Configuración del Cambio de Autorización en Catalyst 1300 Usando la Interfaz de Usuario Web

Objetivo

El objetivo de este artículo es mostrarle cómo configurar el cambio de autorización (CoA) en los switches Catalyst 1300 mediante la interfaz de usuario (UI) web.

Dispositivos y versiones de software aplicables

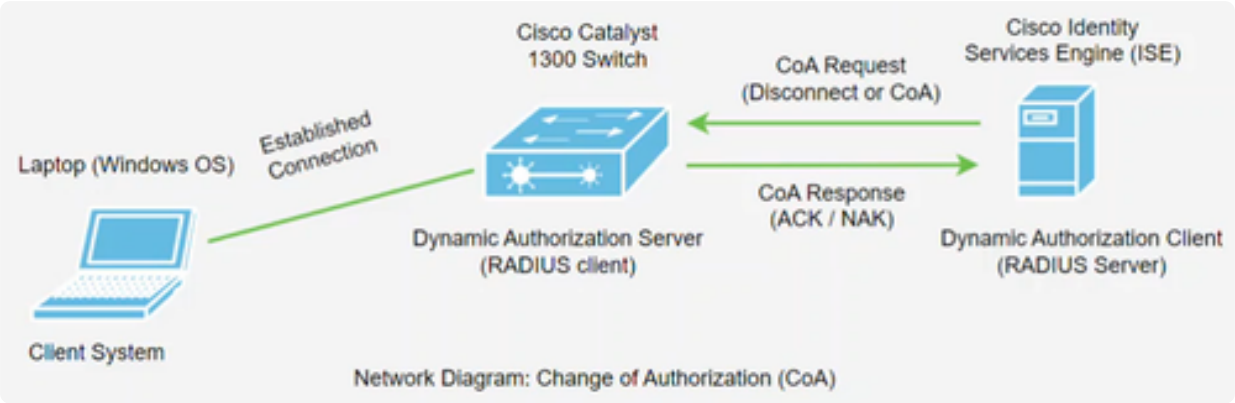
- switches Catalyst 1300 |4.1.6.53

Introducción

Change of Authorization (CoA) es una extensión del protocolo RADIUS que permite cambiar las propiedades de una sesión de usuario de autenticación, autorización y administración de cuentas (AAA) o dot1x después de que se haya autenticado. Cuando cambia una política para un usuario o grupo en AAA, los administradores pueden transmitir paquetes CoA de RADIUS desde el servidor AAA, como Cisco Identity Services Engine (ISE), para reiniciar la autenticación y aplicar la nueva política.

Cisco Identity Services Engine (o ISE) es un motor de aplicación de políticas y control de acceso basado en red con todas las funciones. Proporciona análisis y aplicación de seguridad, servicios RADIUS y TACACS, distribución de políticas y mucho más. Cisco ISE es actualmente el único cliente de autorización dinámica de CoA compatible para los switches Catalyst 1300. Consulte la guía ISE Admin para obtener más información.

Esta función requiere comunicación entre el cliente de autorización dinámica (servidor RADIUS) y el servidor de autorización dinámica (switch Catalyst). Como se observa en el diagrama de red siguiente, el Servidor de autorización dinámica envía un mensaje de desconexión o CoA al Servidor de autorización dinámica y el switch proporciona una respuesta.



Network Diagram: Change of Authorization (CoA)

El soporte de CoA se ha agregado a los switches Catalyst 1300 en la versión de firmware 4.1.3.36. Esto incluye soporte para desconectar usuarios y cambiar autorizaciones aplicables a una sesión de usuario. El dispositivo admite las siguientes acciones de CoA:

- Sesión de desconexión
- Desactivar el comando CoA del puerto del host
- Comando Bounce host port CoA
- Comando Reauthenticate Host CoA

Para configurar CoA mediante la interfaz de línea de comandos (CLI), consulte Configuración del cambio de autorización en el switch Catalyst 1300 mediante CLI.

Table Of Contents

Configuración de Catalyst 1300 RADIUS Client en ISE

En este ejemplo, se utiliza el servidor Cisco ISE versión 3.2. Para obtener una descripción general de ISE, consulte la página del producto Cisco Identity Services Engine.

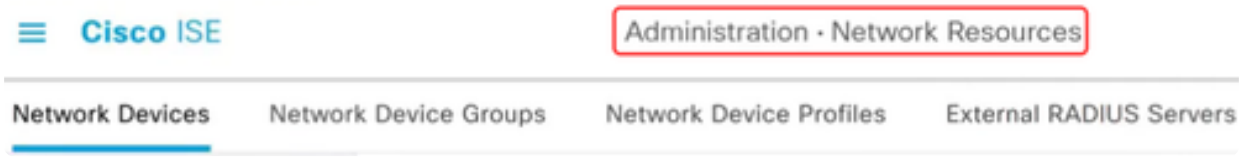
> **Note:**
> CoA es compatible con ISE versión 2.7 y posteriores.

Después de implementar el servidor Cisco ISE, inicie sesión para acceder a la interfaz

de usuario web.

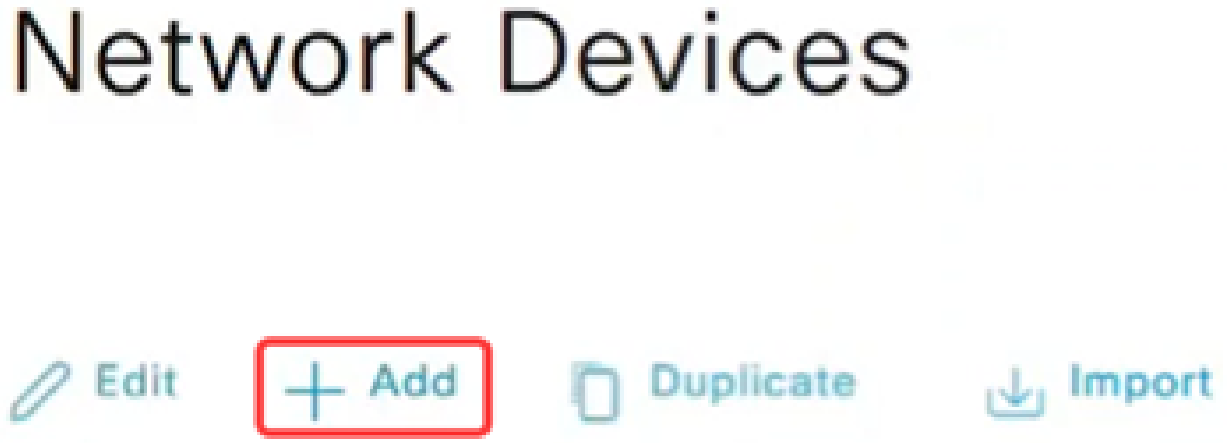
Paso 1

Para agregar dispositivos de red, navegue hasta el menú Administration > Network Resources.



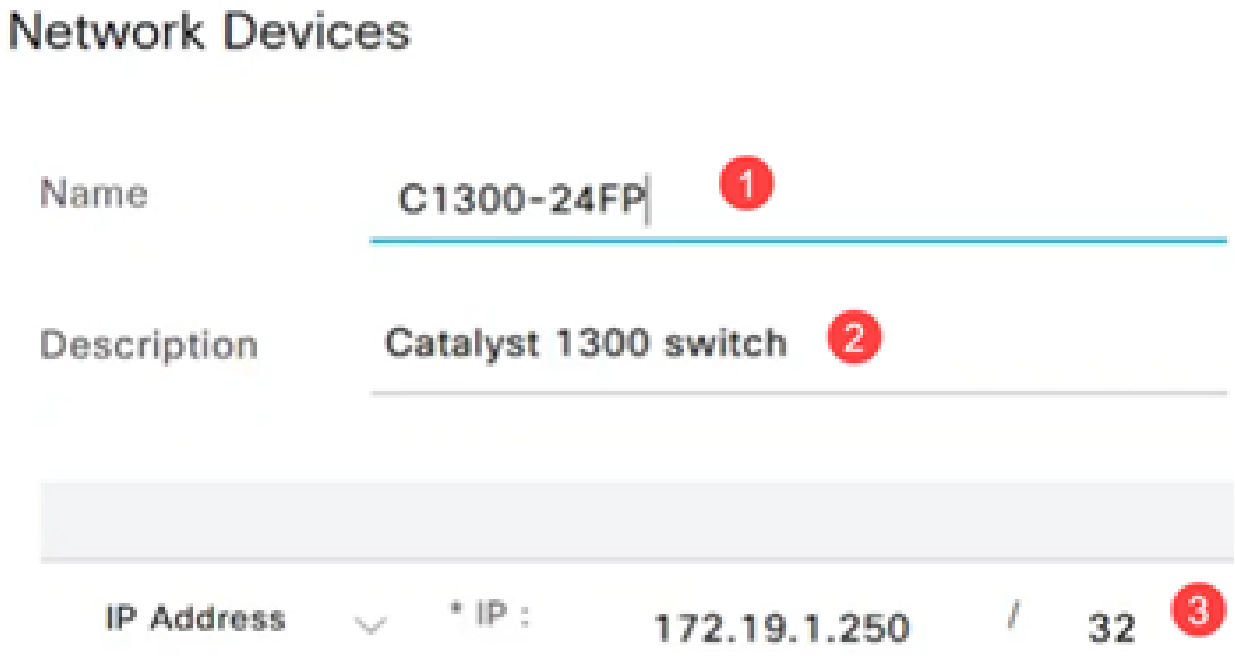
Paso 2

Haga clic en el botón + Add.



Paso 3

Ingrese el Nombre, la Descripción y la dirección IP del switch Catalyst.

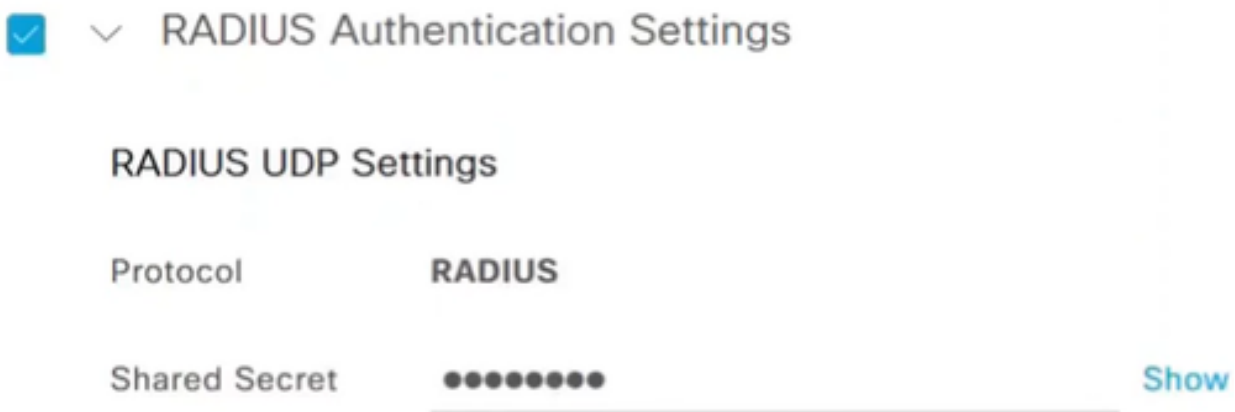


Paso 4

En el menú desplegable Device Profile, seleccione Cisco.

Paso 5

Configure los parámetros de autenticación RADIUS ingresando el secreto compartido.



Paso 6

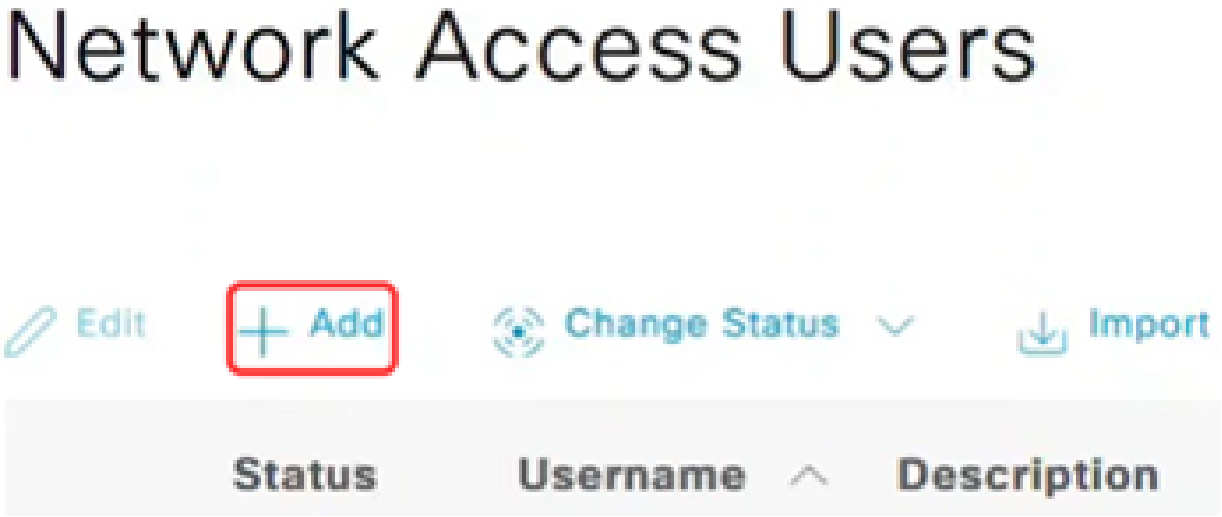
Introduzca el número de puerto CoA. El puerto predeterminado es 1700.

Paso 7

A continuación, vaya a Administration > Identity Management y seleccione Network Access Users.

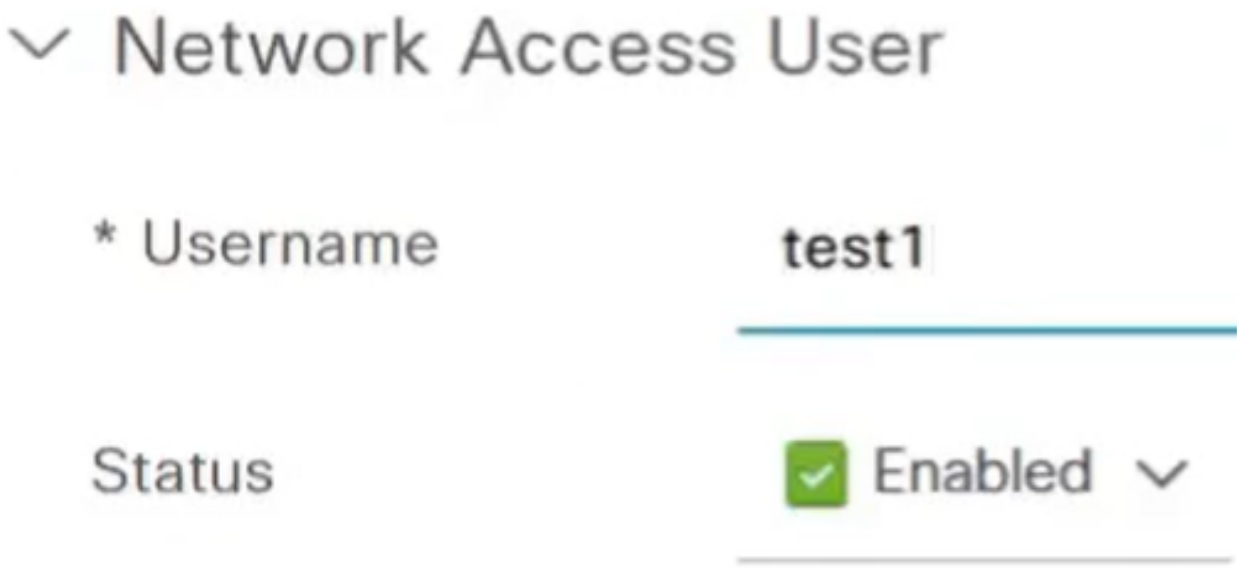
Paso 8

Para definir el nombre de usuario y la contraseña, haga clic en el símbolo +Add.



Paso 9

Introduzca el nombre de usuario y la contraseña y haga clic en Guardar en la parte inferior de la página.



Configuraciones en el switch Catalyst 1300

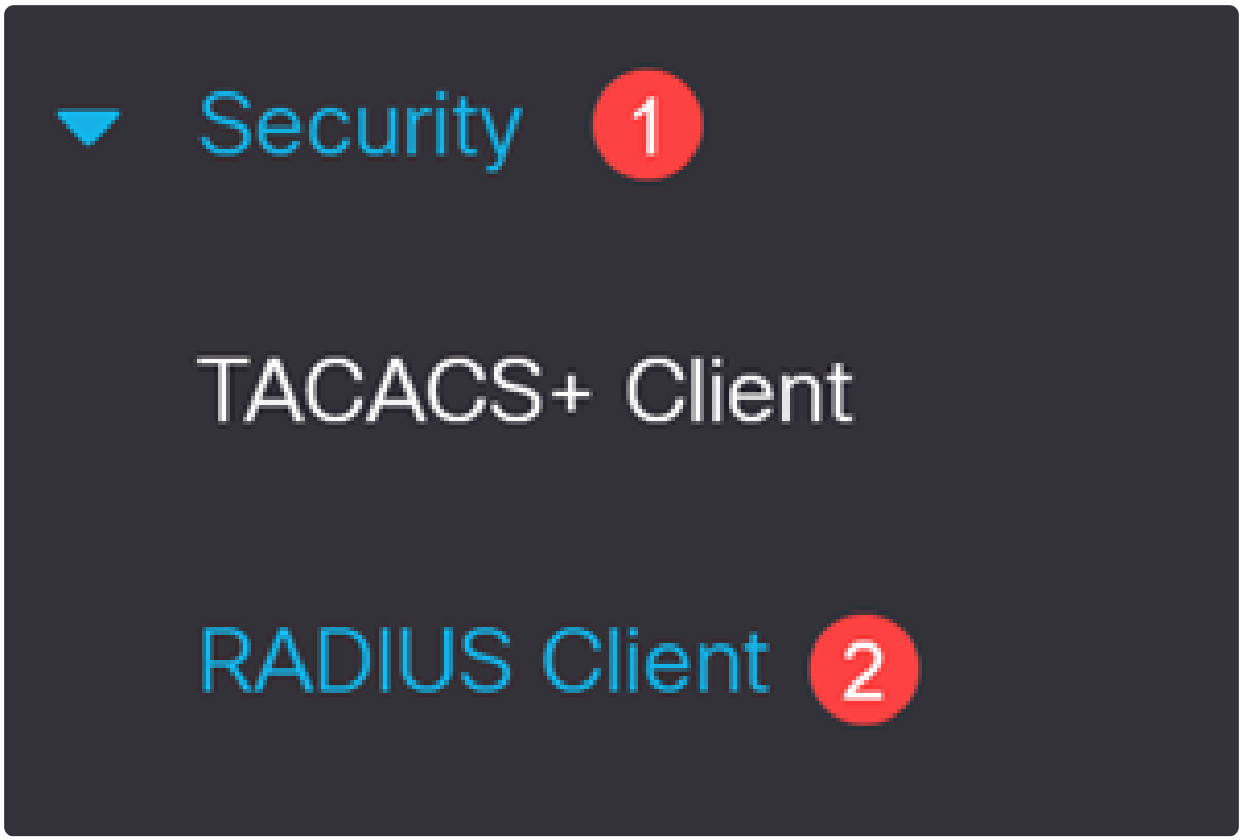
Paso 1

Inicie sesión en el switch Catalyst 1300 y seleccione el modo avanzado. En este ejemplo, se utiliza C1300-24FP-4X.

> Note:
> La compatibilidad con CoA se ha agregado a los switches Catalyst 1300 en la versión de firmware 4.1.3.36.

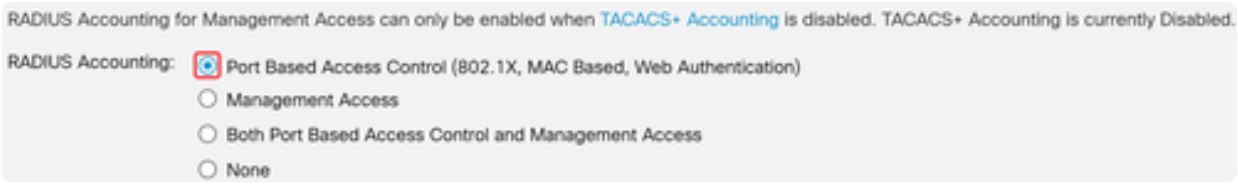
Paso 2

Navegue hasta Security > RADIUS Client en el panel de navegación.



Paso 3

Establezca RADIUS Accounting en Port Based Access Control.



Paso 4

Para agregar el servidor ISE, desplácese hacia abajo hasta la tabla RADIUS y haga clic en el icono más.

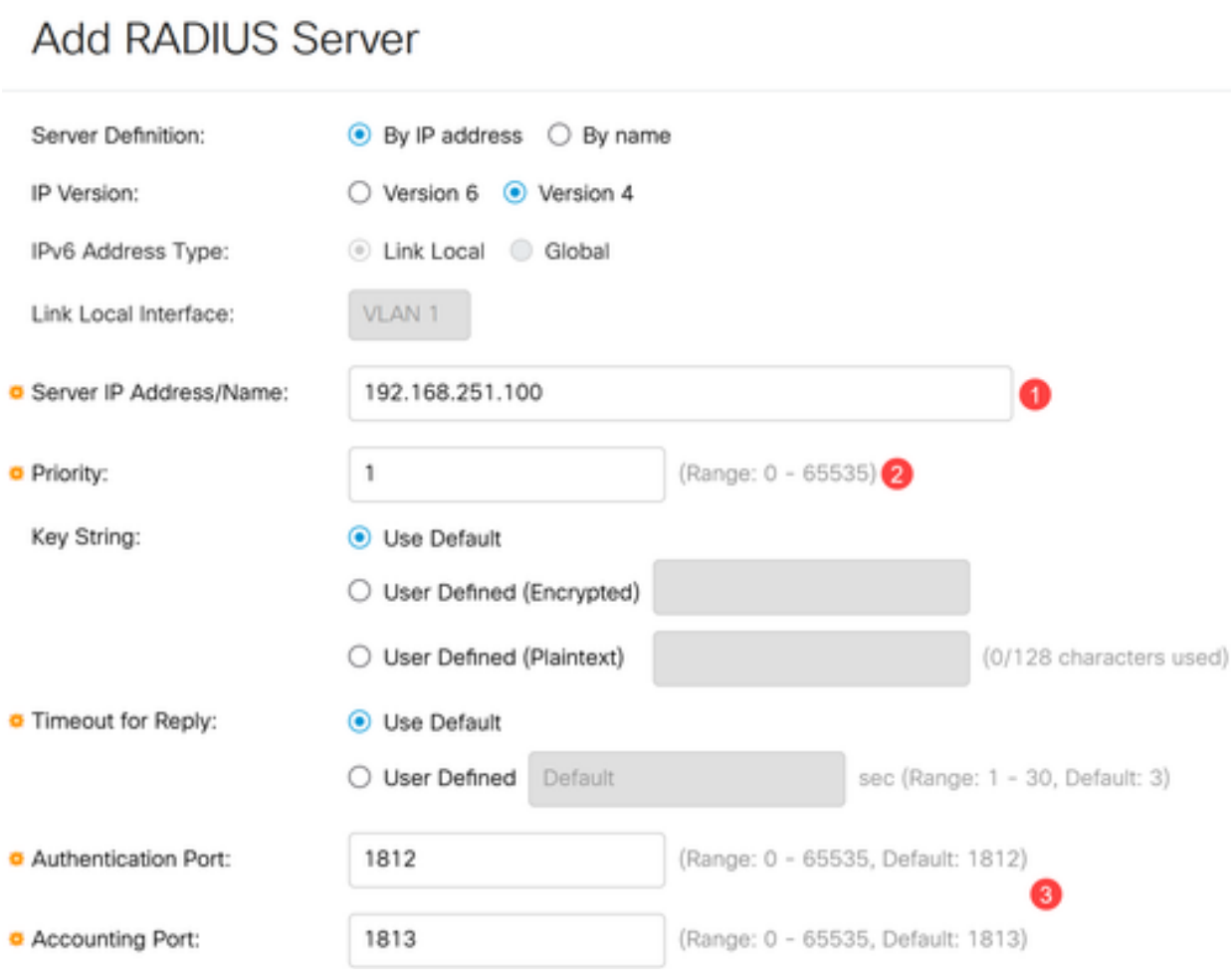
Paso 5

Configure los parámetros del servidor RADIUS.

- Seleccione Server Definition. En este ejemplo, se selecciona Por dirección IP. Introduzca la dirección IP en el campo Server IP Address/Name.
- Establezca una prioridad RADIUS.

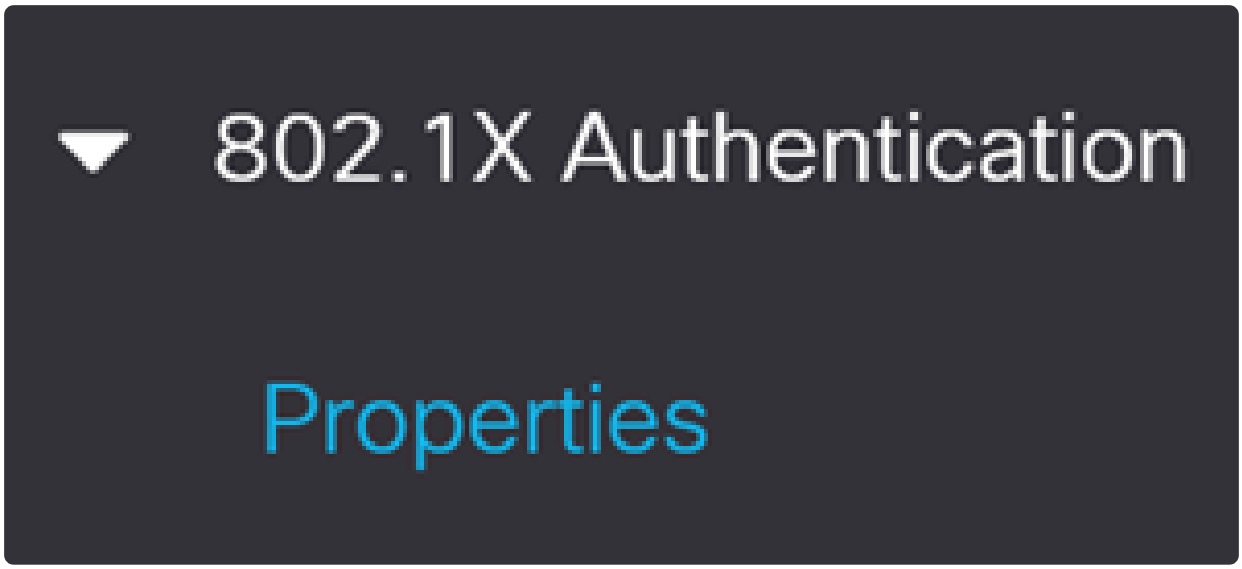
- Los puertos de autenticación y cuentas están configurados en el valor predeterminado.
- El tipo de uso es 802.1x.

Haga clic en Apply (Aplicar).



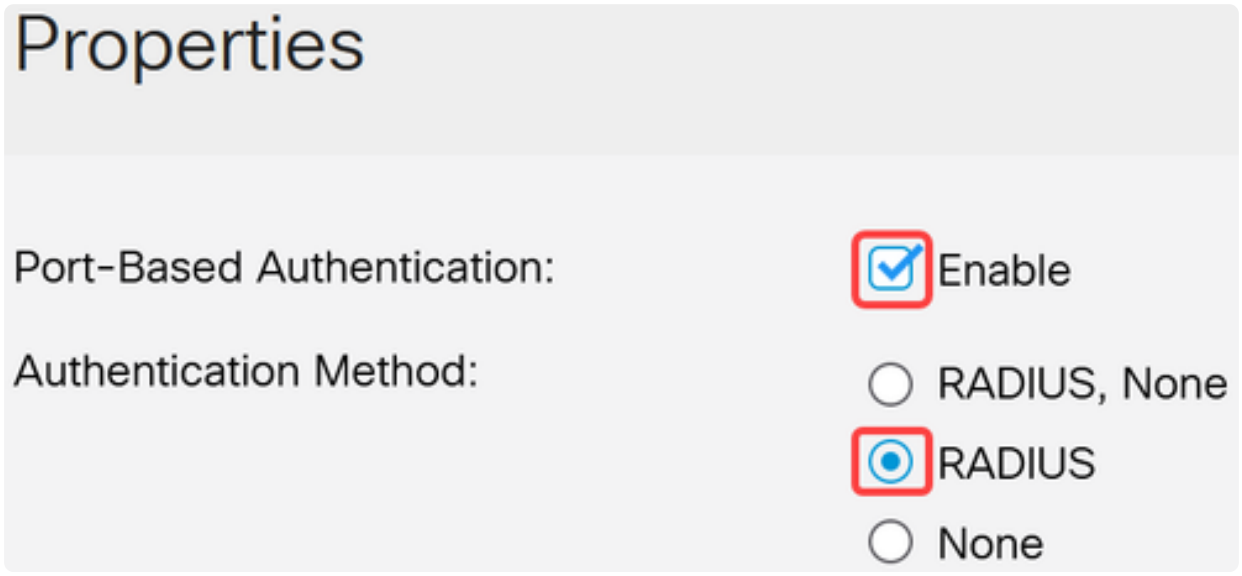
Paso 6

Para configurar la autenticación 802.1x, vaya al menú Seguridad > Autenticación 802.1X > Propiedades.



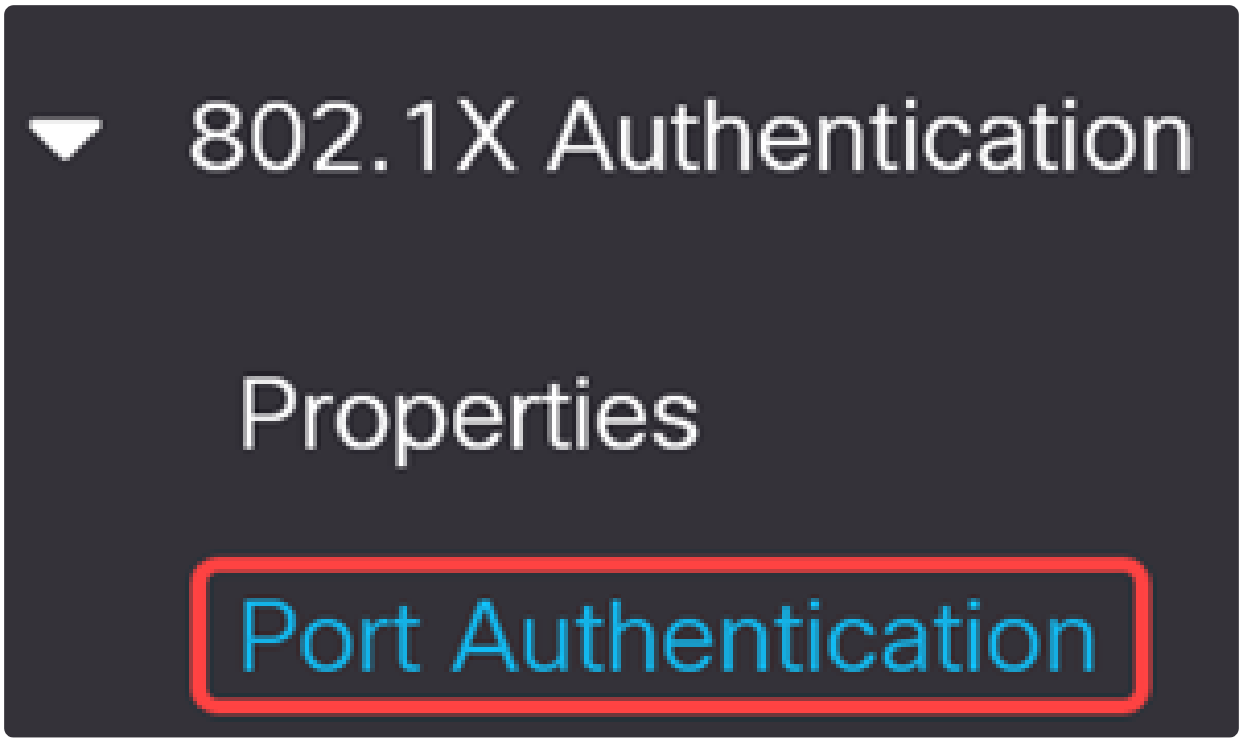
Paso 7

Asegúrese de que la Autenticación Basada en Puerto esté habilitada, y que el Método de Autenticación esté configurado en RADIUS.



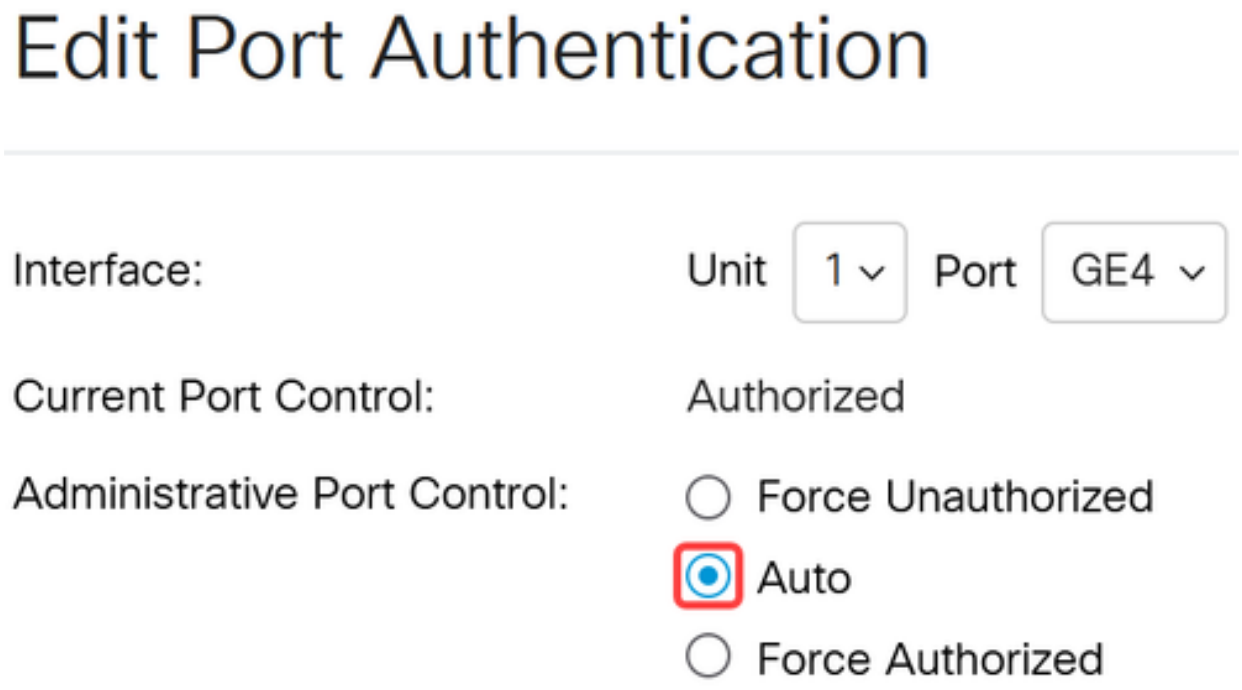
Paso 8

Vaya al menú Port Authentication, seleccione el puerto deseado y haga clic en edit.



Paso 9

Para Administrative Port Control, seleccione la opción Auto que conmutará el puerto entre el estado autorizado y el no autorizado según la respuesta RADIUS.

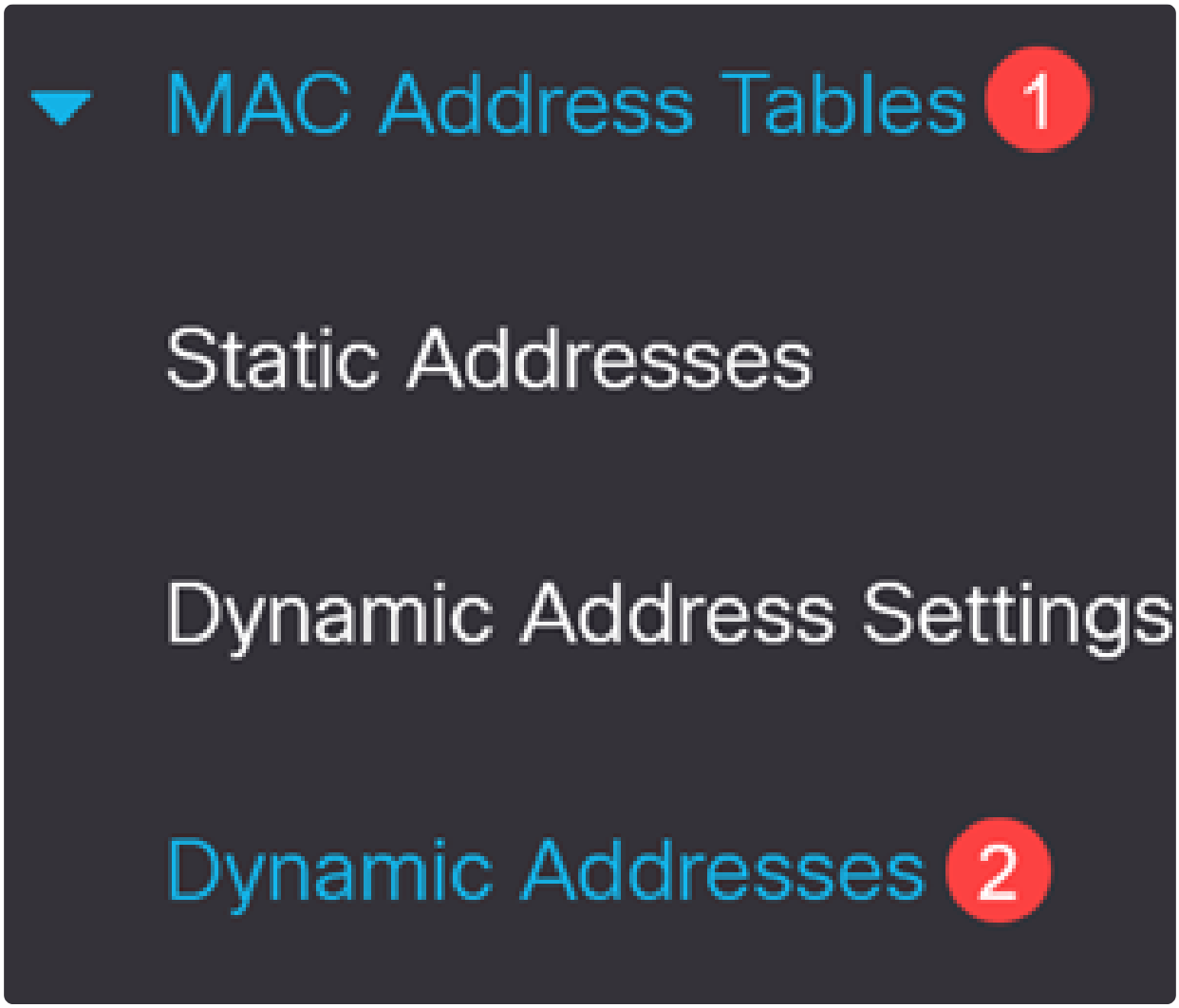


Paso 10

Habilite Autenticación Basada en 802.1x y haga clic en Aplicar.

Paso 11

Necesitará la dirección MAC del dispositivo en el puerto. La operación CoA en ISE se aplicará a esa dirección MAC. En este ejemplo, es el puerto 9. Para obtenerlo, navegue hasta Tablas de direcciones MAC > Direcciones dinámicas.

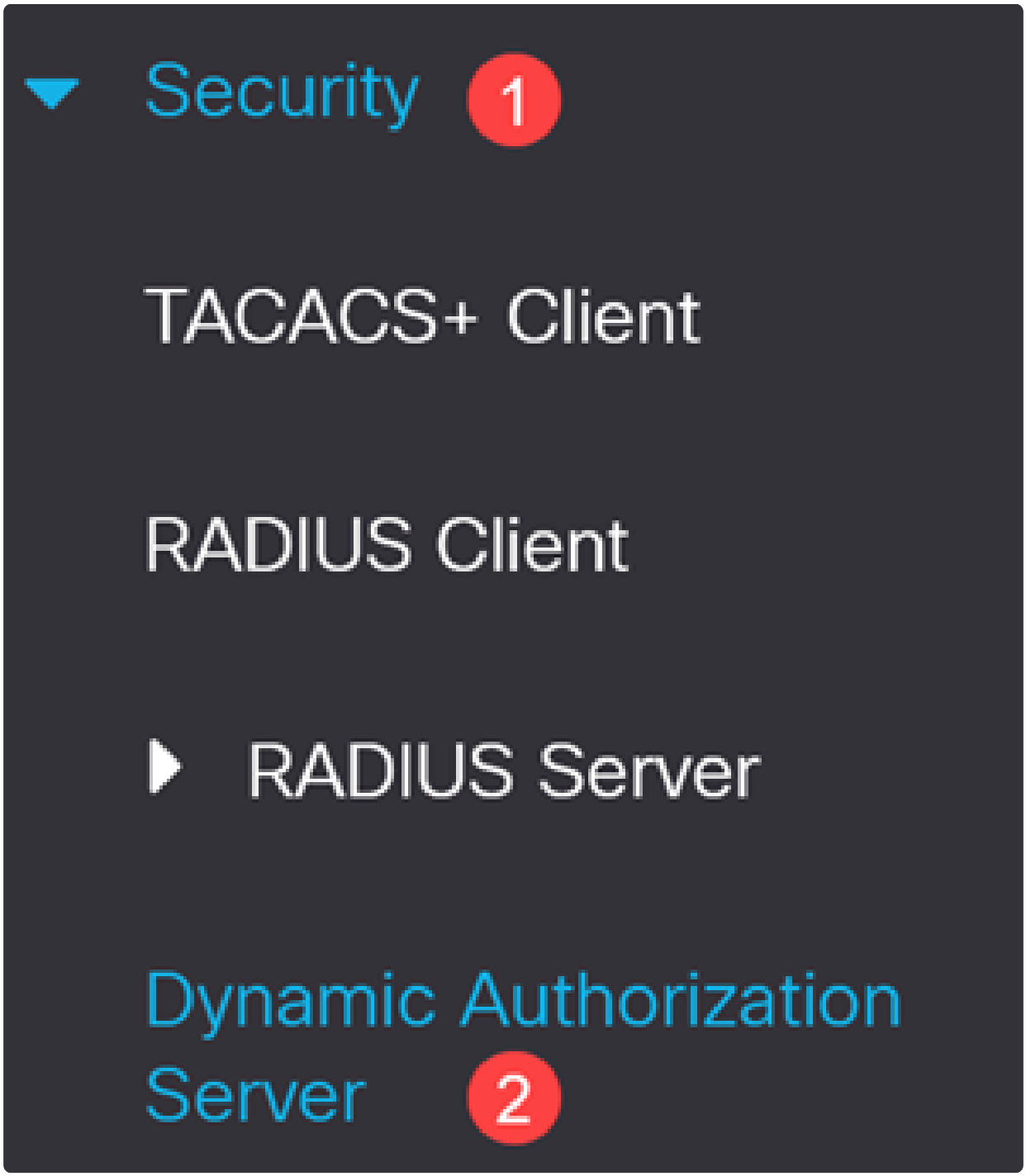


Paso 12

Desplácese hacia abajo hasta el puerto y anote la dirección MAC.

Paso 13

Vaya a Seguridad > Servidor de autorización dinámica.

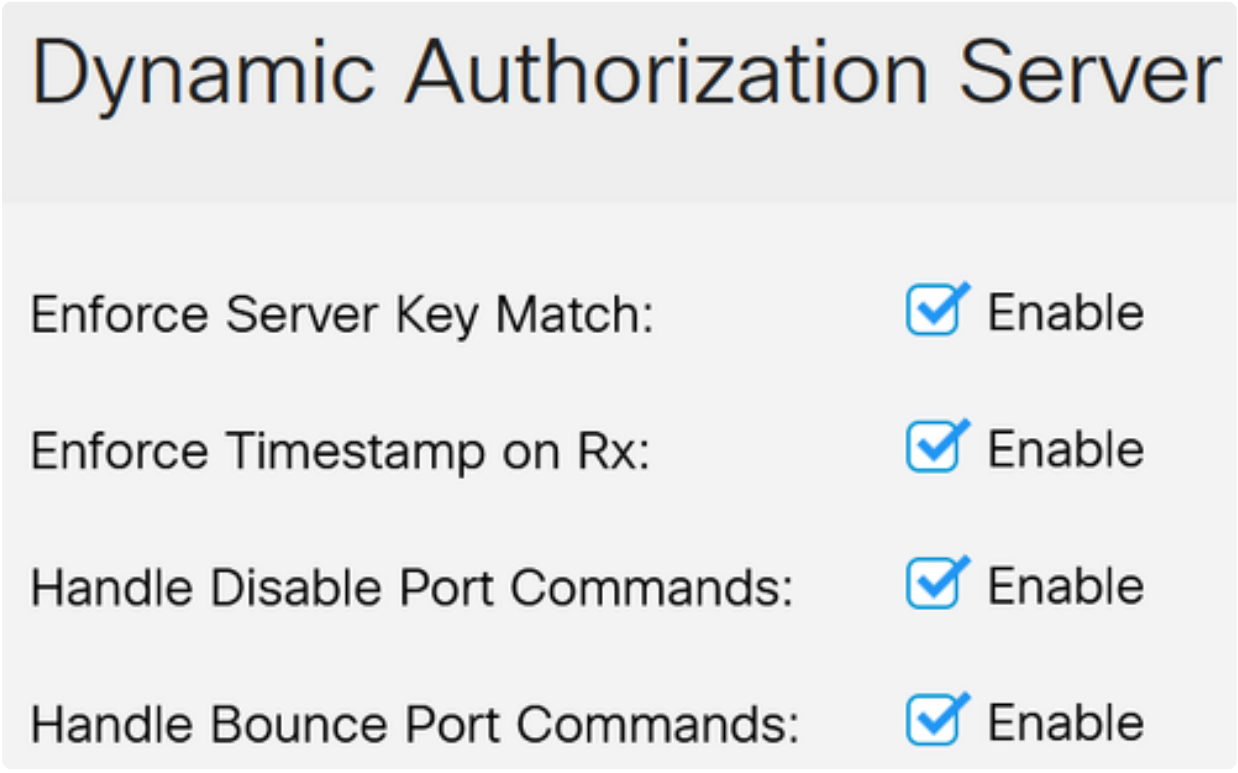


Paso 14

Habilite lo siguiente:

- Aplicar coincidencia de clave de servidor

- Aplicar marca de tiempo en Rx
- Comandos Handle Disable Port
- Manejar comandos de puerto de rebote

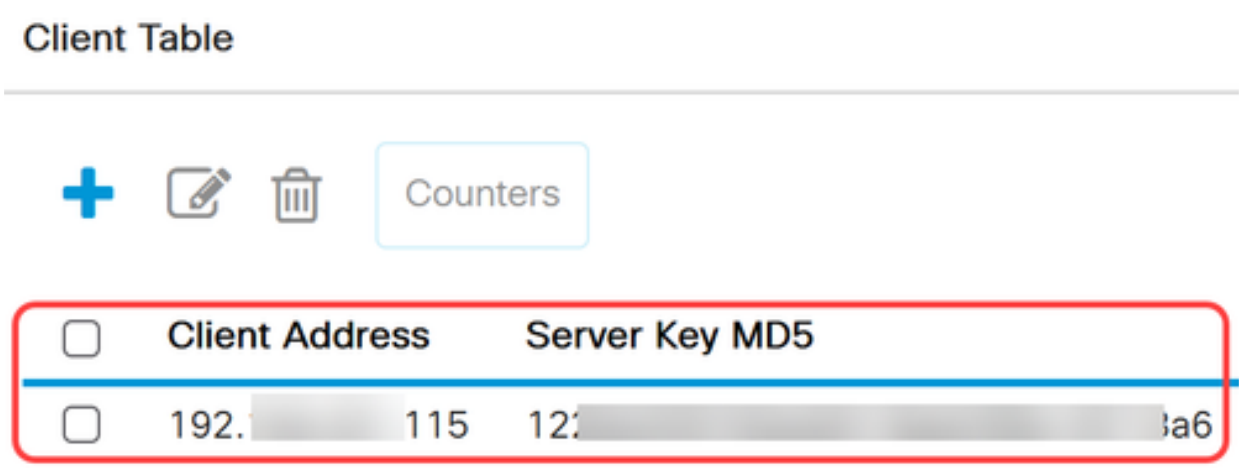


Paso 15

Deje el puerto UDP en el valor predeterminado de 1700.

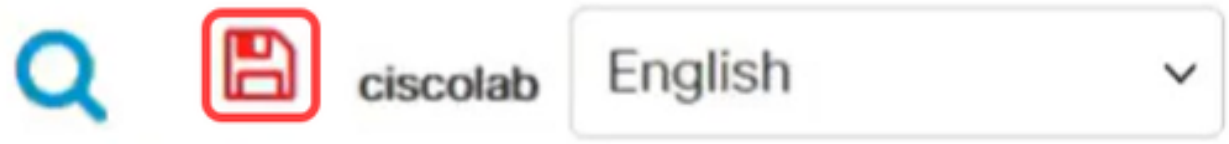
Paso 16

En Tabla de clientes, asegúrese de agregar el servidor ISE con la clave de servidor correcta. Haga clic en Apply (Aplicar).



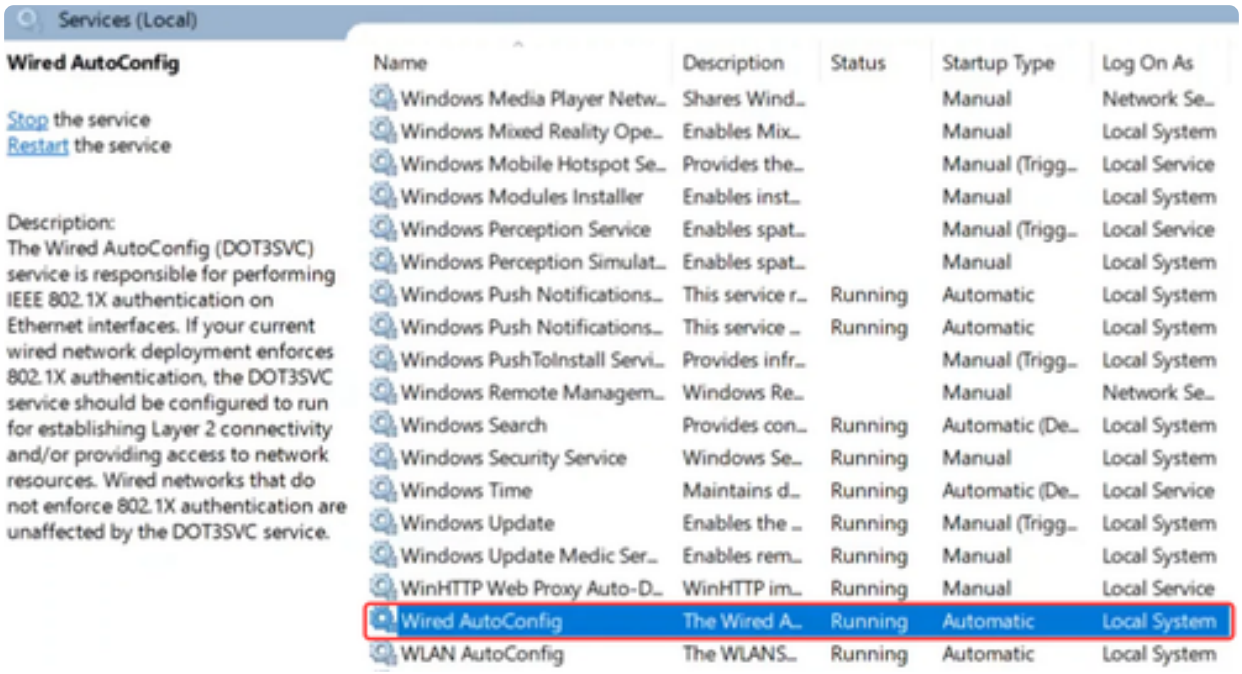
Paso 17

Haga clic en el icono Save que parpadea en rojo para guardar las configuraciones.



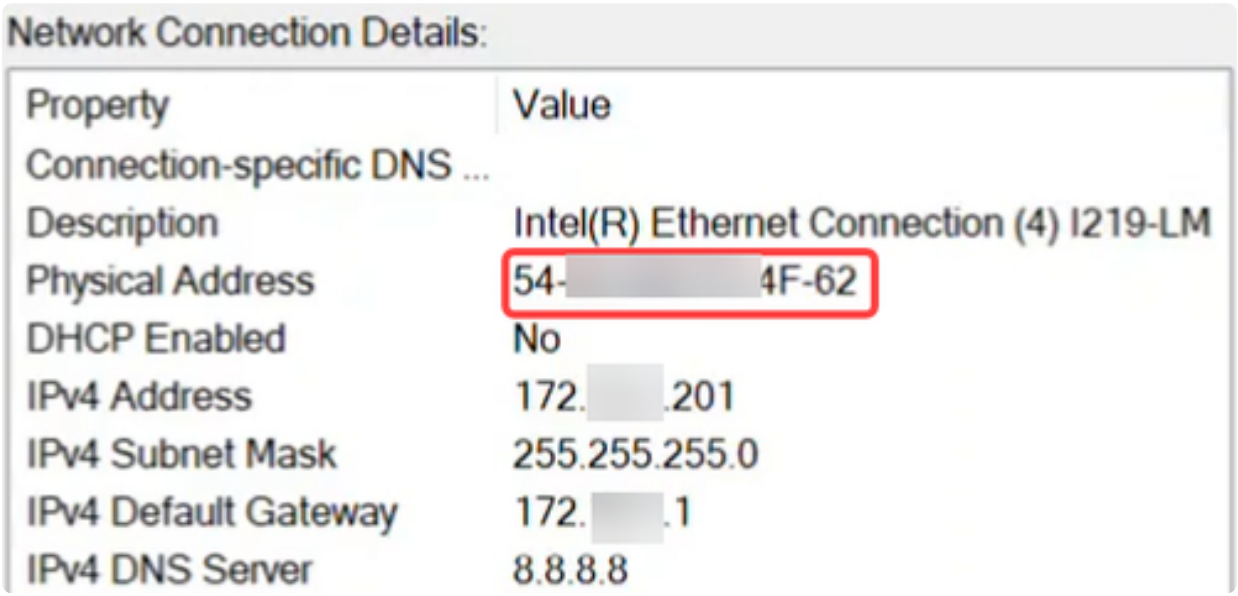
Paso 18

En el equipo portátil cliente conectado al puerto 9, verifique que el servicio Wired AutoConfig esté habilitado para la autenticación 802.1 X.



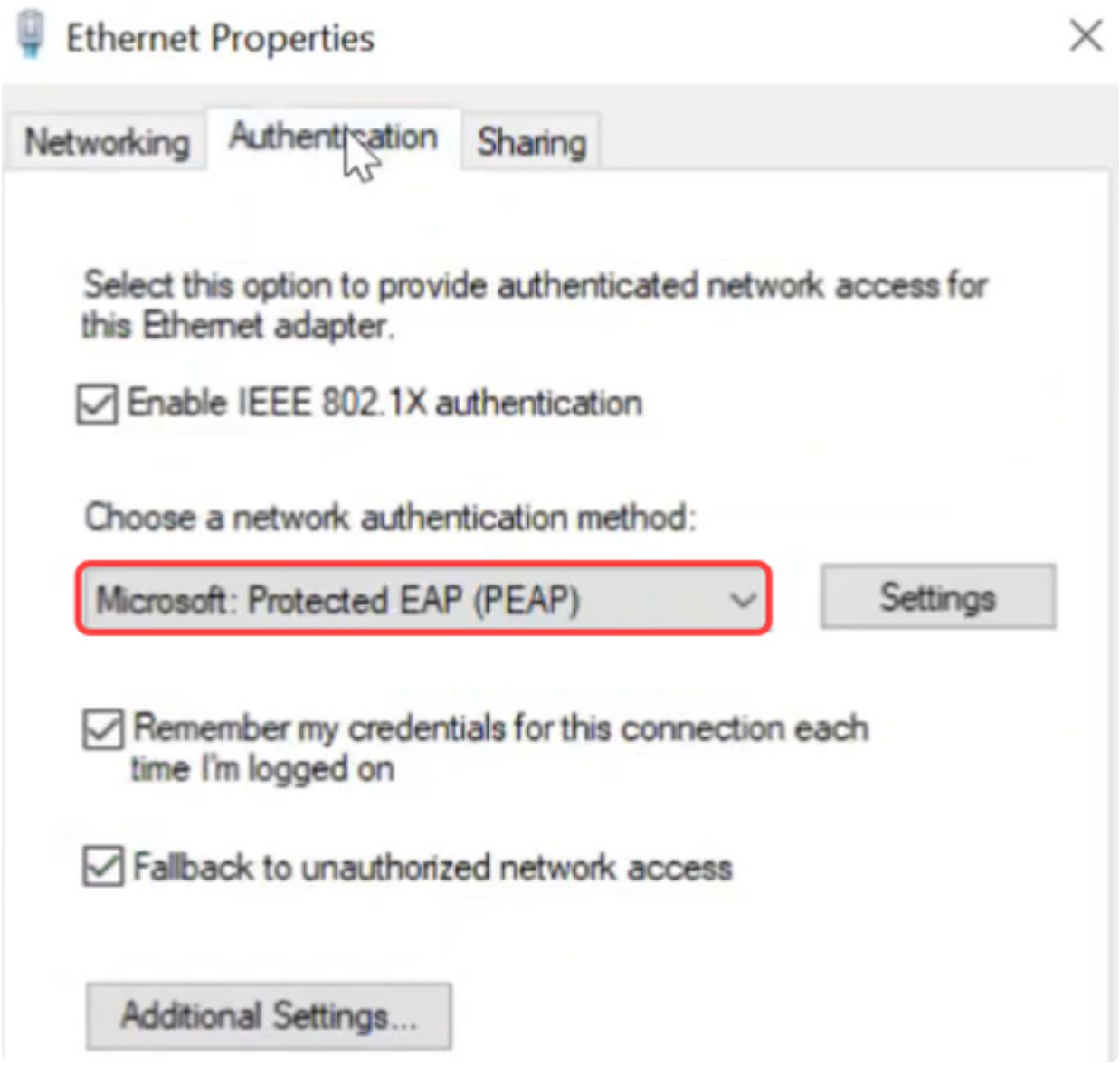
Paso 19

En los parámetros del adaptador Ethernet, verifique que la dirección MAC coincida.



Paso 20

Haga clic en el botón Properties en Ethernet settings y en la ficha Authentication, asegúrese de que las casillas de verificación estén habilitadas. Además, asegúrese de que el método de autenticación es EAP protegido (PEAP).



Paso 21

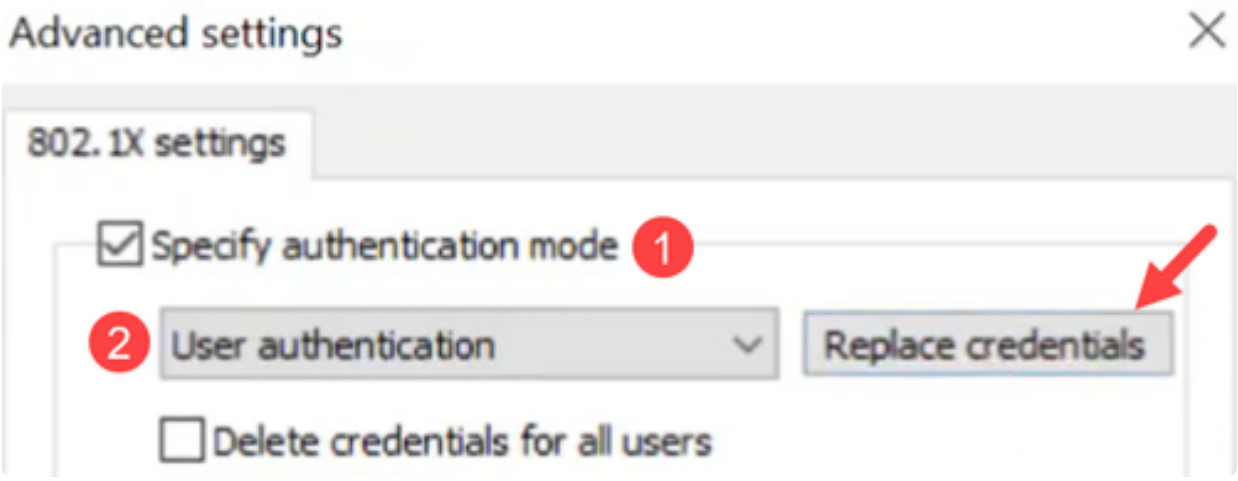
Haga clic en el botón Settings para asegurarse de que la casilla de verificación junto a Verify the server's identity by validating the certificate está desactivada.

Paso 22

Debe estar marcada la casilla Activar reconexión rápida.

Paso 23

En Configuración adicional, asegúrese de que Especificar modo de autenticación esté habilitado y de que Autenticación de usuario esté seleccionada en el menú desplegable. Puede guardar las credenciales creadas en ISE o sustituirlas mediante el botón Reemplazar credenciales.



Operación CoA

Antes de iniciar la operación CoA, habilite la captura de paquetes en el switch.

Paso 1

En PuTTY, inicie sesión en su switch Catalyst y especifique el tamaño del búfer y el modo de captura mediante el comando monitor capture cap1 buffer size 20 circular.

Paso 2

Especifique el plano de control como ambos mediante el comando monitor capture cap1 control-plane both.

Paso 3

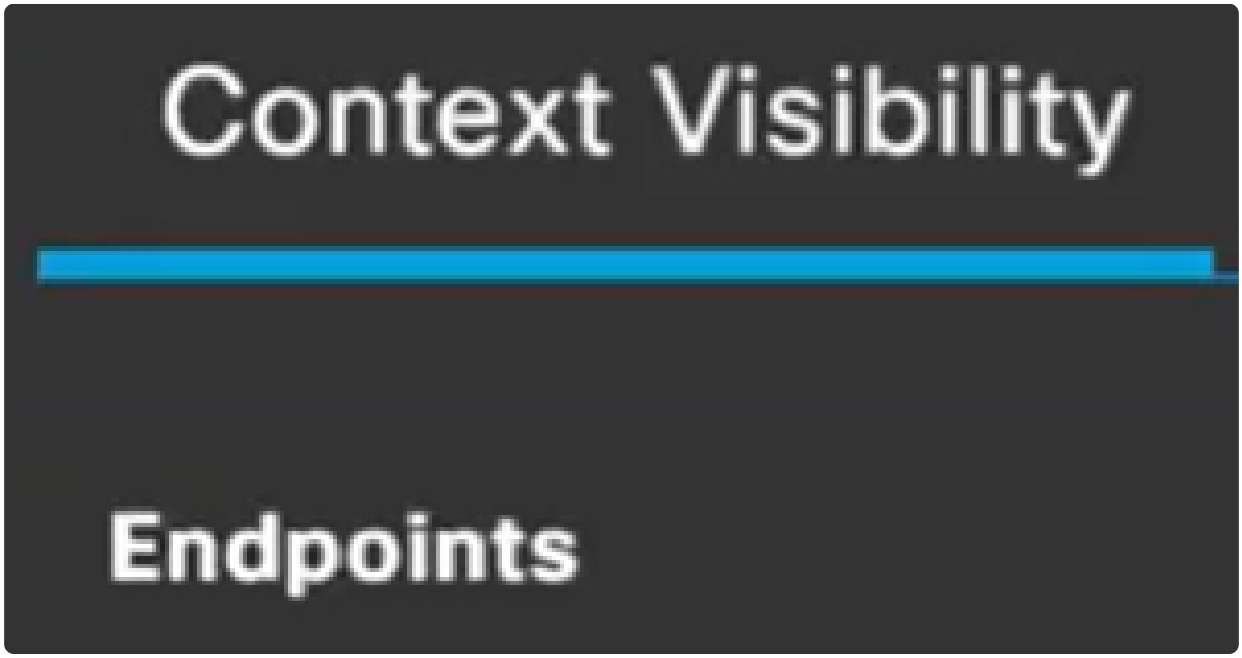
Introduzca los criterios de coincidencia como cualquiera. El comando para esto será monitor capture cap1 match any.

Paso 4

Inicie la captura de paquetes.

Paso 5

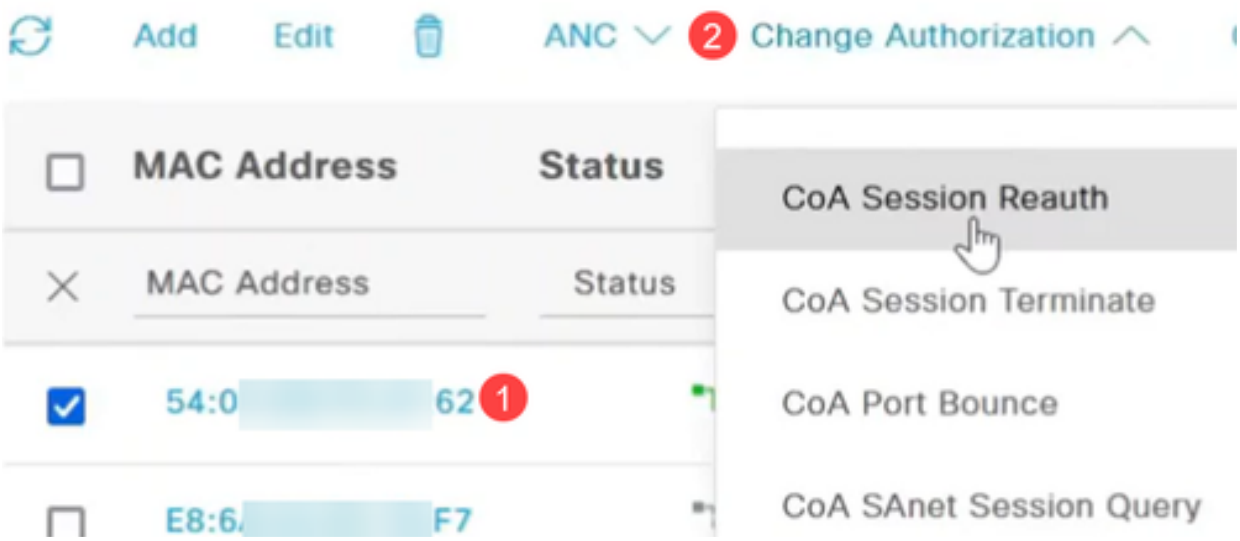
En la interfaz de ISE, desplácese hasta la opción Terminales en Visibilidad del contexto.



Paso 6

Elija la dirección MAC y seleccione la operación CoA en el menú desplegable Change of Authorization. En este ejemplo, se selecciona CoA Session Reauth. Esto fuerza la

reautenticación en el puerto al enviar un paquete CoA con un comando reauthenticate.



Paso 7

Vuelva a la terminal PuTTY para comprobar si la operación CoA se realizó correctamente.

```
Started capture point : capl
Cat1300-1#04-Jul-2024 20:49:45 %SEC-W-COAREAUTHSESSN: 802.1x re-authentication initiated for host 5
4:  62 by CoA Request "reauthenticate"
```

Paso 8

Si selecciona CoA Session Terminate, enviará una solicitud de desconexión con un comando de terminación basado en una solicitud administrativa.

```
Cat1300-1#04-Jul-2024 20:50:02 %SEC-W-PORTUNAUTHORIZED: Port gi1/0/9 is unAuthorized
04-Jul-2024 20:50:02 %SEC-W-COADISCSESSN: 802.1x session for host 54:  :62 on interface gi
1/0/9 has been terminated by Disconnect-Request. Authenticator state on the Interface will be re-in
itialized
04-Jul-2024 20:50:02 %SEC-I-PORTAUTHORIZED: Port gi1/0/9 is Authorized
```

Paso 9

La opción de rebote de puerto CoA enviará un paquete de solicitud CoA con un comando bounce host port, inhabilitando y volviendo a habilitar el puerto en el switch. El adaptador de red se desconecta durante 10 segundos y no está autorizado. Se hará

la reaparición en línea, se autoriza y puede reenviar paquetes.

```
Cat1300-1#04-Jul-2024 20:50:21 %SEC-W-COABNCEPORT: Interface gi1/0/9 suspended for 10 seconds by Co
A Request "bounce host port" for host 54:          :62
04-Jul-2024 20:50:21 %LINK-W-Down:  gi1/0/9
04-Jul-2024 20:50:34 %LINK-I-Up:  gi1/0/9
04-Jul-2024 20:50:34 %SEC-W-PORTUNAUTHORIZED: Port gi1/0/9 is unAuthorized
04-Jul-2024 20:50:36 %LINK-W-Down:  gi1/0/9
04-Jul-2024 20:50:39 %LINK-I-Up:  gi1/0/9
04-Jul-2024 20:50:39 %SEC-I-PORTAUTHORIZED: Port gi1/0/9 is Authorized

Cat1300-1#04-Jul-2024 20:50:45 %STP-W-PORTSTATUS: gi1/0/9: STP status Forwarding
```

Paso 10

La terminación de la sesión CoA con rebote de puerto finalizará la sesión existente, rebotará el puerto durante 10 segundos y se volverá no autorizada. Luego vuelve a estar en línea, se autoriza y puede reenviar paquetes.

```
Cat1300-1#04-Jul-2024 20:51:04 %SEC-W-COABNCEPORT: Interface gi1/0/9 suspended for 10 seconds by Co
A Request "bounce host port" for host 54:          :62
04-Jul-2024 20:51:04 %LINK-W-Down:  gi1/0/9
04-Jul-2024 20:51:22 %LINK-I-Up:  gi1/0/9
04-Jul-2024 20:51:22 %SEC-W-PORTUNAUTHORIZED: Port gi1/0/9 is unAuthorized
04-Jul-2024 20:51:22 %SEC-I-PORTAUTHORIZED: Port gi1/0/9 is Authorized
04-Jul-2024 20:51:29 %STP-W-PORTSTATUS: gi1/0/9: STP status Forwarding
```

Paso 11

La terminación de la sesión CoA con el cierre del puerto finalizará la sesión y cerrará administrativamente el puerto.

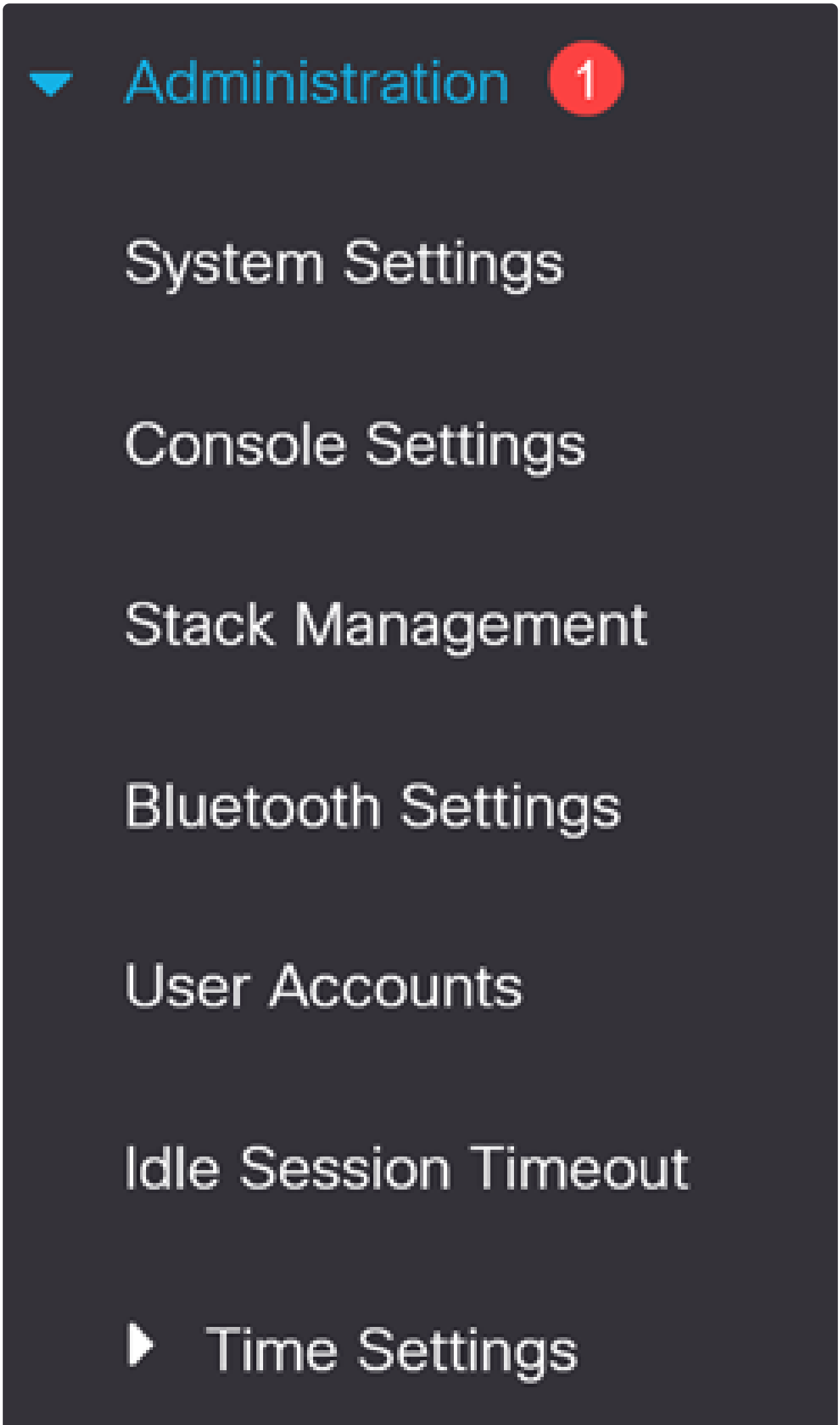
```
Cat1300-1#04-Jul-2024 20:51:47 %SEC-W-COADISPORT: Interface gi1/0/9 suspended by CoA Request "disab
le host port" for host 54:          :62
04-Jul-2024 20:51:47 %LINK-W-Down:  gi1/0/9
```

Paso 12

Para detener la captura de paquetes, utilice el comando monitor capture cap1 stop.

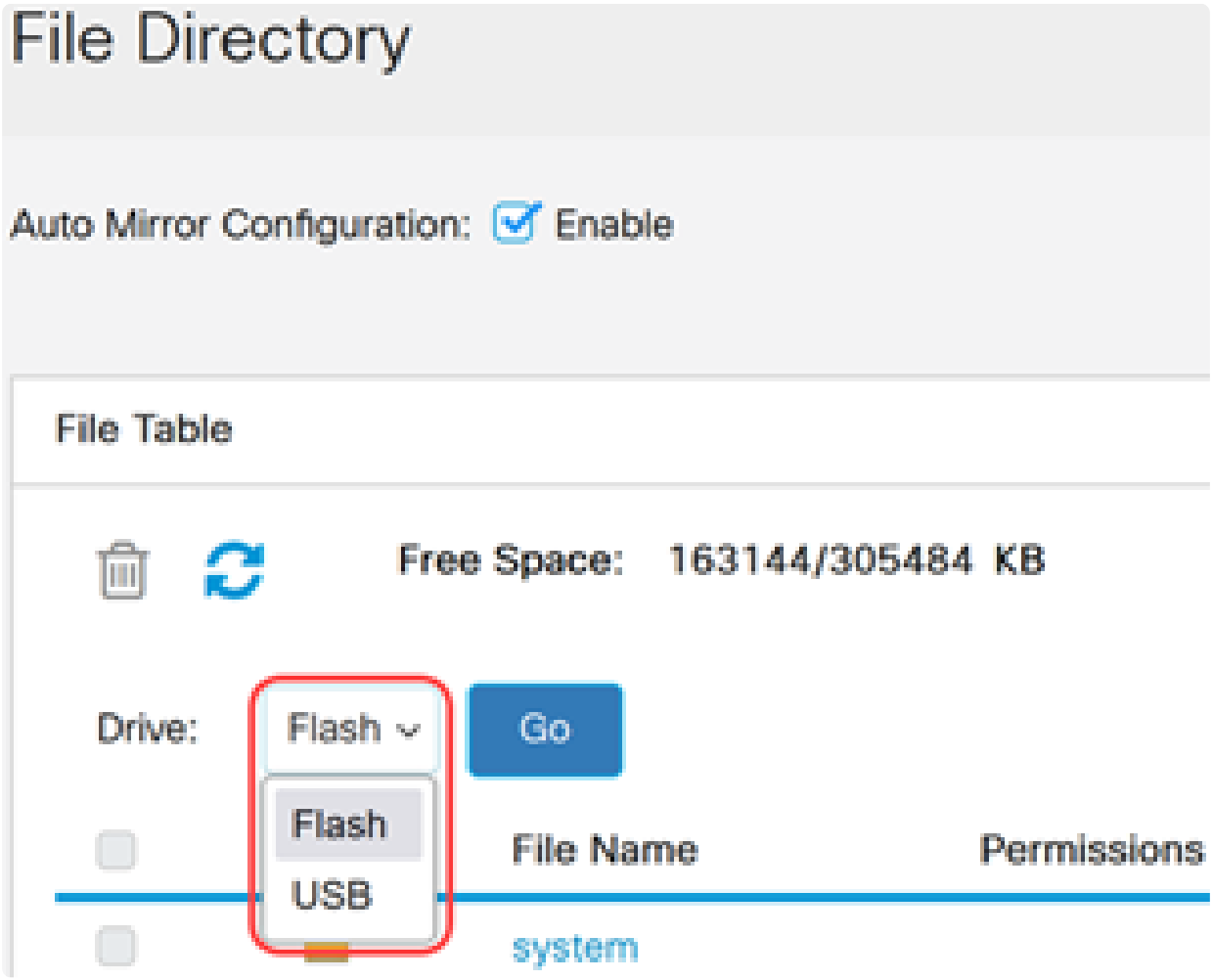
Paso 13

Para copiar los archivos, navegue hasta Administration > File Management > File Directory.


Administration
1
System Settings
Console Settings
Stack Management
Bluetooth Settings
User Accounts
Idle Session Timeout
Time Settings

Paso 14

El Flash predeterminado está disponible. También puede seleccionar USB en el menú desplegable Drive.



Conclusión

Ahora ya sabe todo sobre ISE y cómo configurar CoA en los switches Catalyst serie 1300.

Para obtener más información, vea el siguiente vídeo.

Vea un video relacionado con este artículo...

Haga clic aquí para ver otras ediciones de Tech Talks 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).