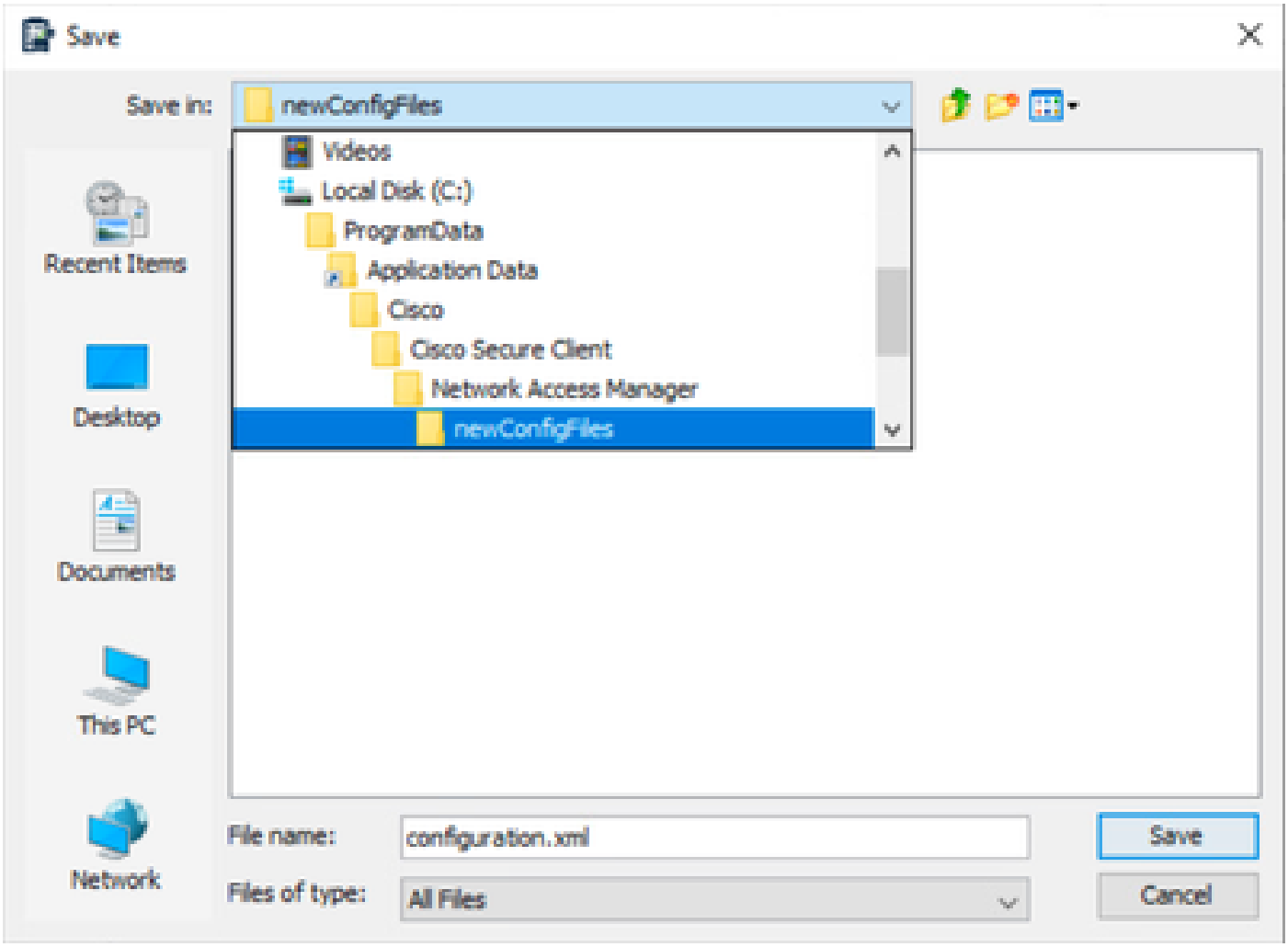
Parte 6: Guardar el archivo de configuración de red

Paso 1. Haga clic en Archivo > Guardar.



Guardar configuración de red de NAM Profile Editor

Paso 2. Guarde el archivo como configuration.xml en la carpeta newConfigFiles.

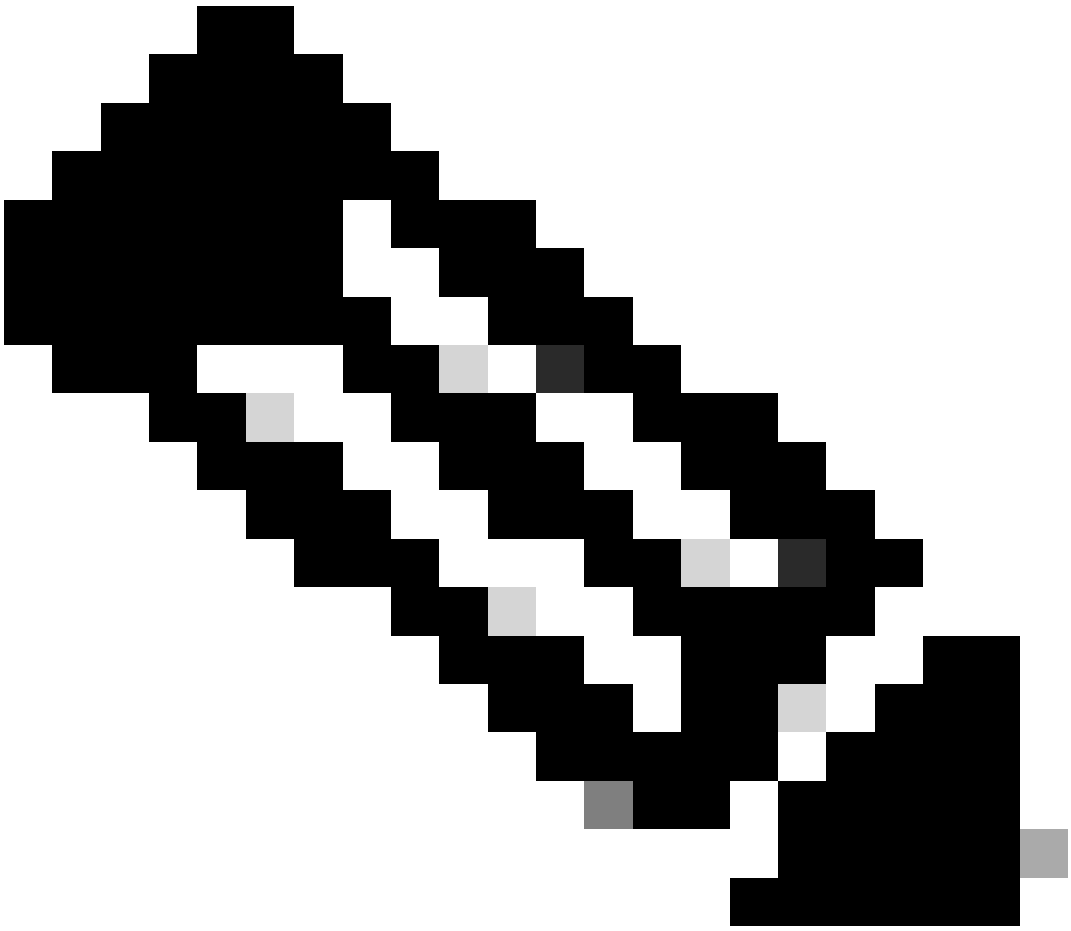


Guardar configuración de red

Parte 7: Configuración de AAA en el switch

```
C9300-1#sh run aaa
!
aaa authentication dot1x default group labgroup
aaa authorization network default group labgroup
aaa accounting dot1x default start-stop group labgroup
aaa accounting update newinfo periodic 2880
!
!
!
!
aaa server radius dynamic-author
 client 10.76.112.135 server-key cisco
!
!
radius server labserver
 address ipv4 10.76.112.135 auth-port 1812 acct-port 1813
 key cisco
!
!
aaa group server radius labgroup
 server name labserver
!
```

```
!
!
!
aaa new-model
aaa session-id common
!
!



C9300-1(config)#dot1x system-auth-control
```



> Nota: El comando dot1x system-auth-control no aparece en la salida show running-config, pero es necesario habilitar 802.1X globalmente.

Configuración de la interfaz del switch para 802.1X:

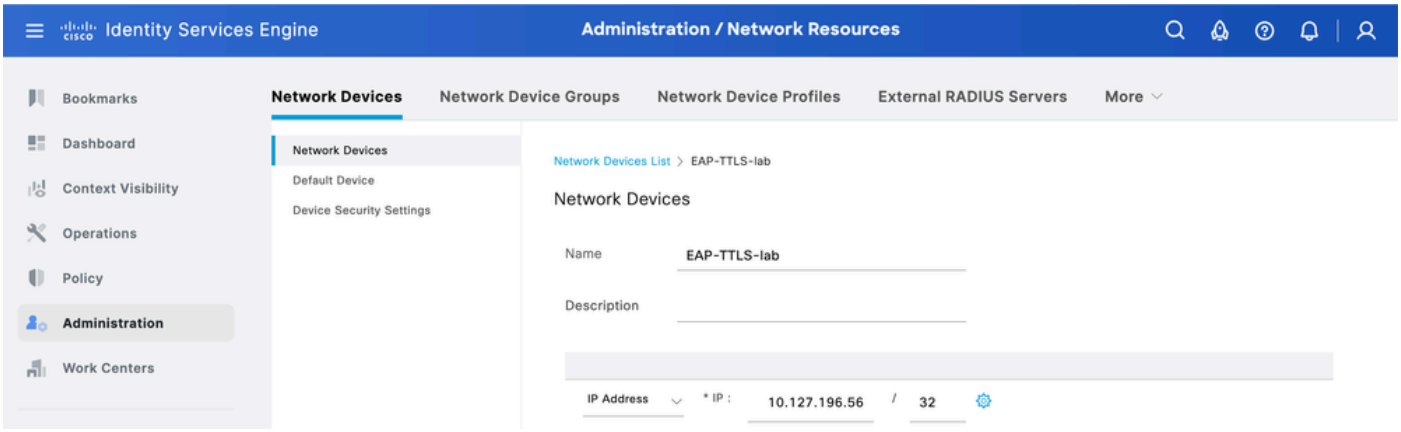
```
C9300-1(config)#do sh run int gig1/0/44
Building configuration...

Current configuration : 242 bytes
!
interface GigabitEthernet1/0/44
 switchport access vlan 96
 switchport mode access
 device-tracking
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication host-mode multi-auth
 authentication periodic

 mab
 dot1x pae authenticator
end
```

Parte 8: Configuraciones de ISE

Paso 1. Configuración del switch en ISE.

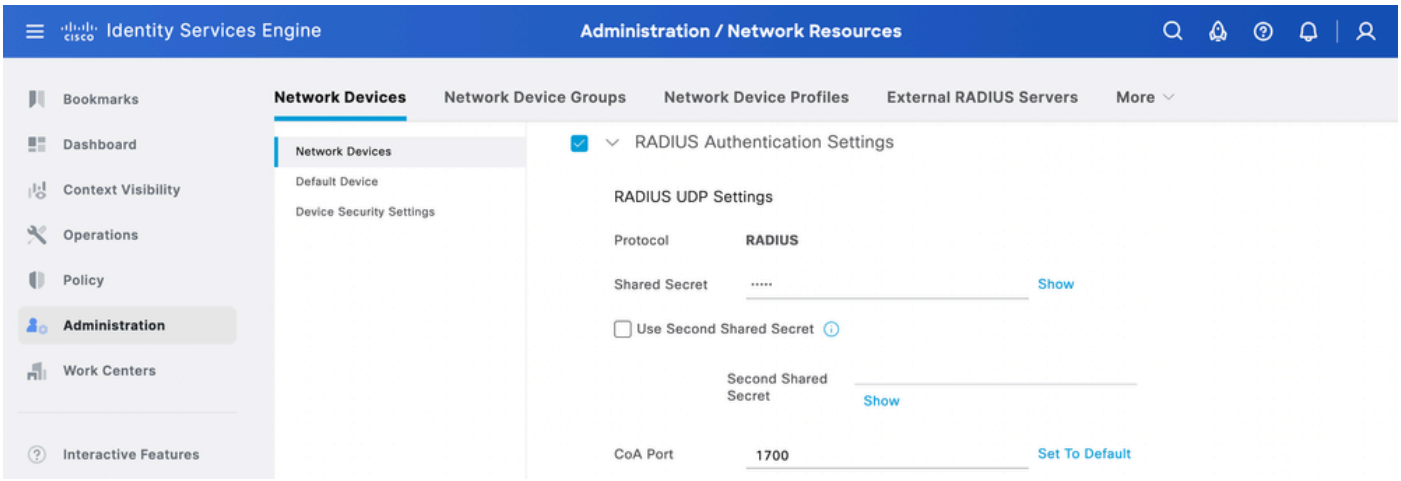
Vaya a Administration > Network Resources > Network Devices y haga clic en Add.

Introduzca el nombre del switch y la dirección IP aquí.



Adición de ISE de dispositivo de red

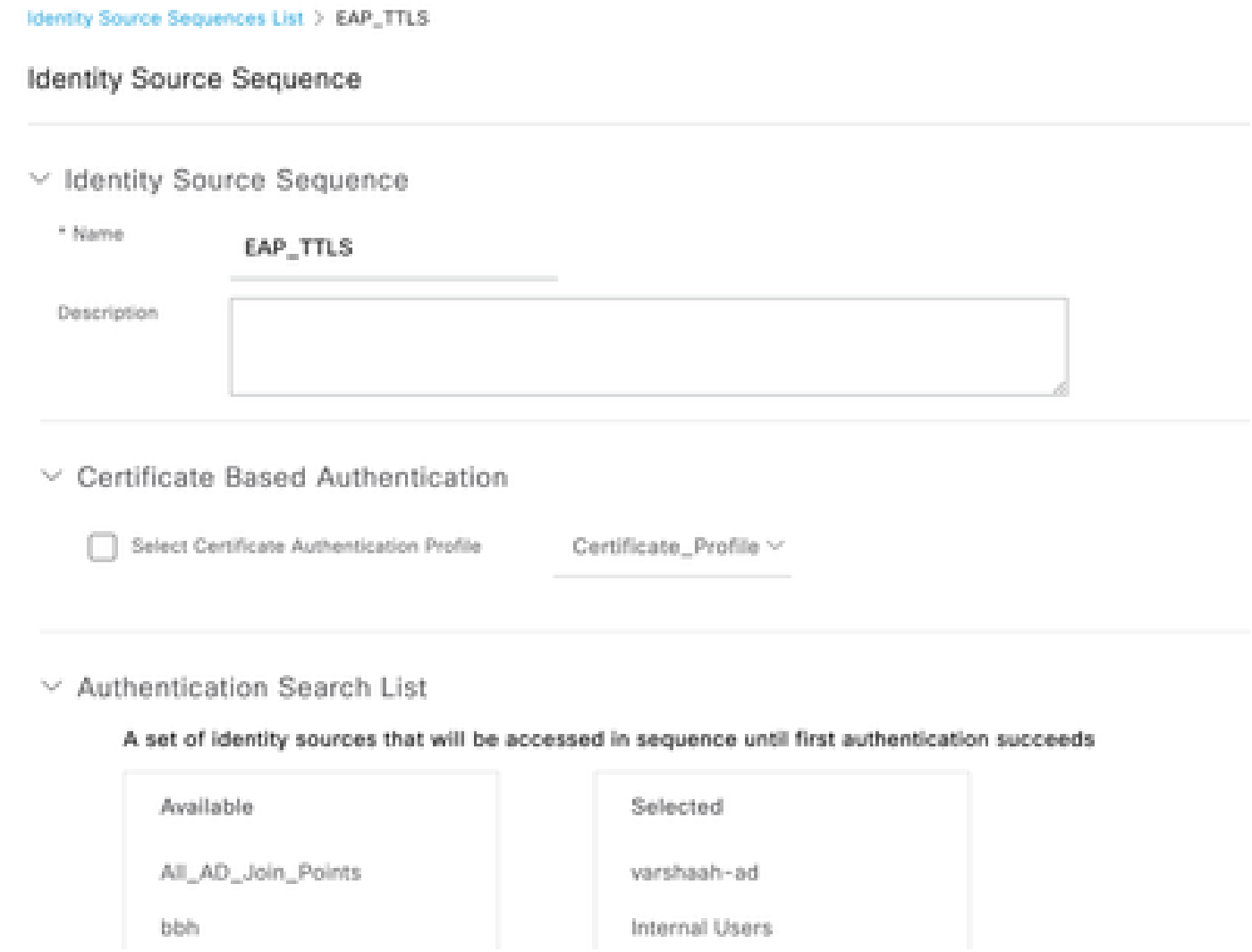
Introduzca el secreto compartido RADIUS, el mismo que se configuró anteriormente en el switch.



ISE de secreto compartido RADIUS

Paso 2. Configure la secuencia de origen de identidad.

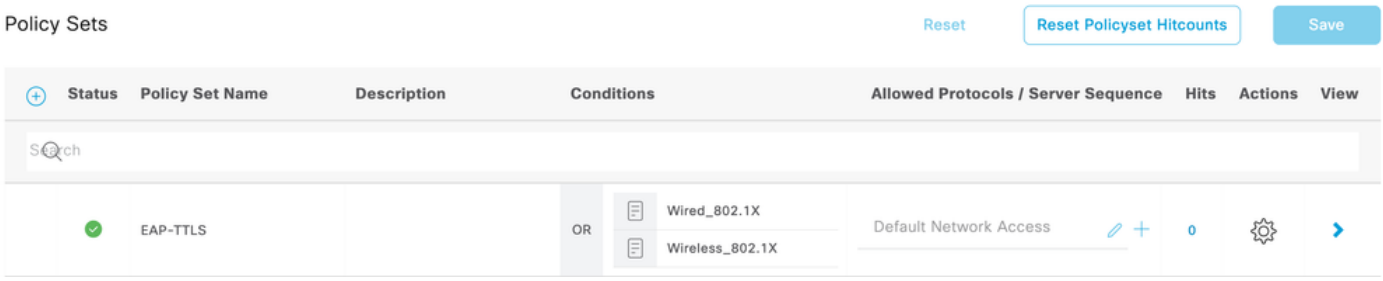
- Vaya a Administration > Identity Management > Identity Source Sequences.
- Haga clic en Agregar para crear una nueva secuencia de origen de identidad.
- Configure los orígenes de identidad en Lista de búsqueda de autenticación.



Secuencia de origen de identidad ISE

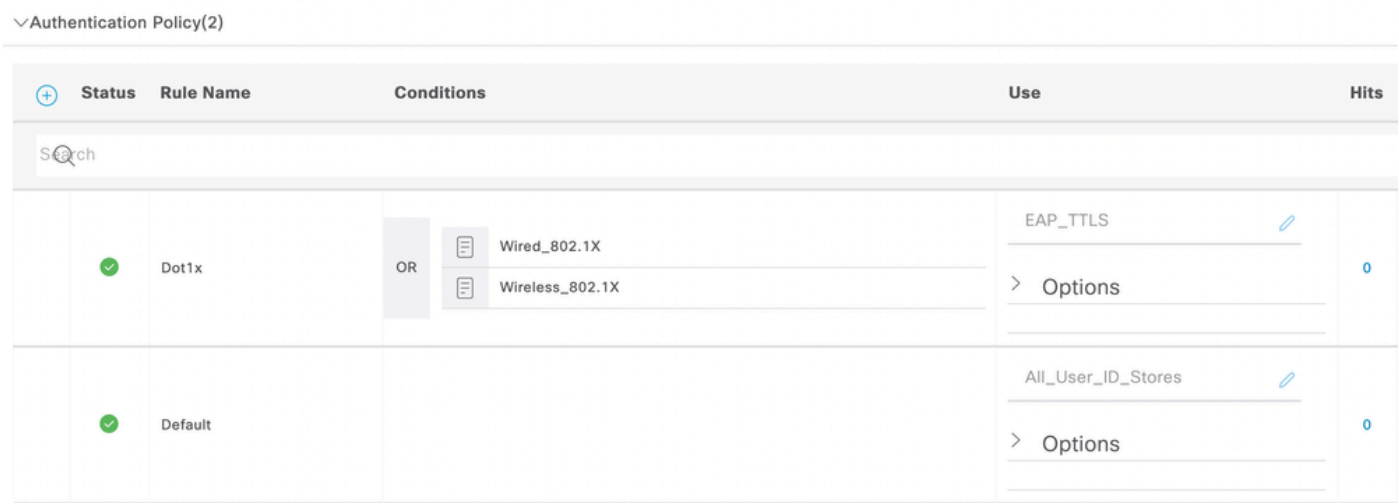
Paso 3. Configure el conjunto de políticas.

Navegue hasta Policy > Policy Sets y cree un nuevo conjunto de políticas. Configure las condiciones como Wired_802.1x O Wireless_802.1x. Para Protocolos permitidos, elija Default Network Access:



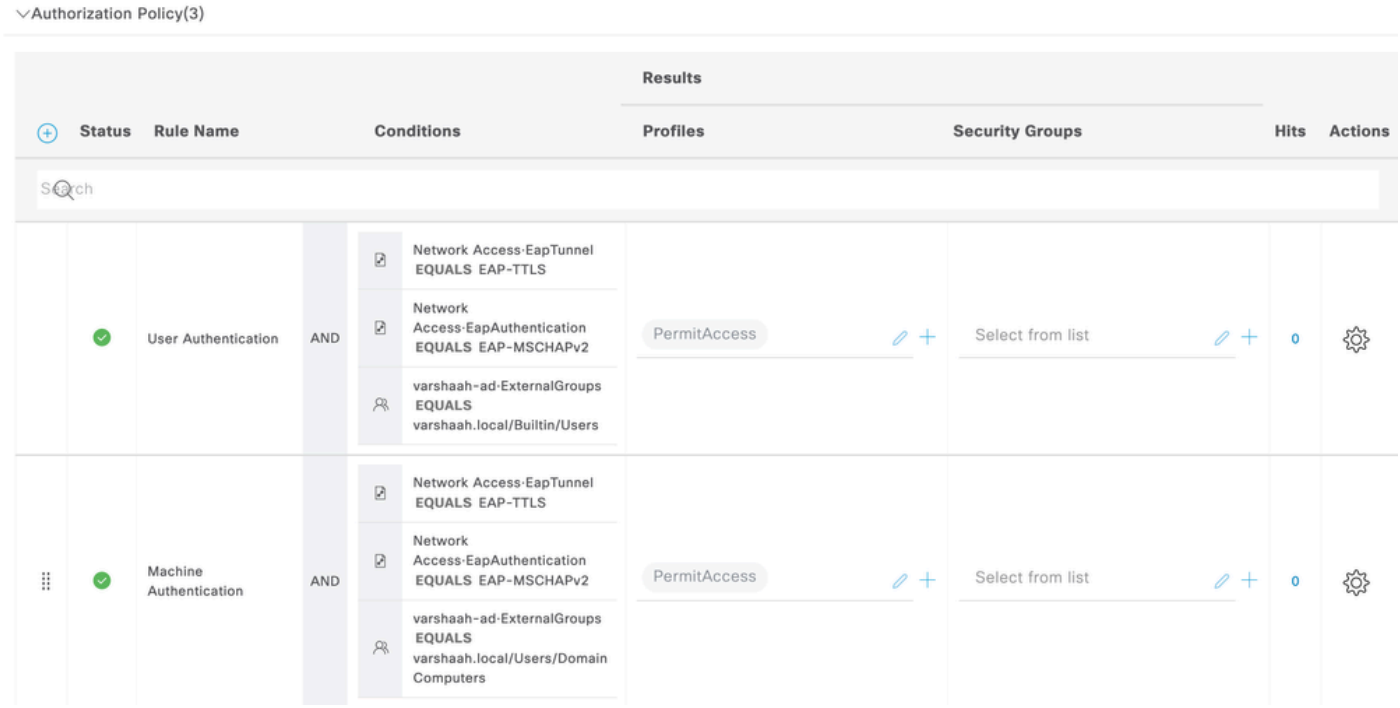
Conjunto de políticas EAP-TTLS

Cree la política de autenticación para dot1x y elija la secuencia de origen de identidad creada en el Paso 4.



Política de autenticación EAP-TTLS

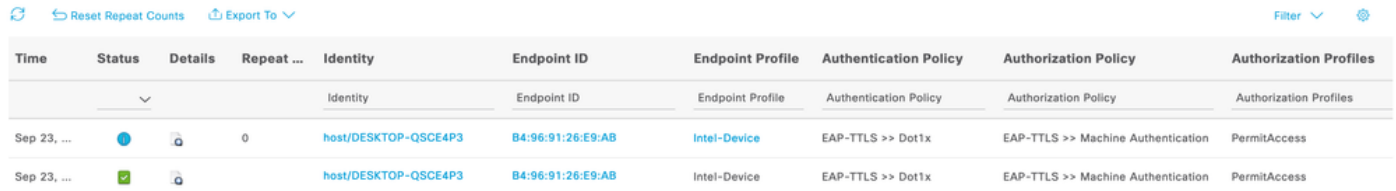
Para la directiva de autorización, cree la regla con tres condiciones. La primera condición verifica la condición de que se utiliza el túnel EAP-TTLS. La segunda condición comprueba que EAP-MSCHAPv2 se utiliza como el método EAP interno. La tercera condición comprueba para el grupo AD respectivo.



Directiva de autorización Dot1x

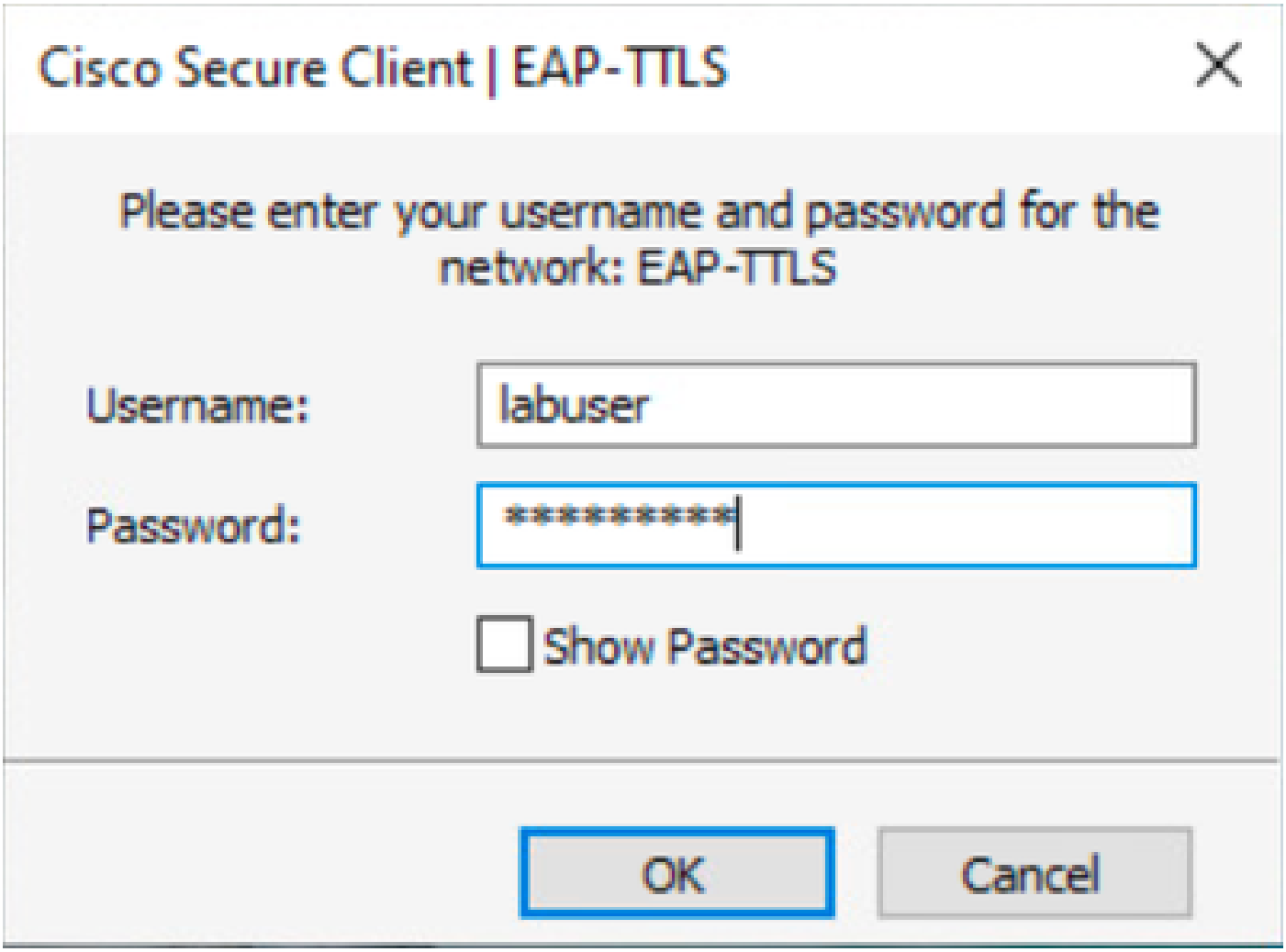
Verificación

Puede reiniciar el equipo con Windows 10 o cerrar sesión y, a continuación, iniciar sesión. Siempre que se muestre la pantalla de inicio de sesión de Windows, se activará la autenticación del equipo.

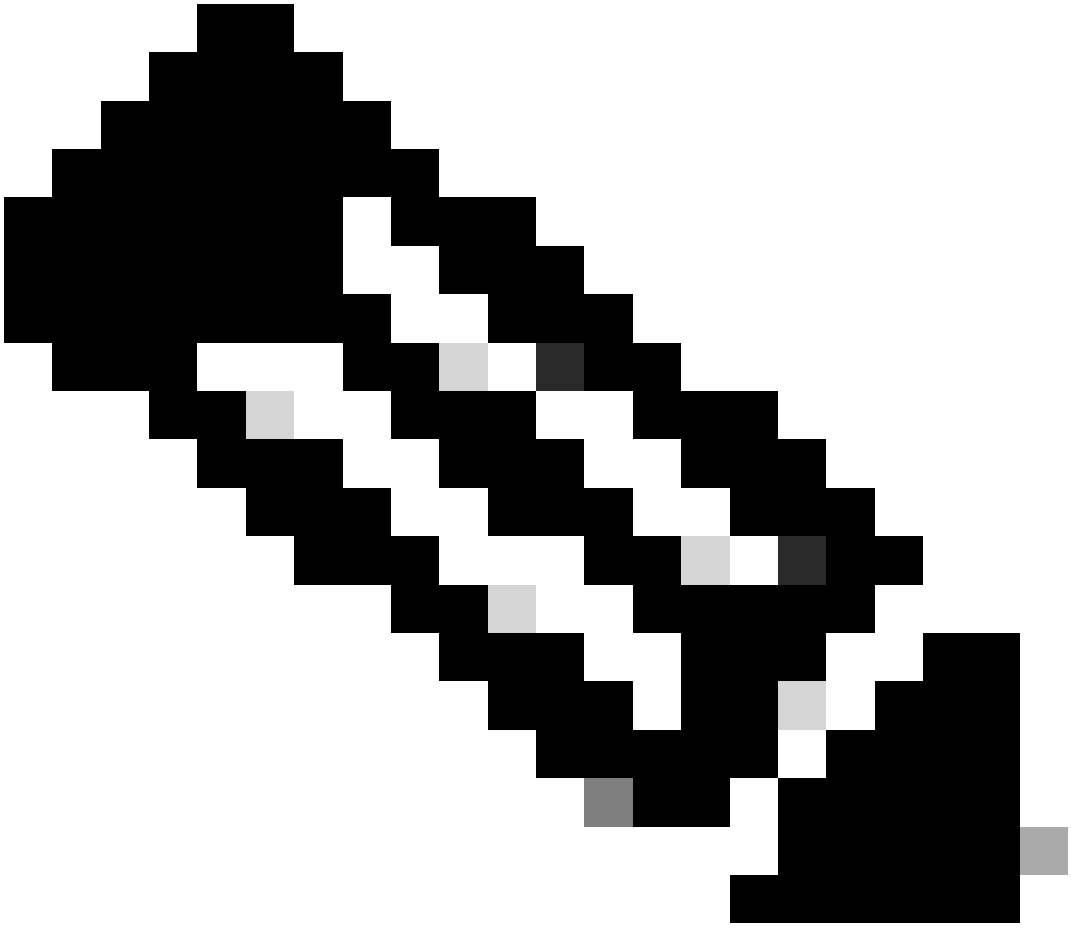


Autenticación de máquina de Live Log

Al iniciar sesión en el equipo con credenciales, se activa la autenticación de usuario.

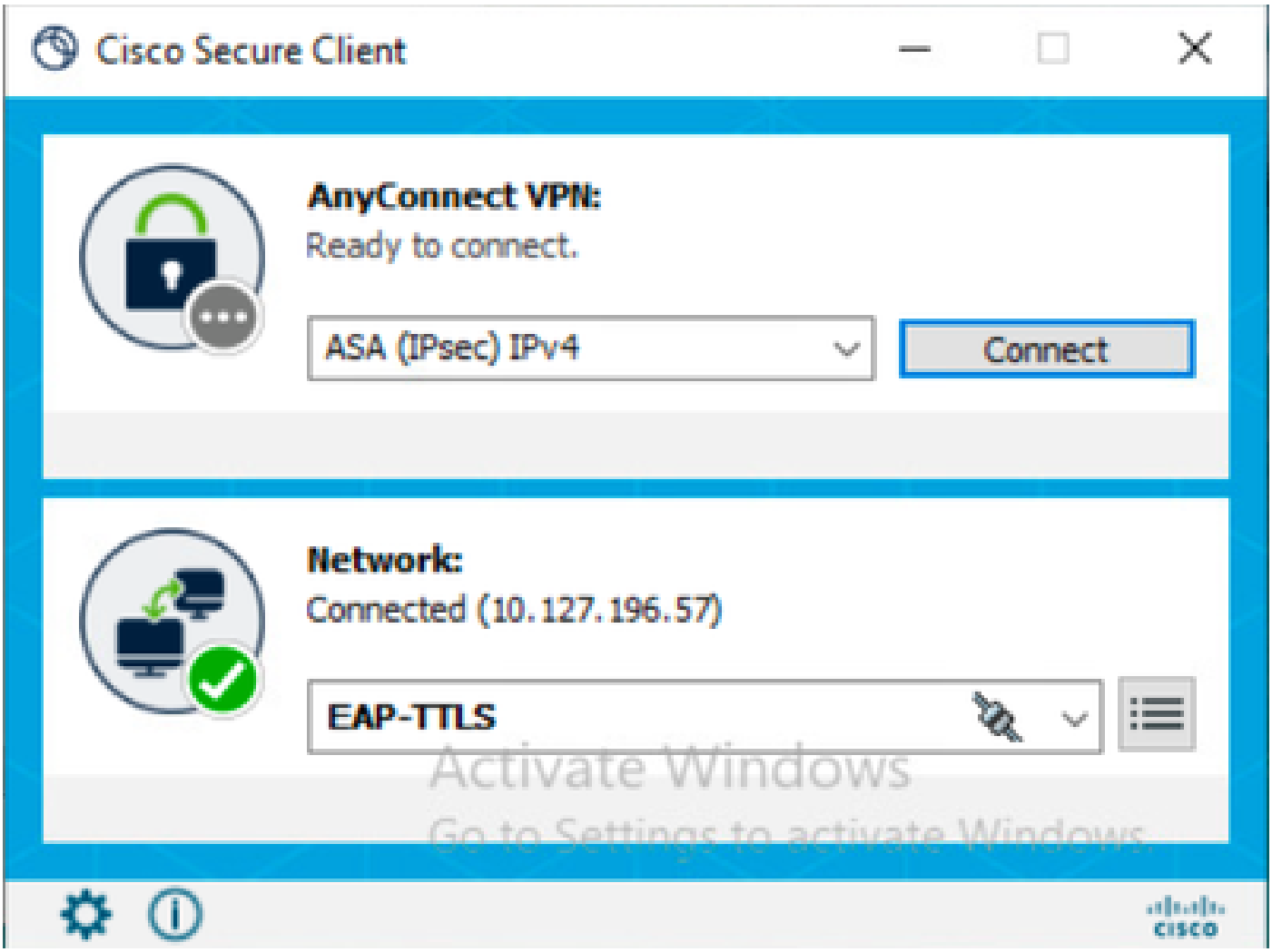


Credenciales de autenticación de usuario

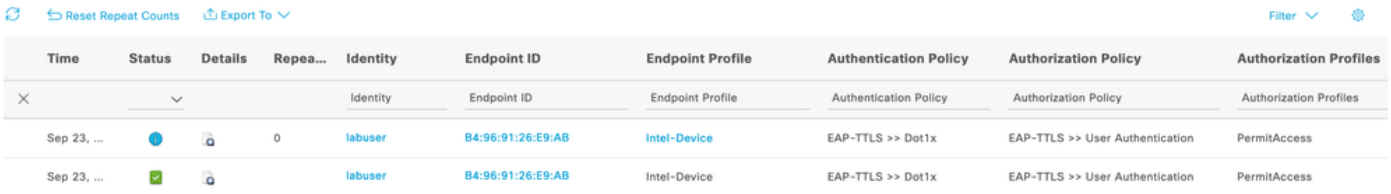


Nota: Este ejemplo utiliza las credenciales de usuario de Active Directory para la autenticación. También puede crear un usuario interno en Cisco ISE y utilizar esas credenciales para iniciar sesión.

Una vez introducidas las credenciales y verificadas correctamente, el terminal se conecta a la red mediante la autenticación de usuario.



EAP-TTLS conectado



Autenticación de usuario de Live Log

Análisis de registros en directo de ISE RADIUS

Esta sección ilustra las entradas del registro en vivo de RADIUS para una autenticación exitosa de máquina y usuario.

Autenticación de máquina

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... ... 11507 Extracted EAP-Response/Identity **12983 Prepared EAP-Request proposing EAP-TTLS with challenge** ... ... **12978 Extracted EAP-Response containing EAP-TTLS challenge-response and accepting EAP-TTLS as negotiated** 12800 Extracted first TLS record; TLS handshake started 12805 Extracted TLS ClientHello message 12806 Prepared TLS ServerHello message 12807 Prepared TLS Certificate message 12808 Prepared TLS ServerKeyExchange message 12810 Prepared TLS ServerDone message ... ... 12803 Extracted TLS ChangeCipherSpec message 12804 Extracted TLS Finished message

12801 Prepared TLS ChangeCipherSpec message 12802 Prepared TLS Finished message **12816 TLS handshake succeeded** ... ... **11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge** 12985 Prepared EAP-Request with another EAP-TTLS challenge 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response **11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated** ... ... 24431 Authenticating machine against Active Directory - varshaah-ad 24325 Resolving identity - host/DESKTOP-QSCE4P3 ... ... 24343 RPC Logon request succeeded - DESKTOP-QSCE4P3$@varshaah.local **24470 Machine authentication against Active Directory is successful - varshaah-ad** 22037 Authentication Passed ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response 11810 Extracted EAP-Response for inner method containing MSCHAP challenge-response 11814 Inner EAP-MSCHAP authentication succeeded 11519 Prepared EAP-Success for inner EAP method **12975 EAP-TTLS authentication succeeded** ... ... 15036 Evaluating Authorization Policy 24209 Looking up Endpoint in Internal Endpoints IDStore - host/DESKTOP-QSCE4P3 24211 Found Endpoint in Internal Endpoints IDStore 15048 Queried PIP - Network Access.Device IP Address 15048 Queried PIP - Network Access.EapTunnel **15016 Selected Authorization Profile - PermitAccess** ... ... 11002 Returned RADIUS Access-Accept

Autenticación de usuario

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... ... 11507 Extracted EAP-Response/Identity **12983 Prepared EAP-Request proposing EAP-TTLS with challenge** ... ... **12978 Extracted EAP-Response containing EAP-TTLS challenge-response and accepting EAP-TTLS as negotiated** 12800 Extracted first TLS record; TLS handshake started 12805 Extracted TLS ClientHello message 12806 Prepared TLS ServerHello message 12807 Prepared TLS Certificate message 12808 Prepared TLS ServerKeyExchange message 12810 Prepared TLS ServerDone message ... ... 12812 Extracted TLS ClientKeyExchange message 12803 Extracted TLS ChangeCipherSpec message 12804 Extracted TLS Finished message 12801 Prepared TLS ChangeCipherSpec message 12802 Prepared TLS Finished message **12816 TLS handshake succeeded** ... ... **11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge** 12985 Prepared EAP-Request with another EAP-TTLS challenge 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response **11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated** ... ... 24430 Authenticating user against Active Directory - varshaah-ad 24325 Resolving identity - labuser@varshaah.local ... ... 24343 RPC Logon request succeeded - labuser@varshaah.local **24402 User authentication against Active Directory succeeded - varshaah-ad** 22037 Authentication Passed ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response 11810 Extracted EAP-Response for inner method containing MSCHAP challenge-response 11814 Inner EAP-MSCHAP authentication succeeded 11519 Prepared EAP-Success for inner EAP method **12975 EAP-TTLS authentication succeeded** ... ... 15036 Evaluating Authorization Policy 24209 Looking up Endpoint in Internal Endpoints IDStore - labuser 24211 Found Endpoint in Internal Endpoints IDStore 15048 Queried PIP - Network Access.Device IP Address 15048 Queried PIP - Network Access.EapTunnel **15016 Selected Authorization Profile - PermitAccess** ... ... 11002 Returned RADIUS Access-Accept

Analizar registros NAM

Los registros de NAM, especialmente después de habilitar el registro extendido, contienen una gran cantidad de datos, la mayoría de los cuales son irrelevantes y se pueden ignorar. Esta sección enumera las líneas de depuración para demostrar cada paso que el NAM lleva a cabo para establecer una conexión de red. Cuando se trabaja a través de un registro, estas frases clave pueden ser útiles para localizar parte del registro relevante para el problema.

Autenticación de máquina

```
2160: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11812][comp=SAE]: 80
```

El cliente recibe un paquete EAP-TTLS del switch de red, iniciando la sesión EAP-TTLS. Este es el punto de partida para el túnel de autenticación de la máquina.

```
2171: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11812][comp=SAE]: EA
2172: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-6-INFO_MSG: %[tid=11812][comp=SAE]: CER
2173: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-6-INFO_MSG: %[tid=11812][comp=SAE]: CER
```

El cliente recibe el mensaje de saludo del servidor de ISE y comienza a validar el certificado del servidor (CN=varsha.varshaah.local). El certificado se encuentra en el almacén de confianza del cliente y se agrega para su validación.

```
2222: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-6-INFO_MSG: %[tid=11768]: Validating th
2223: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-6-INFO_MSG: %[tid=11768]: Server certif
```

El certificado del servidor se ha validado correctamente, completando el establecimiento del túnel TLS.

```
2563: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.789 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
2564: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.789 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11812][comp=SAE]: NE
2565: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.789 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
```

El cliente indica que la autenticación ha pasado. La interfaz está desbloqueada y la máquina de estado interno pasa a USER_T_NOT_DISCONNECTED, lo que indica que la máquina ahora puede pasar tráfico.

```
2609: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
2610: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11824][comp=SAE]: NE
2611: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
2612: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11824][comp=SAE]: NE
2613: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
2614: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11824][comp=SAE]: NE
2615: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
```

El adaptador informa authenticated, y el AccessStateMachine de NAM pasa a ACCESS_AUTHENTICATED. Esto confirma que la máquina ha completado con éxito la autenticación y tiene acceso completo a la red.

Autenticación de usuario

```
100: DESKTOP-QSCE4P3: Sep 25 2025 14:01:26.669 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9664]: Network EAP-TT
```

El cliente NAM comienza el proceso de conexión EAP-TTLS.

```
195: DESKTOP-QSCE4P3: Sep 25 2025 15:09:11.780 +0900: %csc_nam-7-DEBUG_MSG: %[tid=3252]: Binding adapte
198: DESKTOP-QSCE4P3: Sep 25 2025 15:09:11.780 +0900: %csc_nam-7-DEBUG_MSG: %[tid=3252]: Network EAP-TT
```

NAM enlaza el adaptador físico a la red EAP-TTLS y pasa al estado ACCESS_ATTACHED, confirmando que el adaptador está listo para la autenticación.

```
204: DESKTOP-QSCE4P3: Sep 25 2025 15:09:11.780 +0900: %csc_nam-7-DEBUG_MSG: %[tid=3252]: Network EAP-TT
247: DESKTOP-QSCE4P3: Sep 25 2025 15:09:11.780 +0900: %csc_nam-7-DEBUG_MSG: %[tid=3680][comp=SAE]: STAT
```

El cliente pasa de ATTACHED a CONNECTING, comenzando el intercambio 802.1X.

```
291: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.388 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6644][comp=SAE]: 8021
```

El cliente envía un EAPOL-Start para activar el proceso de autenticación.

```
331: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.435 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6644][comp=SAE]: PORT
332: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.435 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6644][comp=SAE]: 8021
340: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.435 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6644][comp=SAE]: EAP
```

El switch solicita una identidad y el cliente se prepara para responder con una identidad externa.

```
402: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.685 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9580]: EAP-CB: creden
422: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.685 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6088]: EAP: processin
460: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.685 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6088]: EAP: credentia
```

El NAM envía la identidad externa. De forma predeterminada, es anonymous, lo que indica que el intercambio es para la autenticación de usuarios (no para el equipo).

```
488: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.497 +0900: %csc_nam-6-INFO_MSG: %[tid=6088]: EAP: EAP sugges
```

```
489: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.497 +0900: %csc_nam-6-INFO_MSG: %[tid=6088]: EAP: EAP reques
490: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.497 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6088]: EAP: EAP metho
491: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.497 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6088]: EAP: credentia
```

Tanto el cliente como el servidor aceptan utilizar EAP-TTLS como el método externo.

```
660: DESKTOP-QSCE4P3: Sep 25 2025 14:01:27.185 +0900: %csc_nam-7-DEBUG_MSG: %[tid=8296][comp=SAE]: EAP
661: DESKTOP-QSCE4P3: Sep 25 2025 14:01:27.185 +0900: %csc_nam-7-DEBUG_MSG: %[tid=8296][comp=SAE]: EAP
```

El cliente envía el mensaje Hello del cliente y recibe el mensaje Hello del servidor, que incluye el certificado de ISE.

```
706: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.967 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: 802
717: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.967 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EAP
718: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.967 +0900: %csc_nam-6-INFO_MSG: %[tid=11932][comp=SAE]: CERT
719: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.983 +0900: %csc_nam-6-INFO_MSG: %[tid=11932][comp=SAE]: CERT
726: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.983 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EAP
```

Se presenta el certificado del servidor. El cliente busca el archivo CN varshaah.varshaah.local, encuentra una coincidencia y valida el certificado. El protocolo de enlace se detiene mientras se comprueba el certificado X.509.

```
729: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.983 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EAP
730: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.983 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11916][comp=SAE]: EAP
1110: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.044 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
1111: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.044 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
```

El túnel está establecido. NAM ahora solicita y prepara la identidad protegida y las credenciales para la autenticación interna.

```
1527: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.169 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11916][comp=SAE]: EA
1528: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.169 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11916][comp=SAE]: EA
1573: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.184 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EA
1574: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.184 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EA
1575: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.184 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EA
```

El intercambio de señales TLS se completa. Ahora se establece un túnel seguro para la autenticación interna.

```
1616: DESKTOP-QSCE4P3: Sep 25 2025 14:01:46.262 +0900: %csc_nam-6-INFO_MSG: %[tid=9664]: Protected iden
1620: DESKTOP-QSCE4P3: Sep 25 2025 14:01:46.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9664]: Auth[EAP-TTLS
1689: DESKTOP-QSCE4P3: Sep 25 2025 14:01:46.277 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9664]: Auth[EAP-TTLS
```

ISE envía y acepta la identidad protegida (nombre de usuario).

```
1708: DESKTOP-QSCE4P3: Sep 25 2025 14:01:46.277 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9456][comp=SAE]: EAP
1738: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.758 +0900: %csc_nam-6-INFO_MSG: %[tid=11768]: Protected pas
1741: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.200 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
```

ISE solicita la contraseña. NAM envía la contraseña protegida dentro del túnel TLS.

```
1851: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
1852: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: STA
1853: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
1854: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: STA
1855: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: STA
```

ISE valida la contraseña, envía transiciones EAP-Success y NAM a AUTHENTICATED. Llegados a este punto, la autenticación de usuario ha finalizado y el cliente tiene permiso para acceder a la red.

Troubleshoot

Al solucionar problemas del Administrador de acceso de red (NAM) con Cisco ISE y la integración de switches, se deben recopilar registros de los tres componentes: Secure Client (NAM), Cisco ISE y el switch.

Registros de Secure Client (NAM)

1. Habilite el registro extendido NAM siguiendo estos pasos.
2. Reproduzca el problema. Si el perfil de red no se aplica, ejecute Reparación de red en Secure Client.
3. Recopile el paquete DART mediante la herramienta de diagnóstico e informes (DART).

Registros de Cisco ISE

Habilite estas depuraciones en ISE para capturar la autenticación y las interacciones de directorio:

- Runtime-AAA

- nsf
- nsf-session

Registros del switch

Depuraciones básicas

```
request platform software trace rotate all
set platform software trace smd switch active R0 radius debug
set platform software trace smd switch active R0 aaa debug
set platform software trace smd switch active R0 dot1x-all debug
set platform software trace smd switch active R0 eap-all debug
debug radius all
```

Depuraciones avanzadas (si es necesario)

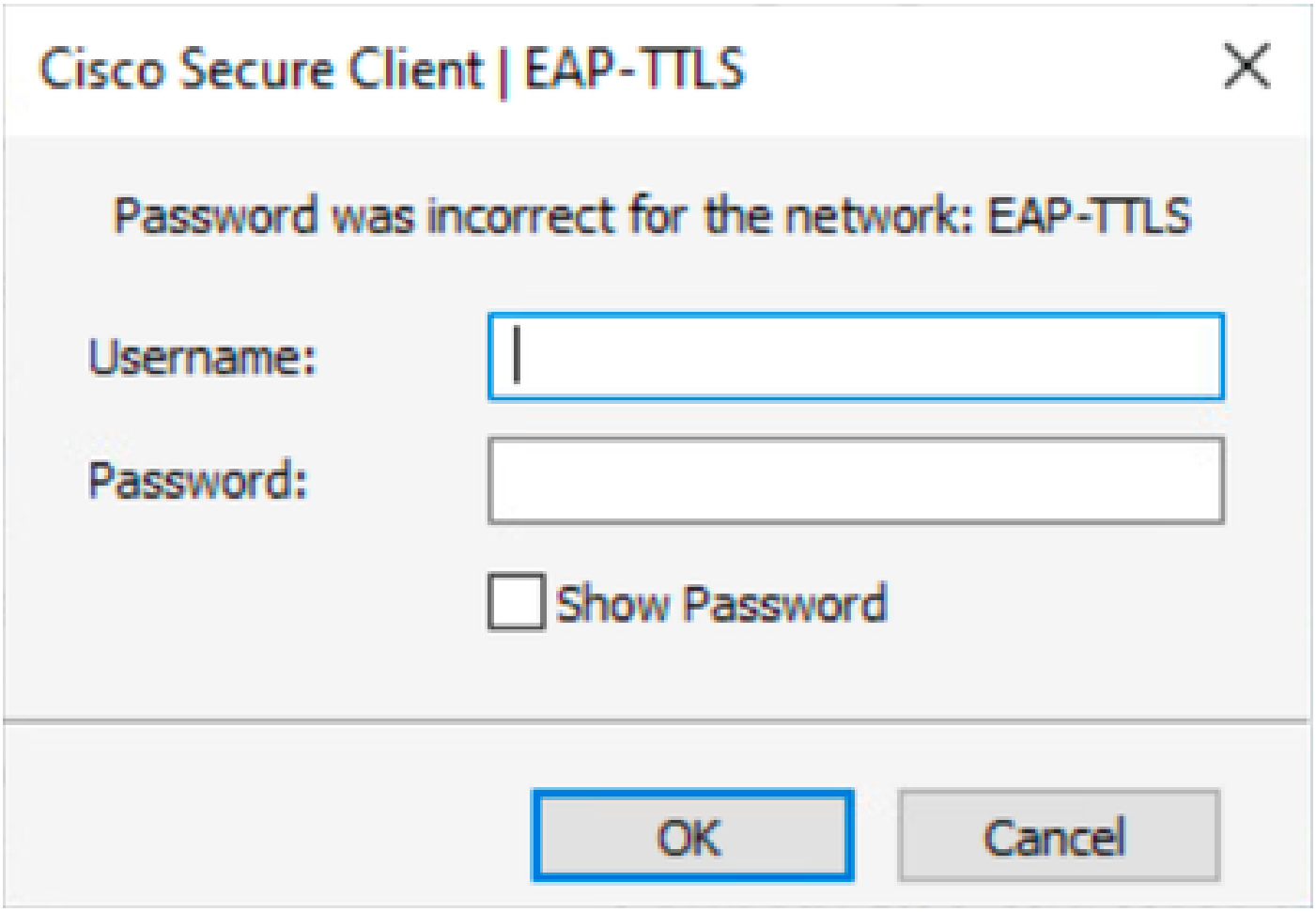
```
set platform software trace smd switch active R0 epm-all debug
set platform software trace smd switch active R0 pre-all debug
```

Comandos show

```
show version
show debugging
show running-config aaa
show authentication session interface gix/x details
show dot1x interface gix/x
show aaa servers
show platform software trace message smd switch active R0
```

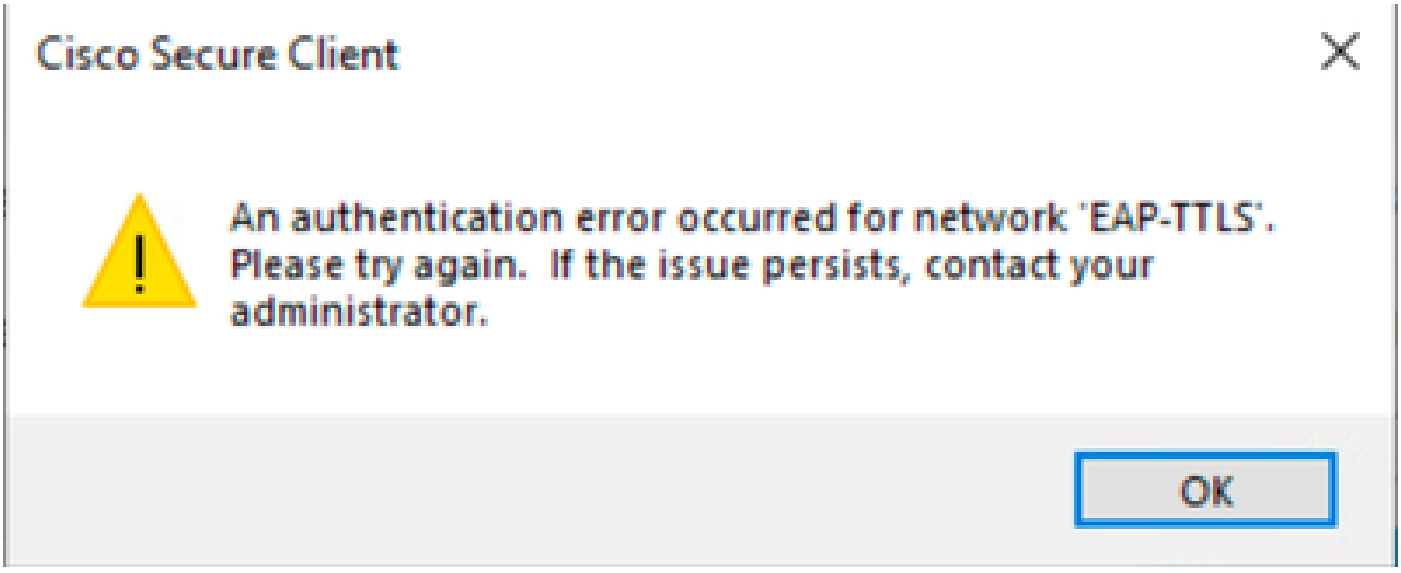
Error de autenticación de usuario debido a credenciales no válidas

Cuando un usuario introduce credenciales incorrectas, Secure Client muestra una contraseña genérica incorrecta para la red: mensaje EAP-TTLS. El error en pantalla no especifica si el problema se debe a un nombre de usuario o contraseña no válidos.



Error de contraseña incorrecta

Si la autenticación falla dos veces consecutivamente, Secure Client muestra este mensaje: Se produjo un error de autenticación para la red 'EAP-TTLS'. Vuelva a intentarlo. Si el problema continúa, póngase en contacto con el administrador.



Problema de autenticación de usuario

Para identificar la causa, revise los registros de NAM.

1. Contraseña incorrecta:

Cuando un usuario ingresa una contraseña incorrecta, los logs de NAM muestran entradas similares a esta salida:

```
3775: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.921 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300][comp=SAE]: EA
3776: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.921 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300][comp=SAE]: EA
3777: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.922 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300][comp=SAE]: EA
```

En los registros en directo de Cisco ISE, el evento correspondiente aparece como:

Event	5400 Authentication failed
Failure Reason	24408 User authentication against Active Directory failed since user has entered the wrong password
Resolution	Check the user password credentials. If the RADIUS request is using PAP for authentication, also check the Shared Secret configured for the Network Device
Root cause	User authentication against Active Directory failed since user has entered the wrong password

Contraseña incorrecta

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... ... 11507 Extracted EAP-Response/Identity 10 **12983 Prepared EAP-Request proposing EAP-TTLS with challenge** ... ... **12978 Extracted EAP-Response containing EAP-TTLS challenge-response and accepting EAP-TTLS as negotiated** 12800 Extracted first TLS record; TLS handshake started ... ... 12810 Prepared TLS ServerDone message ... ... 12812 Extracted TLS ClientKeyExchange message 12803 Extracted TLS ChangeCipherSpec message ... ... **12816 TLS handshake succeeded** ... ... **11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge 0** 12985 Prepared EAP-Request with another EAP-TTLS challenge 11006 Returned RADIUS Access-Challenge 0 11001 Received RADIUS Access-Request ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response 0 **11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated** ... ... 15013 Selected Identity Source - varshaah-ad 0 24430 Authenticating user against Active Directory - varshaah-ad 0 24325 Resolving identity - labuser@varshaah.local 4 24313 Search for matching accounts at join point - varshaah.local 0 24319 Single matching account found in forest - varshaah.local 0 24323 Identity resolution detected single matching account 0 **24344 RPC Logon request failed - STATUS_WRONG_PASSWORD, ERROR_INVALID_PASSWORD, labuser@varshaah.local 20 24408 User authentication against Active Directory failed since user has entered the wrong password - varshaah-ad 1** ... ... 11823 EAP-MSCHAP authentication attempt failed ... ... 11815 Inner EAP-MSCHAP authentication failed 0 ... ... 12976 EAP-TTLS authentication failed 0 ... ... 11003 Returned RADIUS Access-Reject

2. Nombre de usuario incorrecto:

Cuando un usuario ingresa un nombre de usuario incorrecto, los logs de NAM muestran entradas similares a esta salida:

```
3788: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.923 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300][comp=SAE]: EA
3789: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.923 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300]: EAP-CB: EAP
```

En los registros en directo de Cisco ISE, el evento correspondiente aparece como:

Event	5400 Authentication failed
Failure Reason	22056 Subject not found in the applicable identity store(s)
Resolution	Check whether the subject is present in any one of the chosen identity stores. Note that some identity stores may have been skipped due to identity resoultion settings or if they do not support the current authentication protocol.
Root cause	Subject not found in the applicable identity store(s).

Nombre de usuario incorrecto

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... ... 11507 Extracted EAP-Response/Identity **12983 Prepared EAP-Request proposing EAP-TTLS with challenge** ... ... **12978 Extracted EAP-Response containing EAP-TTLS challenge-response and accepting EAP-TTLS as negotiated** 12800 Extracted first TLS record; TLS handshake started ... ... 12810 Prepared TLS ServerDone message ... ... 12812 Extracted TLS ClientKeyExchange message 12803 Extracted TLS ChangeCipherSpec message ... ... **12816 TLS handshake succeeded** ... ... **11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge** 12985 Prepared EAP-Request with another EAP-TTLS challenge 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response **11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated** ... ... 15013 Selected Identity Source - All_AD_Join_Points 24430 Authenticating user against Active Directory - varshaah-ad 24325 Resolving identity - user@varshaah.local 24313 Search for matching accounts at join point - varshaah.local ... ... 24352 Identity resolution failed - ERROR_NO_SUCH_USER **24412 User not found in Active Directory - varshaah-ad** ... ... 15013 Selected Identity Source - Internal Users 24210 Looking up User in Internal Users IDStore - user **24216 The user is not found in the internal users identity store** ... ... 22056 Subject not found in the applicable identity store(s) 22058 The advanced option that is configured for an unknown user is used 22061 The 'Reject' advanced option is configured in case of a failed authentication request **11823 EAP-MSCHAP authentication attempt failed** ... ... **11815 Inner EAP-MSCHAP authentication failed** ... ... 12976 EAP-TTLS authentication failed 0 ... ... 11504 Prepared EAP-Failure 1 **11003 Returned RADIUS Access-Reject**

Defectos conocidos

ID de la falla	Descripción
ID de bug de Cisco 63395	ISE 3.0 no encuentra el almacén de ID de REST después de reiniciar los servicios

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).