Solucionar problemas de punto 1x con cables en ISE 3.2 y Windows

Contenido

Introducción

Este documento describe cómo configurar una autenticación básica PEAP 802.1X para Identity Services Engine (ISE) 3.2 y el suplicante nativo de Windows.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Protocolo de autenticación extensible protegido (PEAP)
- PEAP 802.1x

Componentes Utilizados

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

- Versión de Cisco Identity Services Engine (ISE)
- Cisco C1117 Cisco IOS® XE Software, versión 17.12.02
- Ordenador portátil con Windows 10

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama de la red

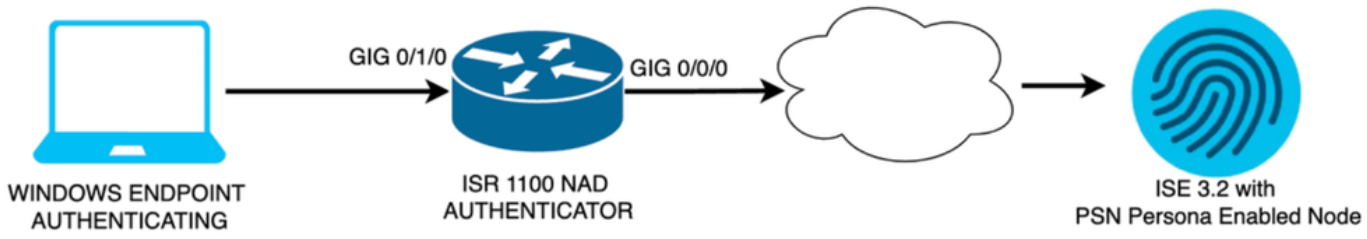


Diagrama de la red

Configuraciones

Realice estos pasos para configurar:

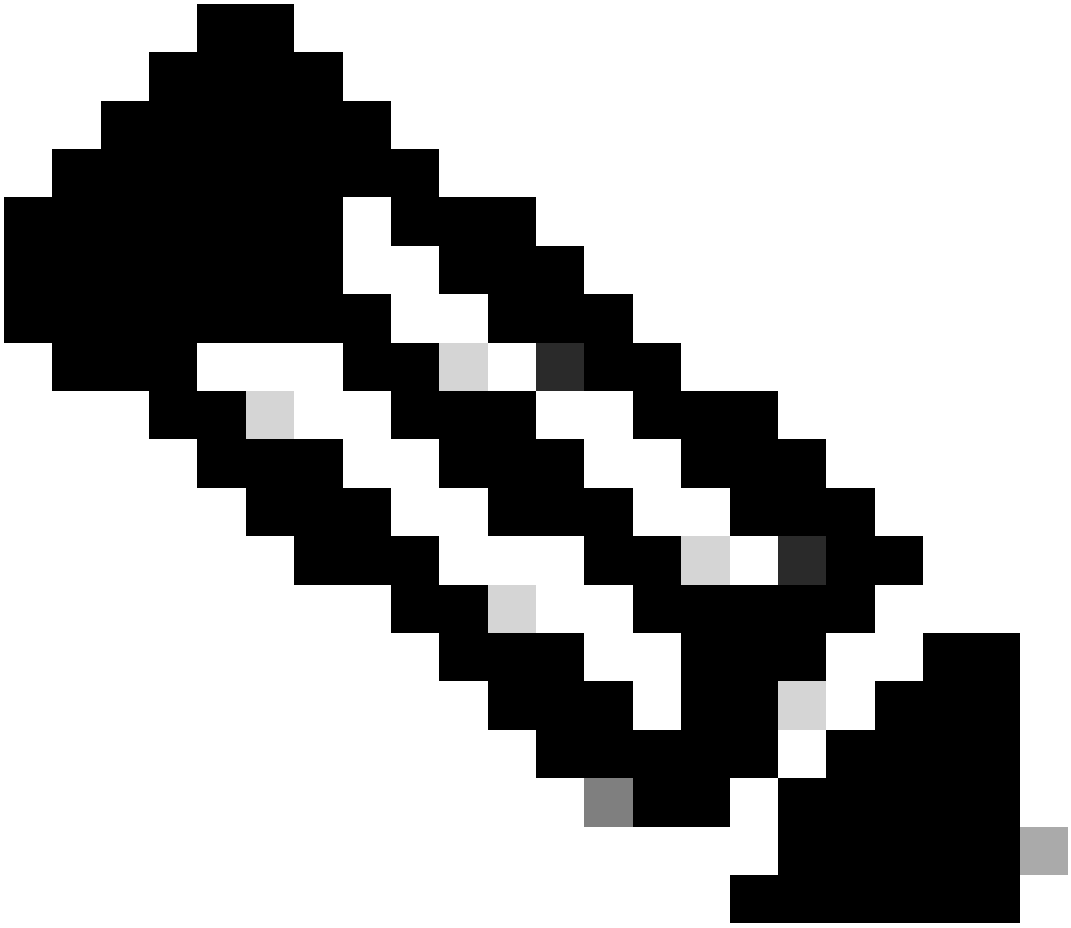
Paso 1. Configuración del router ISR 1100.

Paso 2. Configuración de Identity Service Engine 3.2.

Paso 3. Configuración del suplicante nativo de Windows.

Paso 1. Configuración del router ISR 1100

Esta sección explica la configuración básica que al menos el NAD debe tener para que funcione dot1x.



Nota: para la implementación de ISE de varios nodos, configure la dirección IP del nodo que tenga activada la persona PSN. Esto se puede habilitar si navega 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>
```

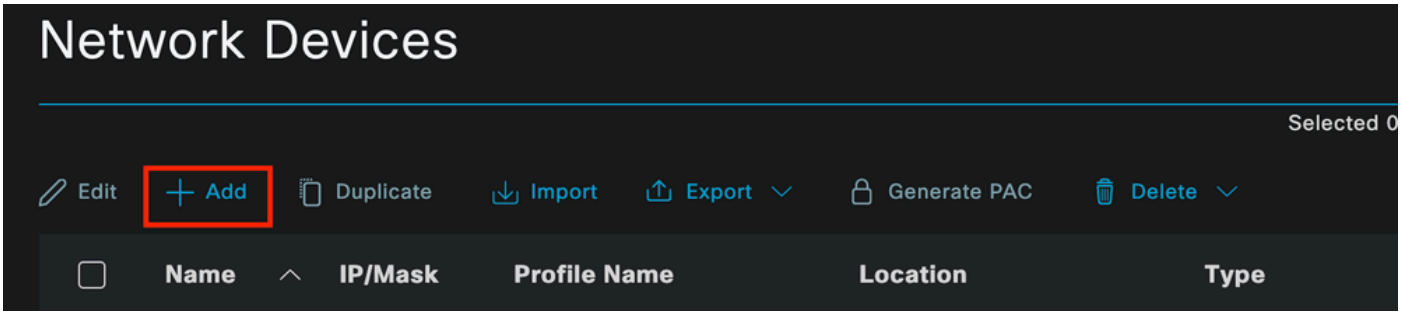
```
!
!
aaa group server radius ISE-CLUSTER
 server name ISE-PSN-1
!
interface GigabitEthernet0/1/0
 description "Endpoint that supports dot1x"
 switchport access vlan 15
 switchport mode access
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication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

Paso 2. Configuración de Identity Service Engine 3.2.

2. a. Configure y agregue el dispositivo de red que se utilizará para la autenticación.

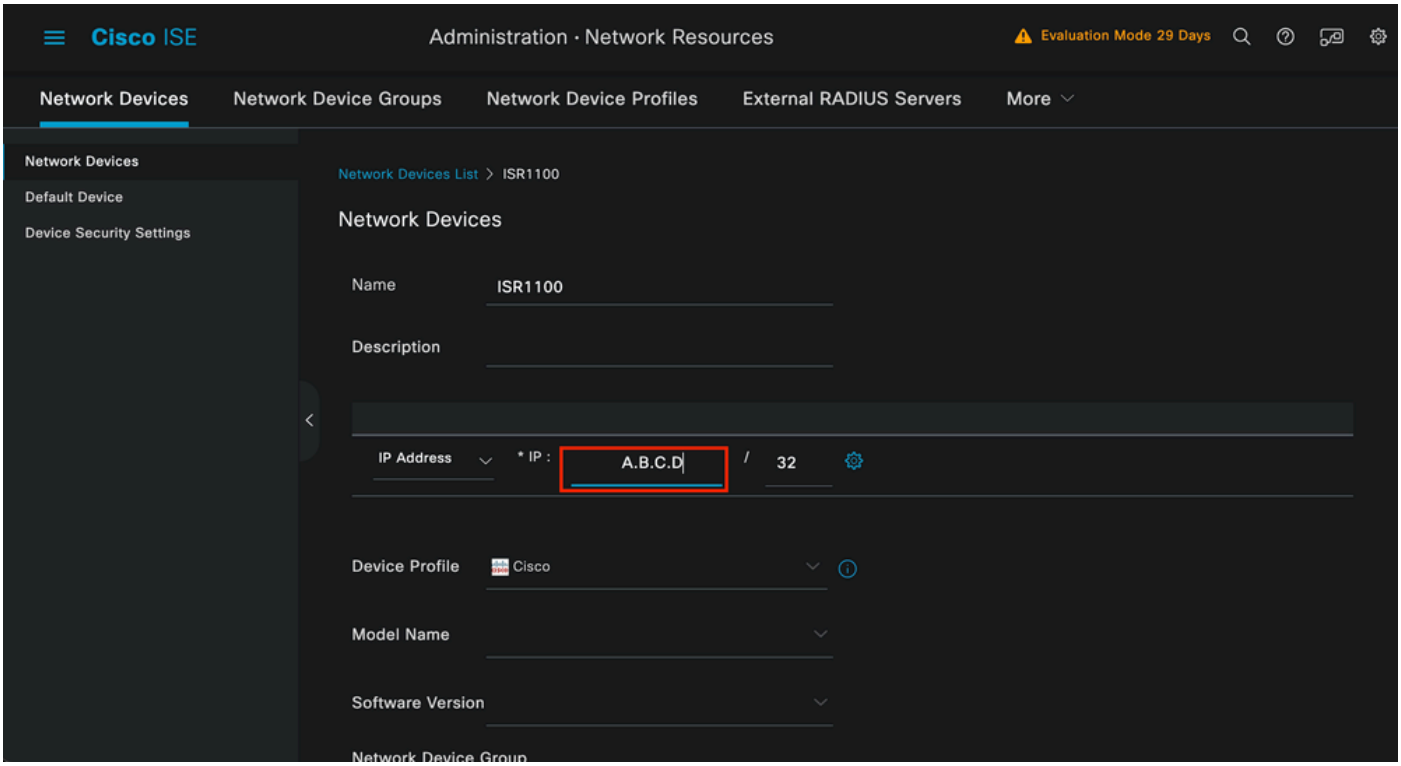
Sección Agregar el dispositivo de red a los dispositivos de red ISE.

Haga clic en el botón Add para comenzar.



Dispositivos de red ISE

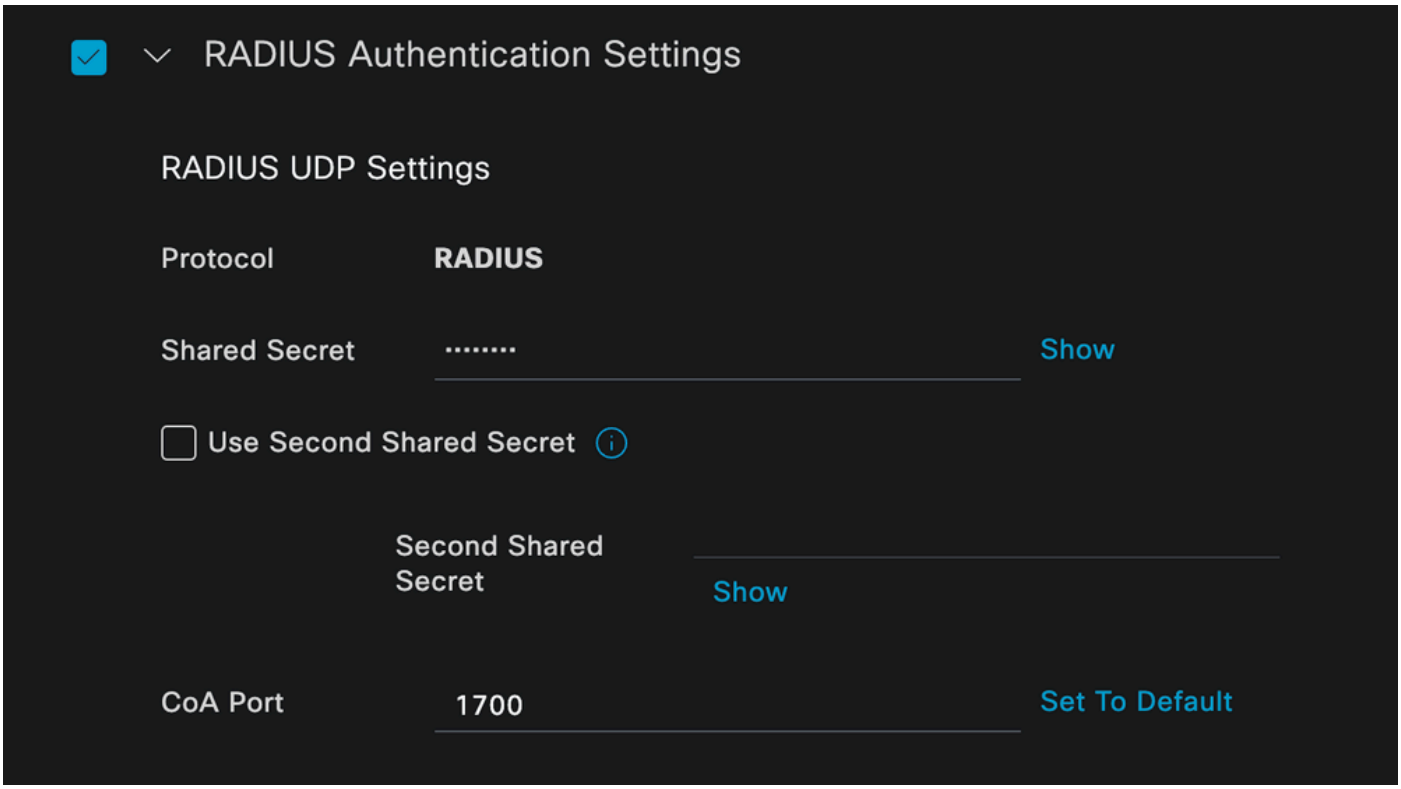
Introduzca los valores, asigne un nombre al NAD que está creando y agregue también la IP que el dispositivo de red utiliza para ponerse en contacto con ISE.



Página de creación de dispositivo de red

En esta misma página, desplácese hacia abajo para buscar Radius Authentication Settings. Como se muestra en la siguiente imagen.

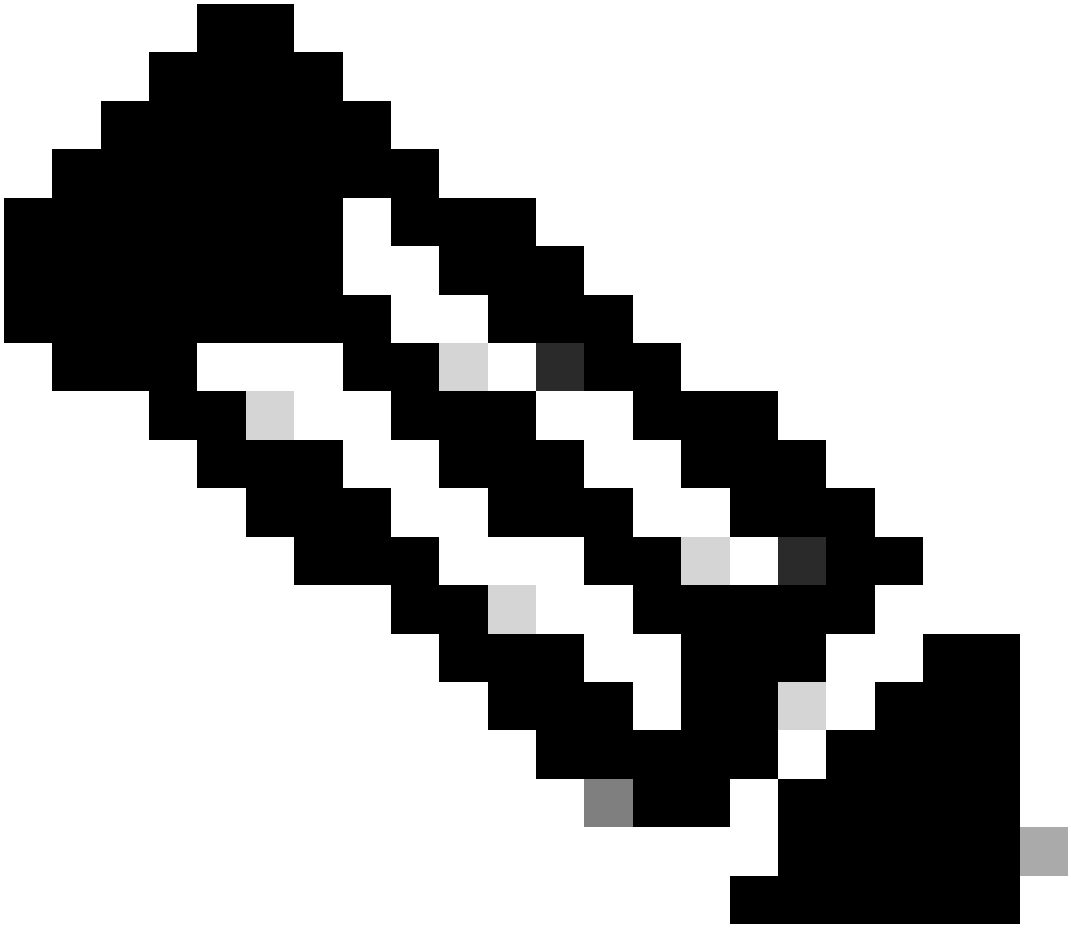
Agregue el secreto compartido que utilizó en la configuración de NAD.



Configuración RADIUS

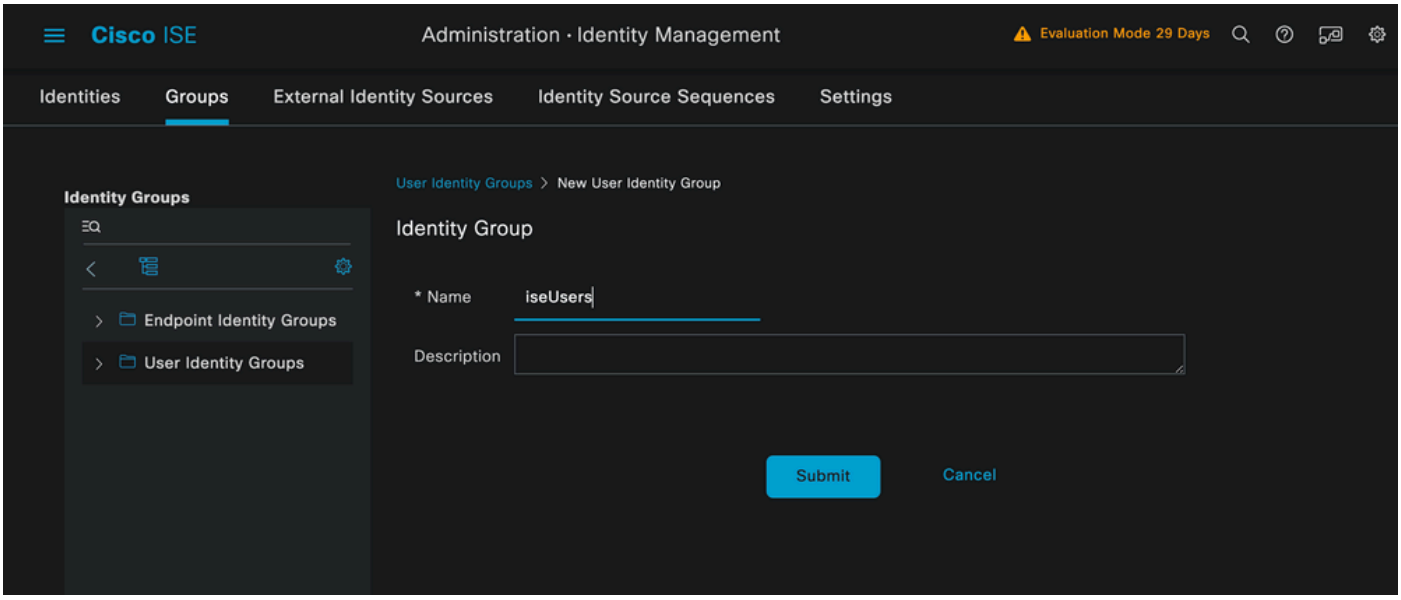
Guarde los cambios.

2. b. Configure la identidad que se utiliza para autenticar el punto final.



> Nota: con el objetivo de mantener esta guía de configuración, se utiliza la autenticación local ISE simple.

Vaya a la pestaña Administration > Identity Management > Groups. Cree el grupo y la identidad; el grupo creado para esta demostración es iseUsers.

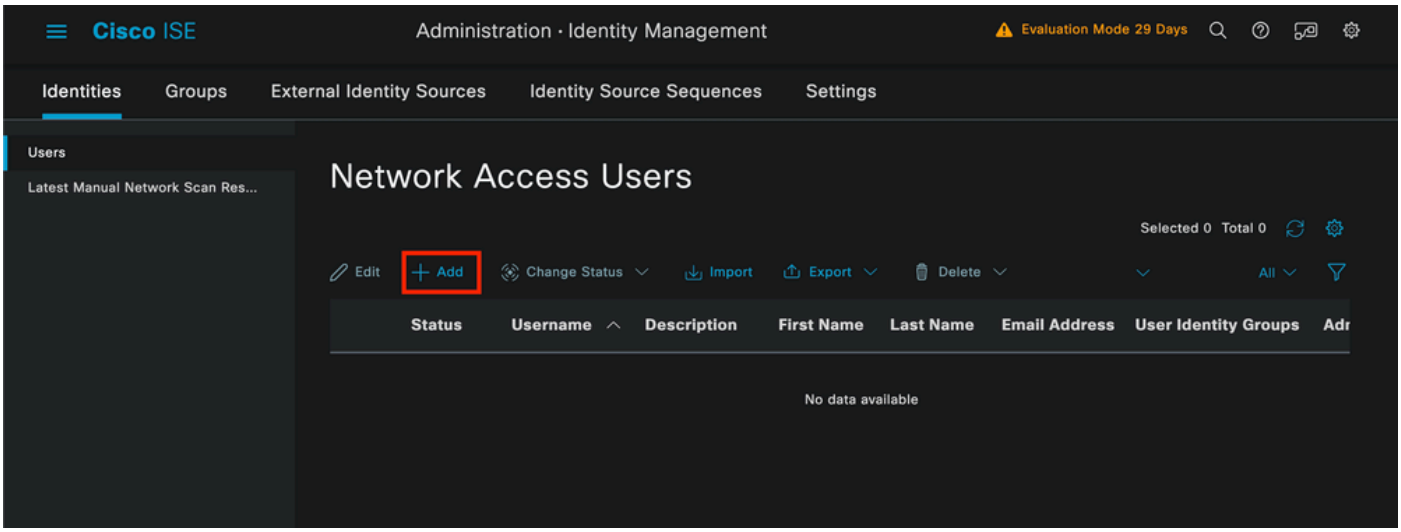


Página Creación de Grupo de Identidad

Haga clic en el botón Submit.

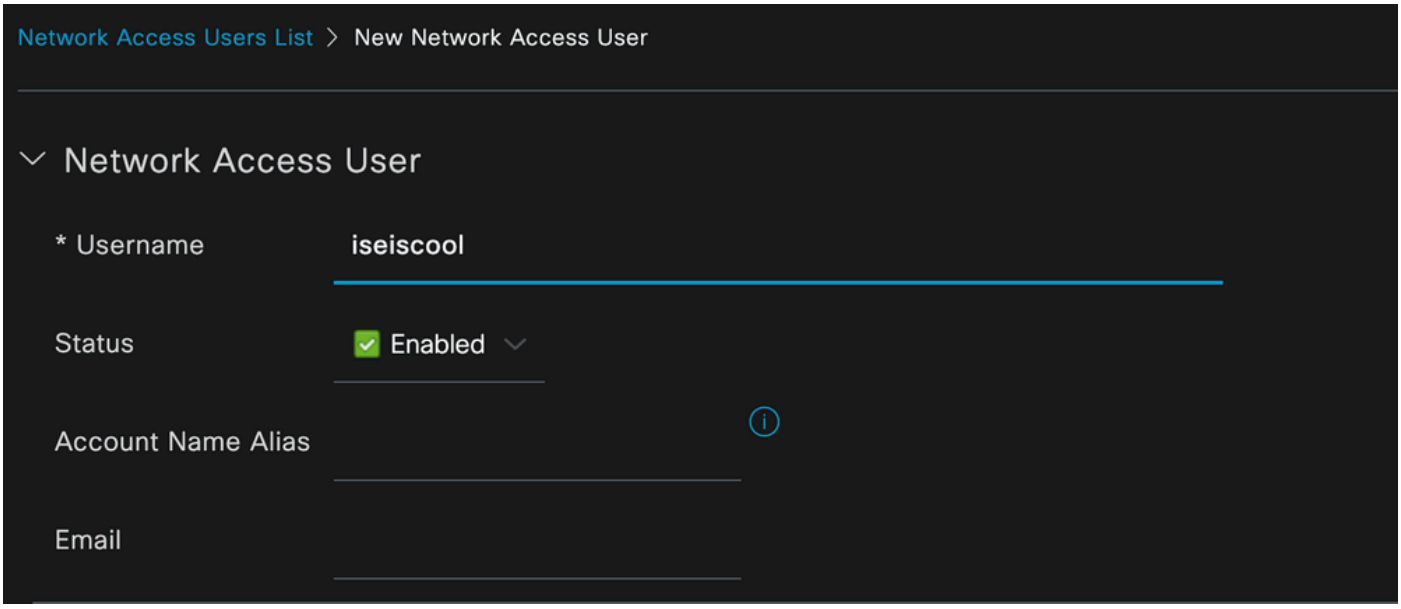
A continuación, vaya a la pestaña Administration > Identity Management > Identity.

Haga clic en Agregar.



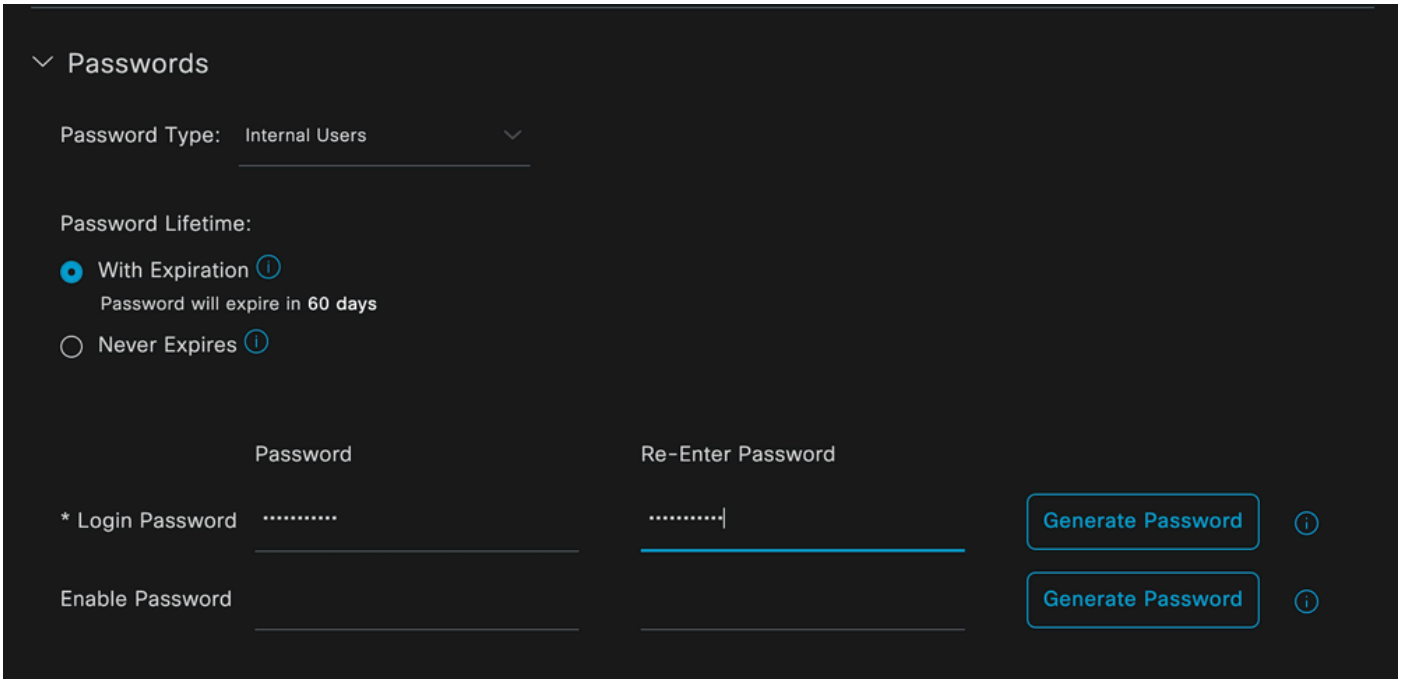
Página de creación de usuario

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



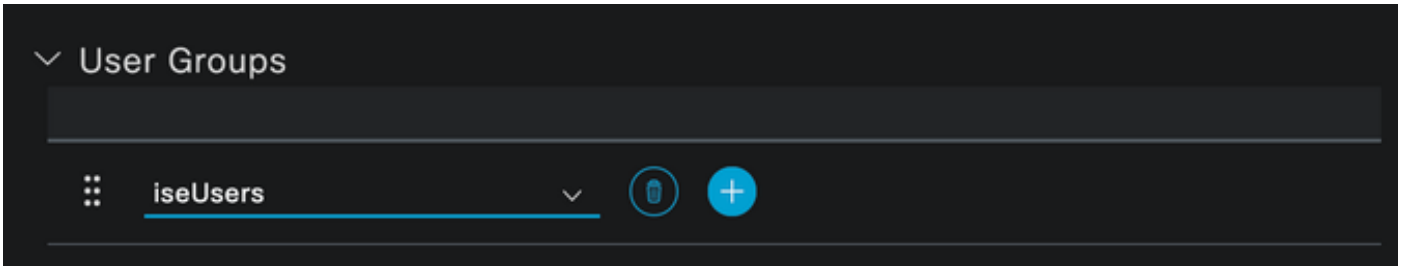
Nombre asignado al nombre de usuario

El siguiente paso es asignar una contraseña al nombre de usuario creado. VainillaISE97 se utiliza en esta demostración.



Creación de contraseña

Asigne el usuario al grupo iseUsers.



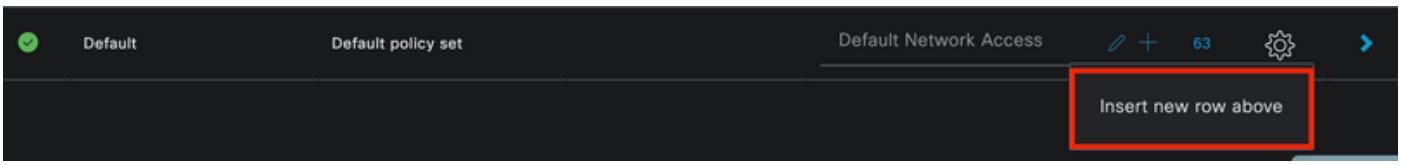
Asignación de grupo de usuarios

2. c. Configurar el conjunto de políticas

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

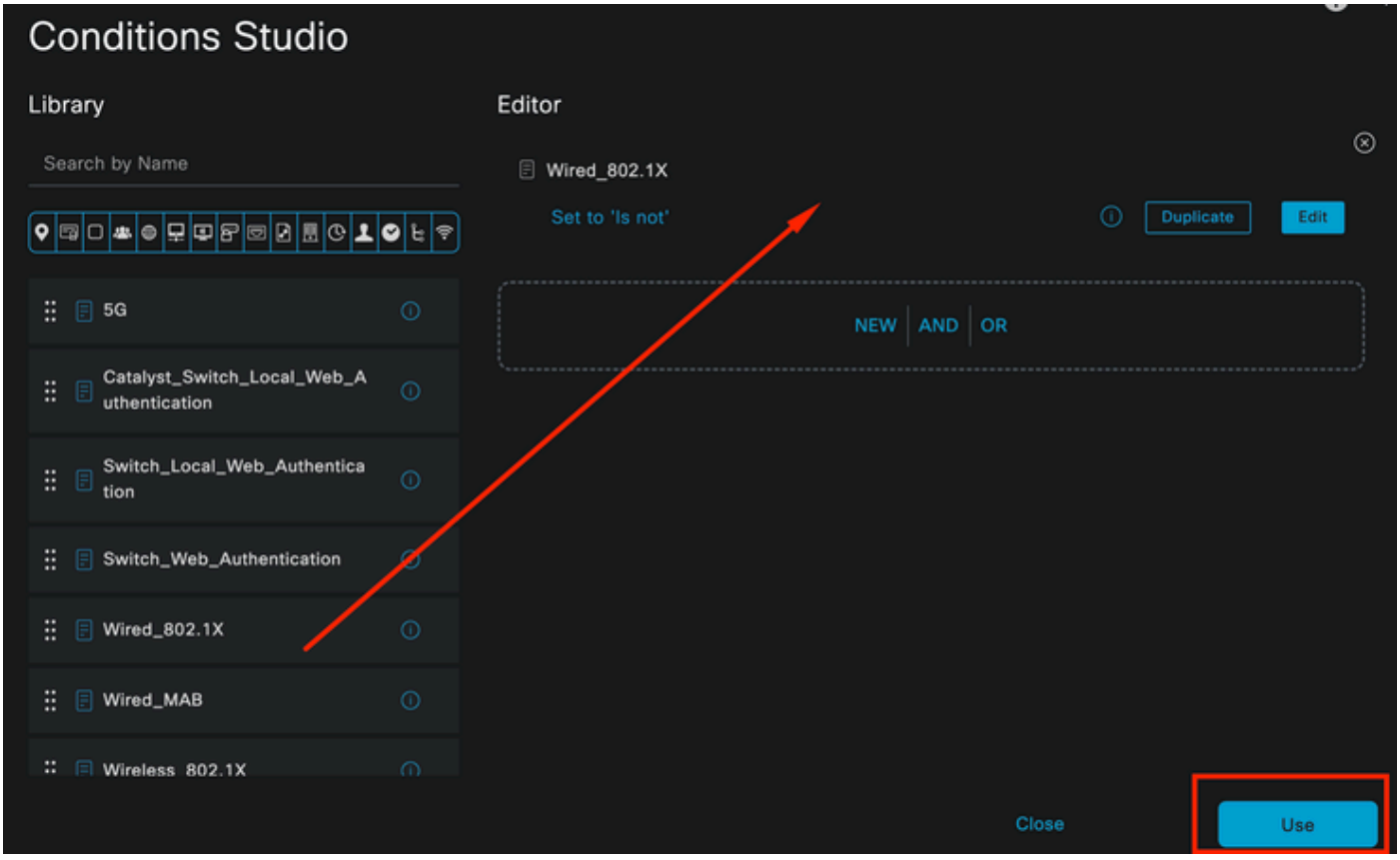
Se puede utilizar el conjunto de políticas predeterminado. Sin embargo, en este ejemplo se crea un conjunto de directivas denominado Wired. La clasificación y diferenciación de los conjuntos de políticas ayuda a solucionar problemas,

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



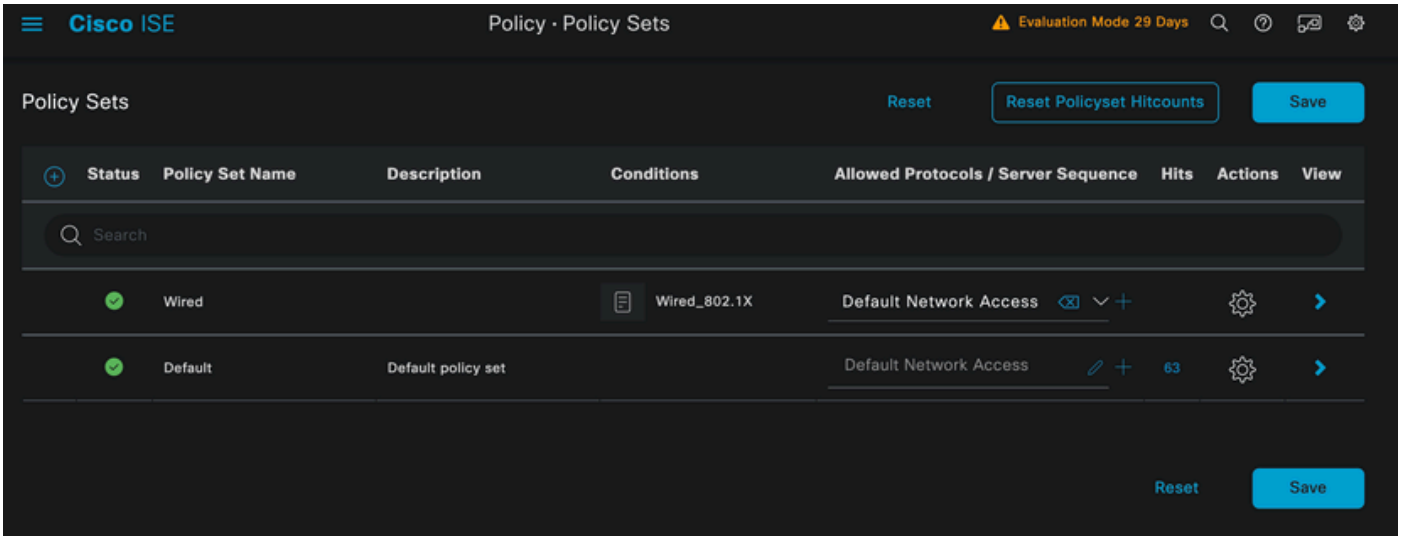
Creación de políticas

La condición configurada en este ejemplo es Wired 8021x, que es una condición preconfigurada en implementaciones nuevas de ISE. Arrástrelo y, a continuación, haga clic en Usar.



Estudio de condiciones

Por último, seleccione Default Network Access preconfigured allowed protocols service.

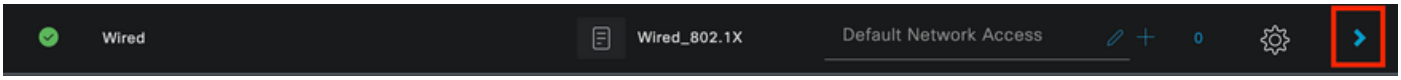


Vista Conjunto de políticas

Click Save.

2. d. Configure las Políticas de Autenticación y Autorización.

Haga clic en la flecha situada en el lado derecho del conjunto de directivas que se acaba de crear.



Conjunto de políticas por cable

Expandir la directiva de autenticación

Haga clic en el icono +.

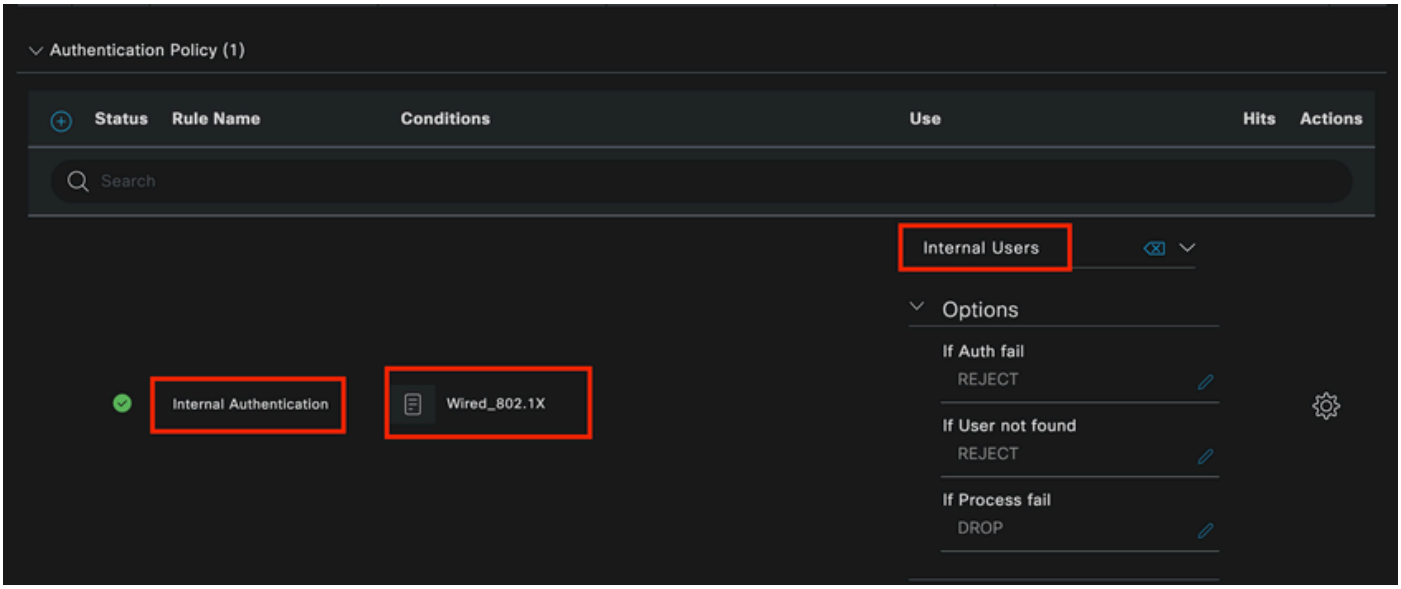
Agregar política de autenticación

Asigne un nombre a la política de autenticación; para este ejemplo, se utiliza Internal Authentication.

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

Se puede utilizar la condición preconfigurada Wired Dot1x ISE incluida.

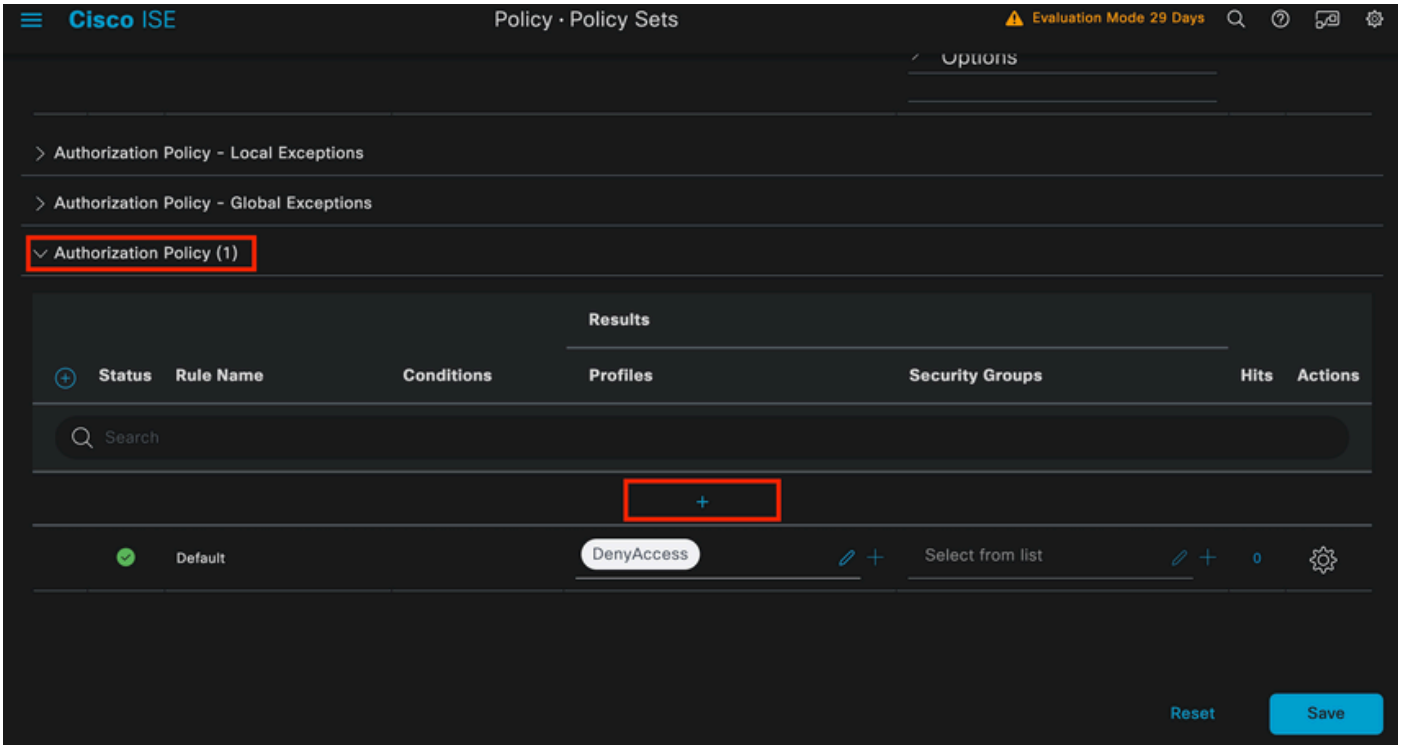
Por último, en la columna Use, seleccione Internal Users (Usuarios internos) en la lista desplegable.



Política de autenticación

Política 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

Dé un nombre a la política de autorización que acaba de agregar; en este ejemplo de configuración, se utiliza el nombre Internal ISE Users.

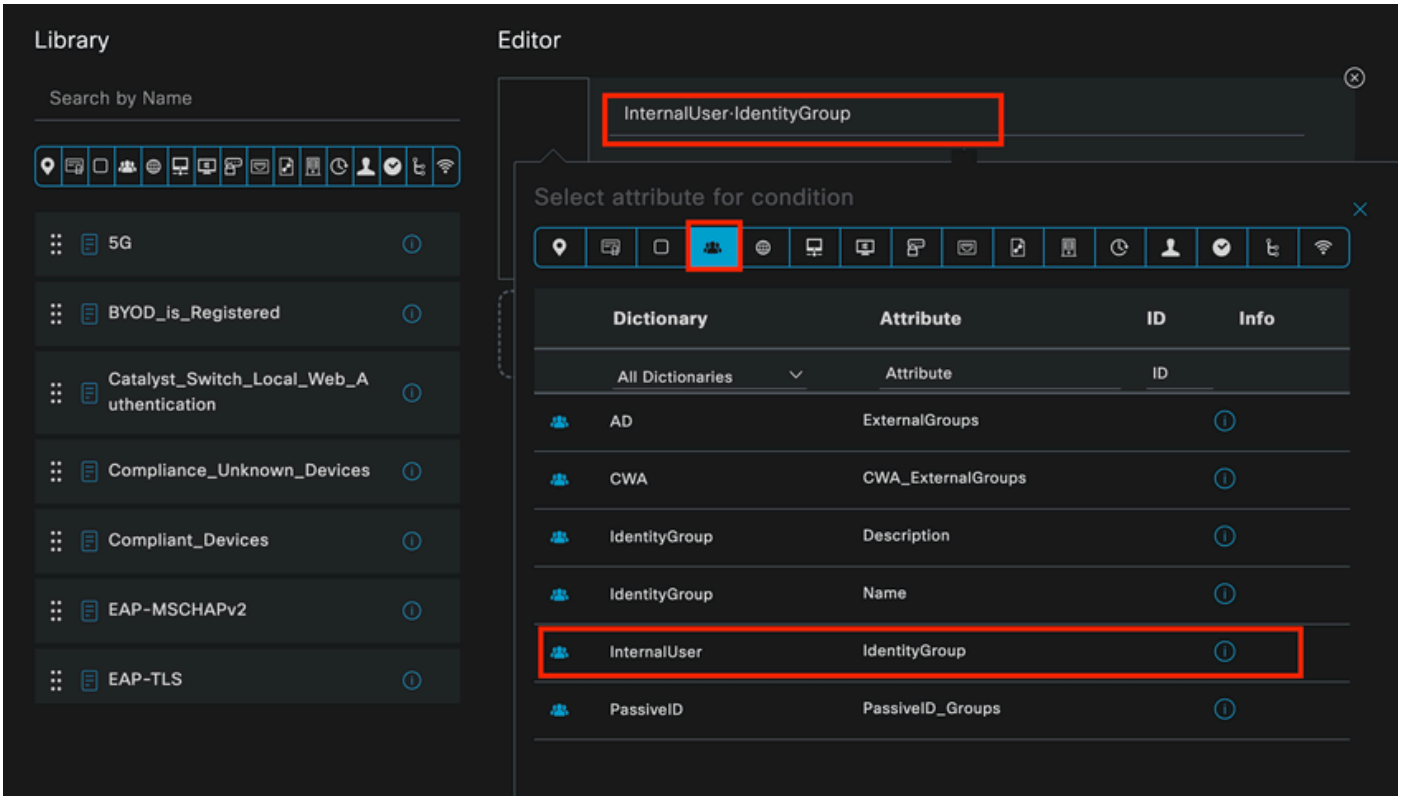
Para crear una condición para esta directiva de autorización, haga clic en el icono + de la columna Condiciones.

El usuario creado anteriormente forma parte del grupo IseUsers.

Una vez en el editor, haga clic en la sección Click to add an attribute.

Seleccione el icono Grupo de identidades.

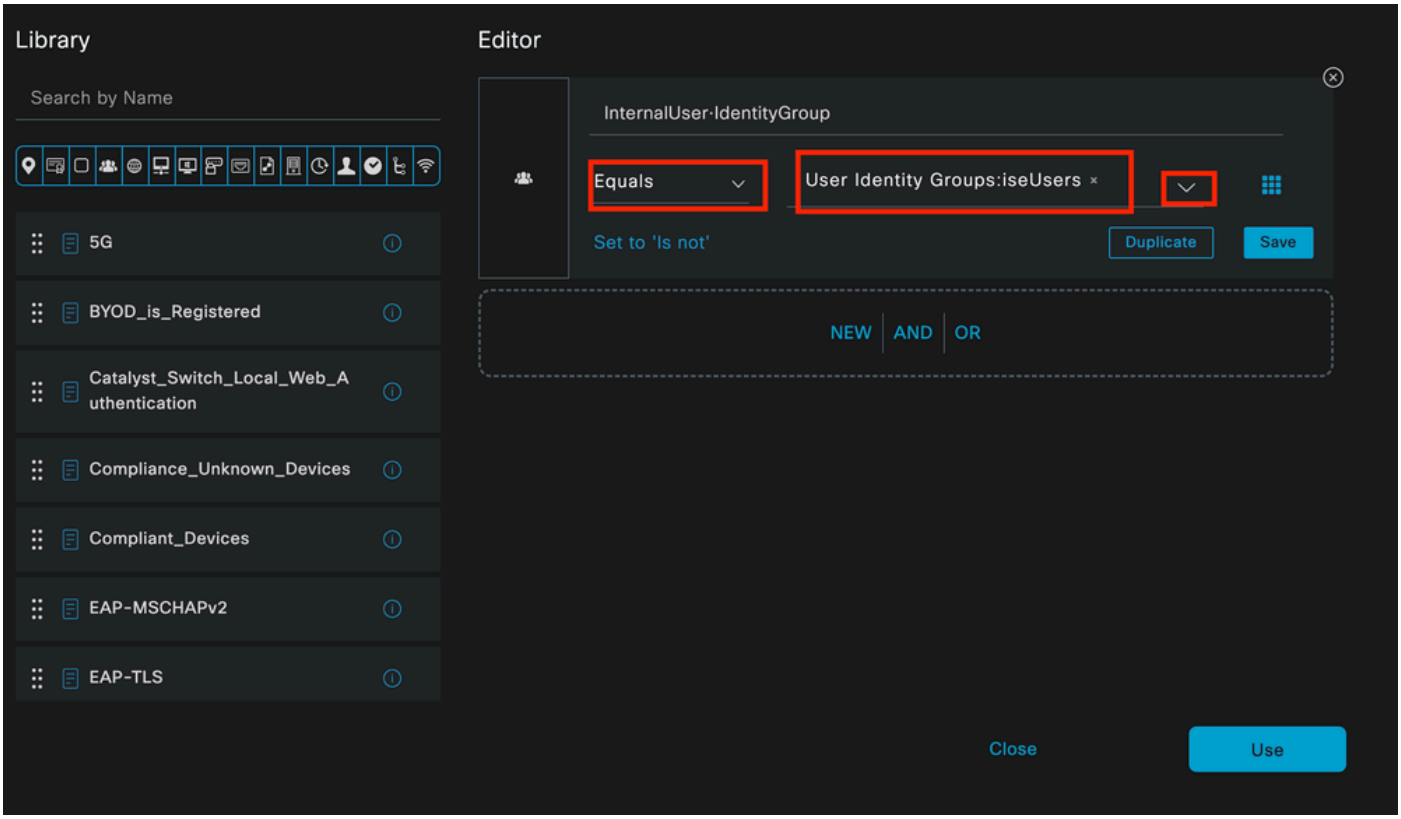
En el diccionario, seleccione el diccionario InternalUser que viene con el atributo Identity Group.



Condition Studio para la directiva de autorización

Seleccione el operador Equals.

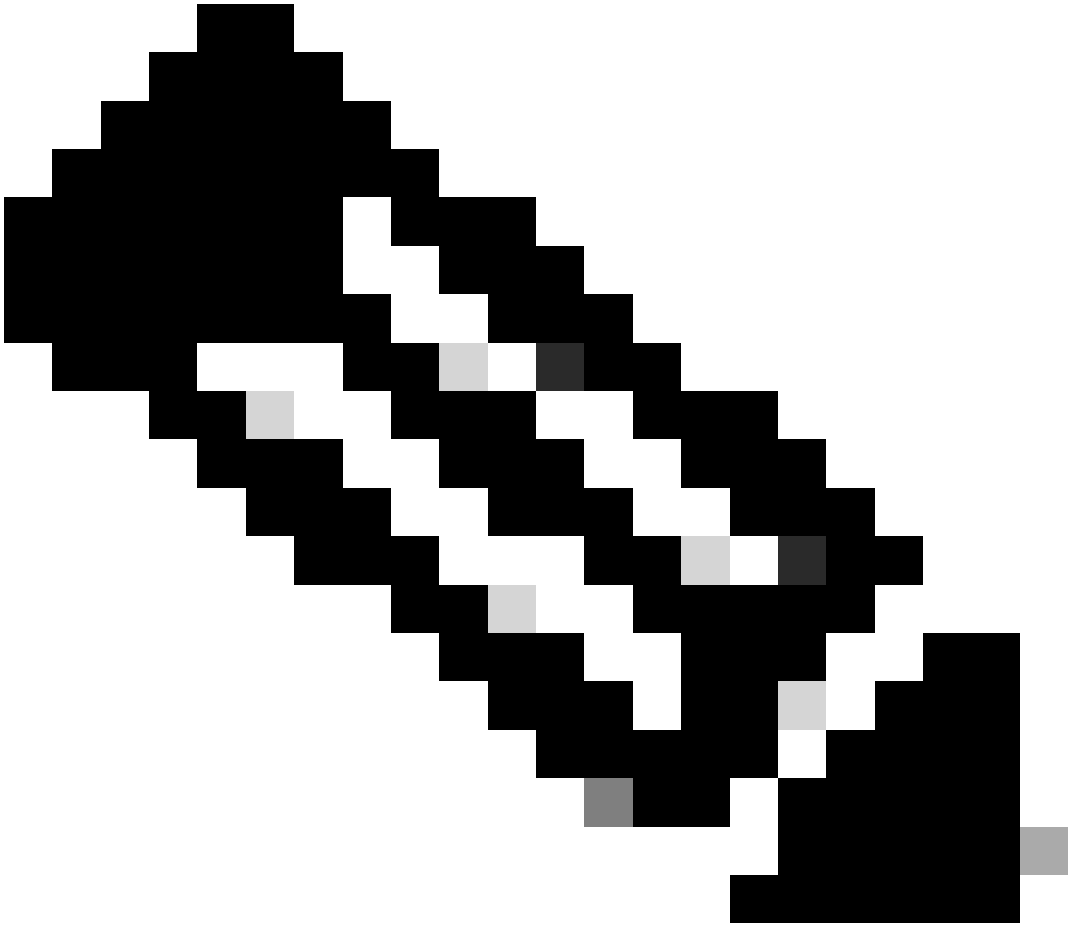
En la lista desplegable Grupos de identidad de usuario, seleccione el grupo IseUsers.



Condición para directiva de autorización finalizada

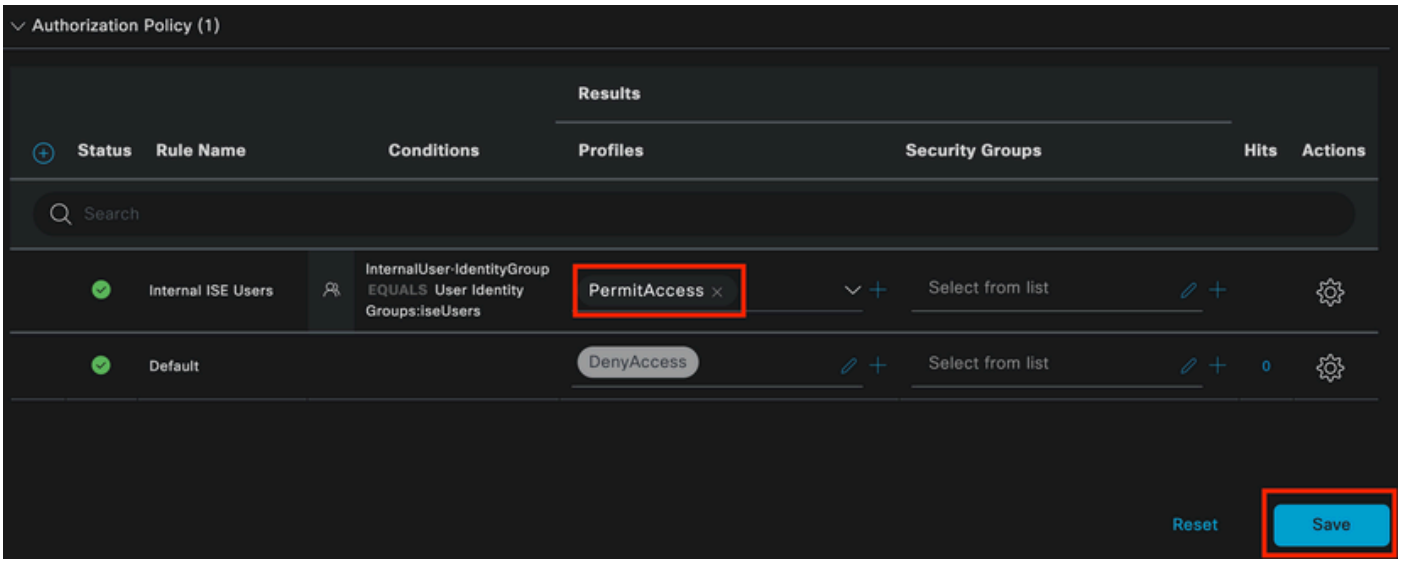
Haga clic en Usar.

Por último, seleccione el perfil de autorización de resultados que recibe la parte de autenticaciones de este grupo de identidades.



Nota: Observe que las autenticaciones que llegan a ISE y que están llegando a este conjunto de políticas Wired Dot1x que no forman parte de los usuarios ISEU del grupo de identidad de usuarios, ahora llegan a la política de autorización predeterminada. Esto tiene el resultado del perfil DenyAccess.

ISE está preconfigurado con el perfil Permit Access. Selecciónela.



Política de autorización finalizada

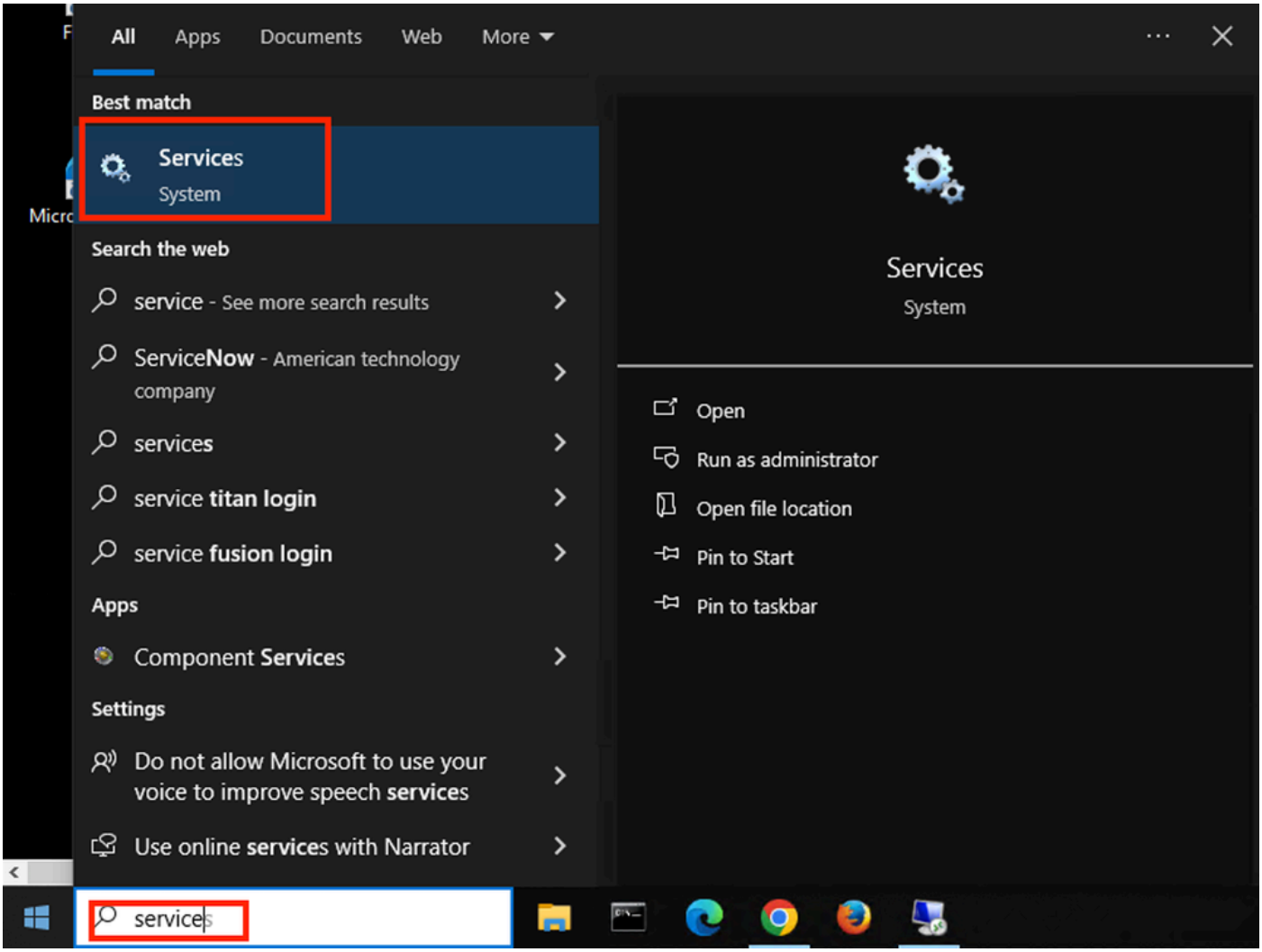
Click Save.

La configuración de ISE ha finalizado.

Paso 3. Configuración del suplicante nativo de Windows

3. a. Habilitar dot1x cableado en Windows.

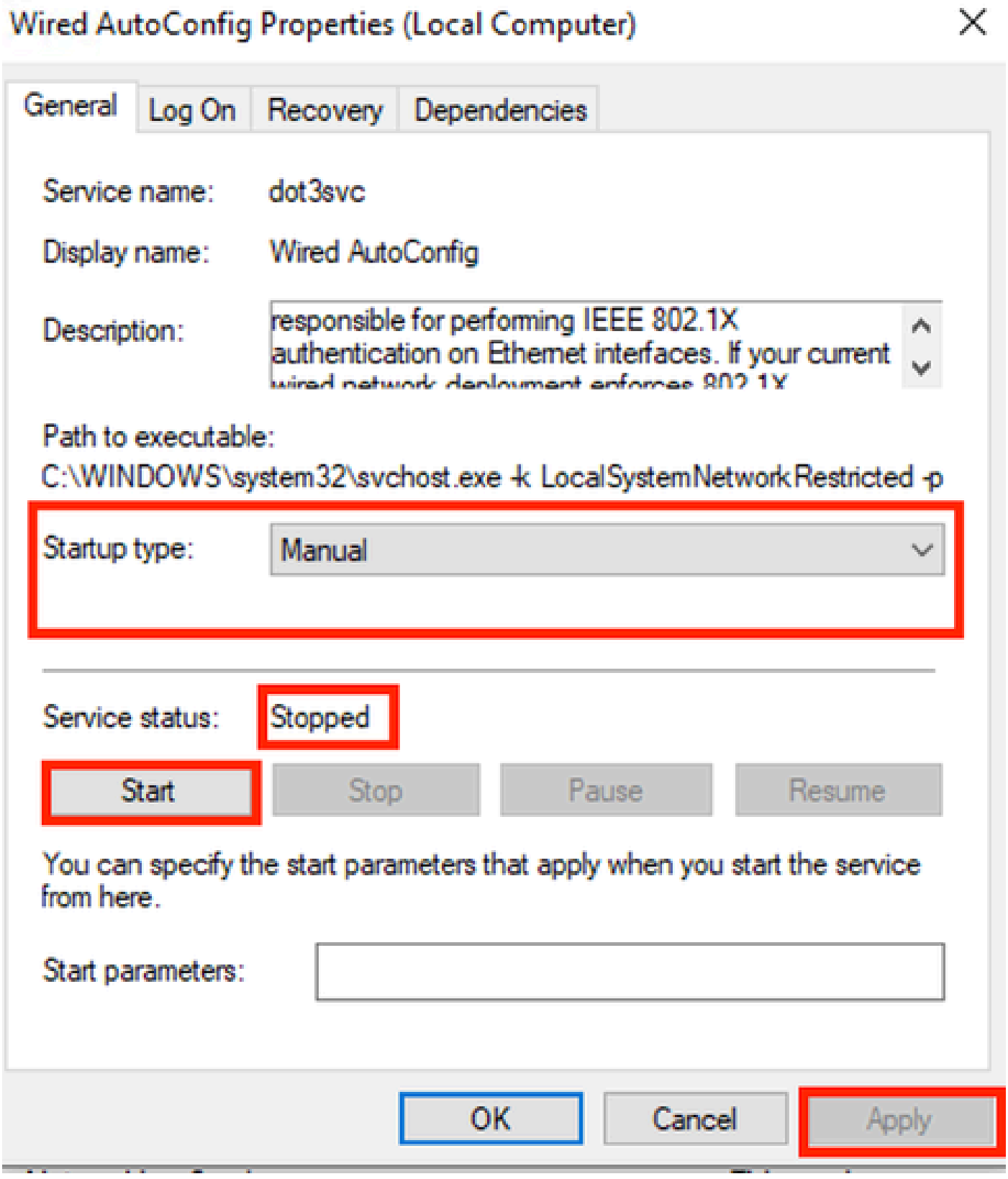
En la barra de búsqueda de Windows, abra Servicios.



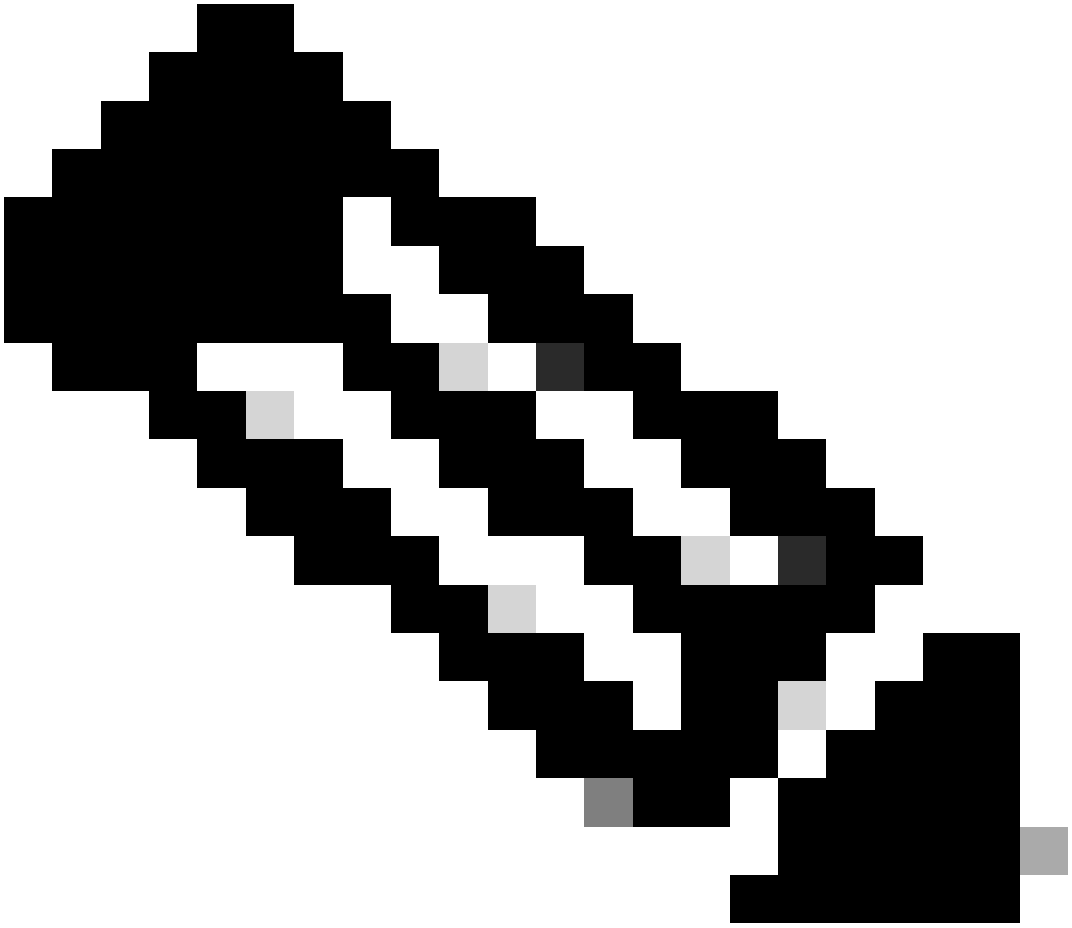
Barra de búsqueda de Windows

En la parte inferior de la lista Services (Servicios), localice Wired Autoconfig.

Haga clic con el botón derecho en Wired AutoConfig y seleccione Properties.



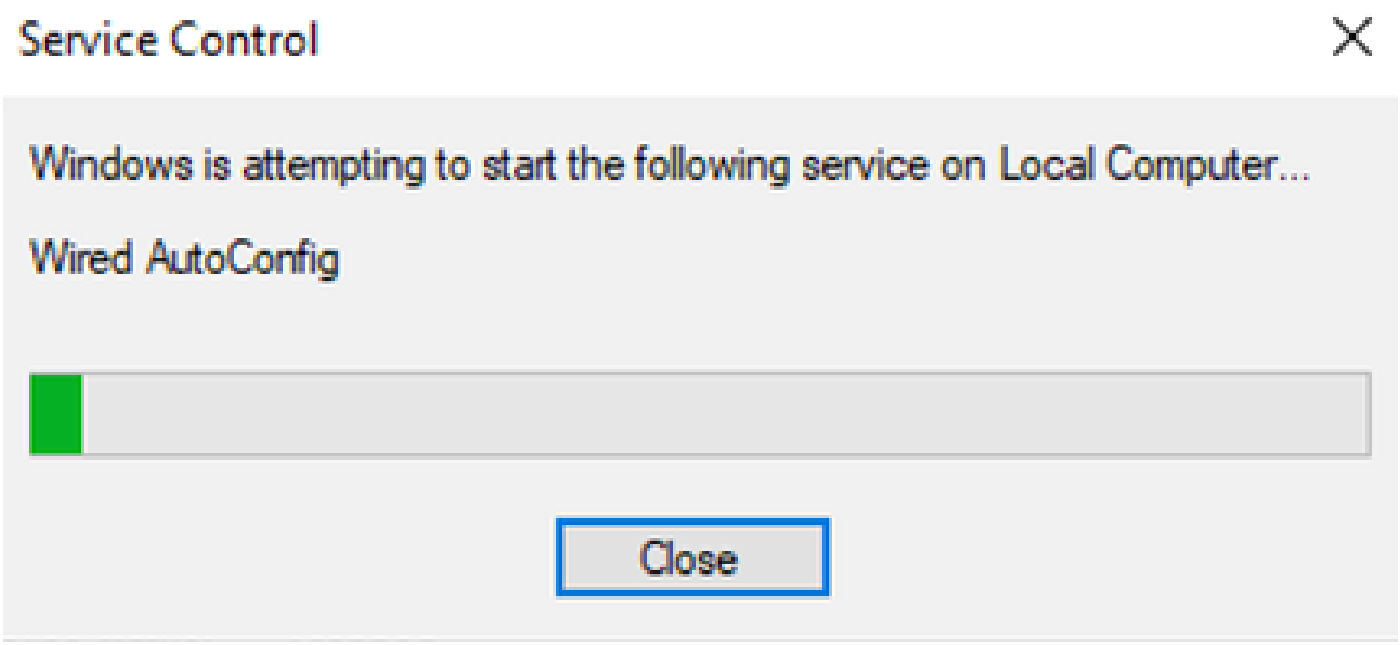
Ventana Propiedades



Nota: el servicio de configuración automática por cable (DOT3SVC) es responsable de realizar la autenticación IEEE 802.1X en las interfaces Ethernet.

Se selecciona el tipo de inicio Manual.

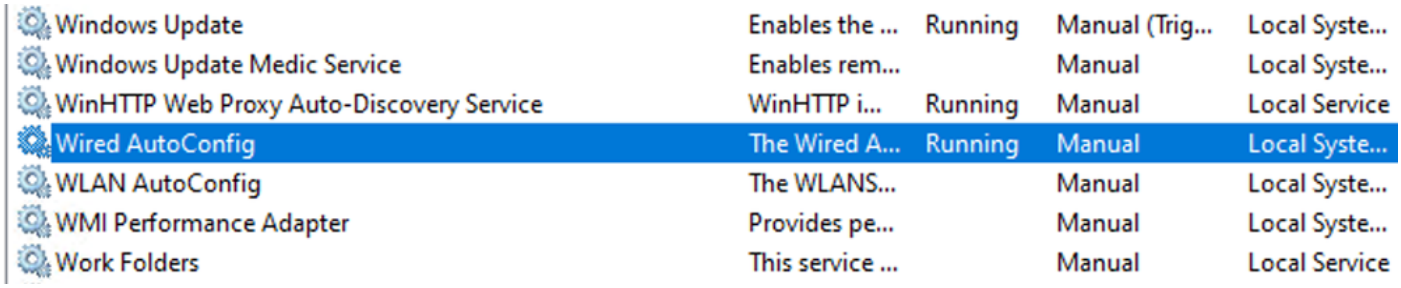
Dado que el estado del servicio es Detenido. Haga clic en Start (Inicio).



Control de servicios

A continuación, haga clic en Aceptar.

El servicio se está ejecutando después de esto.



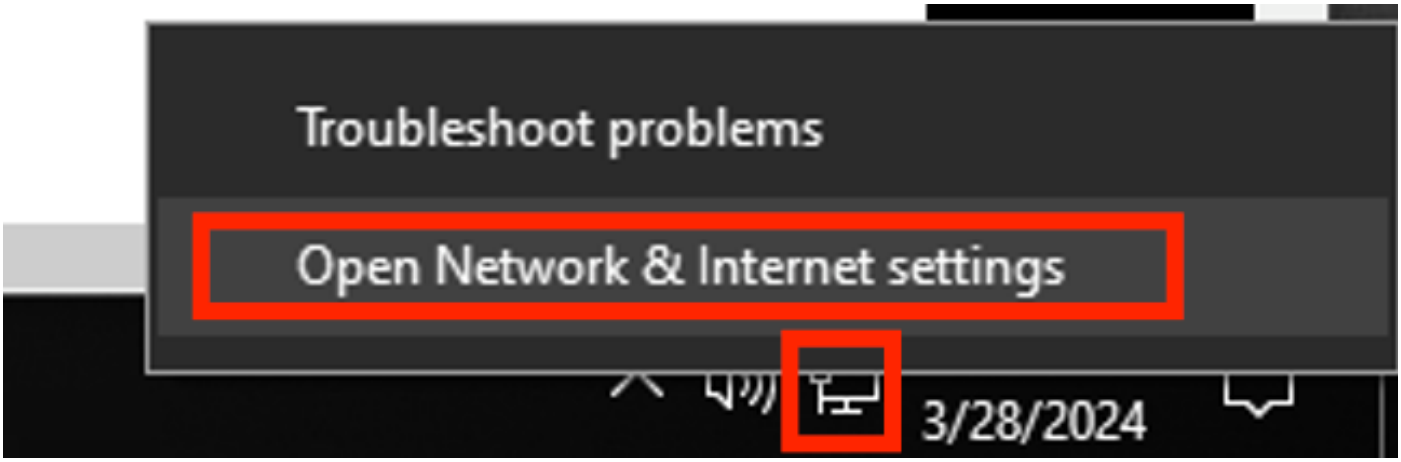
Servicio de configuración automática por cable

3. b. Configure la interfaz de portátil Windows conectada al autenticador NAD (ISR 1100).

En la barra de tareas, localice la esquina derecha y, a continuación, utilice el icono del equipo.

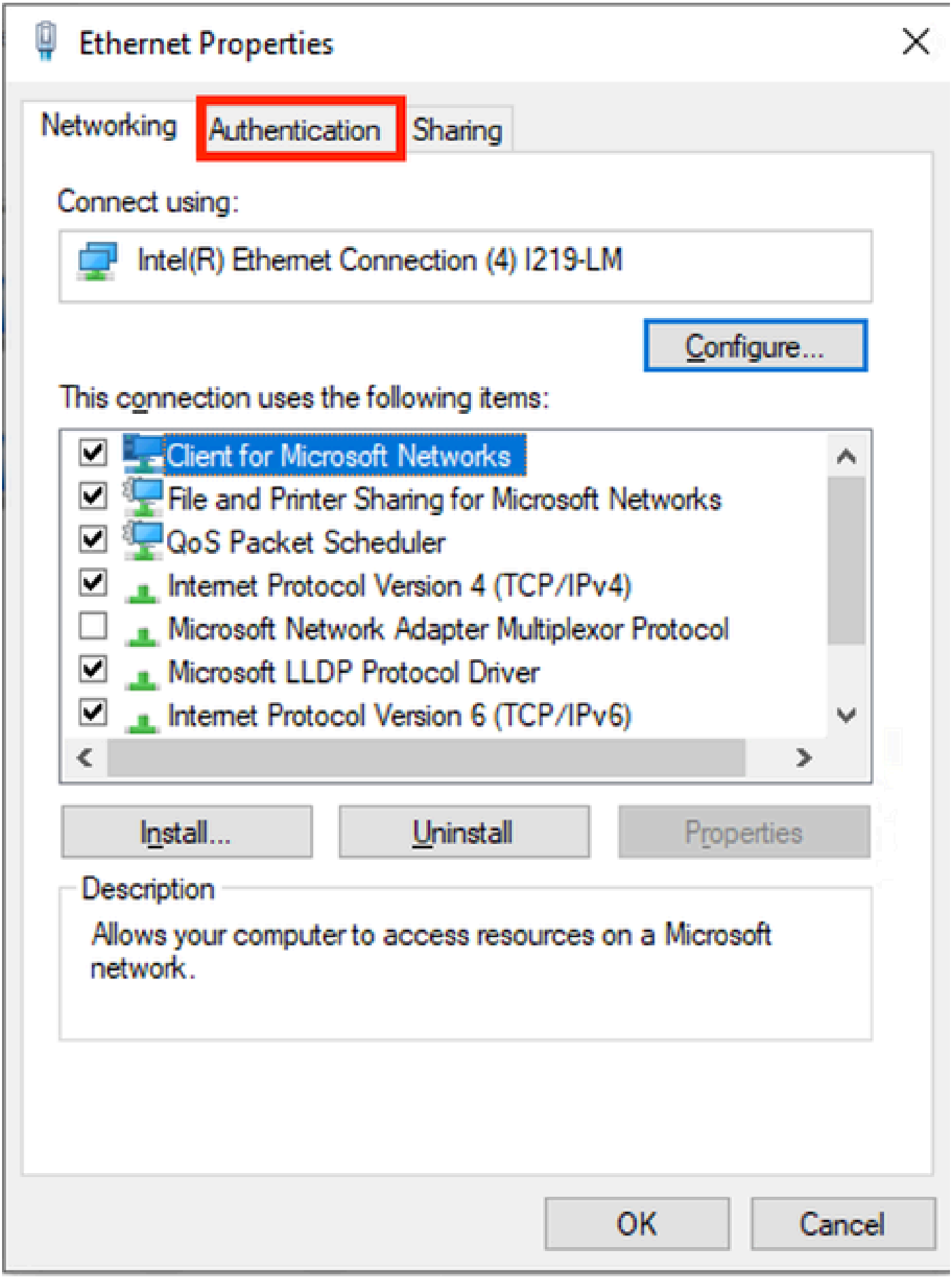
Haga doble clic en el icono del ordenador.

Seleccione Abra la configuración de red e Internet.



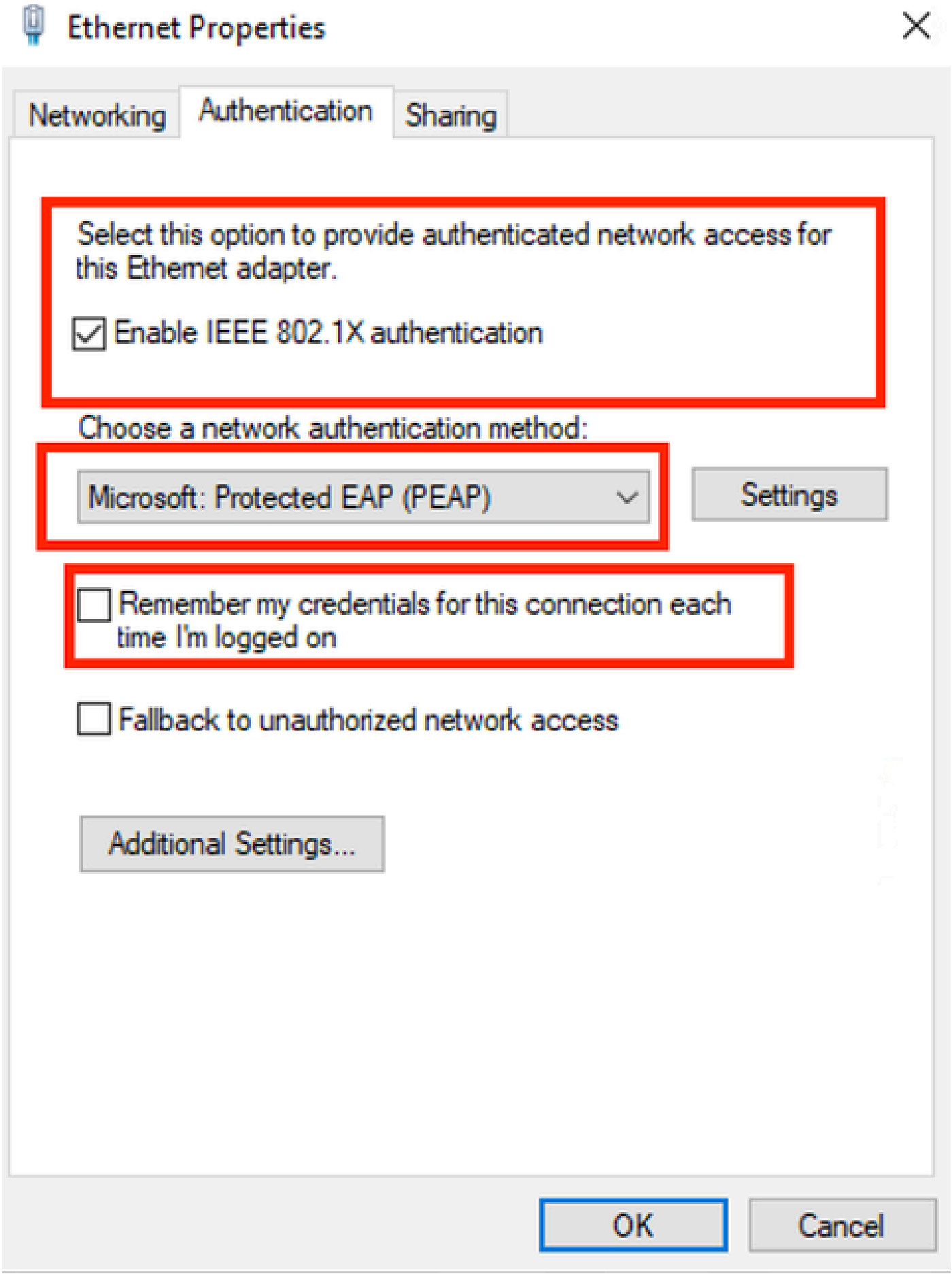
Una vez abierta la ventana Network Connections, haga clic con el botón derecho del ratón en la interfaz Ethernet que está conectada al ISR Gig 0/1/0. Haga clic en la opción Properties.

Haga clic en la pestaña Authentication.



Propiedades de Ethernet de interfaz

Seleccione la casilla de verificación Enable IEEE 802.1X authentication.

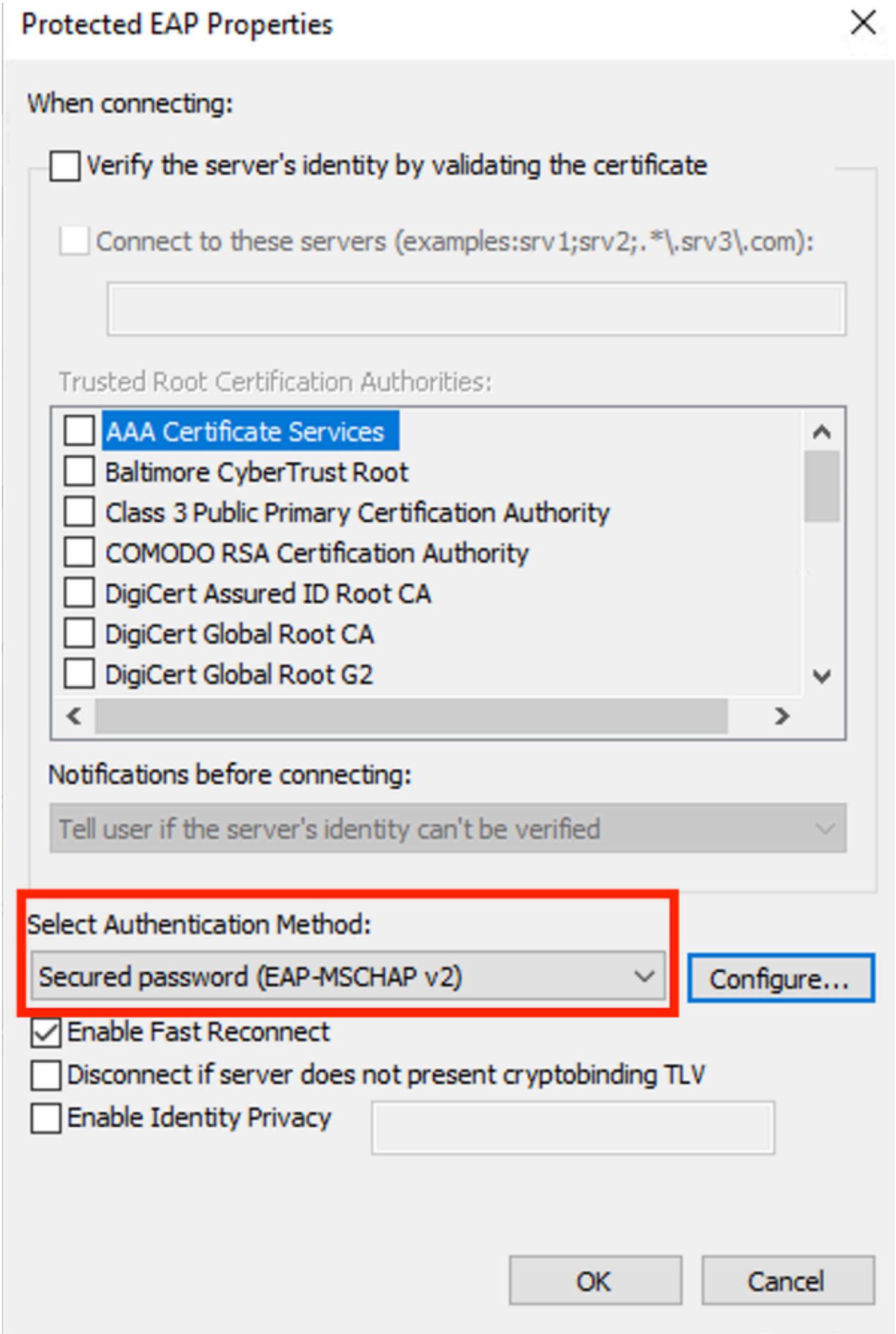


Propiedades Ethernet de autenticación

Seleccione EAP protegido (PEAP).

Desactive la opción Recordar mis credenciales para esta conexión cada vez que inicie sesión.

Haga clic en Configuración.



Propiedades de PEAP

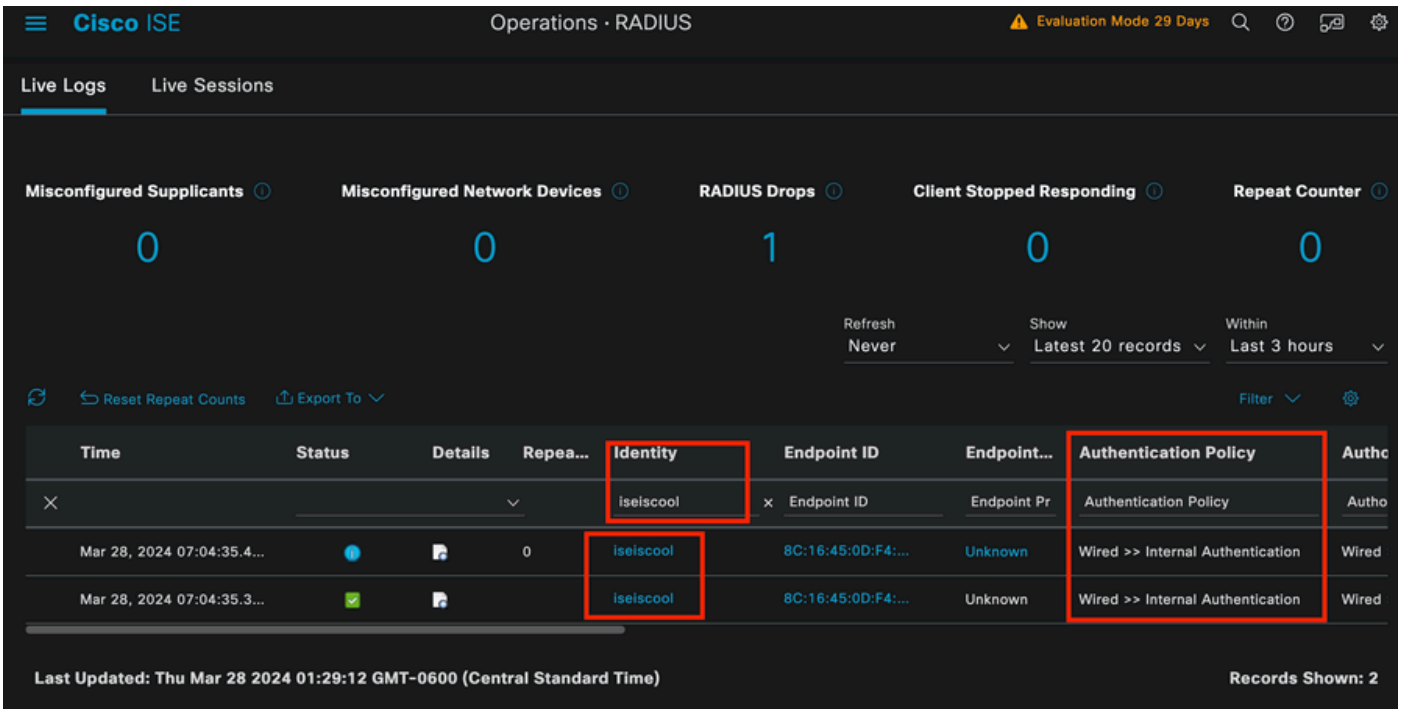
```
            Interface:  GigabitEthernet0/1/0
                IIF-ID:  0x08767C0D
           MAC Address:  8c16.450d.f42b
          IPv6 Address:  Unknown
          IPv4 Address:  Unknown
             User-Name:  iseiscool <--------- The username configured for Windows Native Supplicant
                Status:  Authorized <--------- An indication that this session was authorized by the PSN
                Domain:  DATA
        Oper host mode:  multi-auth
      Oper control dir:  both
       Session timeout:  N/A
     Common Session ID:  22781F0A0000000C83E28461
       Acct Session ID:  0x00000003
                Handle:  0xc6000002
        Current Policy:  POLICY_Gi0/1/0

Local Policies:
         Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
       Security Policy:  Should Secure

Server Policies:


Method status list:
       Method           State
         dot1x          Authc Success <--------- An indication that dot1x is used for this authenticati
```

```
Router#
```

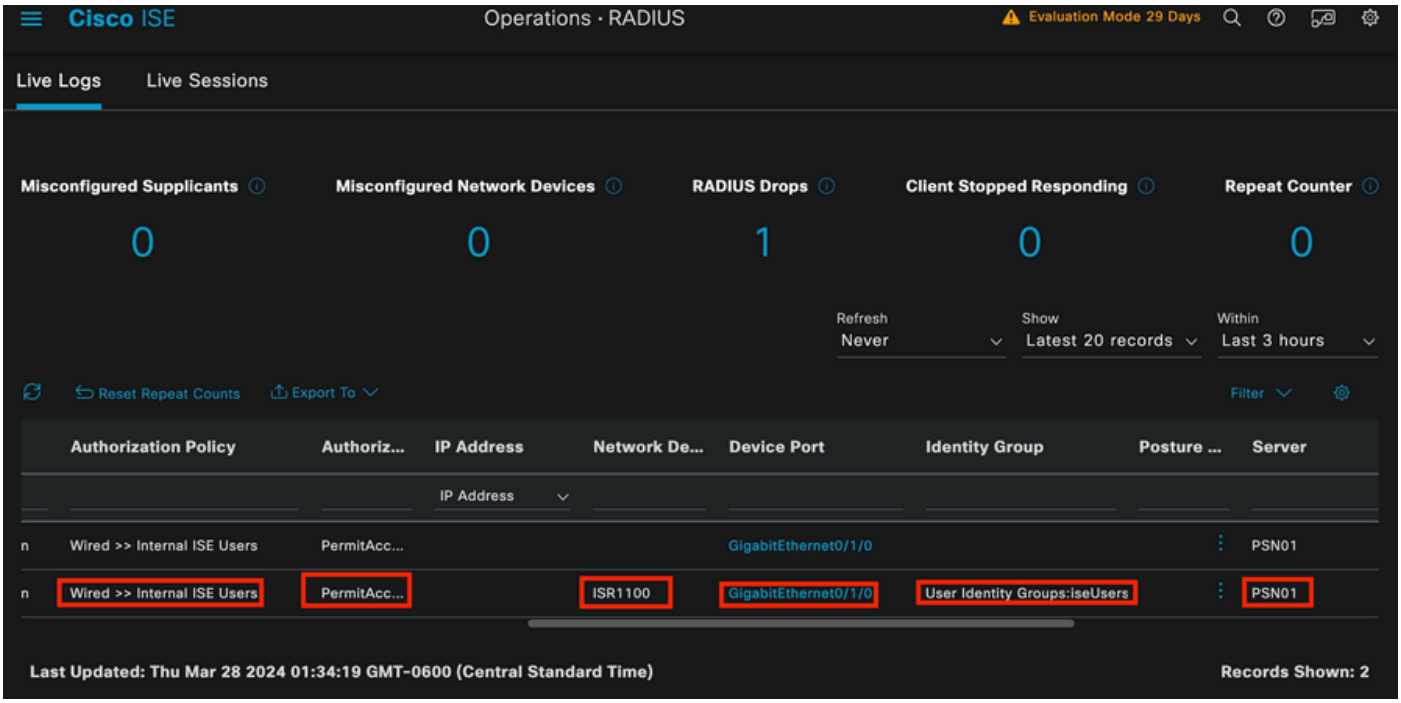
Registros de ISE

Vaya a Operaciones > Radio > Registros en directo.

Filtre por la identidad del nombre de usuario, en este ejemplo se utiliza el nombre de usuario iseiscool.



Livelogs de ISE



Livelogs de ISE

Observe que desde esta vista rápida, los registros activos proporcionan información clave:

- Marca de tiempo de la autenticación.
- Identidad utilizada.
- Dirección MAC del terminal.
- Conjunto de políticas y política de autenticación que se ha alcanzado.
- Conjunto de directivas y directiva de autorización que se ha alcanzado.
- Resultado del perfil de autorización.
- El dispositivo de red que envía la solicitud Radius a ISE.
- La interfaz a la que está conectado el punto final.
- El grupo de identidad del usuario que se autenticó.
- El nodo del servidor de políticas (PSN) que gestionó la autenticación.

Troubleshoot

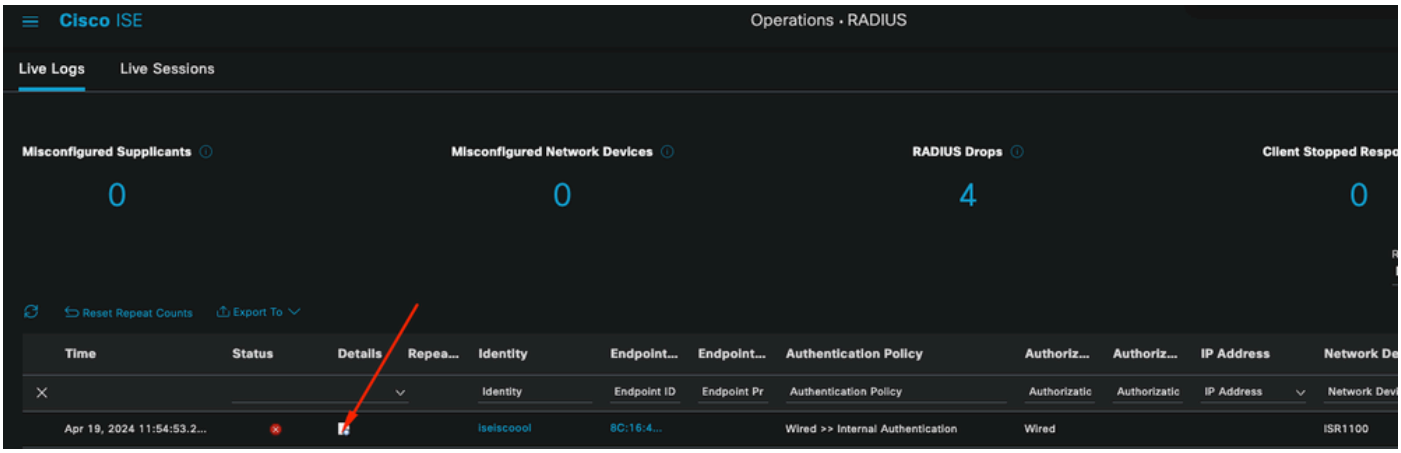
1 - Lectura de los detalles de ISE Live Log

Navegue hasta Operaciones > Radio > Registros en vivo, filtre por estado de autenticación: Error O por el nombre de usuario utilizado O por la dirección MAC O por el dispositivo de acceso a la red utilizado.

Acceda a Operations > Radius > Live logs > Desired authentication > Live log details .

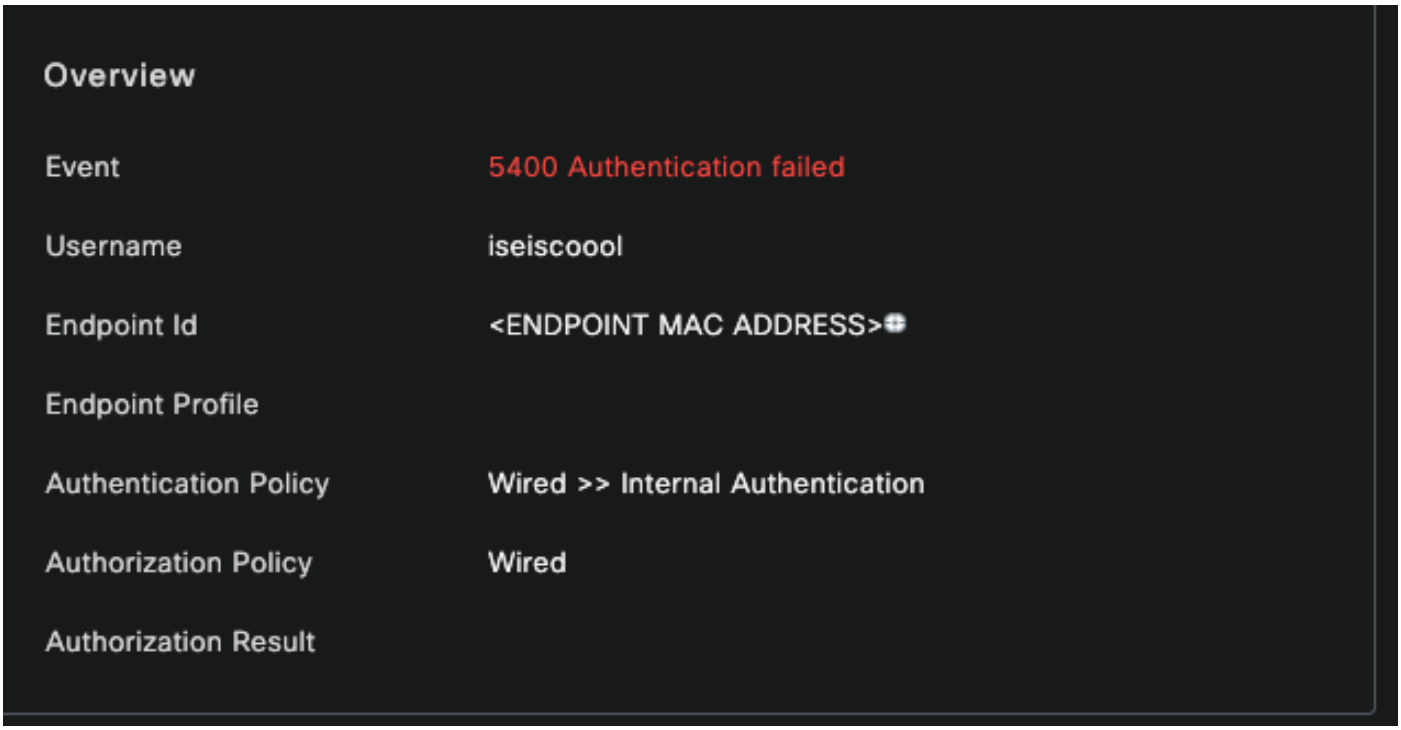
En la misma página, una vez filtrada la autenticación, haga clic en el icono Search.

Primera situación: el usuario introduce su nombre de usuario con un error tipográfico.



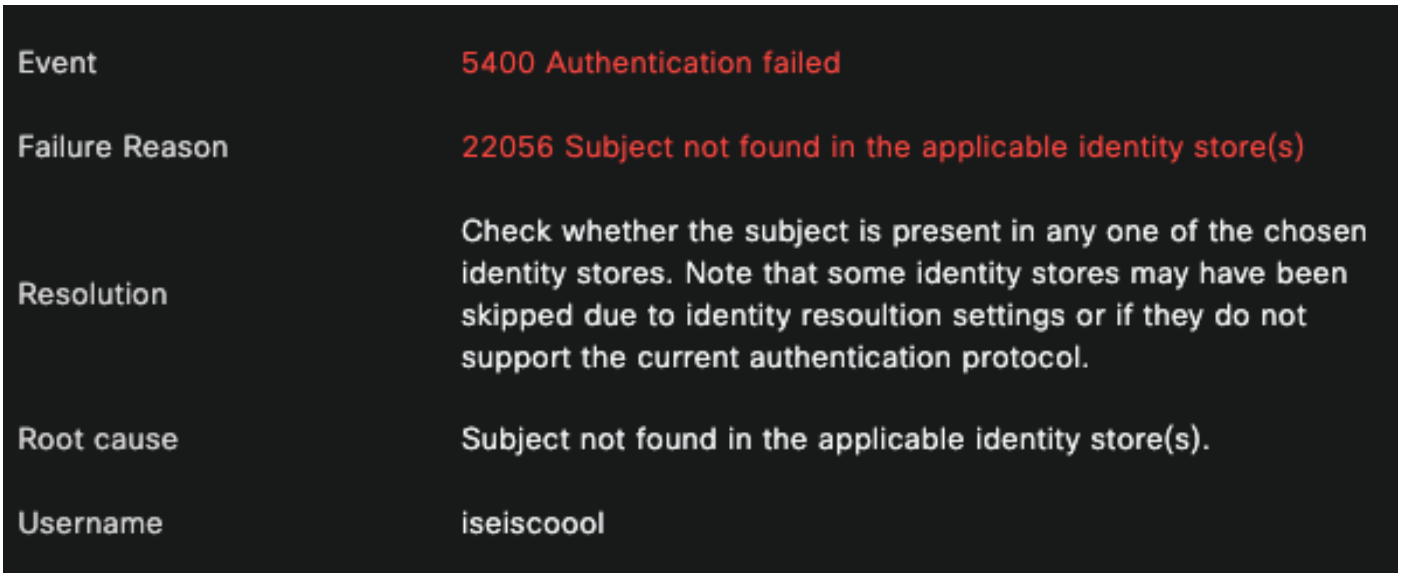
Apertura de detalles de Live Log

Una vez que se abre el detalle del registro activo, puede ver que la autenticación falló y también se muestra el nombre de usuario utilizado.



Sección Visión General

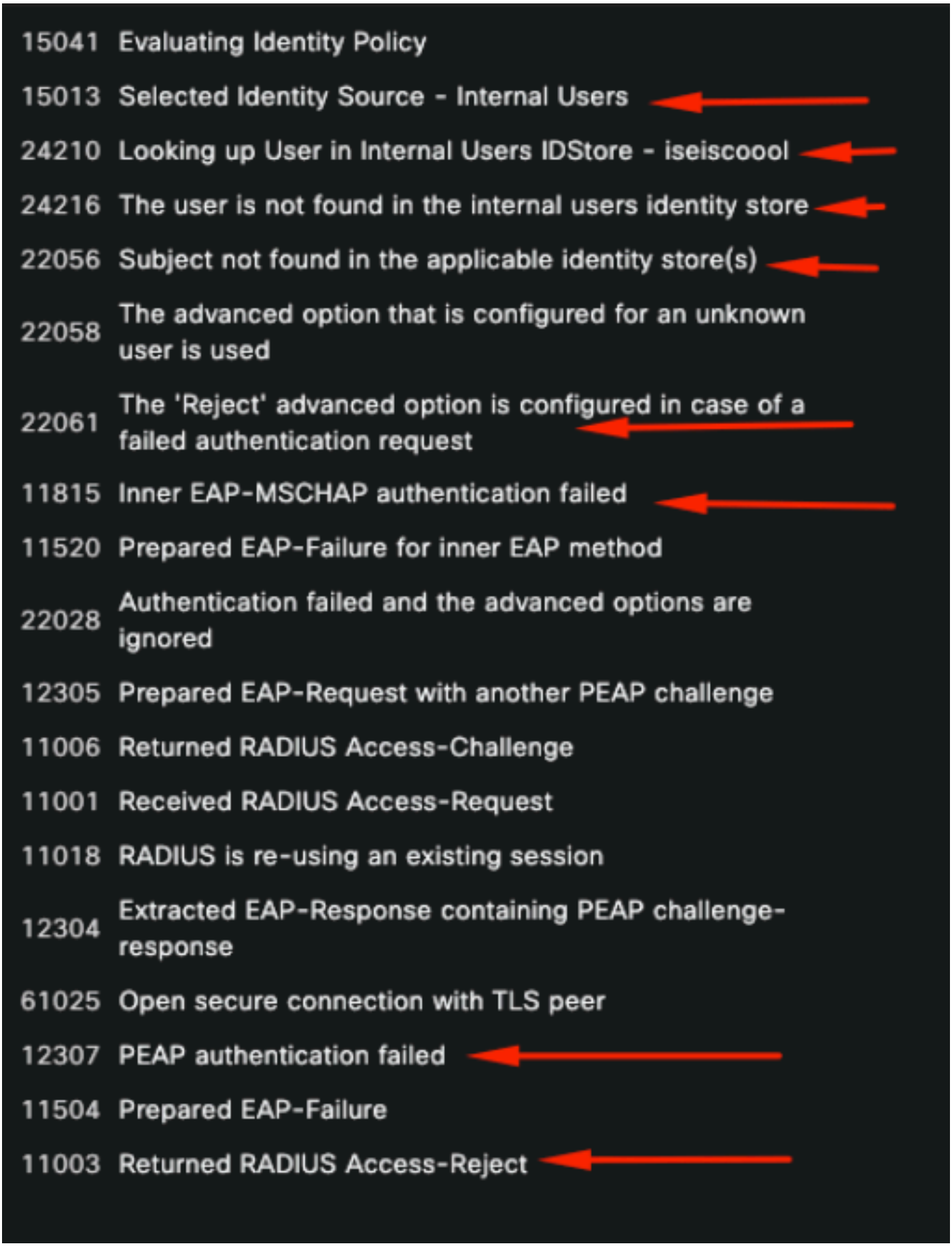
Luego, en el mismo detalle del registro activo, en la sección Detalles de autenticación, se puede encontrar el Motivo del error, la Causa raíz y la Resolución del error.



Detalles de autenticación

En esta situación, la razón por la que falla la autenticación es que el nombre de usuario tiene un error tipográfico; sin embargo, se presentaría el mismo error si el usuario no se crea en ISE o si ISE no pudo validar que el usuario existe en otros almacenes de identidad, por ejemplo, LDAP o AD.

Sección Pasos



Sección Paso de detalles de Live Log

En la sección de pasos se describe en detalle el proceso que ISE ejecutó durante la conversación

RADIUS.

Puede encontrar información aquí como:

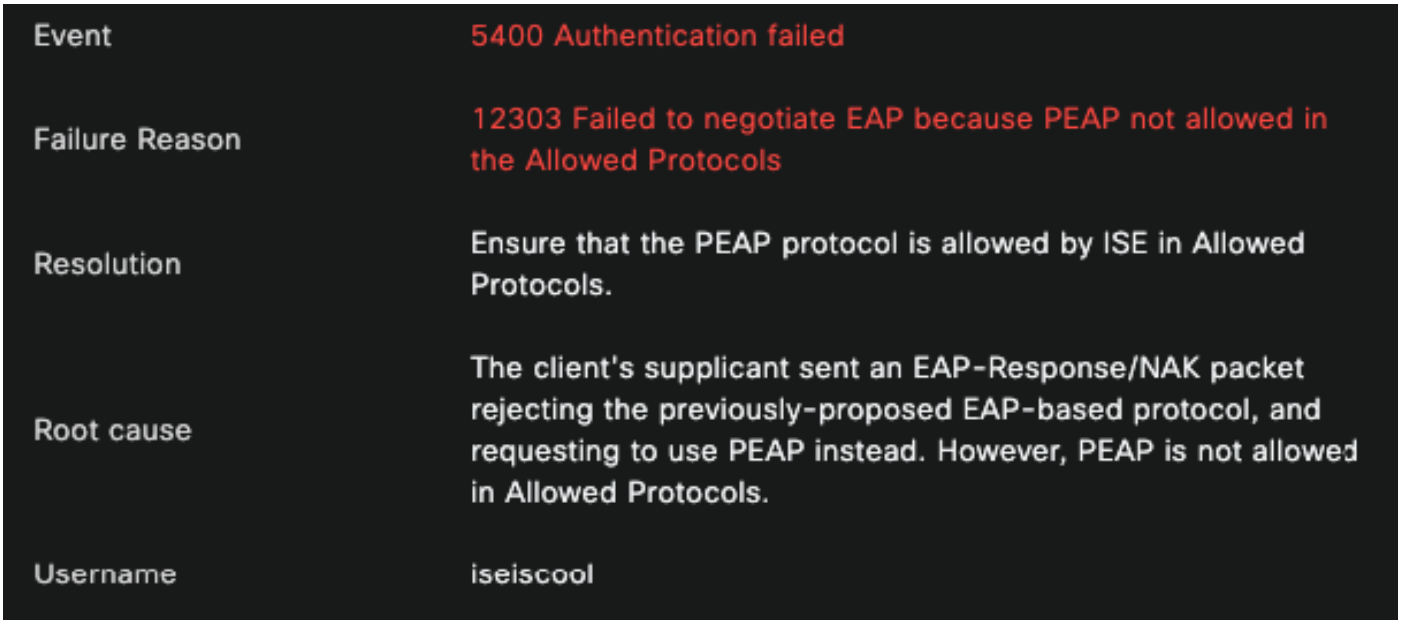
- Cómo se inició la conversación.
- Proceso de intercambio de señales SSL.
- El método EAP negociado.
- Proceso del método EAP.

En este ejemplo, se puede ver que ISE acaba de registrar las identidades internas para esta autenticación. No se encontró el usuario y, por ese motivo, ISE envió como respuesta un mensaje de rechazo de acceso.

Segundo escenario: el administrador de ISE deshabilitó PEAP de los protocolos Conjunto de políticas permitido.

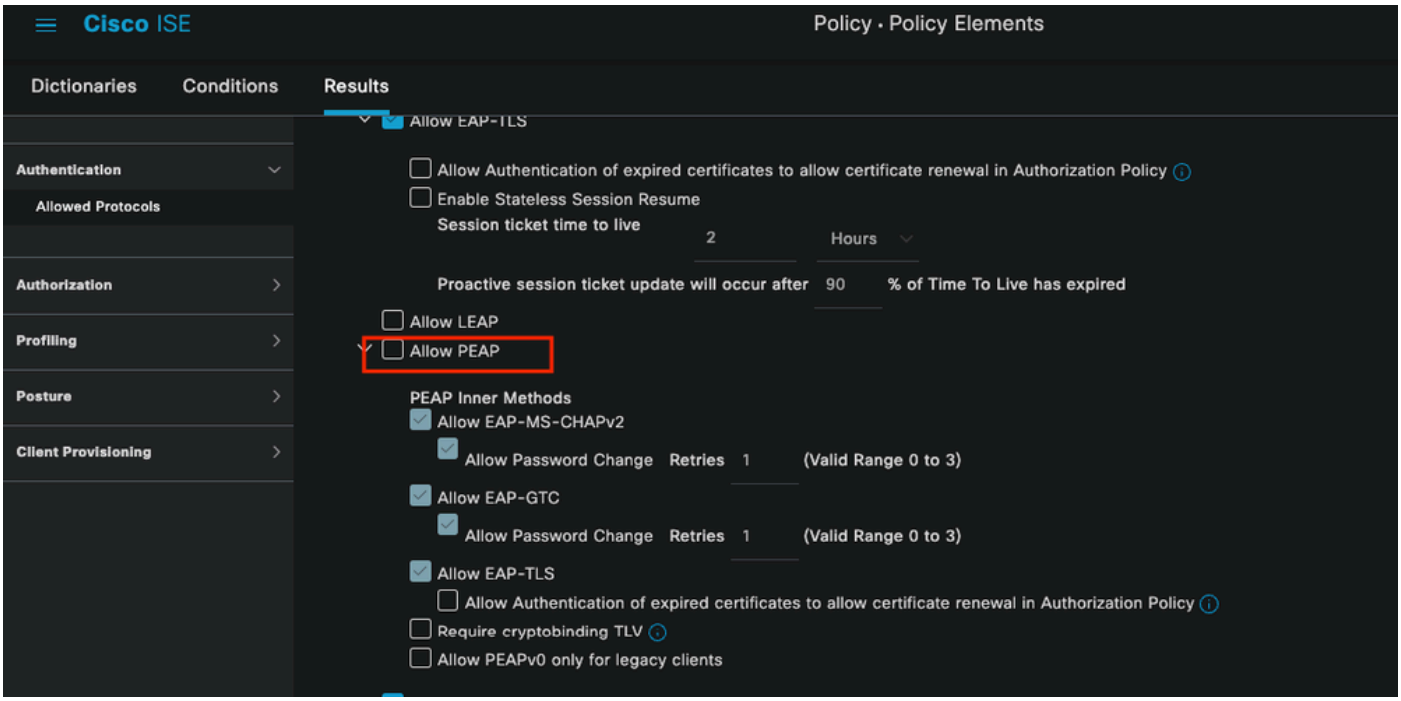
2 - PEAP desactivado

Una vez que se abre el detalle de registro activo de la falla de sesión, se muestra el mensaje de error "PEAP is not allowed in the Allowed Protocols" (PEAP no está permitido en los protocolos permitidos).



Informe detallado de Live Log

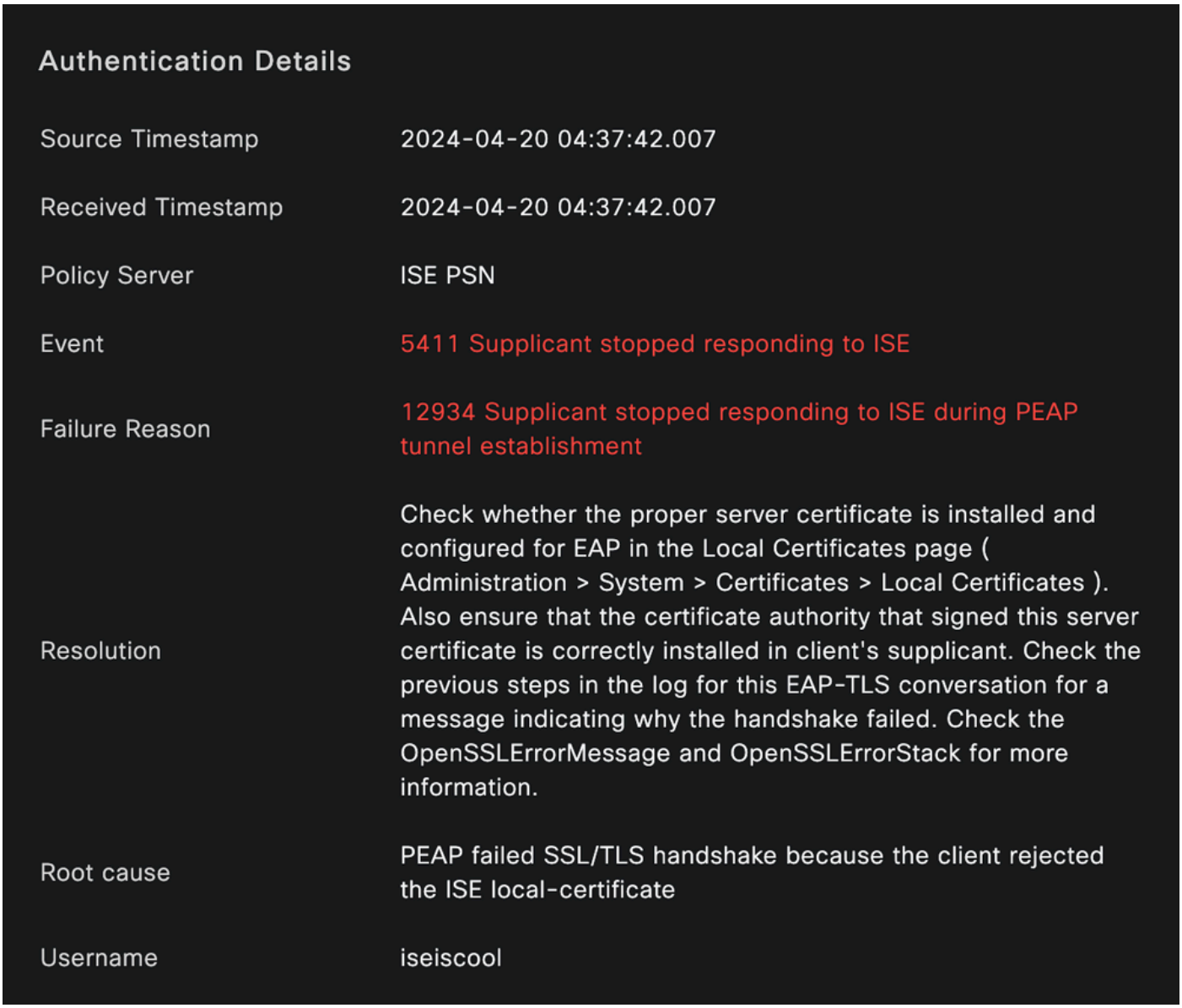
Este error es fácil de resolver, la resolución es navegar hasta Política > Elementos de política > Autenticación > Protocolos permitidos. Verifique si la opción Allow PEAP está inhabilitada.



Sección Protocolos permitidos

Tercer escenario: la autenticación falla porque el terminal no confía en el certificado de ISE.

Desplácese hasta los detalles del registro activo. Busque el registro de la autenticación que falla y compruebe los detalles del registro activo.

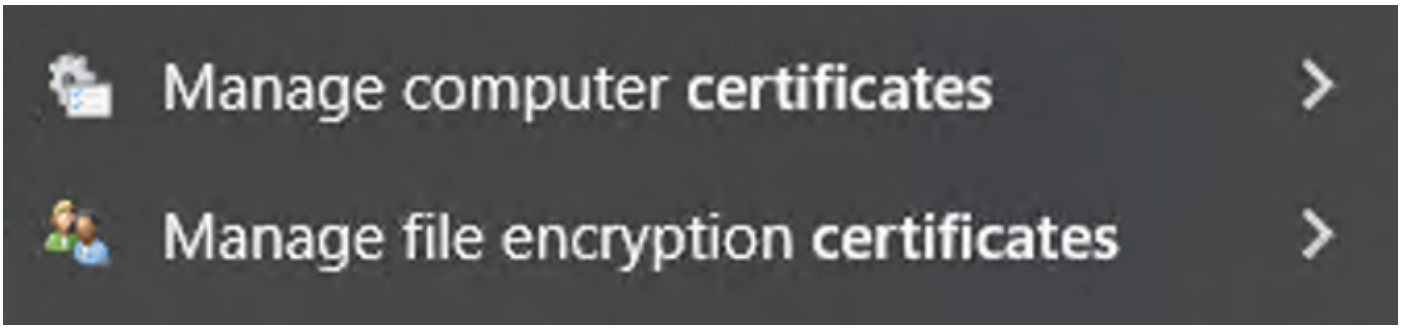


Detalles de Live Log

El punto final rechaza el certificado utilizado para el establecimiento de túnel PEAP.

Para solucionar este problema, en el extremo de Windows donde tiene el problema, compruebe que la cadena de CA que firmó el certificado ISE está en la sección de Windows Administrar certificados de usuario > Entidades de certificación raíz de confianza O Administrar certificados de equipo > Entidades de certificación raíz de confianza.

Puede acceder a esta sección de configuración en su dispositivo Windows buscando en la barra de búsqueda de Windows.

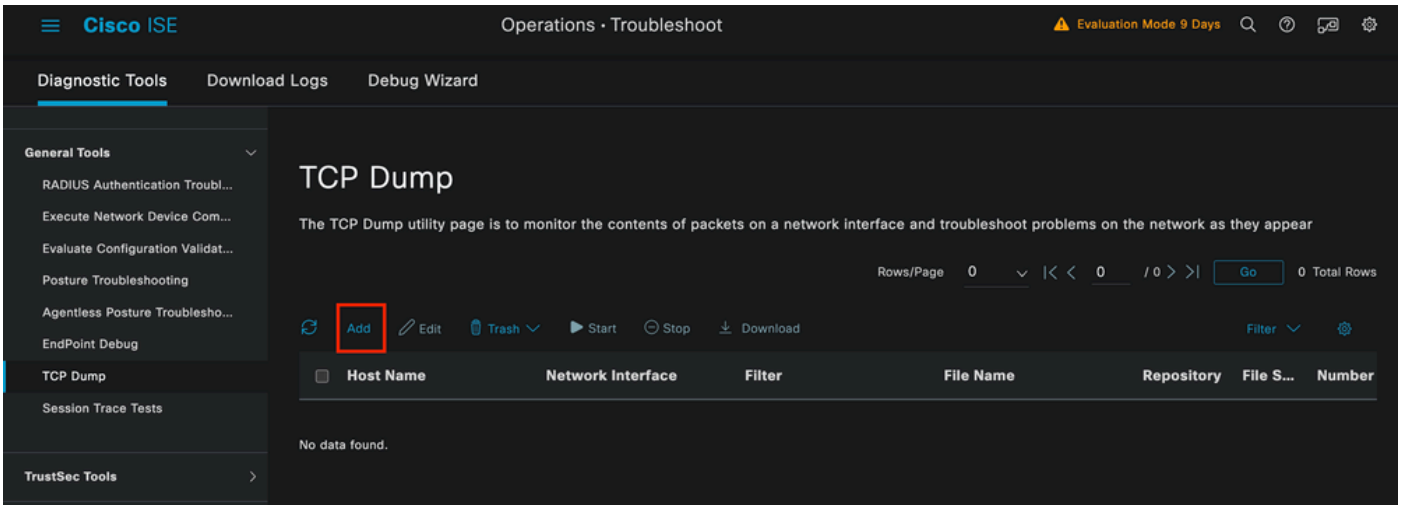


Resultados de la barra de búsqueda de Windows

3 - Herramienta de volcado de ISE TCP (captura de paquetes)

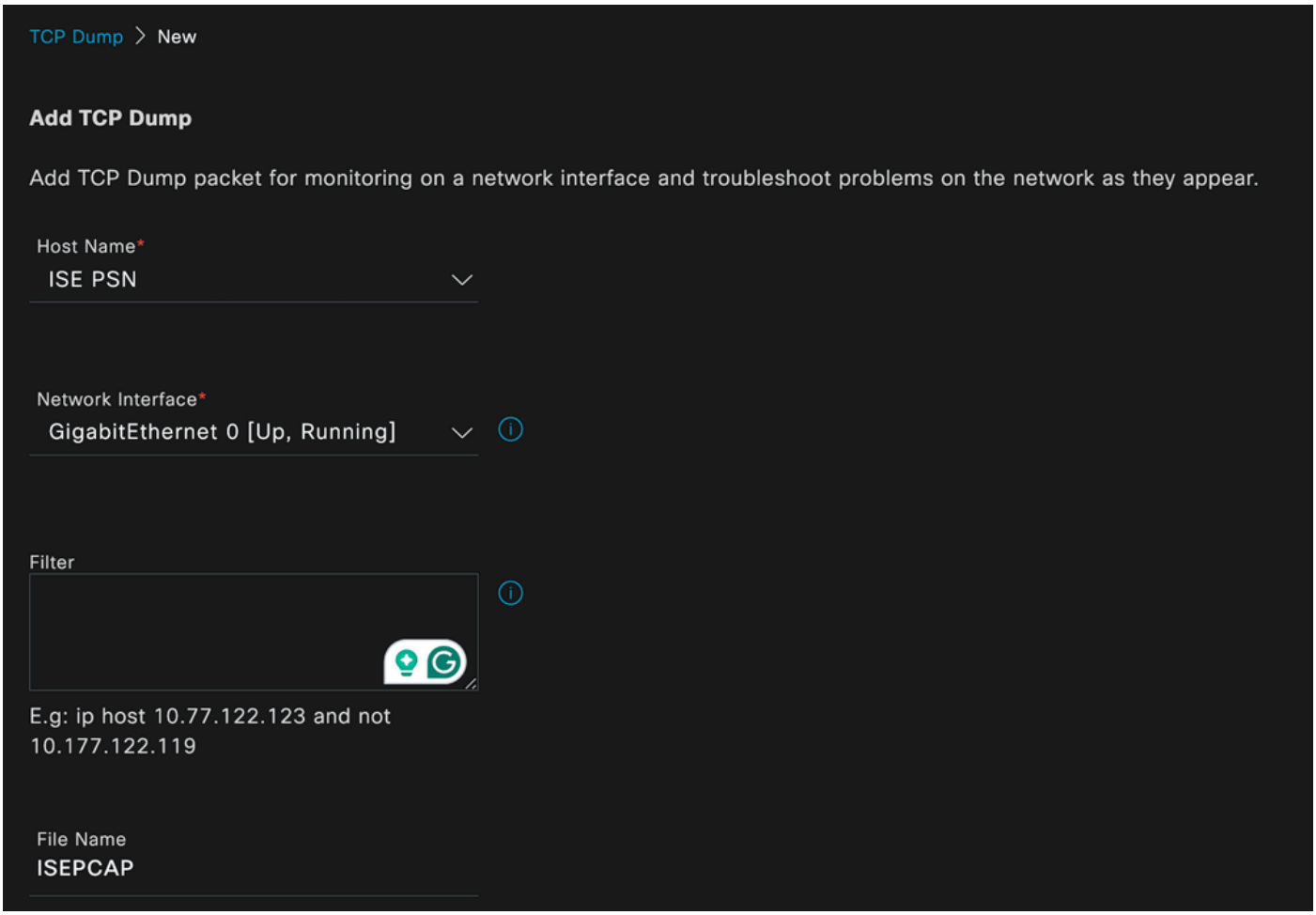
El análisis de captura de paquetes es esencial para solucionar problemas. Las capturas de paquetes directamente desde ISE se pueden realizar en todos los nodos y en cualquier interfaz de los nodos.

Para acceder a esta herramienta, navegue hasta Operaciones > Herramientas de diagnóstico > Herramientas generales > Volcado TCP.

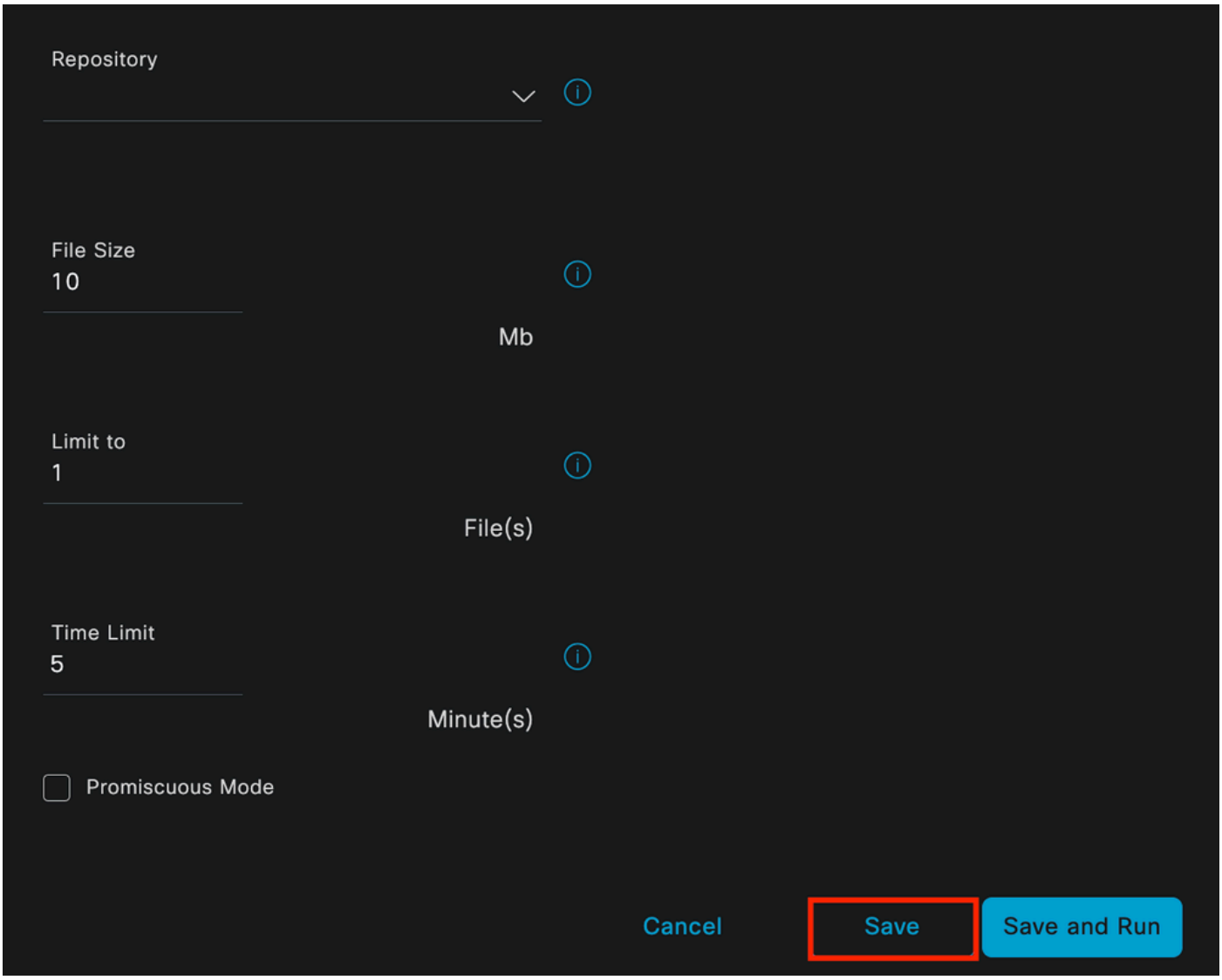


Sección de volcado TCP

Haga clic en el botón Add, para comenzar a configurar un pcap.



Creación de volcado TCP

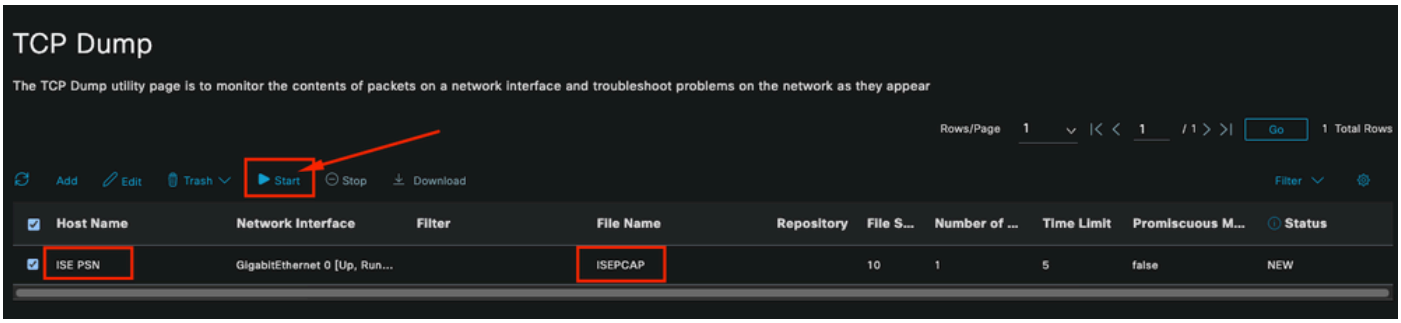


Sección de volcado TCP

Para crear un pcap en ISE, estos son los datos que debe introducir:

- Seleccione el nodo en el que debe tomar el pcap.
- Seleccione la interfaz de nodo de ISE que se utiliza para el pcap.
- En caso de que necesite capturar cierto tráfico, utilice los filtros, ISE le proporciona algunos ejemplos.
- Nombre el pcap. En este escenario, usamos ISEPCAP.
- Seleccione el repositorio; si no se selecciona ningún repositorio, la captura se guarda en el disco local de ISE y se puede descargar de la GUI.
- Además, si es necesario, modifique el tamaño del archivo pcap.
- Si es necesario, use más de 1 archivo, de modo que si el pcap excede el tamaño del archivo, se creará un nuevo archivo posteriormente.
- Amplíe el tiempo de captura de tráfico para el pcap si es necesario.

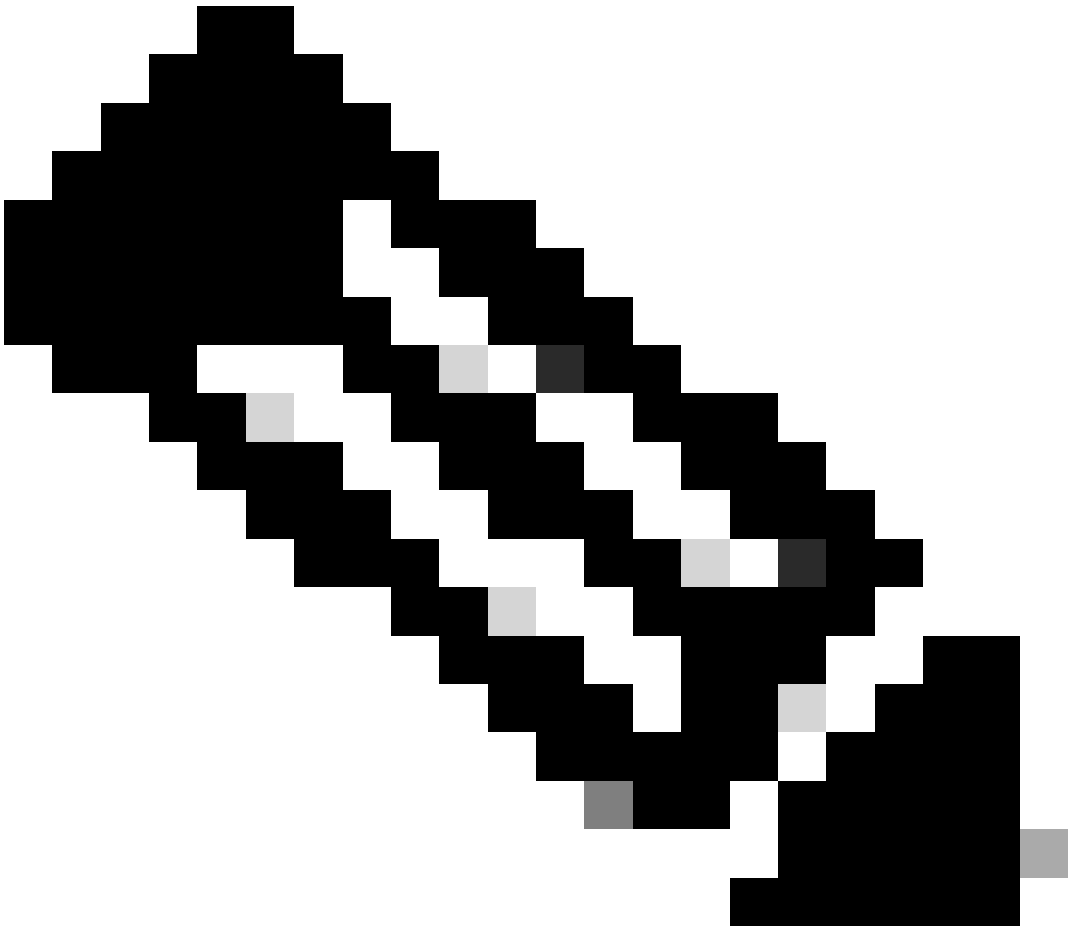
Por último, haga clic en el botón Save.



Sección de volcado TCP

A continuación, cuando esté listo, seleccione el pcap y haga clic en el botón Start.

Una vez que haga clic en Inicio, la columna Estado cambiará al estado EN EJECUCIÓN.



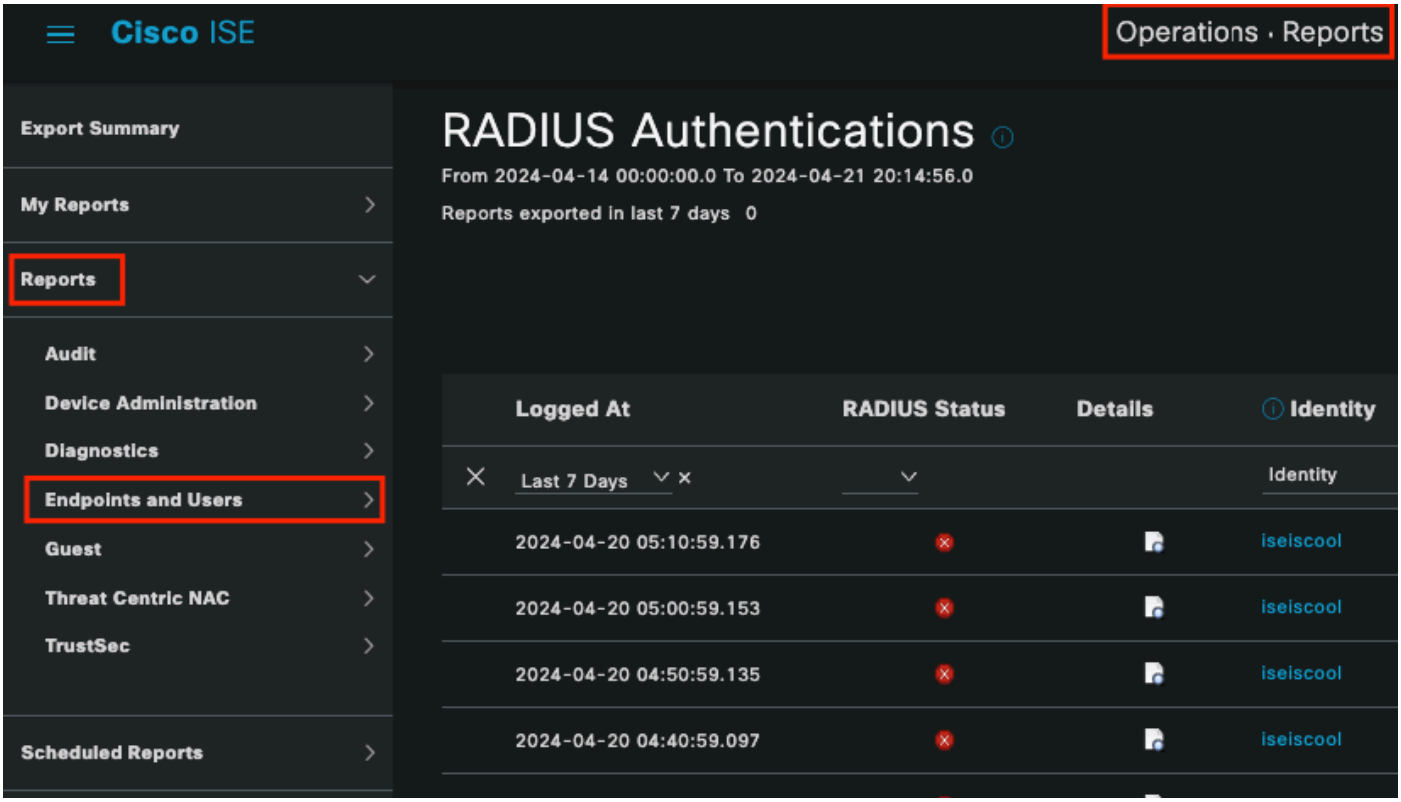
Nota: Mientras el PCAP se encuentra en estado RUNNING, replique el escenario de falla o el comportamiento que necesita capturar. Una vez completados, los detalles de la conversación RADIUS están visibles en PCAP.

Una vez que se hayan capturado los datos que necesita mientras se ejecuta PCAP, finalice la recopilación de pcap. Selecciónelo de nuevo y haga clic en Detener.

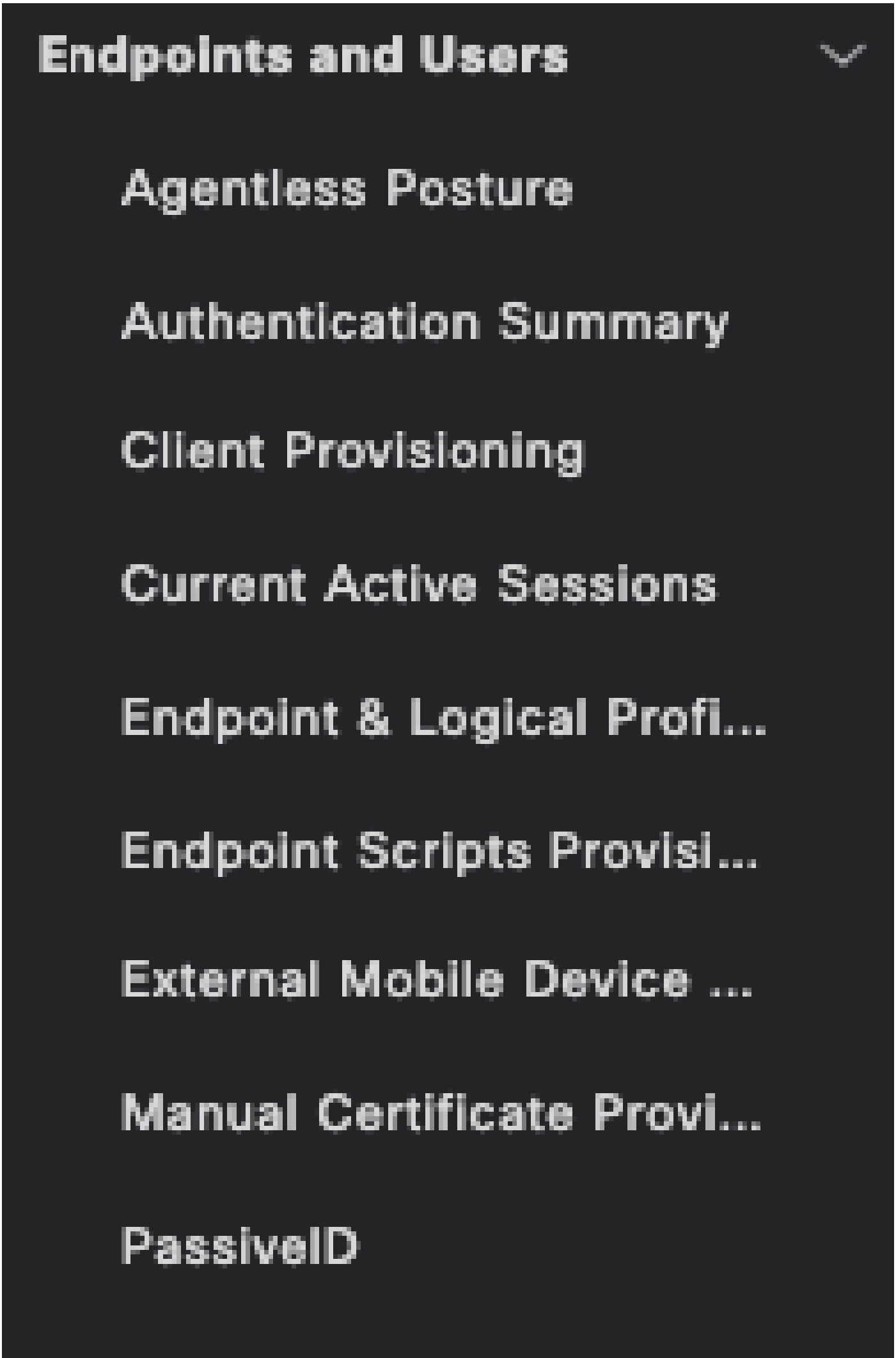
3 - 1 Informes de ISE

En caso de que se requiera un análisis más profundo, ISE ofrece informes útiles para investigar eventos pasados.

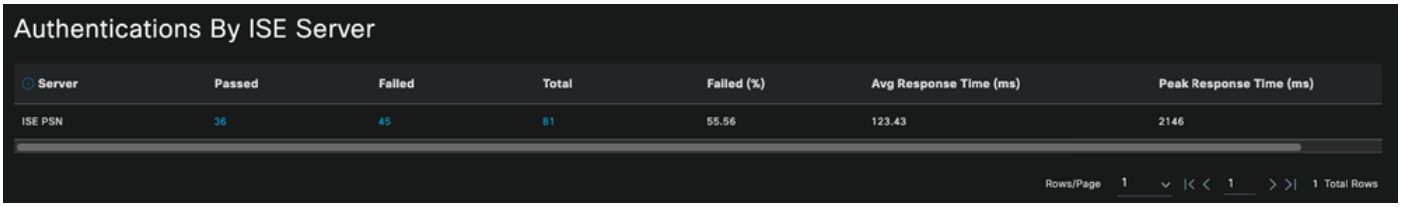
Para encontrarlos, navegue hasta Operaciones > Informes > Informes > Terminales y usuarios



Sección Informes de ISE


Endpoints and Users
Agentless Posture
Authentication Summary
Client Provisioning
Current Active Sessions
Endpoint & Logical Profi...
Endpoint Scripts Provisi...
External Mobile Device ...
Manual Certificate Provi...
PassiveID

: En la implementación utilizada para este documento, solo se utilizó un PSN; sin embargo, para implementaciones más grandes, estos datos son útiles para ver si se necesita equilibrio de carga.



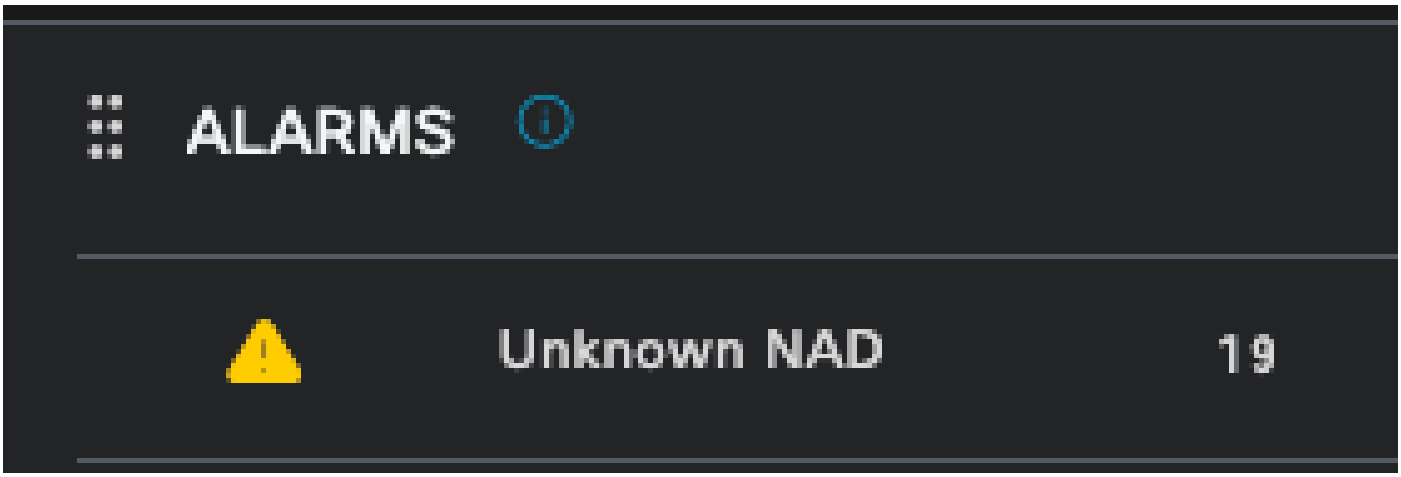
Autenticaciones por servidor ISE

4 - Alarmas ISE

En el Panel de ISE, la sección Alarmas muestra los problemas de implementación.

A continuación se indican varias alarmas de ISE que ayudan con la resolución de problemas.

NAD desconocido: esta alarma se muestra cuando hay un dispositivo de red que autentica un terminal y se comunica con ISE. Sin embargo, ISE no confía en él y descarta la conexión RADIUS. Las razones más comunes son que el dispositivo de red no se ha creado o que la IP que está utilizando el dispositivo de red no es la misma que ha registrado ISE.

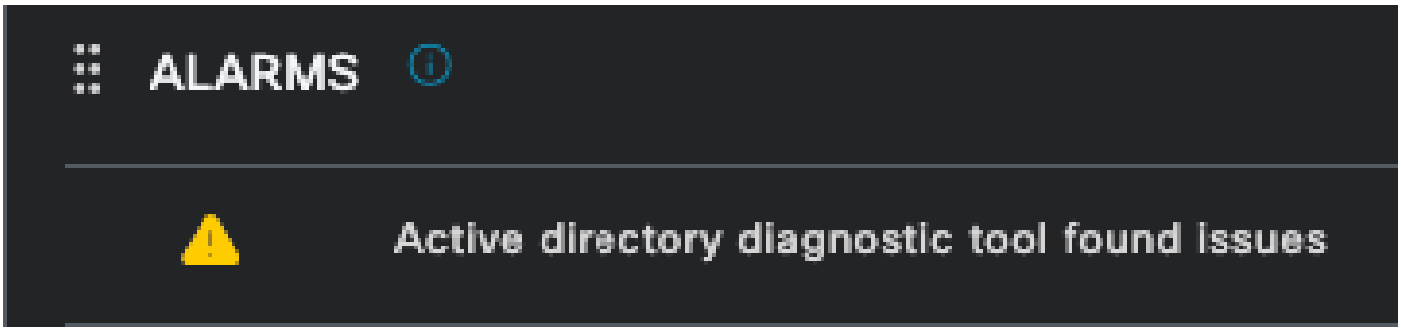


NAD desconocido

Suplicante dejó de responder: esta alarma se produce cuando hay un problema con la comunicación del suplicante, la mayor parte del tiempo se debe a un error de configuración en el suplicante que se tiene que verificar e investigar en el extremo.

El Suplicante Dejó De Responder

La herramienta de diagnóstico de Active Directory encontró problemas: cuando se utiliza Active Directory para validar la identidad del usuario, si comienza a tener problemas con el proceso de comunicación o si la conexión se rompe, verá esta alarma. Entonces se daría cuenta de por qué fallan las autenticaciones de que la identidad existe en el AD.



Error de diagnóstico de AD

COA (cambio de autorización) fallido: varios flujos en ISE utilizan CoA, esta alarma le informa si se encontraron problemas durante la comunicación del puerto CoA a cualquier dispositivo de red.

Error de Coa

5 - Configuración de depuración de ISE y recopilación de registros

Para continuar con los detalles del proceso de autenticación, debe habilitar los siguientes componentes en DEBUG para los problemas de mab y dot1x:

Problema: dot1x/mab

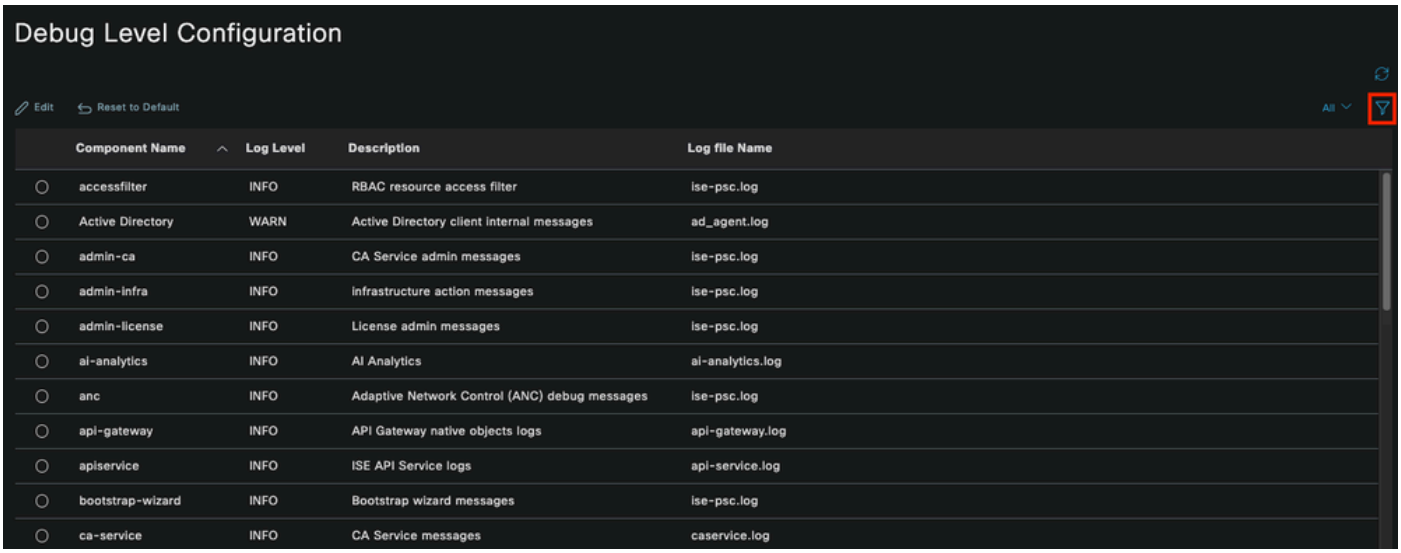
Atributos que se establecerán en el nivel de depuración.

- runtime-AAA (prrt-server.log)

- nsf (ise-psc.log)
- nsf-session (ise-psc.log)

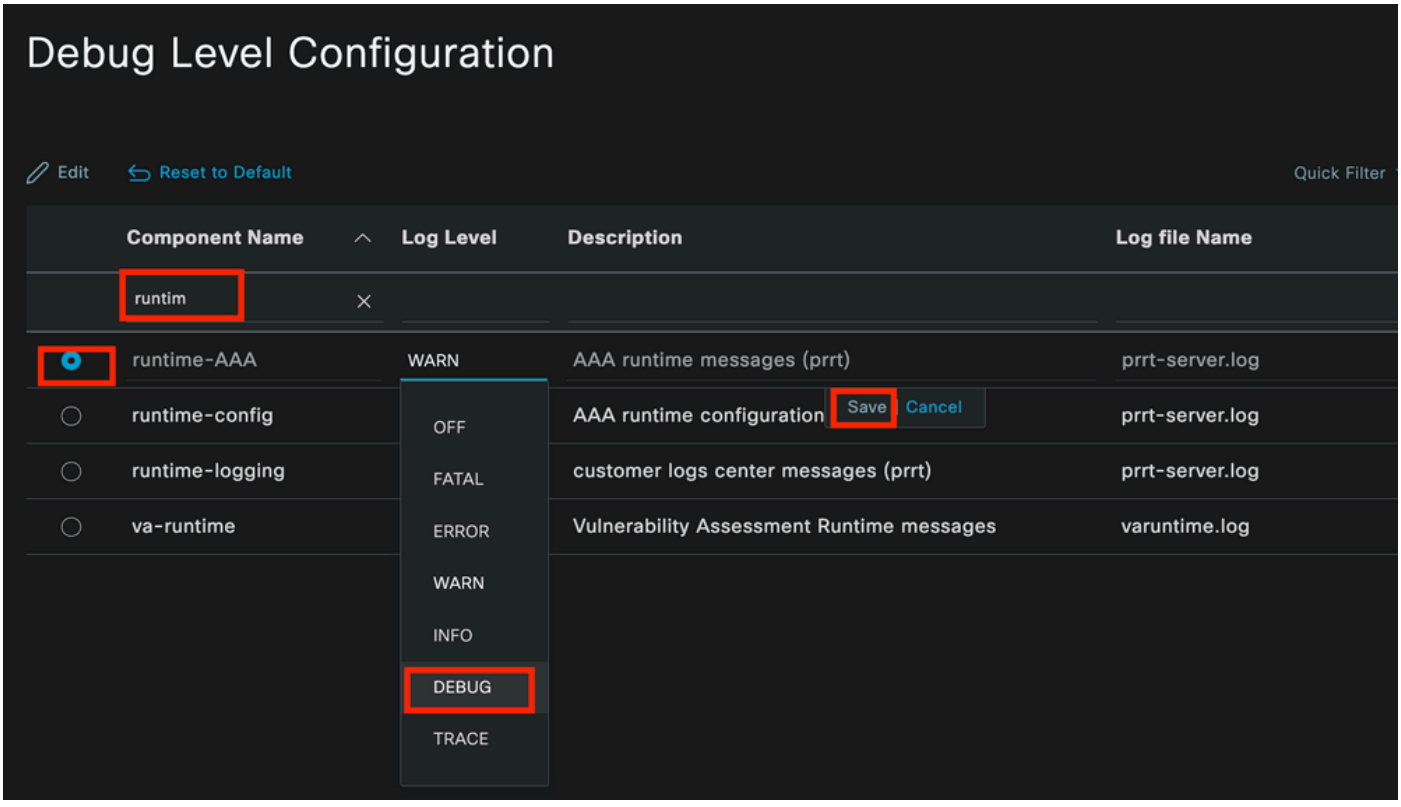
Para habilitar los componentes al nivel DEBUG, primero se requiere identificar cuál es el PSN que recibe la autenticación que está fallando o que necesita ser investigado. Puede obtener esta información de los registros activos. Después de eso, debe ir al menú de ISE > Troubleshooting > Debug Wizard > Debug Log Configuration > Select the PSN > Click the Edit Button.

Se muestra el siguiente menú. Haga clic en el icono de filtro:



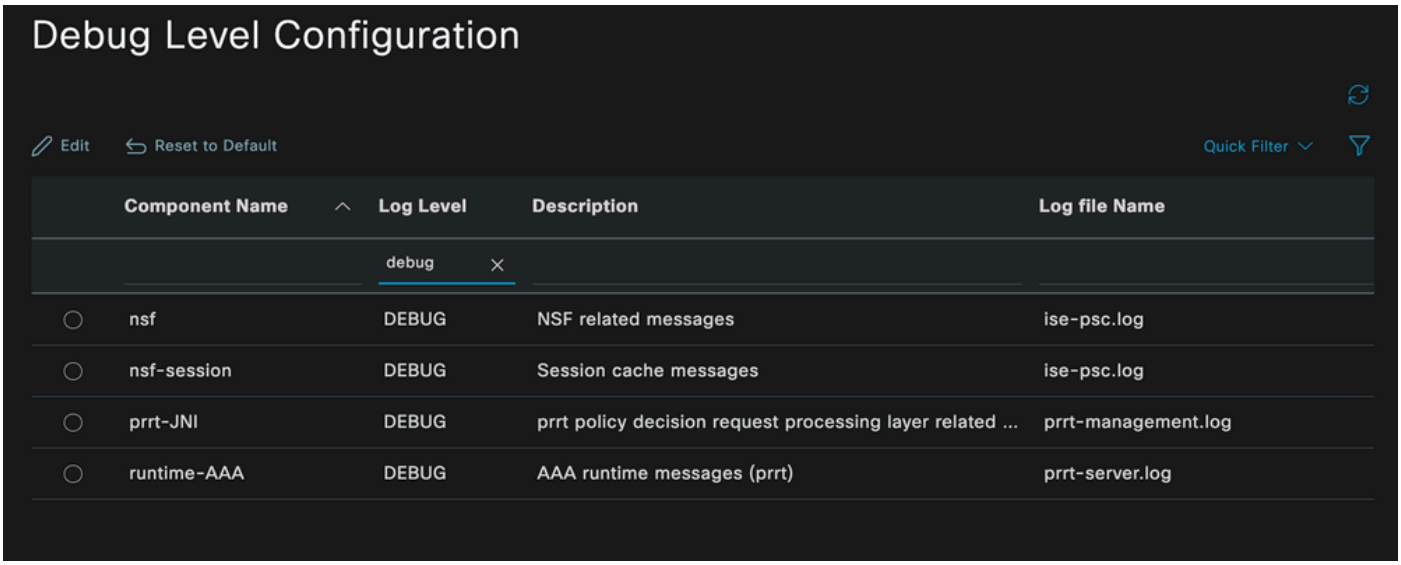
Configuración del registro de depuración

En la columna Nombre de componente, busque los atributos enumerados anteriormente. Seleccione cada nivel de registro y cámbielo a DEBUG. Guarde los cambios.



Configuración del Componente AAA de Runtime

Una vez que haya terminado de configurar cada componente, fíltrelos con DEBUG para que pueda ver si todos los componentes se configuraron correctamente.

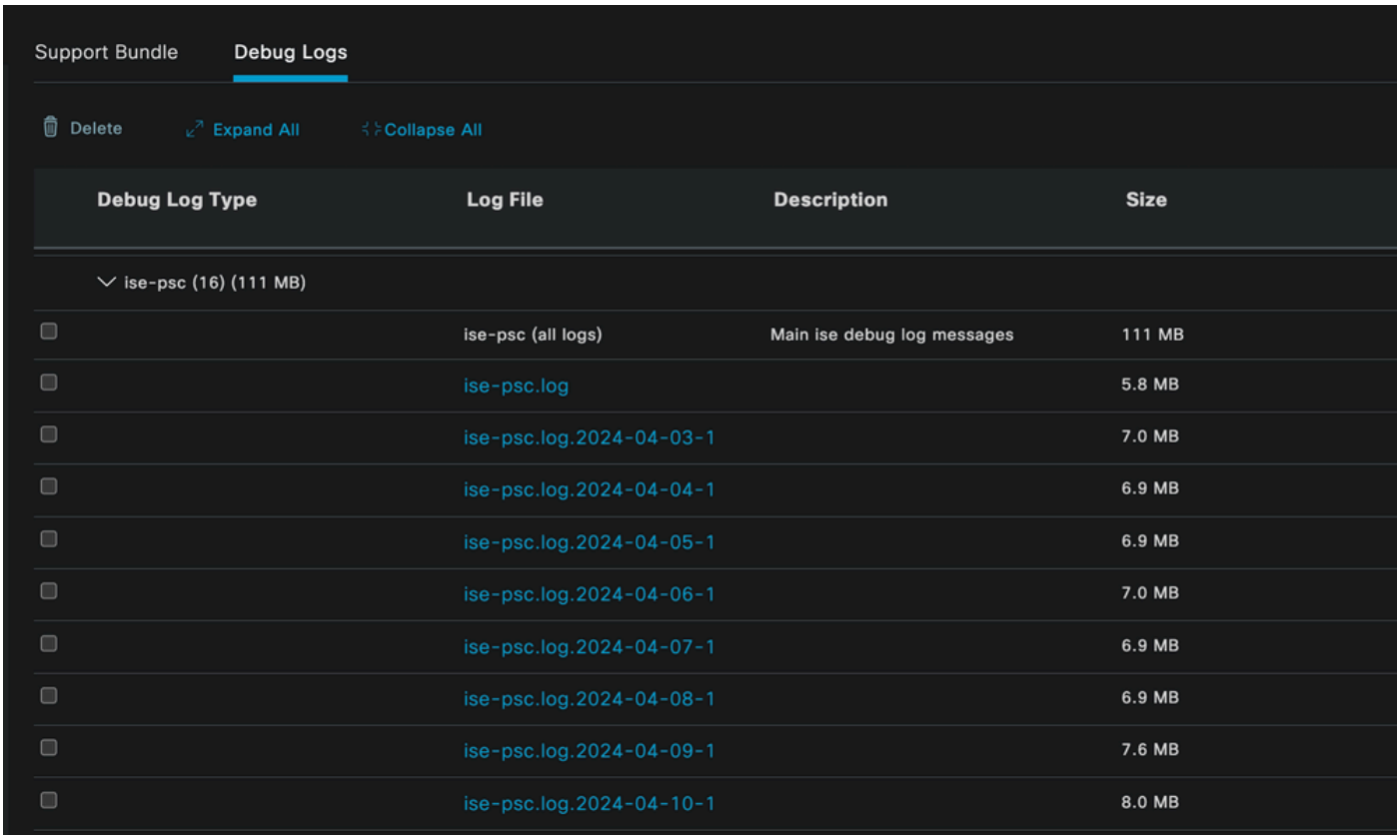


Configuración del registro de depuración

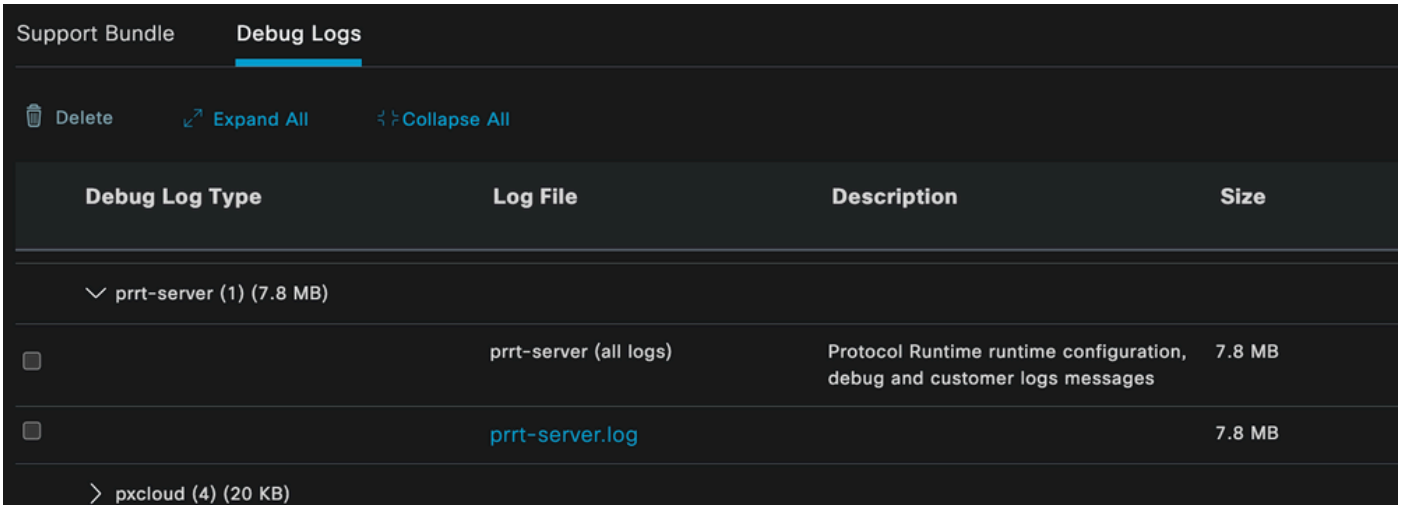
En caso de que sea necesario analizar inmediatamente los registros, puede descargarlos navegando a la ruta Menú ISE > Operaciones > Solucionar problemas > Descargar registros > Lista de nodos del dispositivo > PSN y habilitó DEBUGS > Registros de depuración.

En este caso, debe descargar para los problemas dot1x y mab en port-server.log e ise-psc.log. El registro que debe descargar es el que contiene la fecha de su última prueba.

Solo tiene que hacer clic en el archivo de registro que se muestra en esta imagen y descargarlo (se muestra en texto azul).



Registros de depuración del nodo PSN

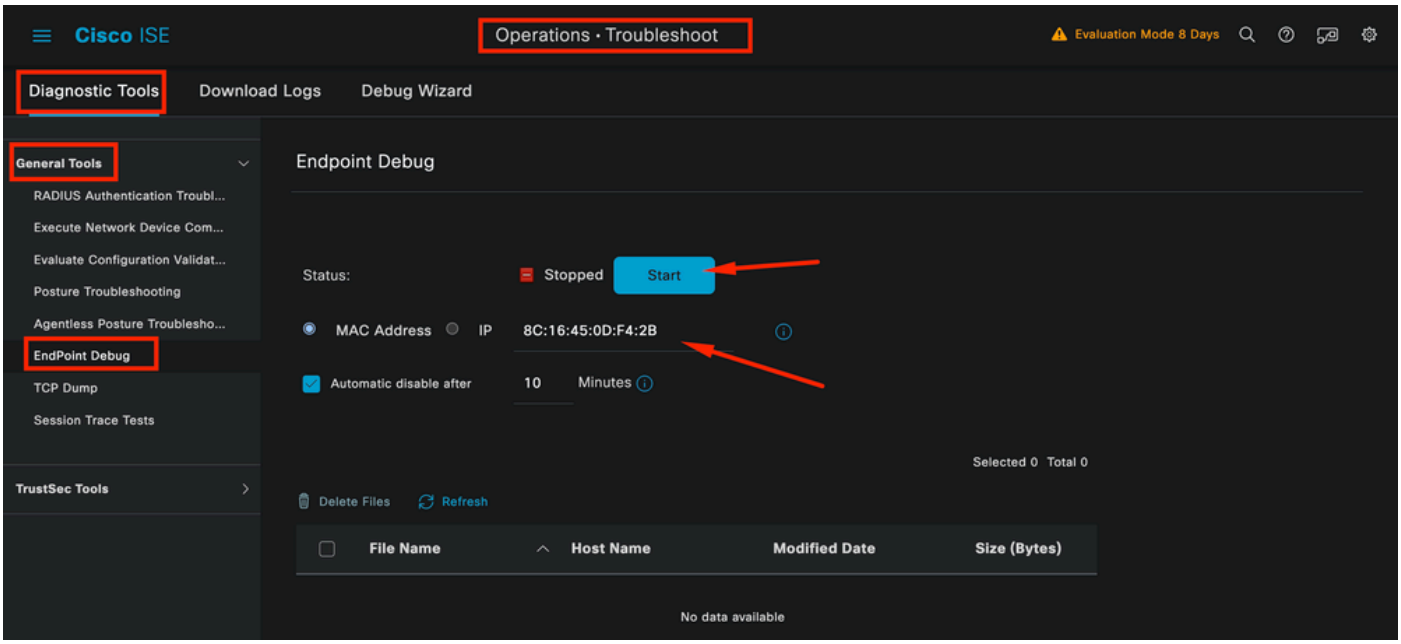


Sección Registros de depuración

6 - Depuración de ISE por terminal

También existe otra opción para obtener registros de DEBUG, por registros de depuración de terminal basados en dirección MAC o IP. Puede utilizar la herramienta Endpoint Debug ISE.

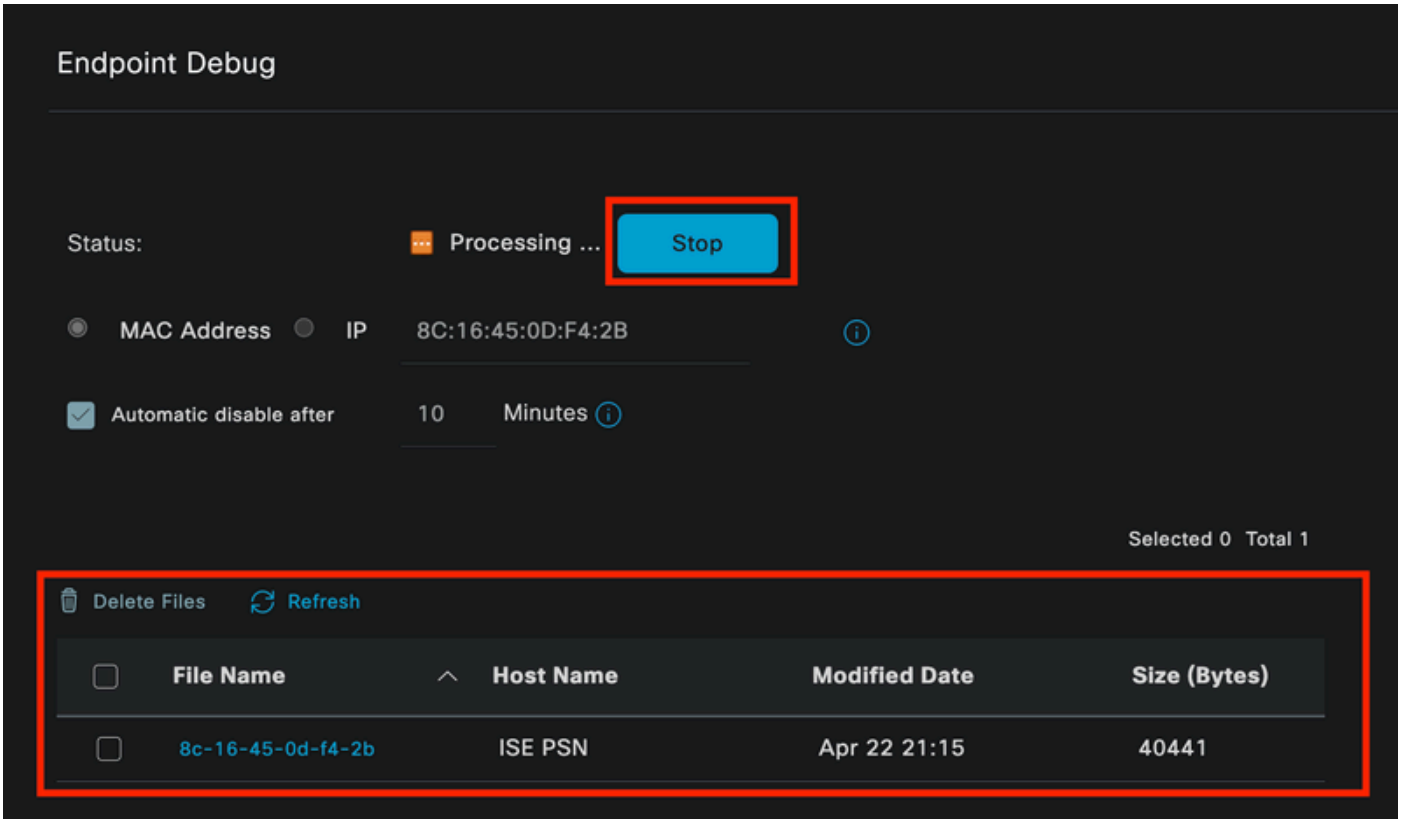
Vaya al menú de ISE > Operaciones > Solucionar problemas > Herramientas de diagnóstico > Herramientas generales > Depuración de terminales.



Depuración de terminales

A continuación, introduzca la información del terminal deseado para iniciar la captura de registros. Haga clic en Start (Inicio).

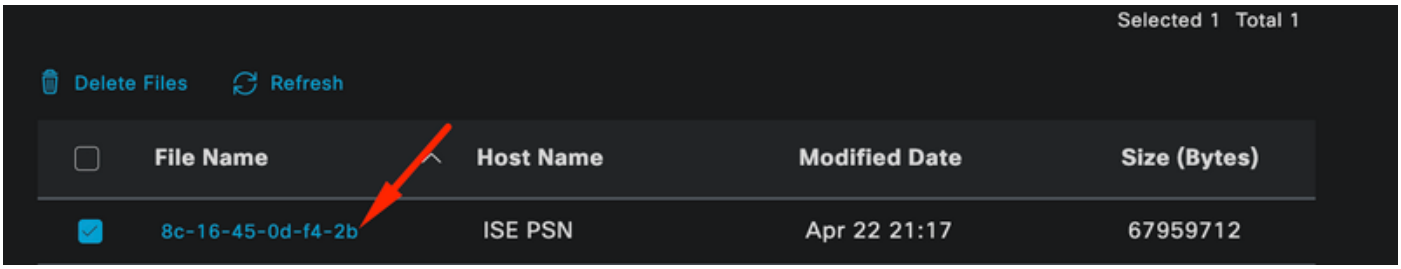
A continuación, haga clic en Continuar en el mensaje de advertencia.



Depuración de terminales

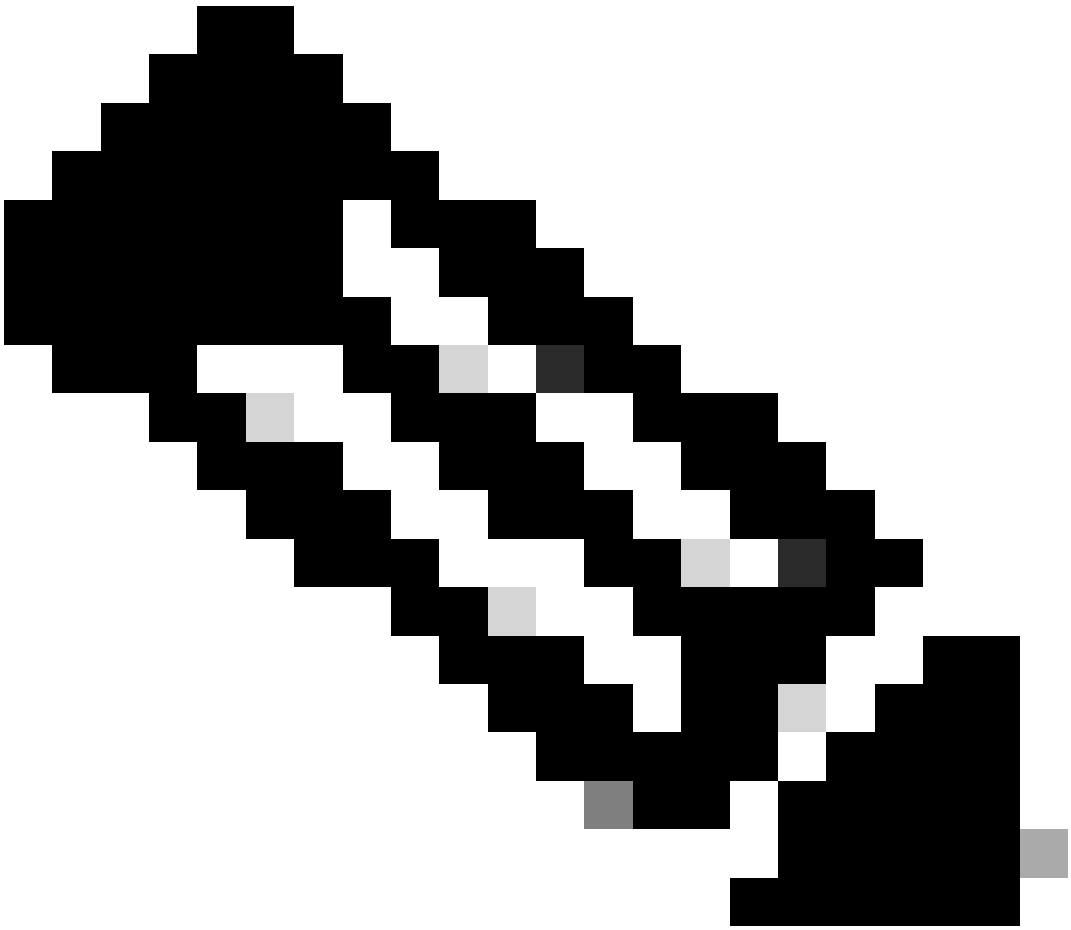
Una vez capturada la información, haga clic en Stop.

Haga clic en el nombre de archivo que se muestra en azul. en esta imagen.



Depuración de terminales

Debe poder ver los registros de autenticación con los registros de DEBUG sin habilitarlos directamente desde la Configuración del registro de depuración.

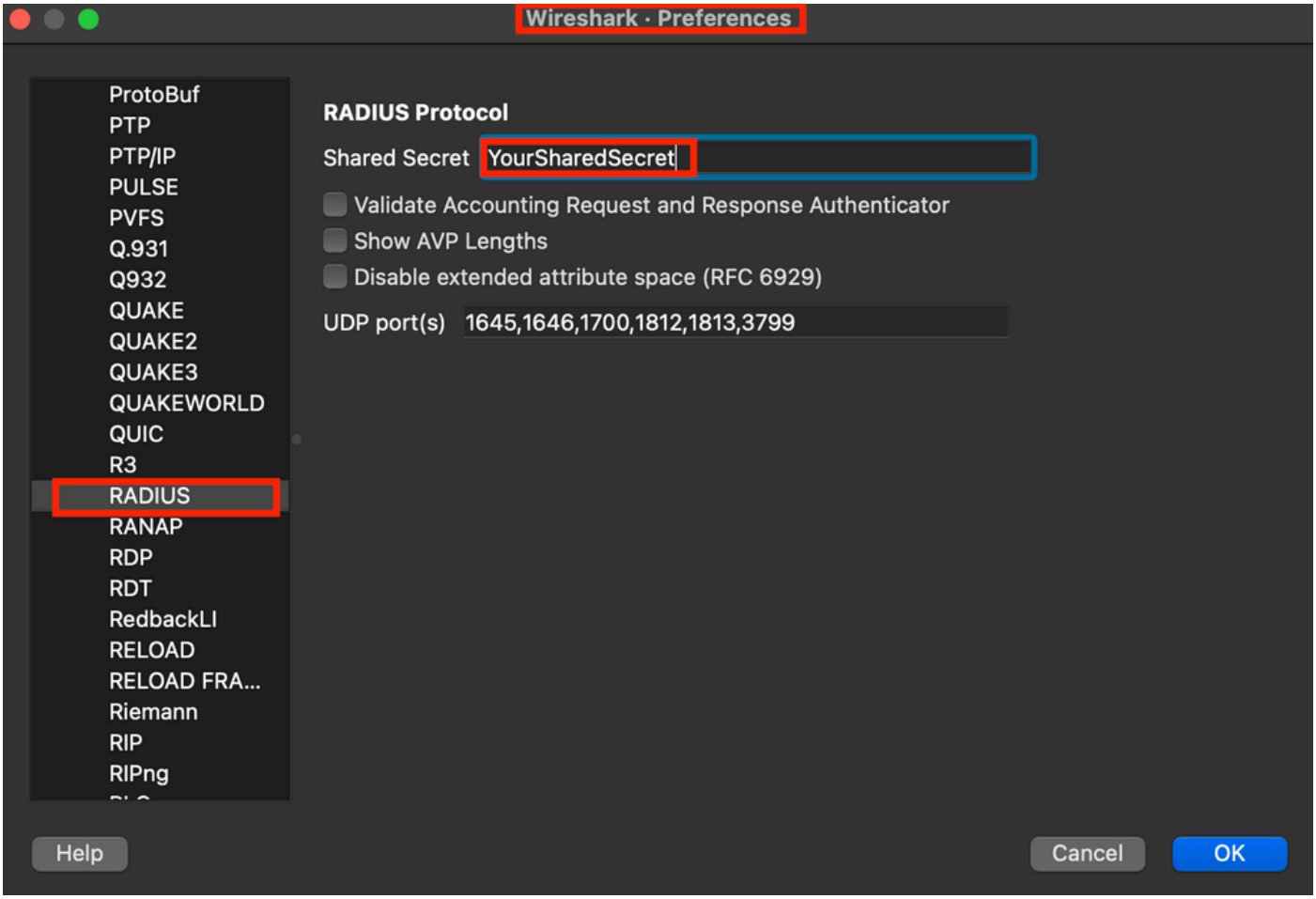


Nota: Debido a que algunas cosas podrían omitirse en el resultado de Endpoint Debug, obtendría un archivo de registro más completo generándolo con Debug Log Configuration y descargando todos los registros requeridos de cualquier archivo que necesite. Como se explicó en la sección anterior Configuración de depuración y recopilación de registros de ISE.

---

7 - Descifrar paquetes RADIUS

Los paquetes Radius no están cifrados excepto para el campo de contraseña de usuario. Sin embargo, debe verificar la contraseña enviada. Puede ver el paquete que envió el usuario navegando hasta Wireshark > Preferences > Protocols > RADIUS y luego agregue la clave compartida RADIUS utilizada por ISE y el dispositivo de red. Después de eso, los paquetes RADIUS se muestran descifrados.



Opciones de Wireshark Radius

8 - Comandos de resolución de problemas de dispositivos de red

El siguiente comando sirve de ayuda a la hora de solucionar problemas en el ISR 1100 o el dispositivo NAD con cables.

8 - 1 Para ver si el servidor AAA o ISE está disponible y es accesible desde el dispositivo de red, utilice show aaa servers.

```
Router>show aaa servers

RADIUS: id 1, priority 1, host 10.88.240.80, auth-port 1645, acct-port 1646, hostname
     State: current UP, duration 2876s, previous duration 0s
     Dead: total time 0s, count 0

     Platform State from SMD: current UP, duration 2876s, previous duration 0s
     SMD Platform Dead: total time 0s, count 0
```

```
Platform State from WNCD (1) : current UP, duration 3015s, previous duration 0s
Platform State from WNCD (2) : current UP, duration 3015s, previous duration 0s
Platform State from WNCD (3) : current UP, duration 3015s, previous duration 0s
Platform State from WNCD (4) : current UP, duration 3015s, previous duration 0s
Platform State from WNCD (5) : current UP, duration 3015s, previous duration 0s
Platform State from WNCD (6) : current UP, duration 3015s, previous duration 0s
Platform State from WNCD (7) : current UP, duration 3015s, previous duration 0s
Platform State from WNCD (8) : current UP, duration 3015s, previous duration 0s

WNCD Platform Dead: total time 0s, count 0UP

Quarantined: No

Authen: request 11, timeouts 0, failover 0, retransmission 0

        Response: accept 1, reject 0, challenge 10
        Response: unexpected 0, server error 0, incorrect 0, time 33ms
        Transaction: success 11, failure 0
        Throttled: transaction 0, timeout 0, failure 0
        Malformed responses: 0
        Bad authenticators: 0
        Dot1x transactions:

        Response: total responses: 11, avg response time: 33ms
        Transaction: timeouts 0, failover 0
        Transaction: total 1, success 1, failure 0

        MAC auth transactions:
        Response: total responses: 0, avg response time: 0ms
        Transaction: timeouts 0, failover 0
        Transaction: total 0, success 0, failure 0

Author: request 0, timeouts 0, failover 0, retransmission 0
        Response: accept 0, reject 0, challenge 0
        Response: unexpected 0, server error 0, incorrect 0, time 0ms
        Transaction: success 0, failure 0

        Throttled: transaction 0, timeout 0, failure 0
        Malformed responses: 0
        Bad authenticators: 0
        MAC author transactions:

        Response: total responses: 0, avg response time: 0ms
        Transaction: timeouts 0, failover 0
        Transaction: total 0, success 0, failure 0

Account: request 6, timeouts 4, failover 0, retransmission 3
        Request: start 1, interim 0, stop 0
        Response: start 1, interim 0, stop 0

        Response: unexpected 0, server error 0, incorrect 0, time 27ms
        Transaction: success 2, failure 1
        Throttled: transaction 0, timeout 0, failure 0
        Malformed responses: 0
        Bad authenticators: 0

Elapsed time since counters last cleared: 47m
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
Estimated Throttled Access Transactions: 0
Estimated Throttled Accounting Transactions: 0
Maximum Throttled Transactions: access 0, accounting 0
```

```
     Consecutive Response Failures: total 0
             SMD Platform : max 0, current 0 total 0
             WNCD Platform: max 0, current 0 total 0
             IOSD Platform : max 0, current 0 total 0

     Consecutive Timeouts: total 3
             SMD Platform : max 0, current 0 total 0
             WNCD Platform: max 0, current 0 total 0
             IOSD Platform : max 3, current 0 total 3

     Requests per minute past 24 hours:
             high - 0 hours, 47 minutes ago: 4
             low  - 0 hours, 45 minutes ago: 0
             average: 0

Router>
```

8-2 Para ver el estado del puerto, los detalles, las ACL aplicadas a la sesión, el método de autenticación y la información más útil, utilice el comando show authentication sessions interface <interface where the laptop is attach> details.

```
Router#show authentication sessions interface gigabitEthernet 0/1/0 details
Interface: GigabitEthernet0/1/0
IIF-ID: 0x01D9BEFB
MAC Address: 8c16.450d.f42b
IPv6 Address: Unknown
IPv4 Address: Unknown
User-Name: iseiscool
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Common Session ID: 22781F0A0000000C0777AECD
Acct Session ID: 0x00000003
Handle: 0x0a000002
Current Policy: POLICY_Gi0/1/0


Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
Security Policy: Should Secure

Server Policies:


Method status list:
Method State
dot1x Authc Success

Router#
```

8-3 Para verificar que tiene todos los comandos requeridos para aaa en la configuración global, ejecute show running-config aaa.

```
Router#sh run aaa
!
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 Cisc0123
!
!
radius server COHVSRADISE01-NEW
address ipv4 <A.B.C.D> auth-port 1645 acct-port 1646
timeout 15
key Cisc0123
!
!
aaa group server radius ISE-CLUSTER
server name COHVSRADISE01-NEW
!
!
!
!
aaa new-model
aaa session-id common
!
!

Router#
```

8-4 Otro comando útil es test aaa group radius server <A.B.C.D> iseiscool VainillaISE97 legacy.

```
Router#test aaa group radius server <A.B.C.D> iseiscool VainillaISE97 legacy
User was successfully authenticated.

Router#
```

9 - Depuraciones relevantes del dispositivo de red

- debug dot1x all - Muestra todos los mensajes EAP dot1x
- debug aaa authentication - Muestra información de depuración de autenticación de aplicaciones AAA
- debug aaa authorization - Muestra información de depuración para la autorización AAA
- debug radius authentication - Proporciona información detallada sobre las actividades de nivel de protocolo sólo para la autenticación
- debug radius - Proporciona información detallada sobre las actividades de nivel de protocolo

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).