ACL descargable en switches Catalyst 1300

Objetivo

El objetivo de este artículo es demostrar cómo funciona la lista de control de acceso (DACL) descargable en los switches Cisco Catalyst 1300 con Cisco Identity Service Engine (ISE).

Dispositivos aplicables | Versión de software

- Catalyst 1300 Series |4.1.6.54

Introducción

Las ACL dinámicas son ACL asignadas a un puerto de switch en función de una política o criterios como la pertenencia a grupos de cuentas de usuario, la hora del día, etc. Pueden ser ACL locales que se especifican mediante ID de filtro o ACL descargables (DACL).

Las ACL descargables son ACL dinámicas que se crean y descargan del servidor Cisco ISE. Aplican dinámicamente reglas de control de acceso basadas en la identidad del usuario y el tipo de dispositivo. DACL tiene la ventaja de que le permite tener un repositorio central para las ACL, por lo que no necesita crearlas manualmente en cada switch. Cuando un usuario se conecta a un switch, solo tiene que autenticarse y el switch descargará las ACL aplicables del servidor Cisco ISE.

Casos prácticos de ACL descargable

1. Los diferentes usuarios recibirán diferentes ACL cuando se conecten a un switch (Usuarios locales de ISE).
2. Los usuarios con conectividad de red limitada pueden iniciar sesión en un portal web central para obtener acceso completo a la red (autenticación web central).
3. Avanzado: uso de MAC Authentication Bypass (MAB) para permitir la comunicación con Windows Active Directory (AD) y algunos servicios relacionados mientras se conecta el servidor ISE a AD y se supervisa la autenticación de usuarios. Antes del inicio de sesión en Windows AD, la red solo permitirá el acceso a recursos muy limitados, pero la autenticación de AD descargará diferentes ACL basadas en grupos de Windows y permitirá el acceso completo a la red.
4. Avanzado: los usuarios reciben diferentes ACL según el día de la semana, la hora del día o cualquier otro factor debido a las políticas del servidor ISE.

En este artículo, el primer caso práctico se tratará en detalle.

Table Of Contents

- Configurar cliente RADIUS
- Configuración de la autenticación 802.1x
- Configuración del servidor Cisco ISE para ACL descargable
- Configuraciones de cliente
- Verificación de DACL

Prerequisites

- Asegúrese de que el switch Catalyst 1300 esté actualizado al firmware más reciente (el firmware del switch debe ser 4.1.6 o superior).
- Asigne una IP estática al switch para fines de administración.

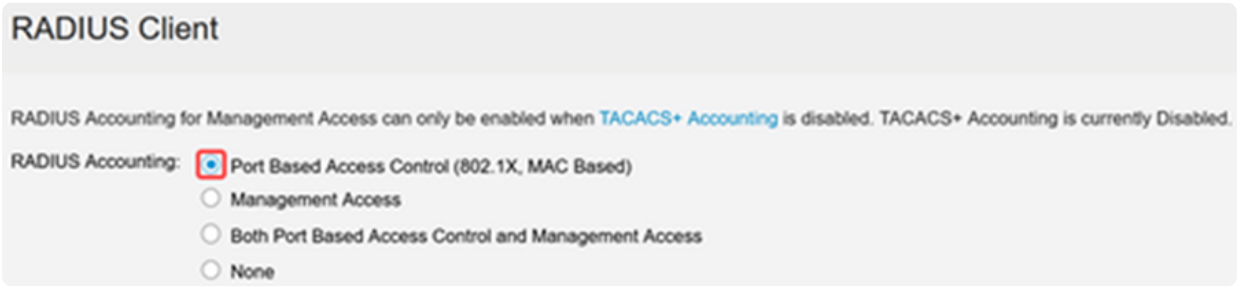
Configurar cliente RADIUS

Paso 1

Inicie sesión en el switch Catalyst 1300 y navegue hasta el menú Security > RADIUS Client.

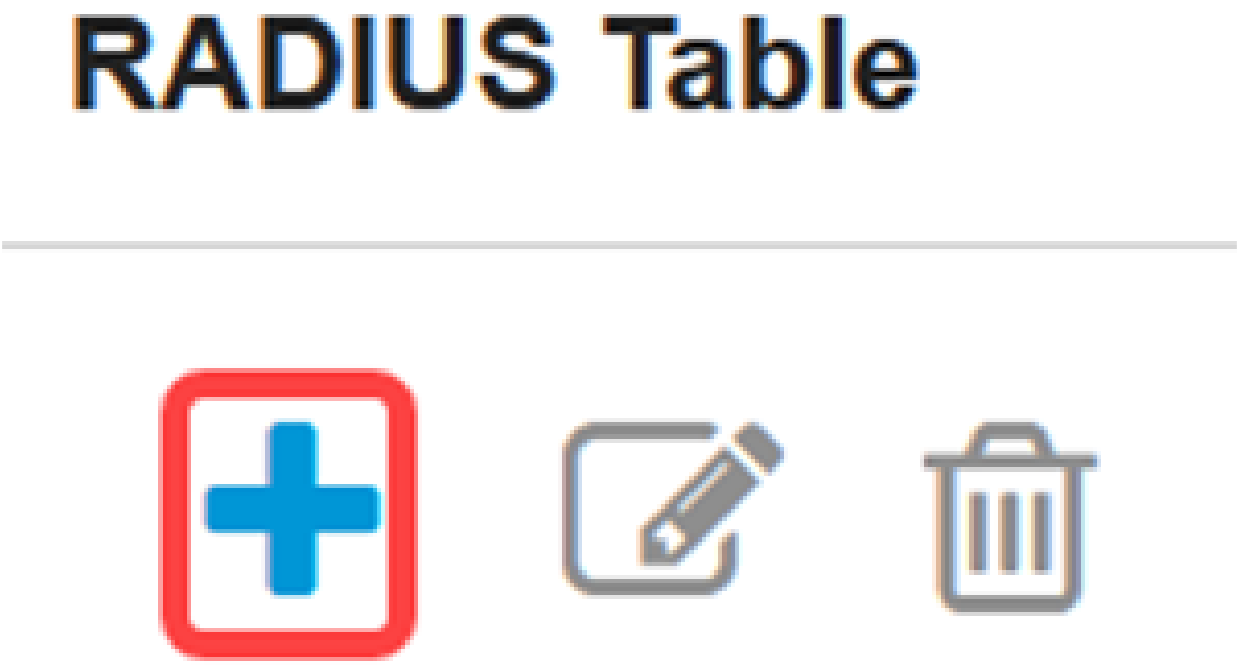
Paso 2

Para RADIUS Accounting, seleccione la opción Port Based Access Control.



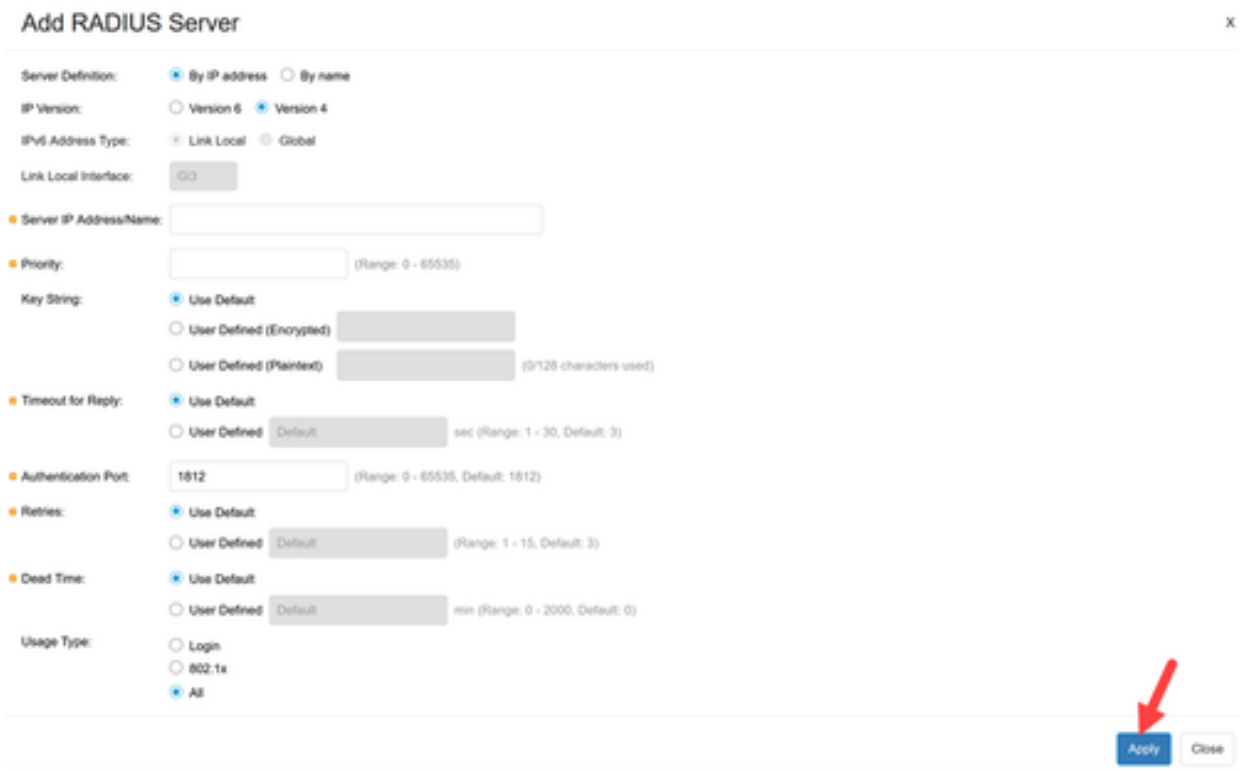
Paso 3

En Tabla RADIUS, haga clic en el icono más para agregar el servidor Cisco ISE.



Paso 4

Introduzca los detalles del servidor Cisco ISE y haga clic en Apply.



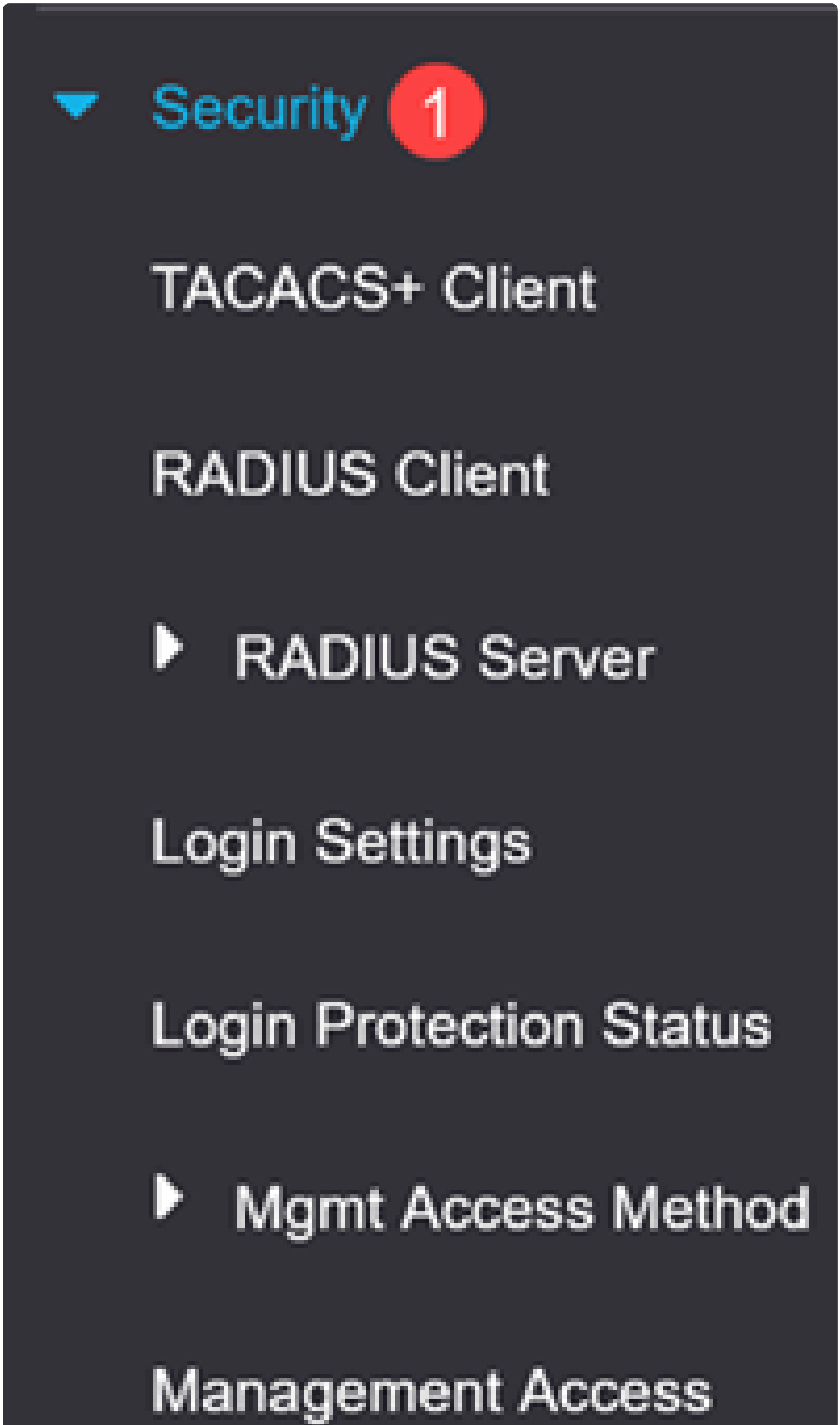
Note:

El tipo de uso debe seleccionarse como 802.1x.

Configuración de la autenticación 802.1x

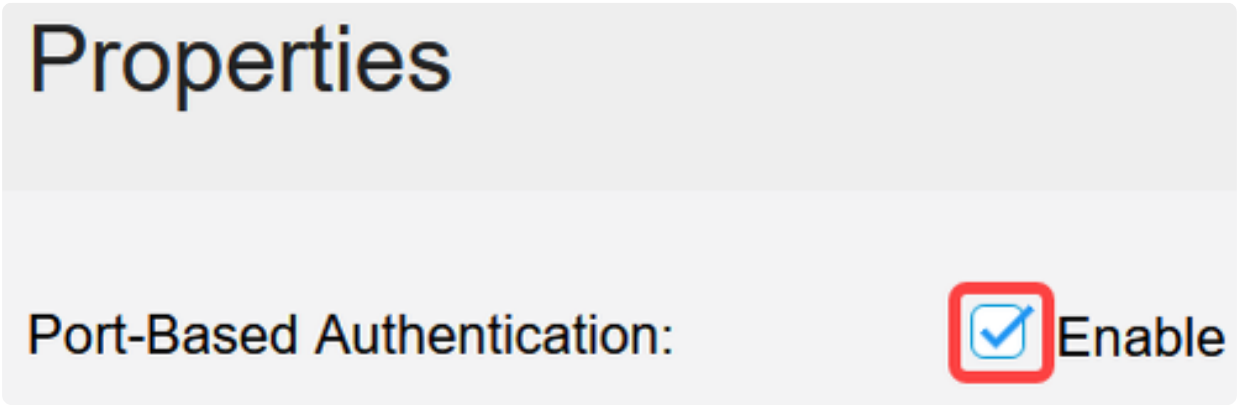
Paso 1

Vaya al menú Security > 802.1X Authentication > Properties.


Security 1
TACACS+ Client
RADIUS Client
RADIUS Server
Login Settings
Login Protection Status
Mgmt Access Method
Management Access

Paso 2

Haga clic en la casilla de verificación para habilitar la autenticación basada en puerto.

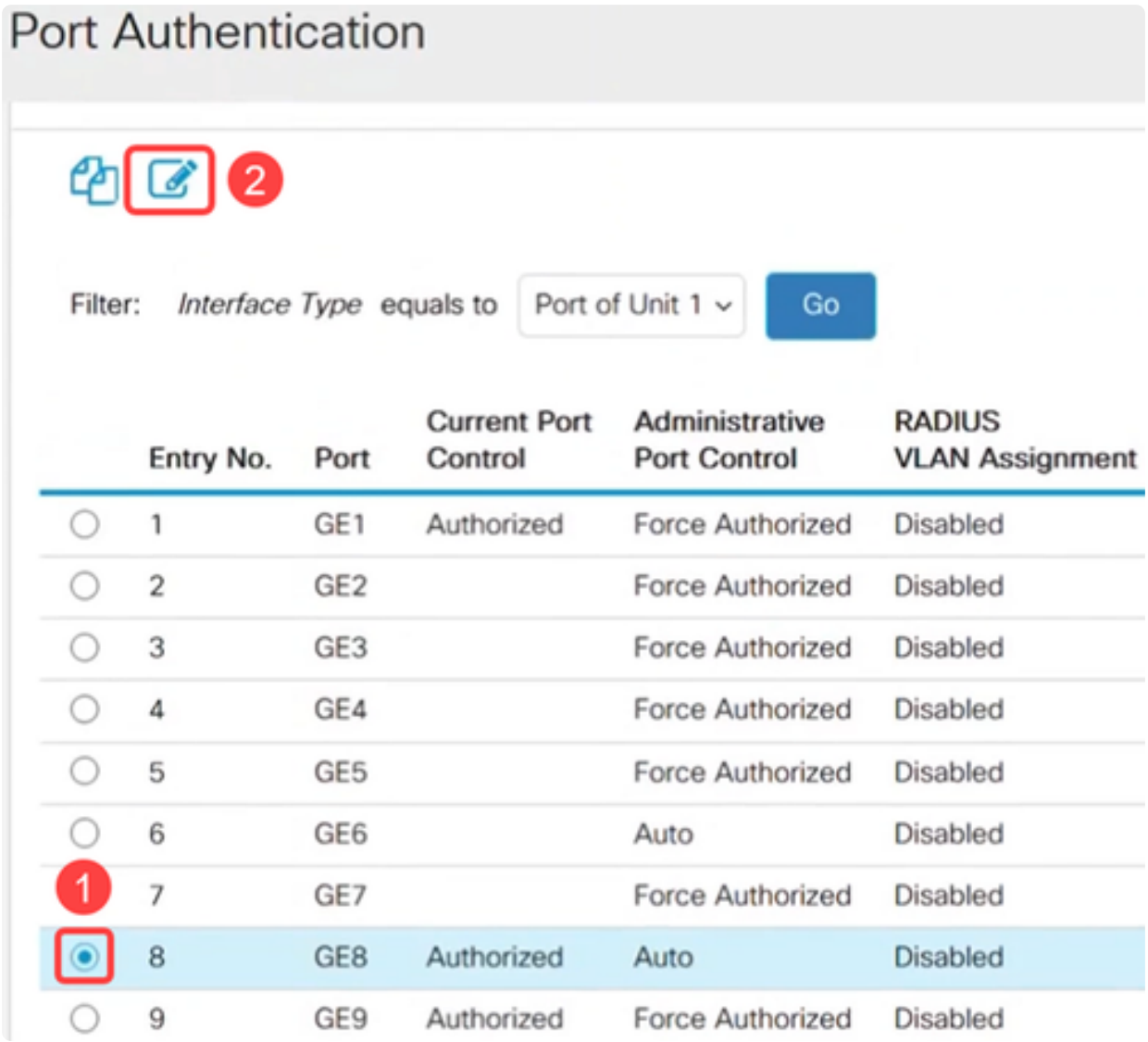


Paso 3

En Método de autenticación, seleccione RADIUS y haga clic en Aplicar.

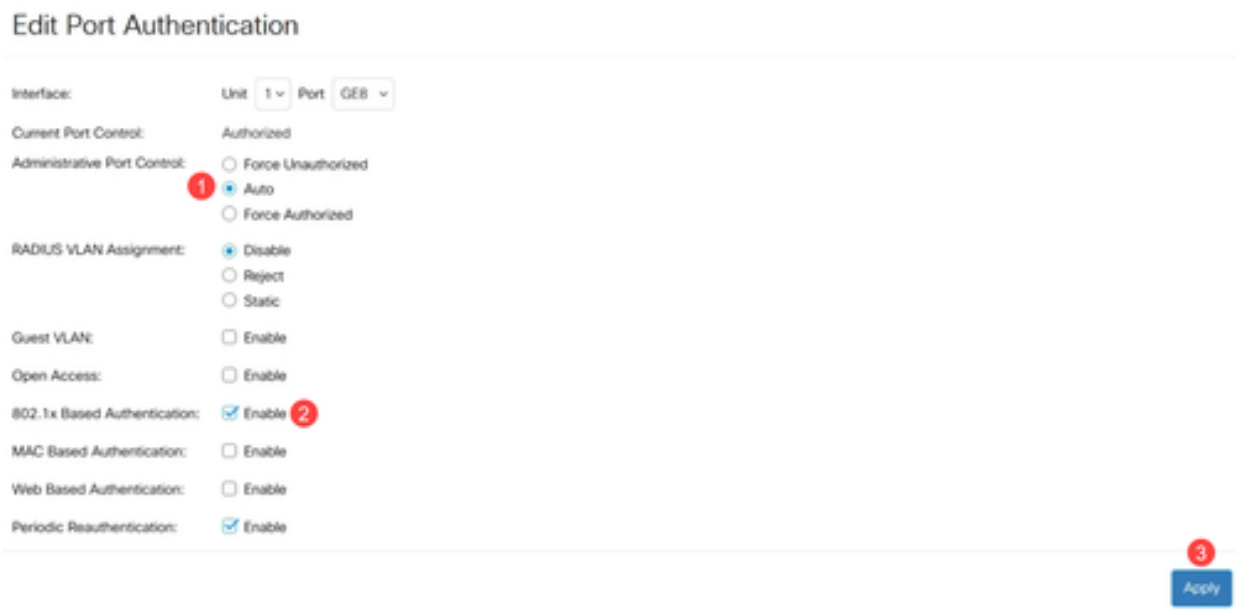
Paso 4

Vaya al menú Security > 802.1X Authentication > Port Authentication. Seleccione el puerto al que está conectado el portátil y haga clic en el icono de edición. En este ejemplo, se selecciona GE8.



Paso 5

Seleccione Administrative Port Control como Auto y habilite la autenticación basada en 802.1x. Haga clic en Apply (Aplicar).



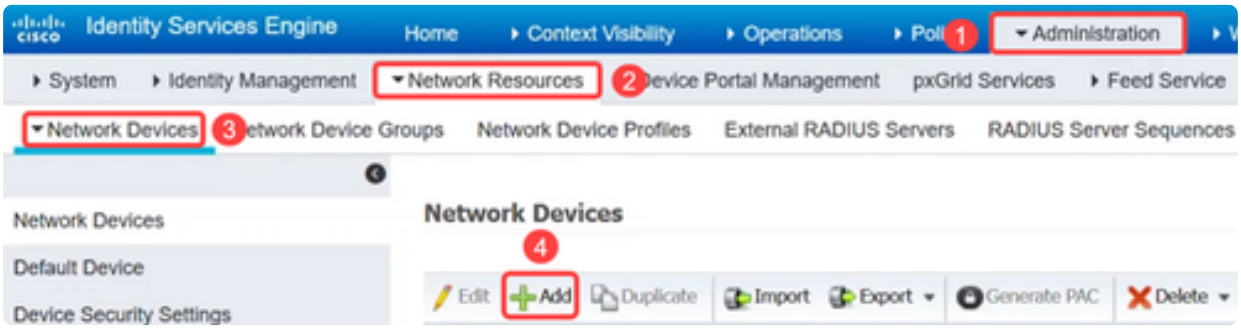
Configuración del servidor Cisco ISE para ACL descargable

> **Note:**
> La configuración de ISE está fuera del alcance de la asistencia empresarial de Cisco. Consulte la guía ISE Admin para obtener más información.

Las configuraciones que se muestran en este artículo son un ejemplo de ACL descargable para funcionar con el switch Catalyst de Cisco serie 1300.

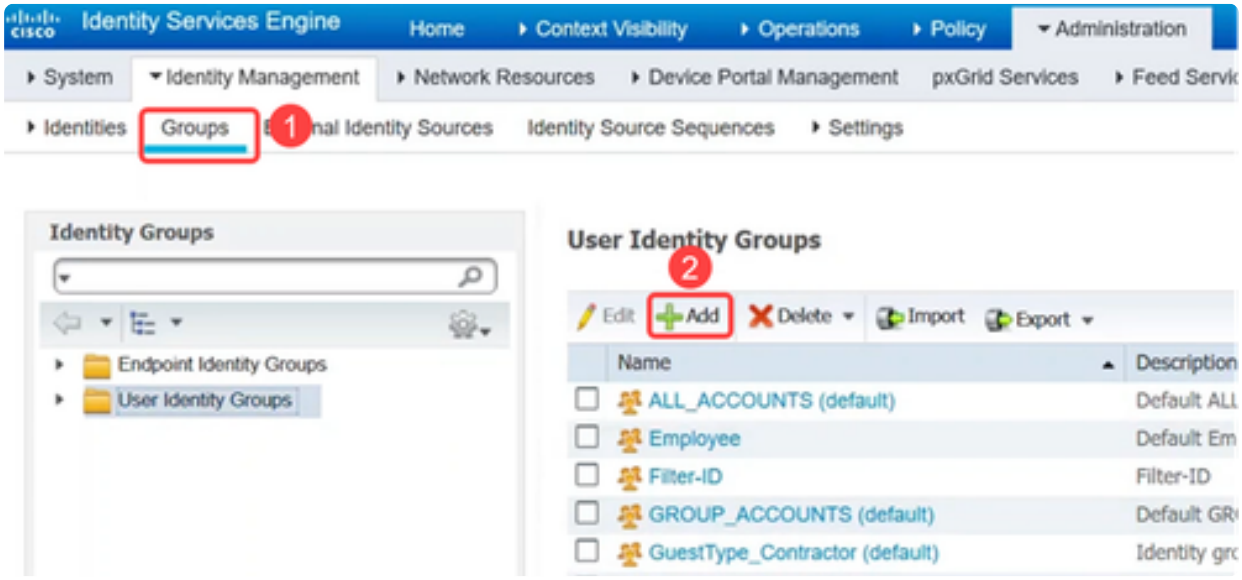
Paso 1

Inicie sesión en su servidor Cisco ISE y navegue hasta Administration > Network Resources > Network Devices y agregue el dispositivo de switch Catalyst.



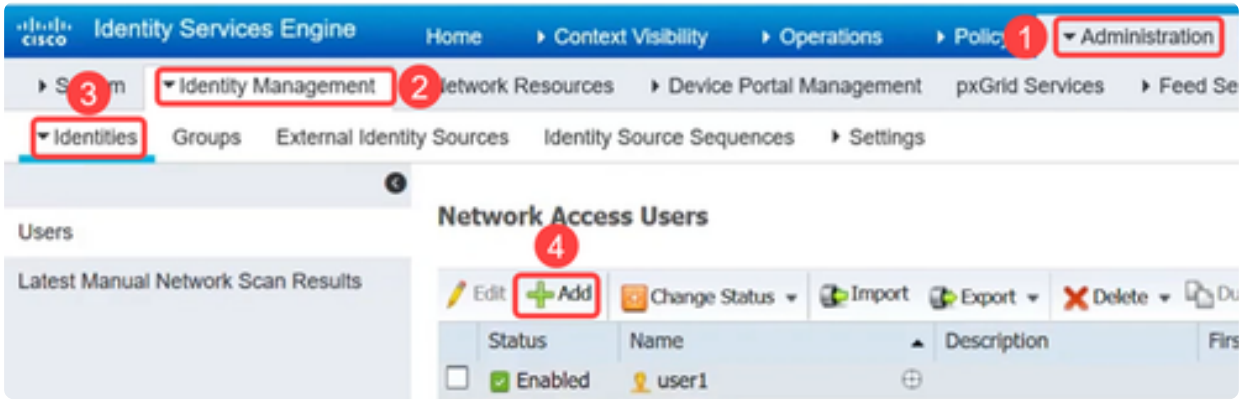
Paso 2

Para crear grupos de identidad de usuario, vaya a la ficha Groups y agregue los grupos de identidad de usuario.



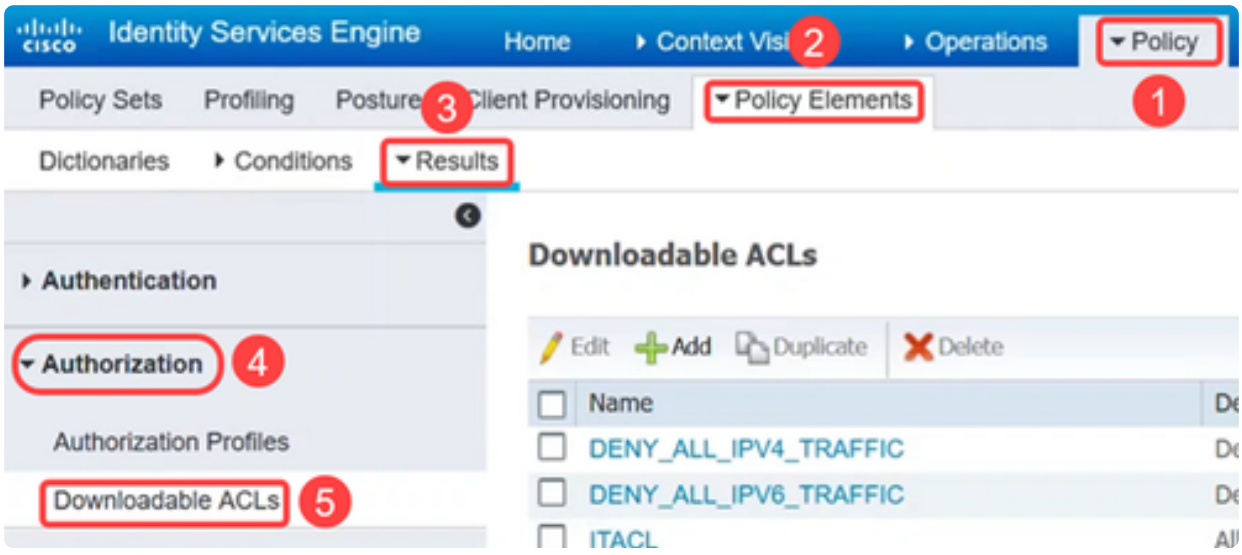
Paso 3

Vaya al menú Administration > Identity Management > Identities para definir los usuarios y asignarlos a los grupos.



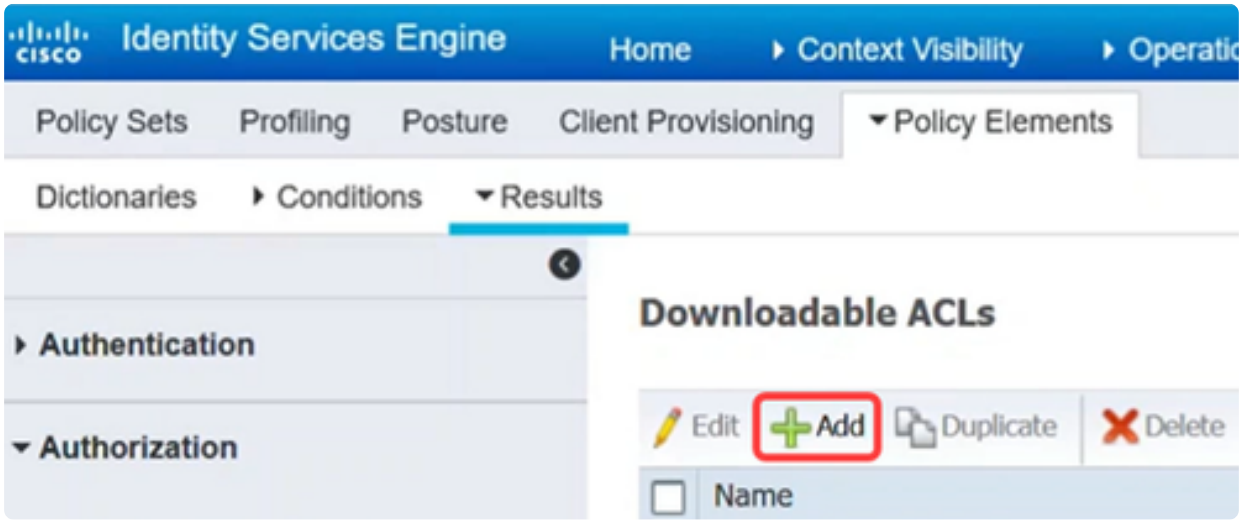
Paso 4

Vaya al menú Policy > Policy Elements > Results. En Autorización, haga clic en ACL descargables.



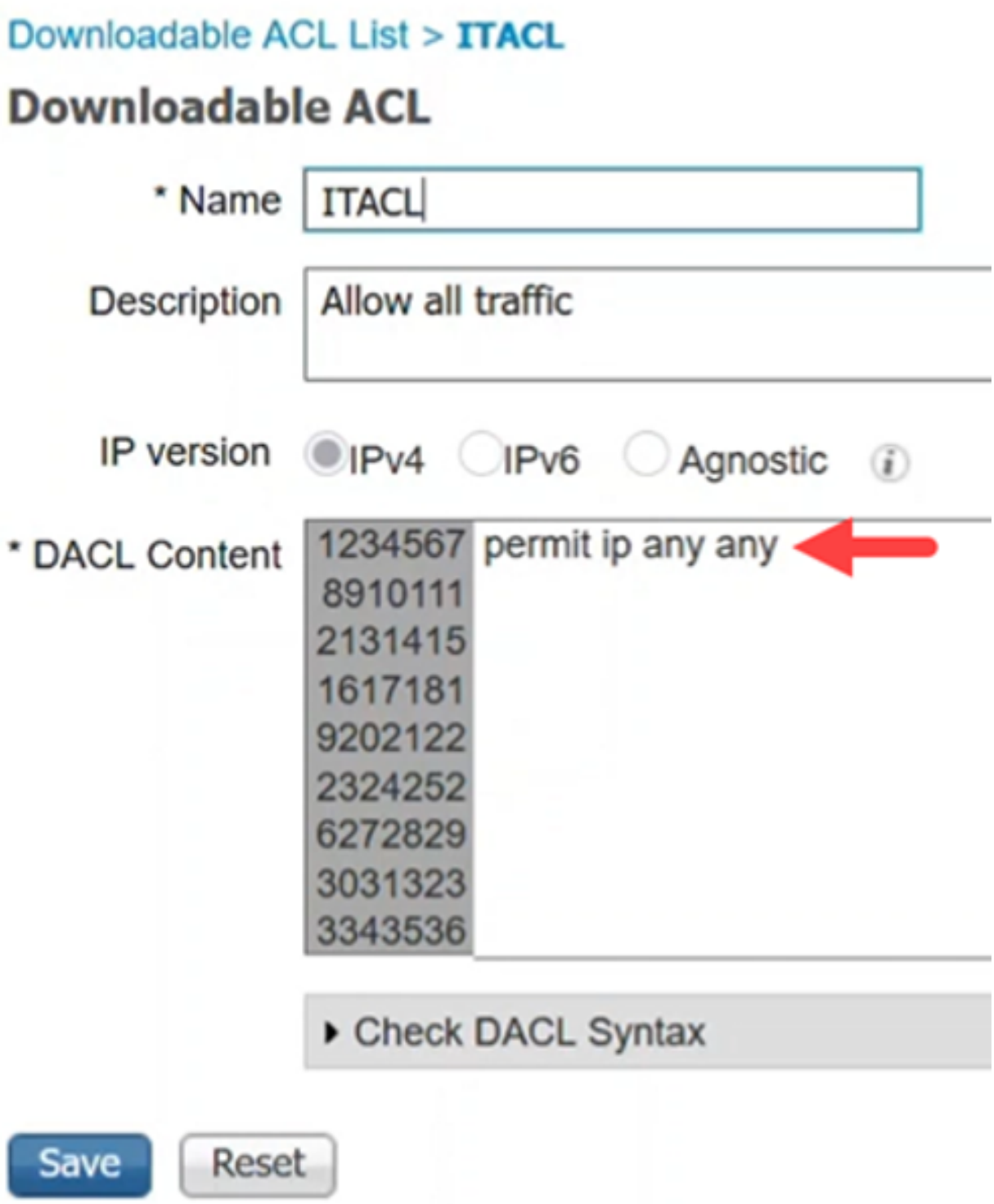
Paso 5

Haga clic en el icono Add para crear la ACL descargable.



Paso 6

Configure el Nombre, la Descripción, seleccione la versión de IP e ingrese las entradas de control de acceso (ACE) que conformarán la ACL descargable en el campo DACL Content. Click Save.



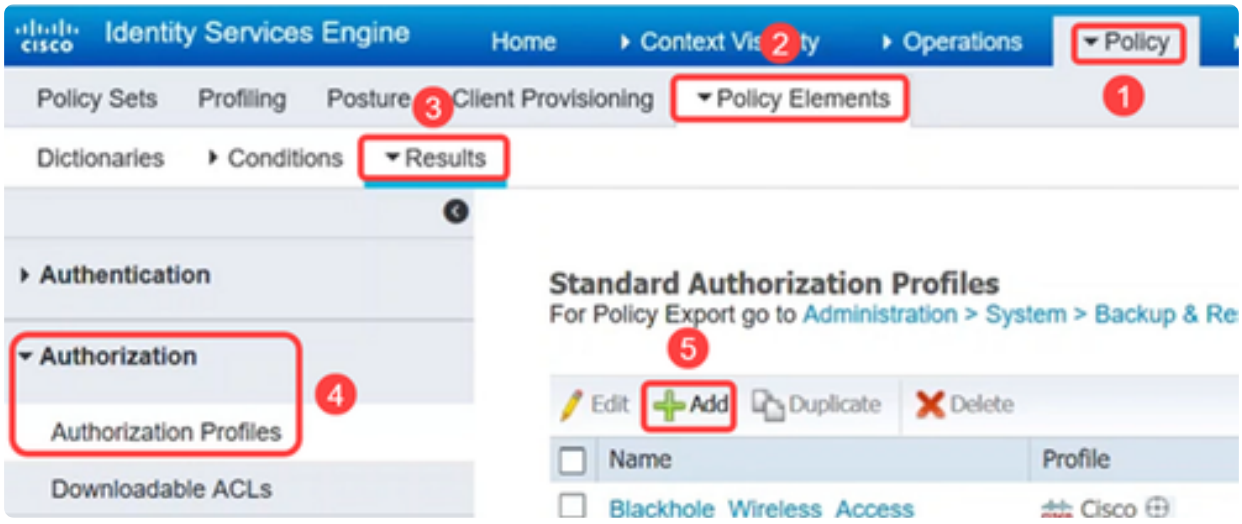
Note:

Sólo se admiten ACL IP y el origen debe ser ANY. Para ACL en ISE, ahora solo se admite IPv4. Si se ingresa una ACL con otro origen, aunque la sintaxis puede ser correcta en lo que respecta a ISE, fallará cuando se aplique al switch.

Paso 7

Cree perfiles de autorización que se utilizarán para asociar lógicamente su DACL y otras políticas dentro de los conjuntos de políticas de ISE.

Para ello, navegue hasta Política > Elementos de política > Resultados > Autorización > Perfiles de autorización y haga clic en Agregar.

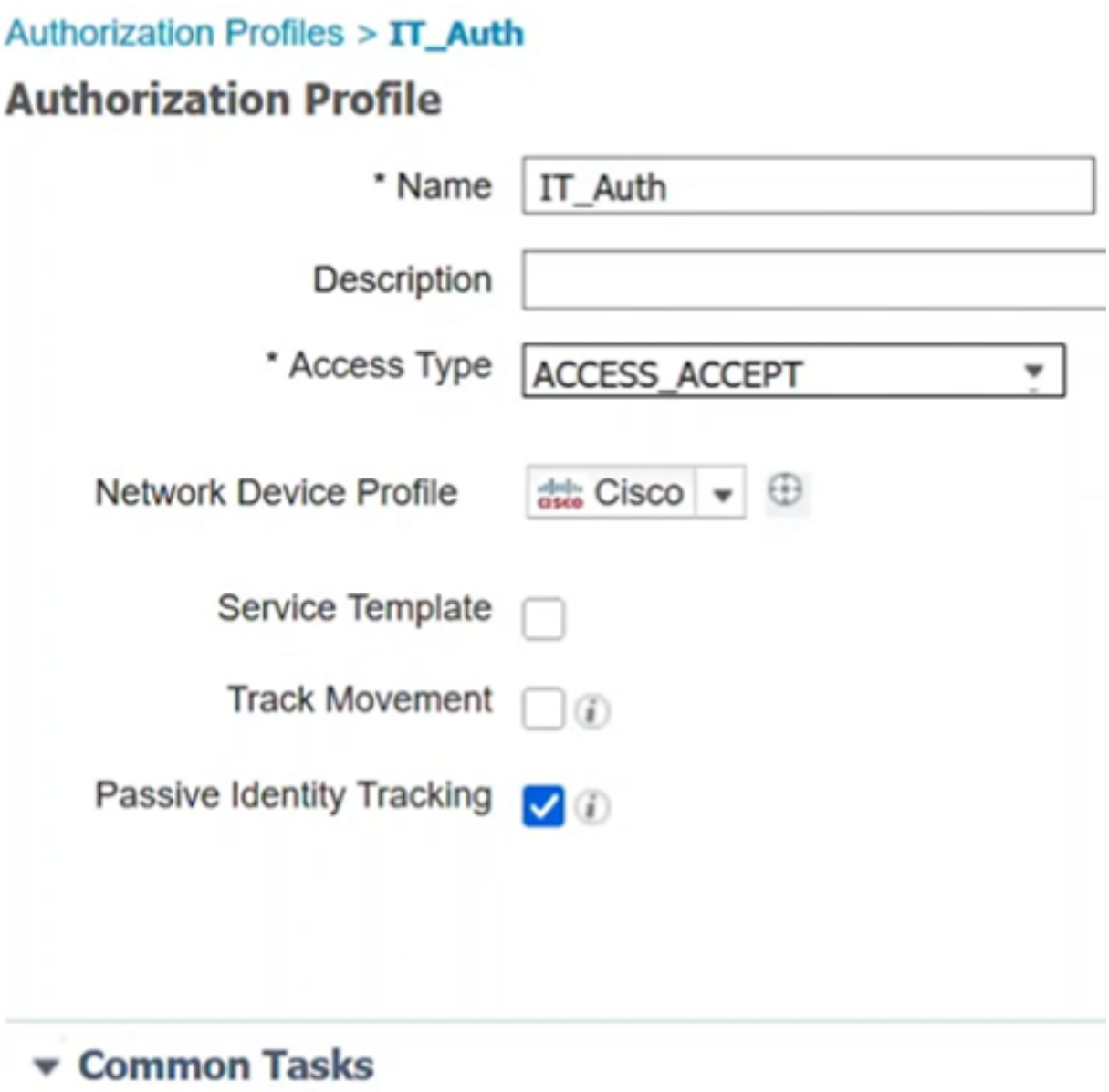


Paso 8

En la página Perfil de autorización, configure lo siguiente:

- Nombre
- Descripción
- Tipo de acceso: debe establecerse en ACCESS_ACCEPT. Si se establece en ACCESS_REJECT, se rechazará la autenticación.
- Network Device Profile: debe seleccionarse como Cisco.
- Seguimiento pasivo de la identidad: es posible que deba activarse para algunos escenarios de autenticación. Es necesario para los escenarios EasyConnect_PassiveID vinculados a AD.
- Tareas comunes: esta sección tiene muchas opciones. Para este ejemplo, se configura DACL Name.

Click Save.



Paso 9

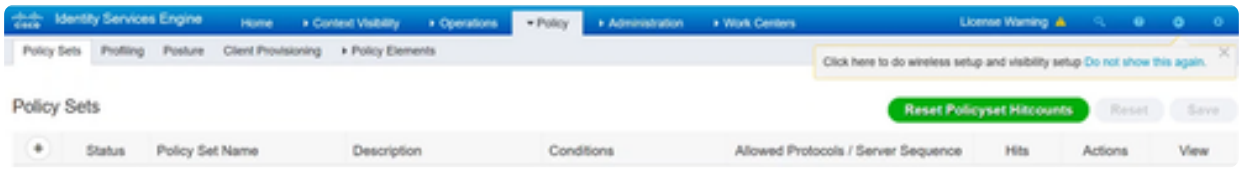
Para configurar conjuntos de directivas que sean agrupaciones lógicas de directivas de autenticación y autorización, haga clic en el menú Directiva > Conjuntos de directivas.

Puede ver lo siguiente al consultar una lista de conjuntos de políticas:

- Estado: una marca de verificación verde indica que está activada, un círculo blanco vacío indica que está desactivada y un icono de ojo es para una configuración solo de monitor.
- Nombre y descripción del conjunto de políticas: se explican por sí mismos
- Condiciones: definen dónde se aplica el conjunto de políticas.
- Protocolos/Secuencia de servidor permitidos: establece controles más avanzados.
- Aciertos: muestra el número de veces que se ha utilizado el conjunto de políticas.
- Acciones: permiten cambiar el orden en el que se pueden aplicar conjuntos de directivas, copiar

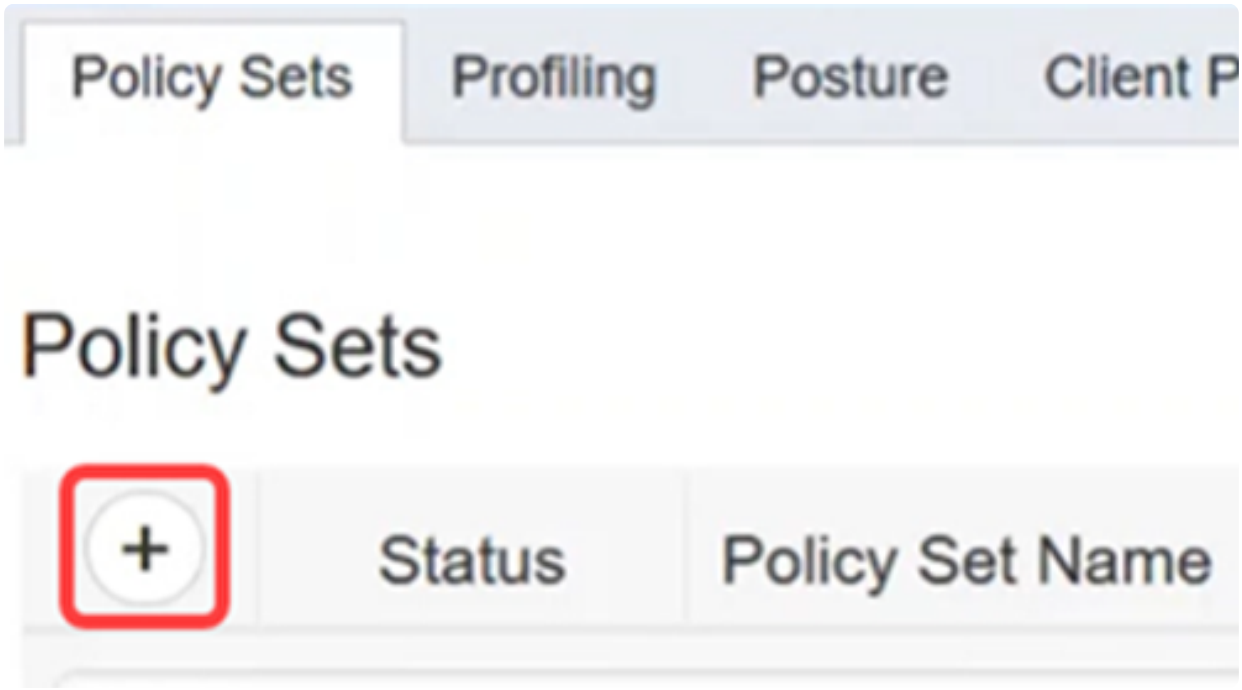
un conjunto de directivas existente o eliminar uno existente.

- Ver: permite editar los detalles del conjunto de políticas.



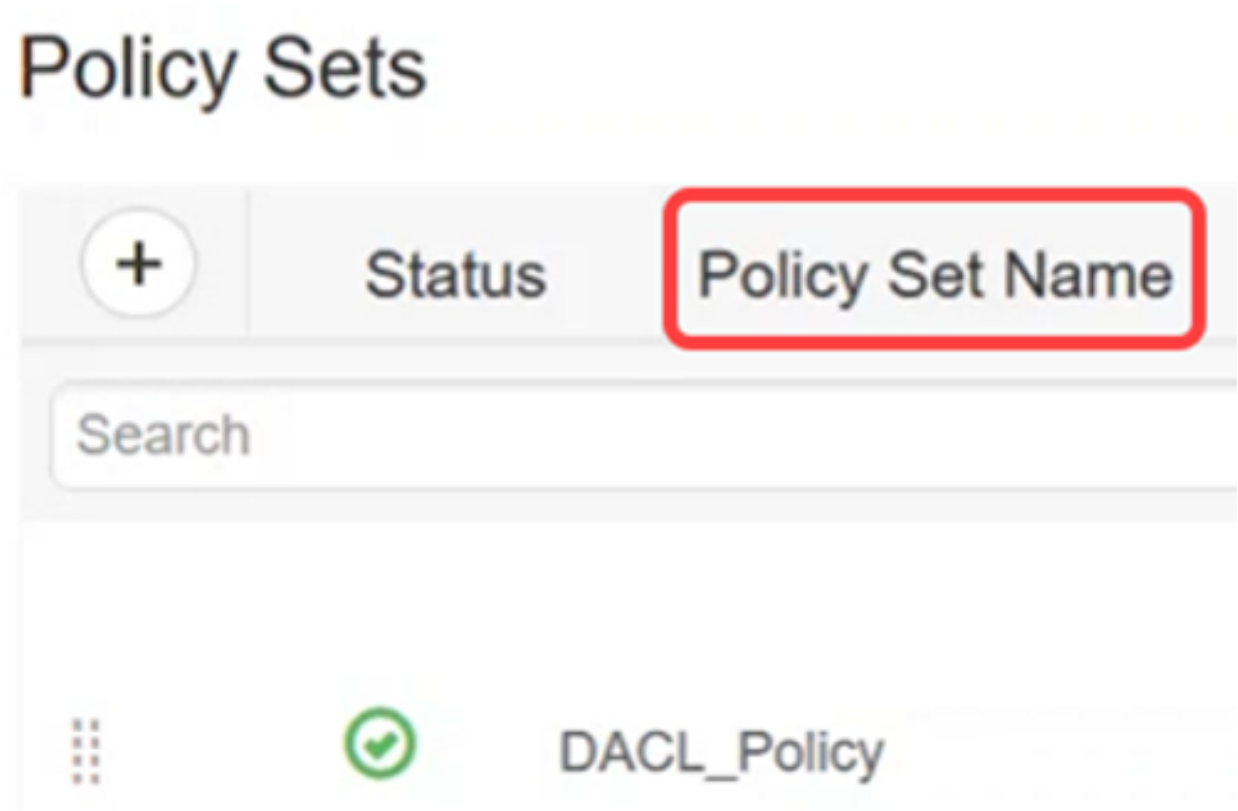
Paso 10

Para crear un conjunto de políticas, haga clic en el botón add.



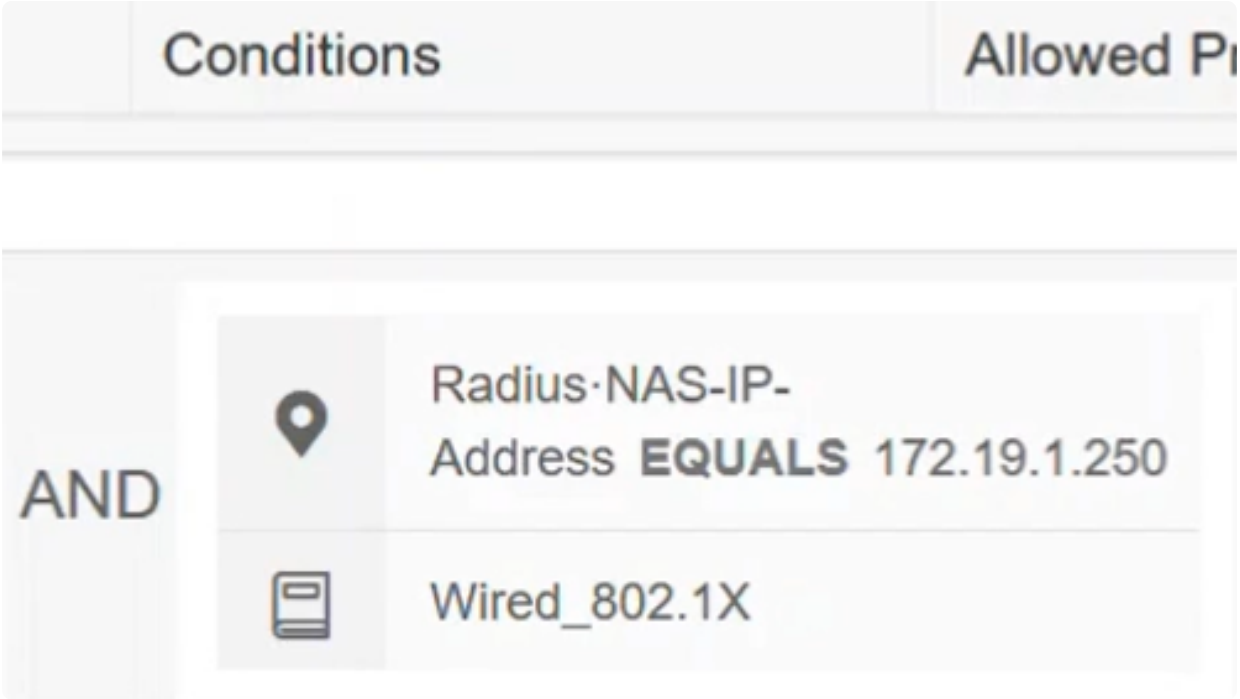
Paso 11

Defina un nombre de conjunto de políticas.



Paso 12

En Condiciones, haga clic en el botón Agregar. Esto abre Conditions Studio, donde puede definir dónde se utilizará este perfil de autenticación. En este ejemplo, se ha aplicado al Radius-NAS-IP-Address (el switch) que es tráfico 172.19.1.250 y wired_802.1x.

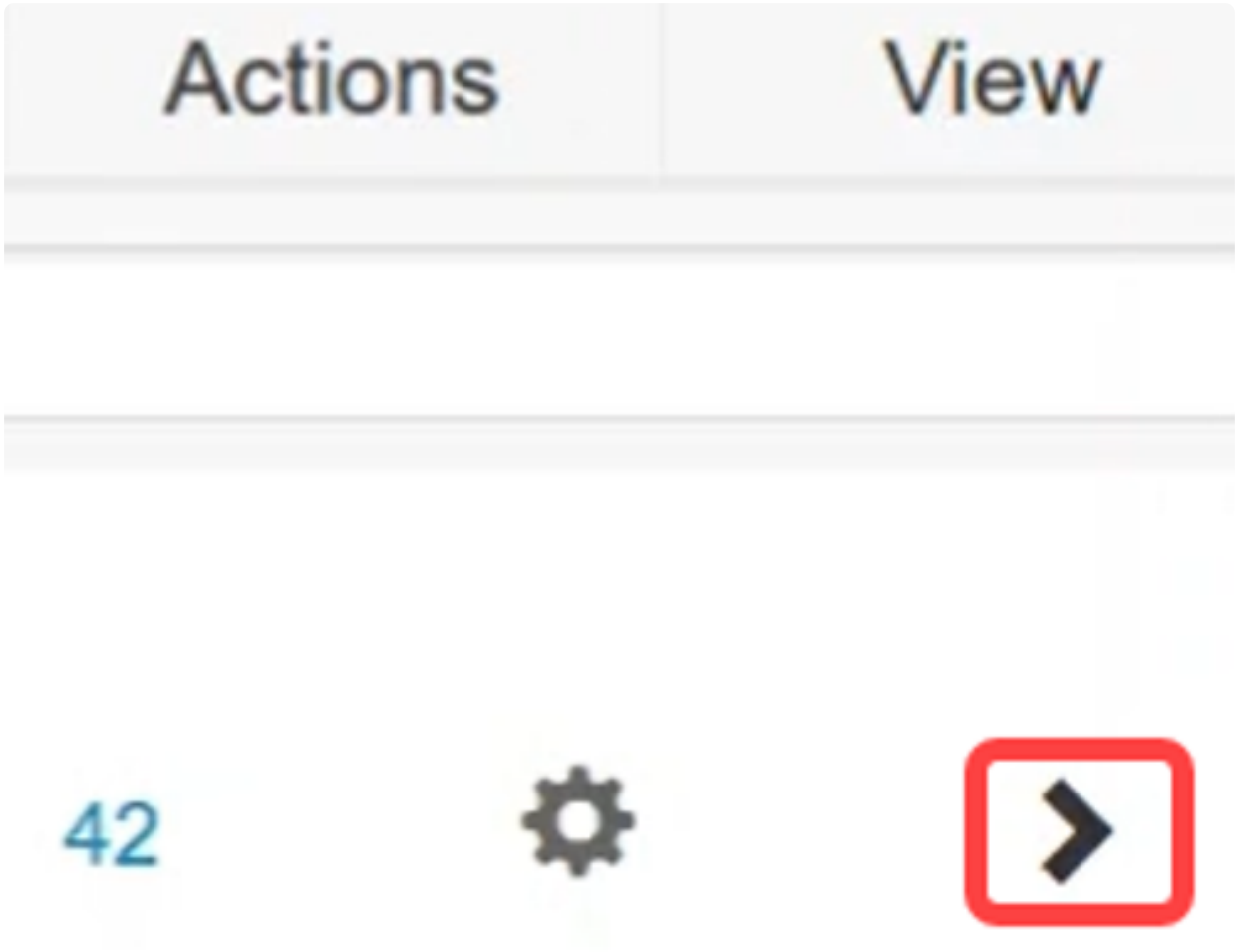


Paso 13

Configure los Protocolos Permitidos para el Acceso a la Red Predeterminado y haga clic en Guardar.

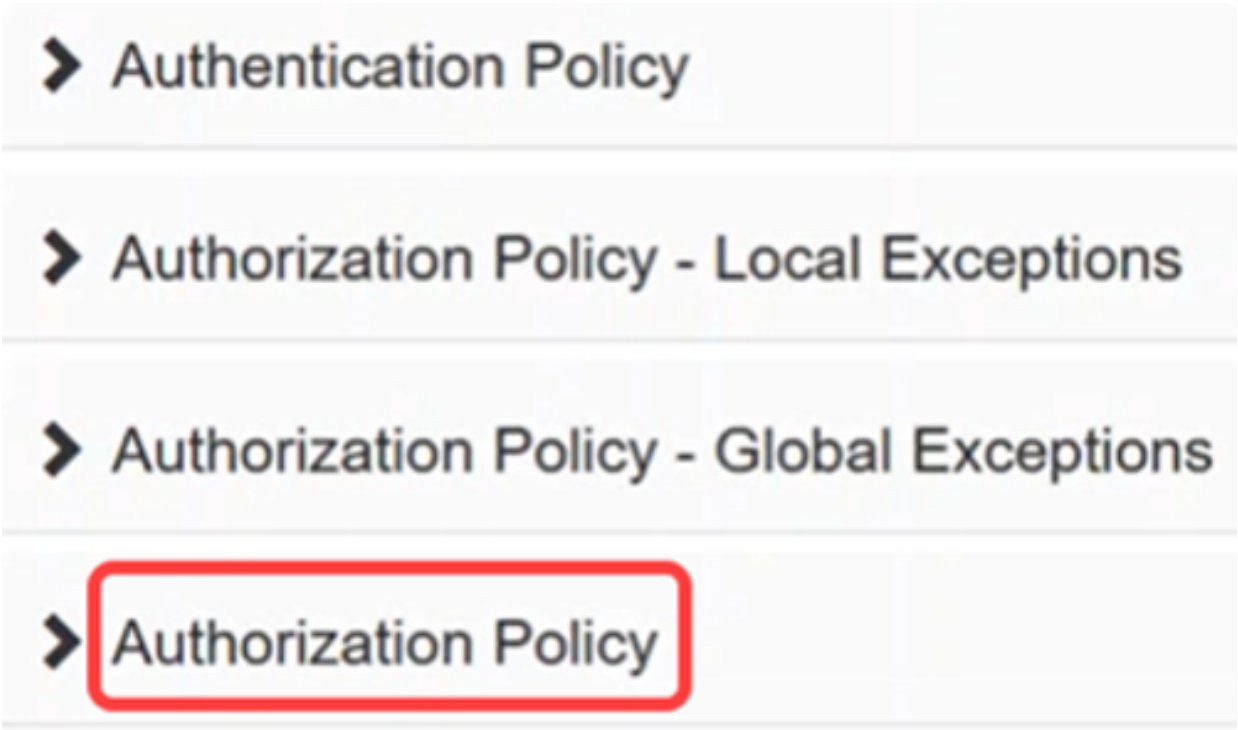
Paso 14

En Ver, haga clic en el icono de flecha para configurar las políticas de autenticación y autorización en función de la configuración y los requisitos de la red o puede elegir los valores predeterminados. En este ejemplo, haga clic en Directiva de autorización.



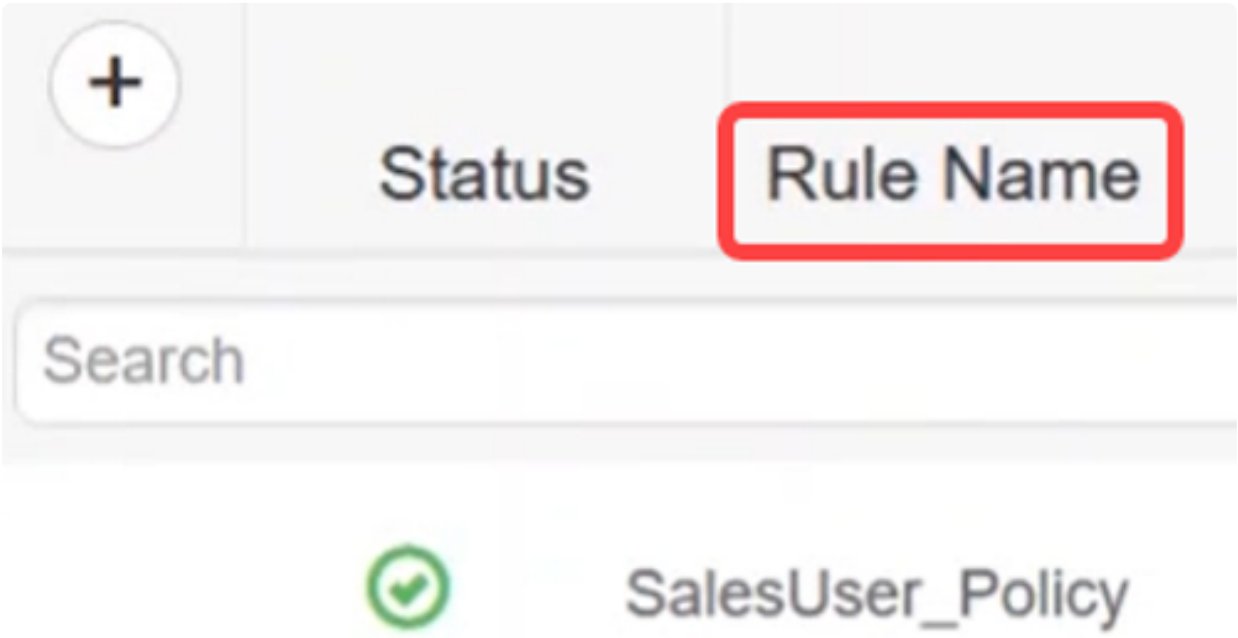
Paso 15

Haga clic en el icono más para agregar una política.



Paso 16

Introduzca el nombre de la regla.



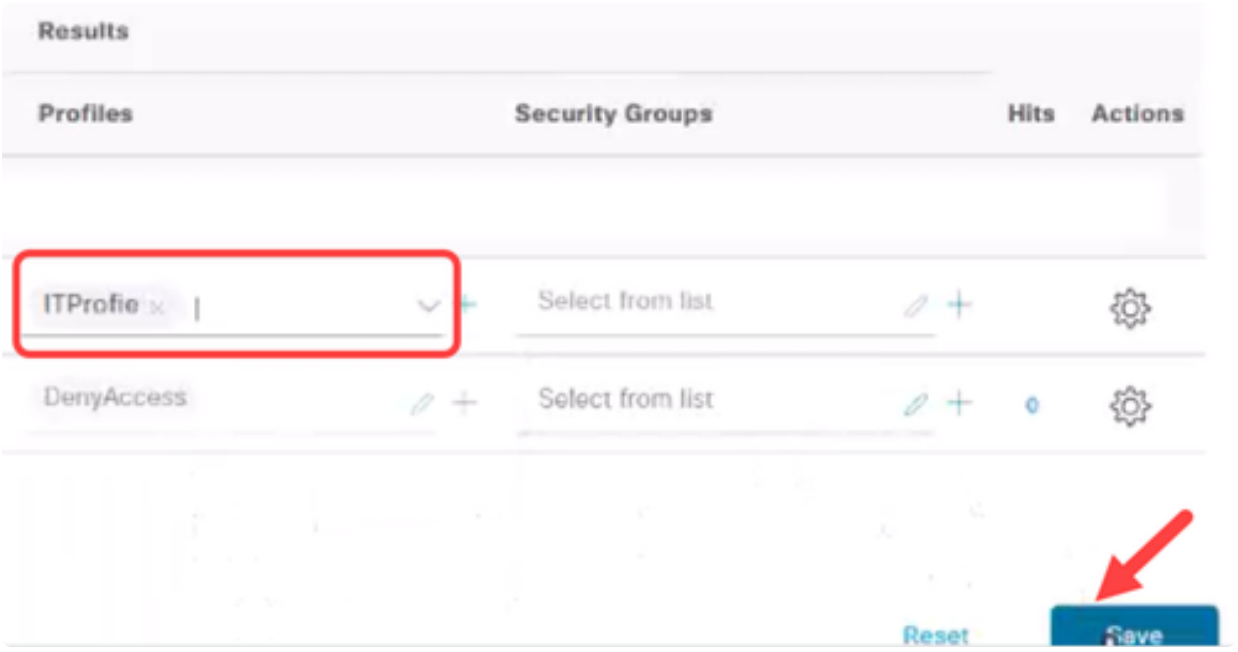
Paso 17

En Condiciones, haga clic en el icono más y seleccione el grupo de identidad. Haga

clic en Usar.

Paso 18

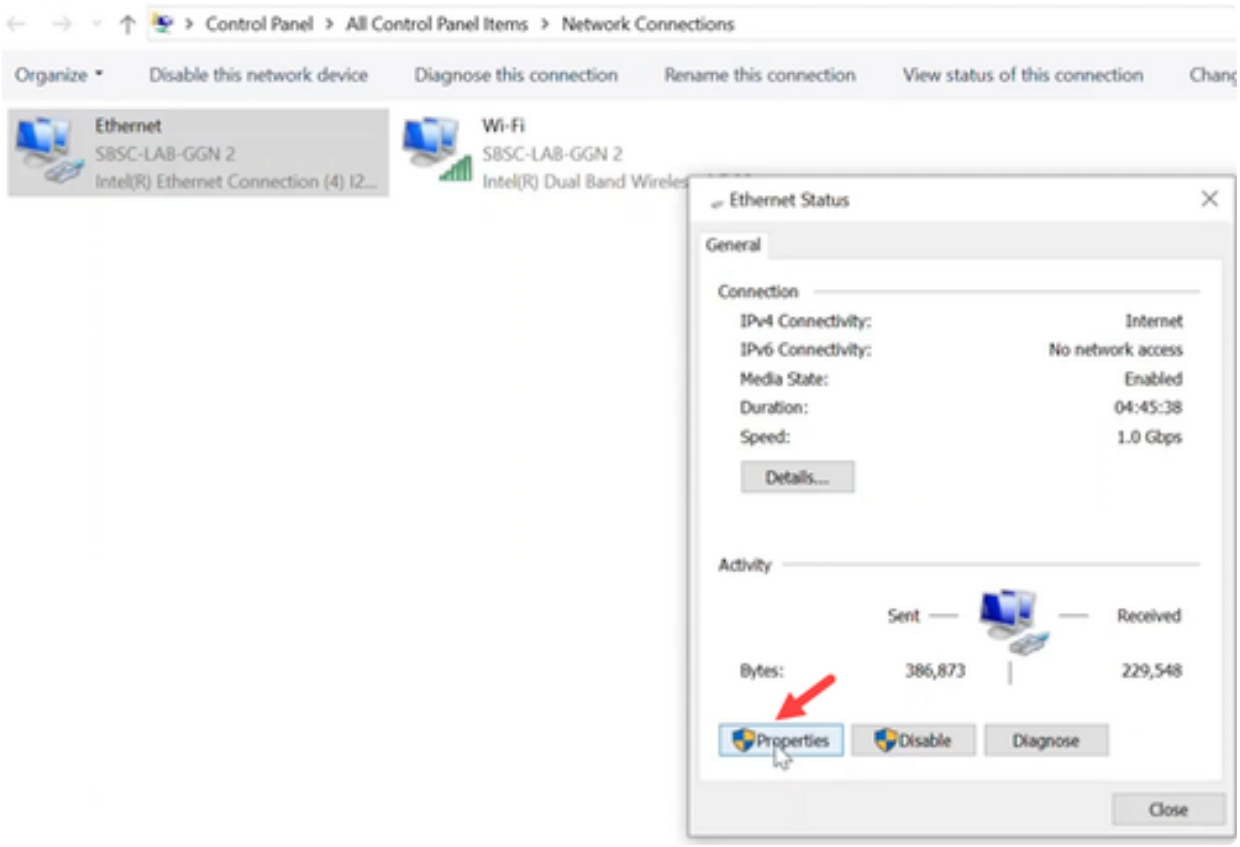
Aplique el perfil necesario y haga clic en Guardar.



Configuraciones de cliente

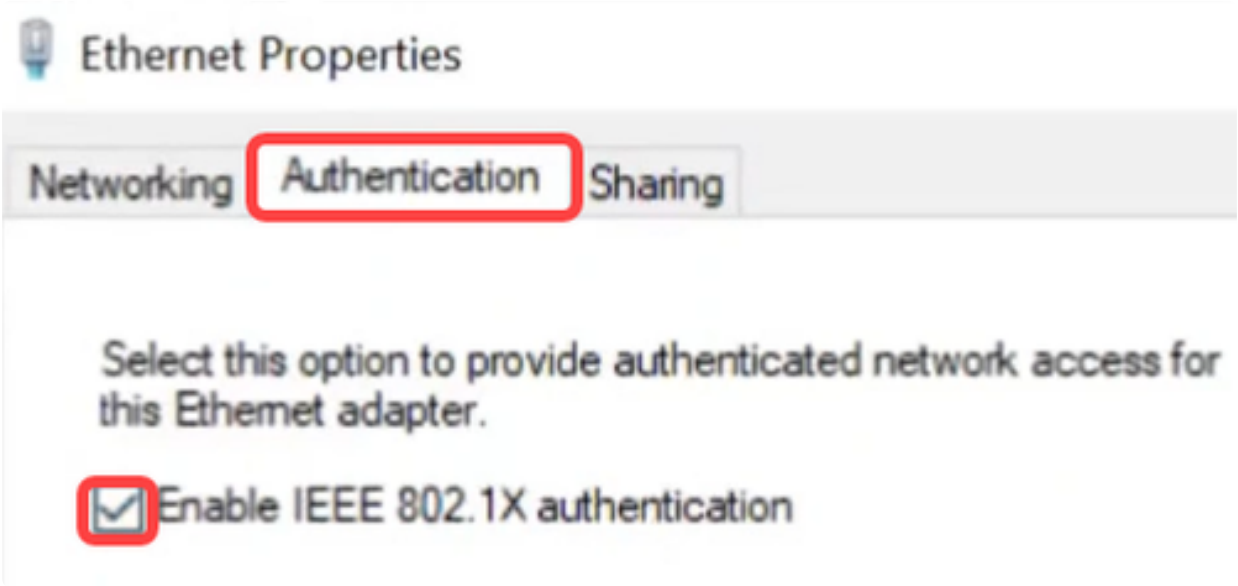
Paso 1

En el equipo portátil del cliente, navegue hasta Conexiones de red > Ethernet y haga clic en Propiedades.



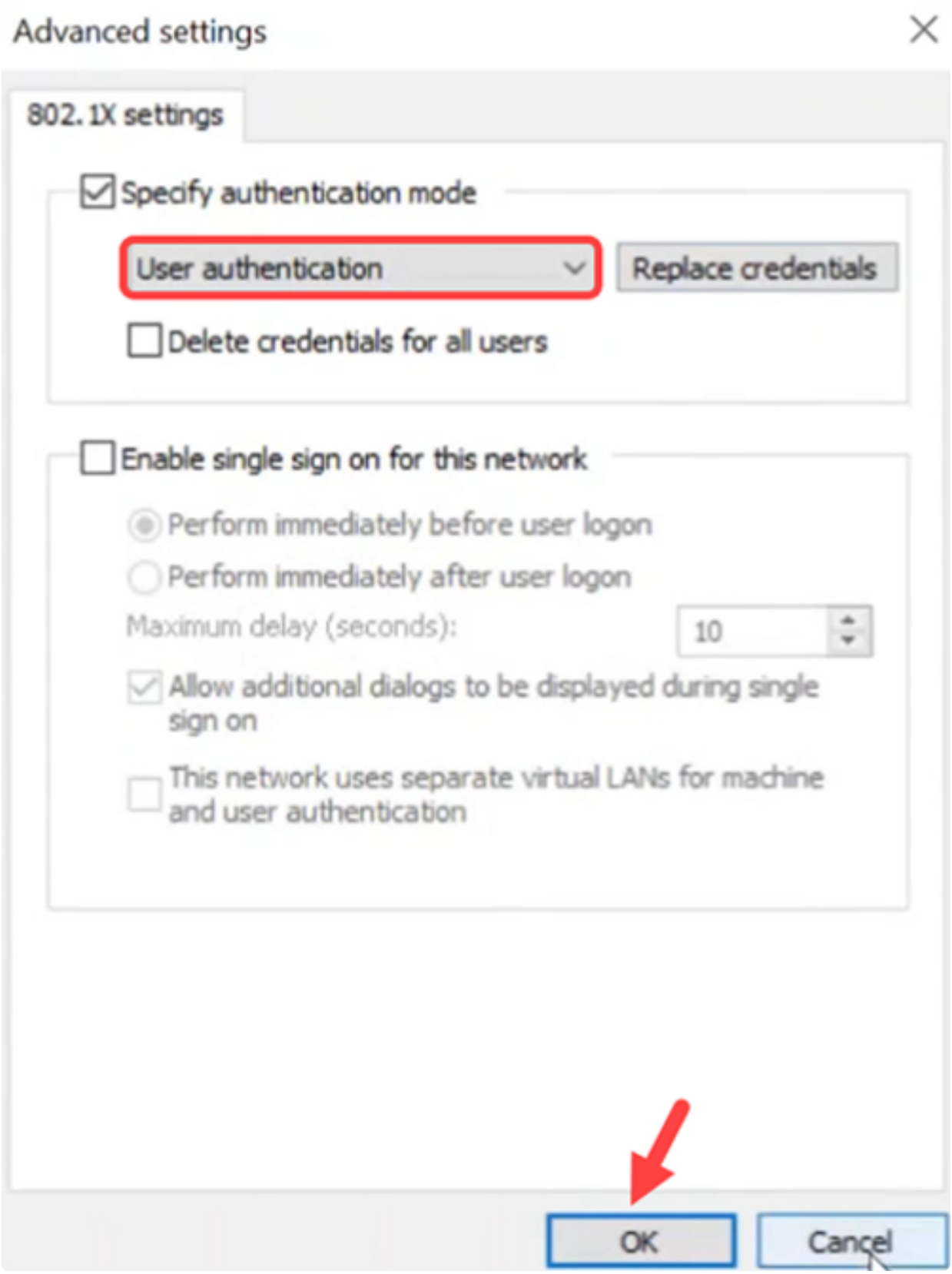
Paso 2

Haga clic en la pestaña Authentication y asegúrese de que la autenticación 802.1X esté habilitada.



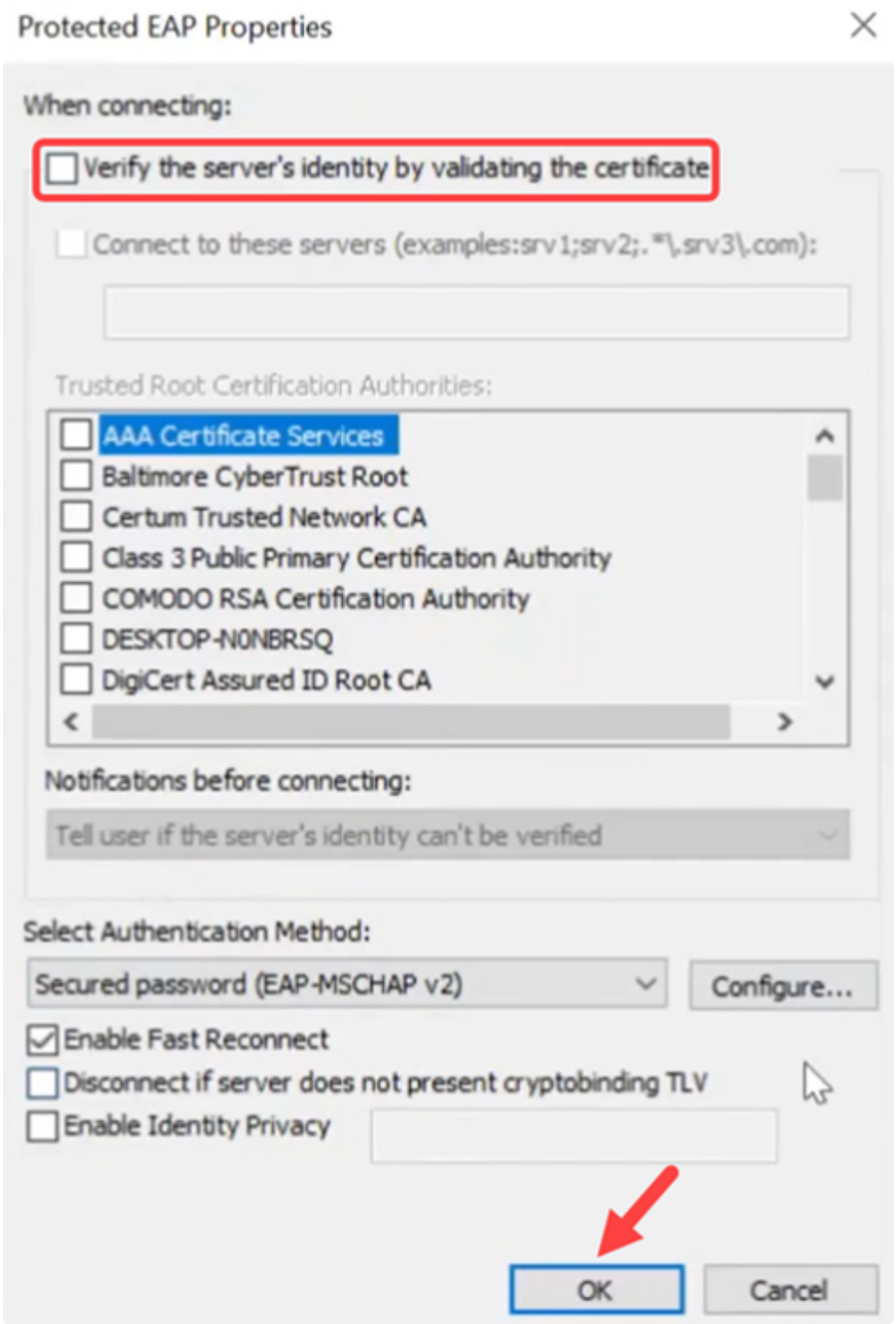
Paso 3

En Configuración adicional, seleccione Autenticación de usuario como modo de autenticación. Haga clic en Save Credentials y luego en OK.



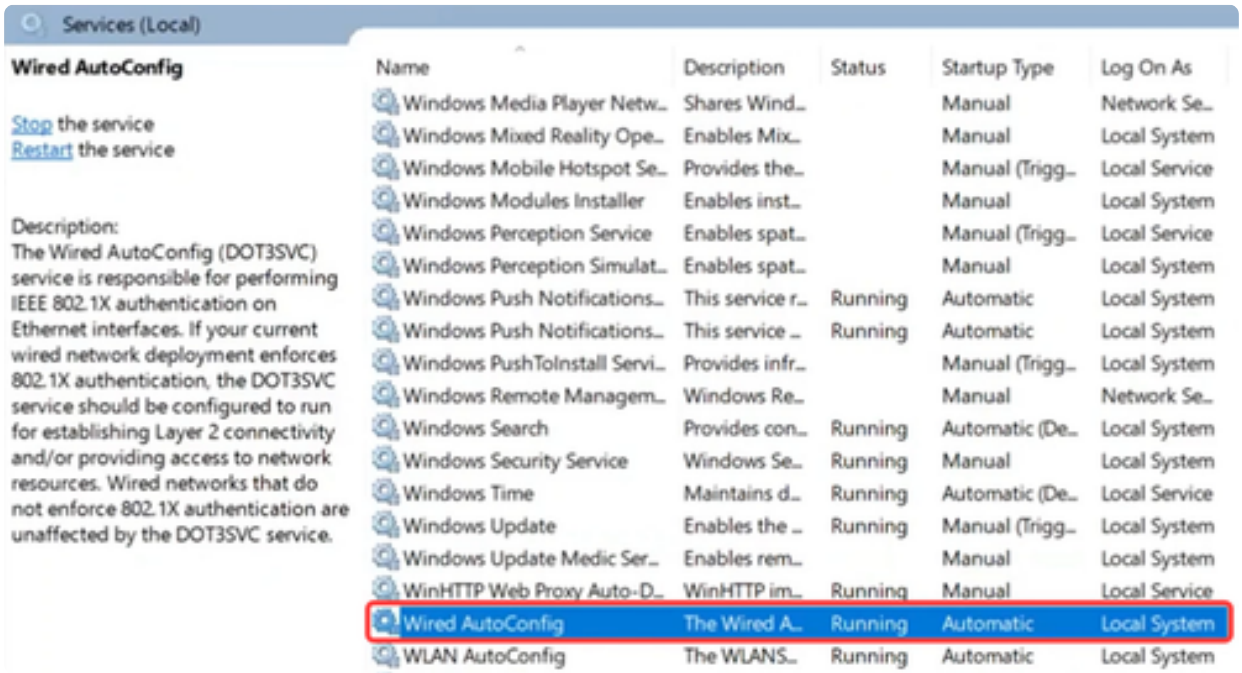
Paso 4

Haga clic en Configuración y asegúrese de que la casilla junto a Verificar la identidad del servidor validando el certificado esté desactivada. Click OK.


Protected EAP Properties
When connecting:
Verify the server's identity by validating the certificate
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):
Trusted Root Certification Authorities:
AAA Certificate Services
Baltimore CyberTrust Root
Certum Trusted Network CA
Class 3 Public Primary Certification Authority
COMODO RSA Certification Authority
DESKTOP-N0NBRSQ
DigiCert Assured ID Root CA
Notifications before connecting:
Tell user if the server's identity can't be verified
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
Configure...
Enable Fast Reconnect
Disconnect if server does not present cryptobinding TLV
Enable Identity Privacy
OK
Cancel

Paso 5

En Services, habilite Wired AutoConfig.

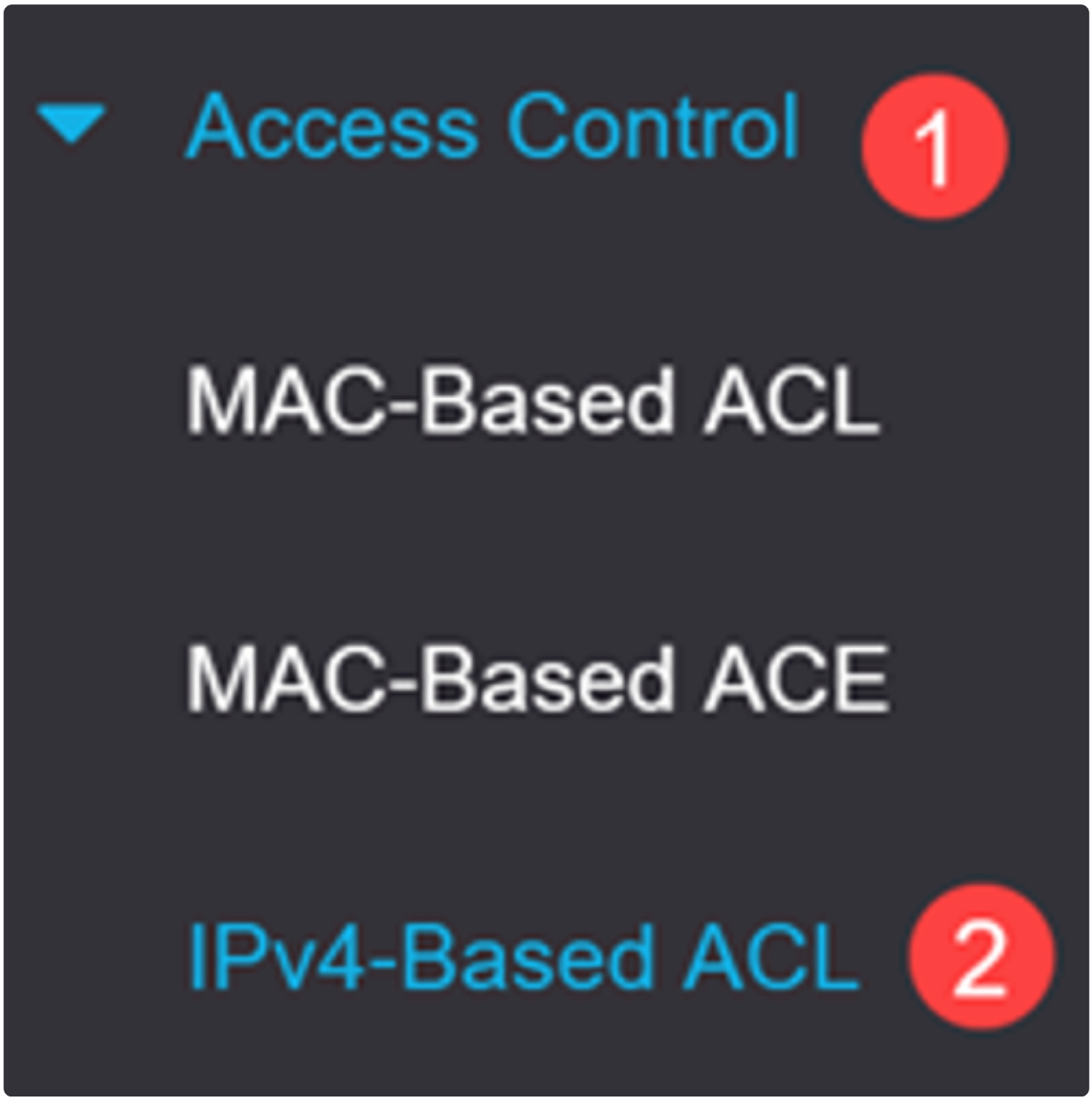


Verificación de DACL

Una vez autenticado el usuario, puede verificar la ACL descargable.

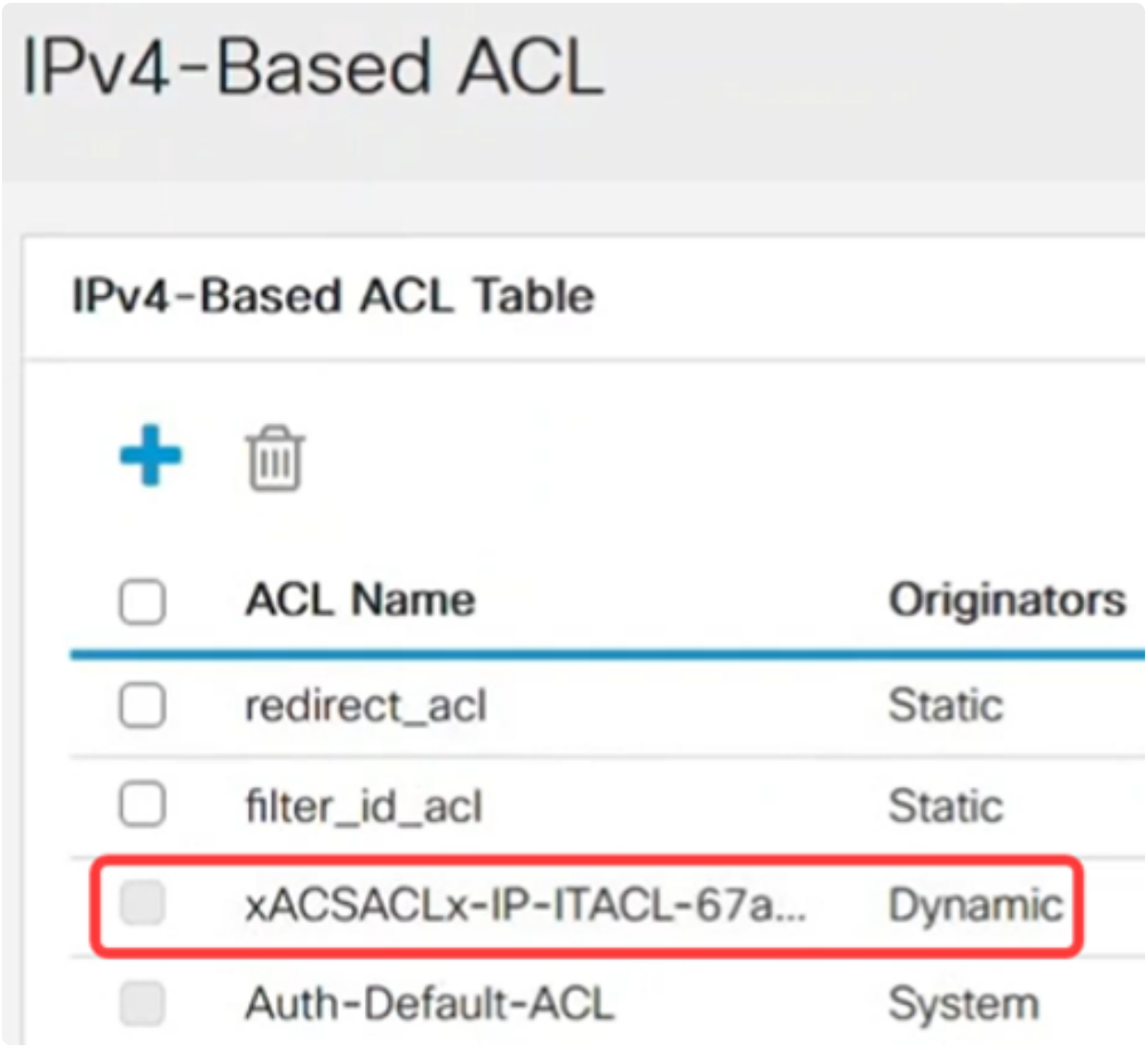
Paso 1

Inicie sesión en el switch Catalyst 1300 y navegue hasta Access Control > IPv4-Based ACL menu.



Paso 2

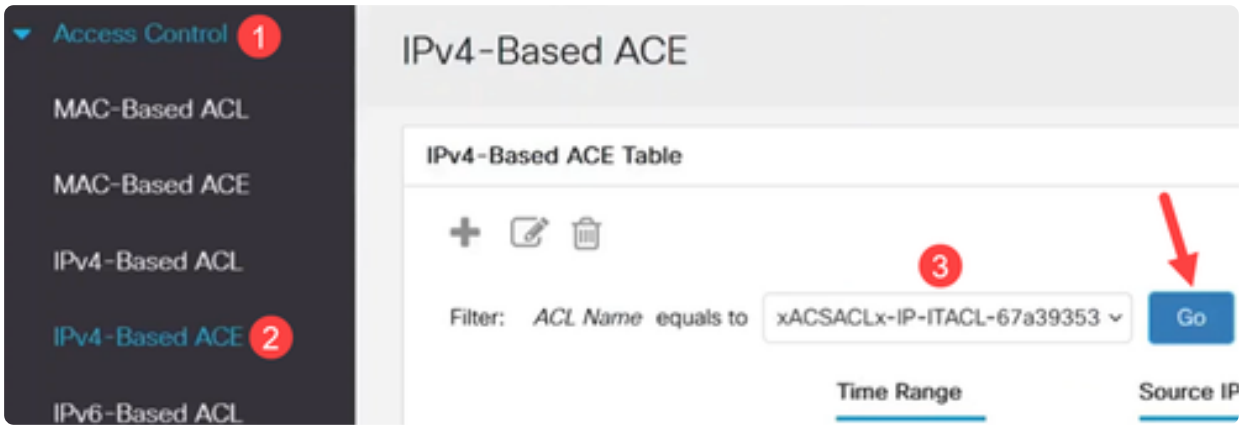
La Tabla ACL Basada en IPv4 mostrará la ACL descargada.



Note:
Las ACL descargables no se pueden editar.

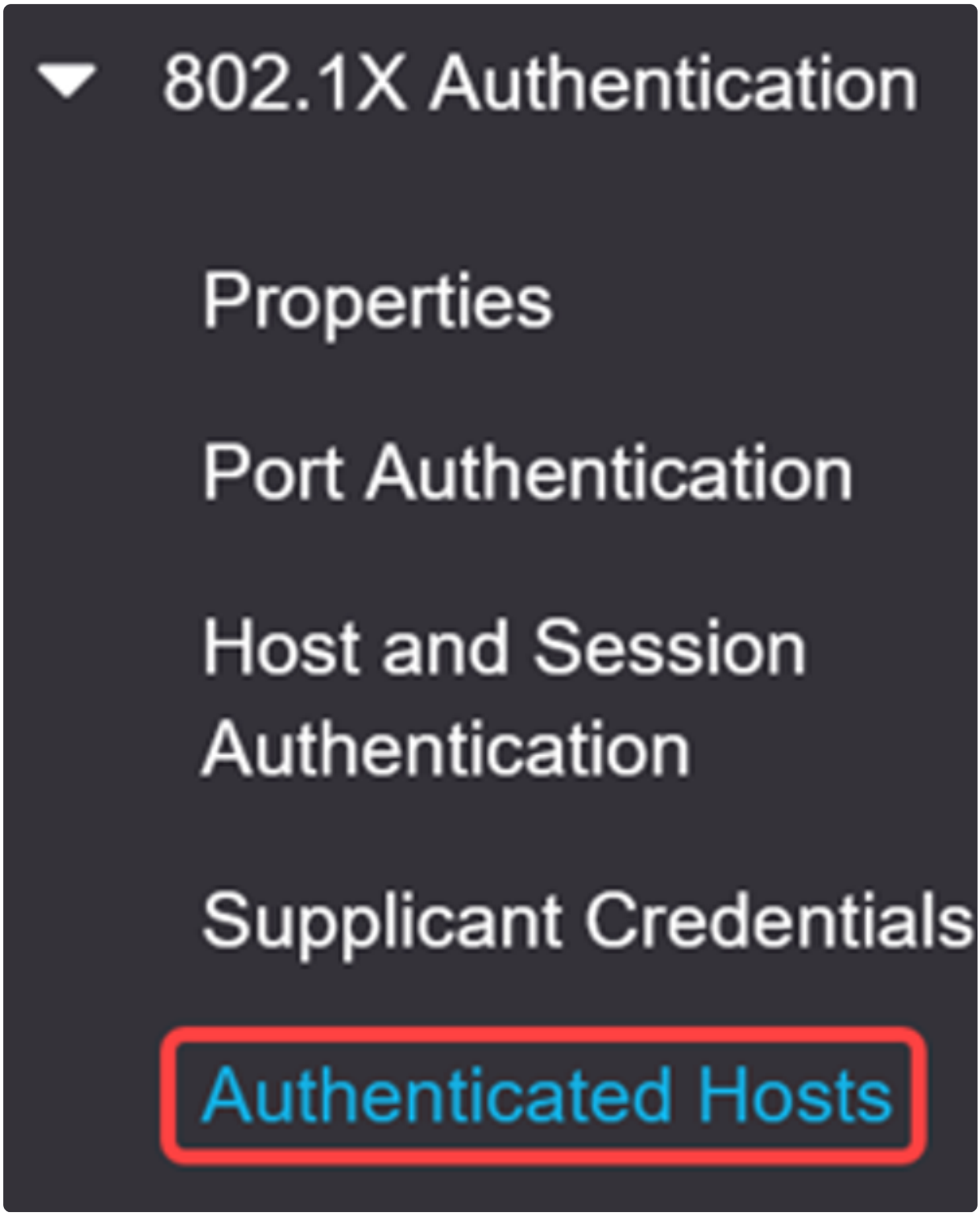
Paso 3

Otra forma de verificarlo es navegar a la ACE basada en IPv4, seleccionar la ACL descargable del menú desplegable Nombre de ACL y hacer clic en Ir. Se mostrarán las reglas que se han configurado en ISE.



Paso 4

Vaya al menú Security > 802.1 Authentication > Authenticated Hosts . Puede comprobar los usuarios autenticados. Haga clic en Authenticated Sessions para ver más detalles.



Paso 5

Desde la CLI, ejecute el comando show ip access-lists interface seguido del ID de interfaz.

En este ejemplo, se pueden ver las ACL y ACE aplicadas a Gigabit Ethernet 3.

```
switch4a7d55#show ip access-lists interface ge1/0/3
ip access-list extended xACSACLx-IP-SalesACL-6760399d
    deny    ip any host 192.168.251.10 ace-priority 1
    permit  ip any any ace-priority 2
ip access-list extended Auth-Default-ACL
    permit  udp any any any domain ace-priority 20
    permit  tcp any any any domain ace-priority 40
    permit  udp any bootps any any ace-priority 60
    permit  udp any any any bootpc ace-priority 80
    permit  udp any bootpc any any ace-priority 100
    deny    ip any any ace-priority 120
```

Paso 6

También puede ver la configuración relacionada con la conexión ISE y las descargas de ACL mediante el comando

show dot1x sessions interface <ID> detailed. Puede ver el estado, el estado de autenticación 802.1x y las ACL descargadas.

```
switch4a7d55#show dot1x sessions interface ge1/0/3 detailed

          Interface: gi1/0/3
        MAC Address: e4:[redacted]:31
       IPv4 Address: 192.168.251.11
          User-Name: user5
             Status: Authorized
     Oper host mode: multi-host
    Session timeout: N/A
     Session Uptime: 196 sec
  Common Session ID: 14FBA8C00500032222C35D9E
    Acct Session ID: 0x05000322
 Server Policies:
            ACS ACL: xACSACLx-IP-SalesACL-6760399d

 Method status list:
    Method                  State
    802.1x                  Authentication success
```

Conclusión

¡Ahí tienes! Ahora ya sabe cómo funciona la ACL descargable en los switches Cisco Catalyst 1300 con Cisco ISE.

Para obtener más información, consulte la Guía de administración de Catalyst 1300 y la Página de soporte de Cisco Catalyst 1300 Series.

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).