Configuración de TACACS+ Device Administration en Palo Alto con ISE

Contenido

Introducción

Este documento describe la configuración de TACACS+ en Palo Alto con Cisco ISE.

Prerequisites

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco ISE y protocolo TACACS+.
- Firewall de Palo Alto.

Componentes Utilizados

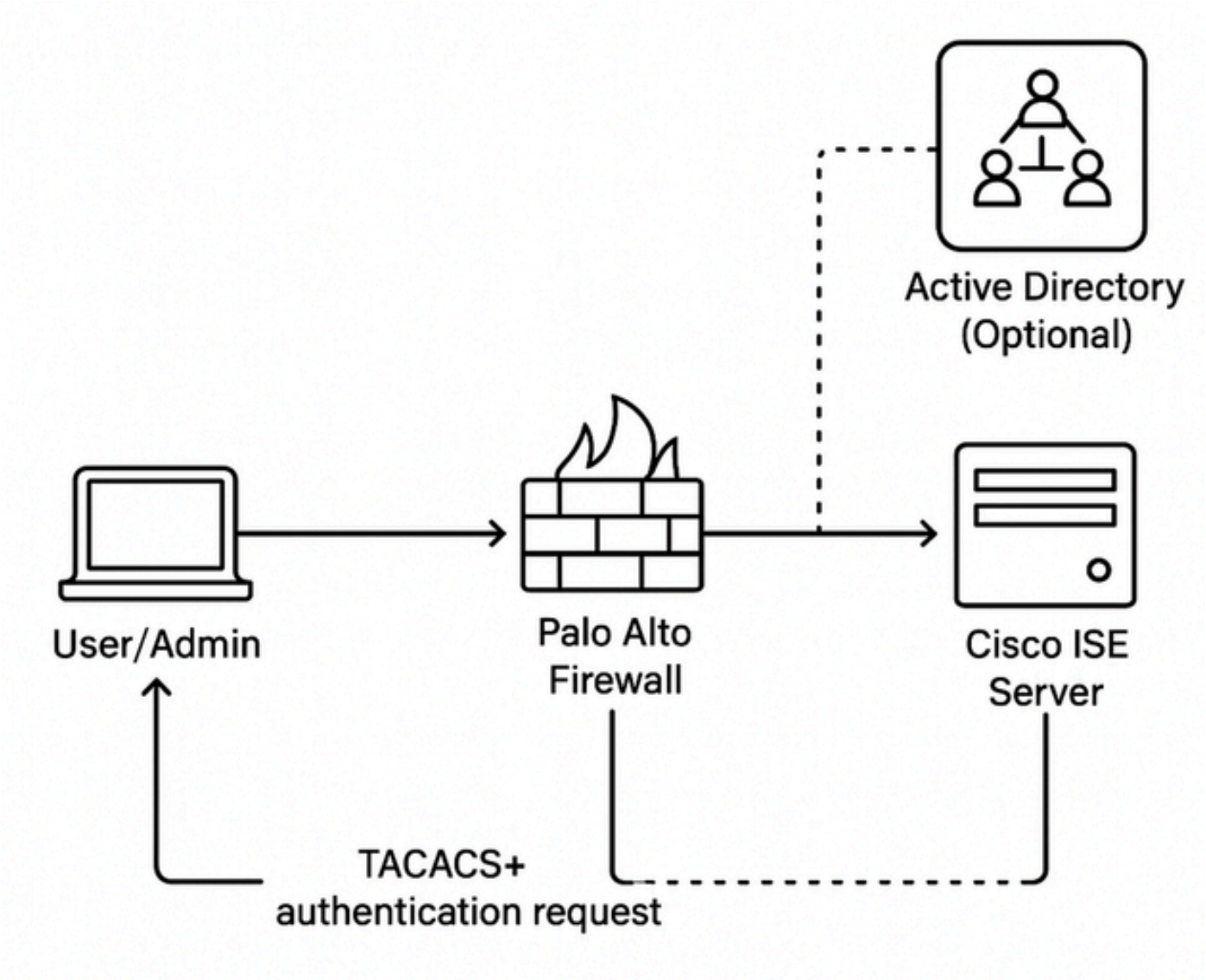
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Palo Alto Firewall versión 10.1.0
- Parche 4 de Cisco Identity Services Engine (ISE) versión 3.3

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.

Diagrama de la red



Flujo de autenticación

1. El administrador inicia sesión en el firewall de Palo Alto.

2. Palo Alto envía una solicitud de autenticación TACACS+ a Cisco ISE.

3. Cisco ISE:

- Si AD está integrado, solicita autenticación y autorización a AD.
- Si no hay AD, usa almacenes de identidad o políticas locales.
- Cisco ISE envía una respuesta de autorización a Palo Alto en función de las políticas configuradas.
- El administrador obtiene acceso con el nivel de privilegio adecuado.

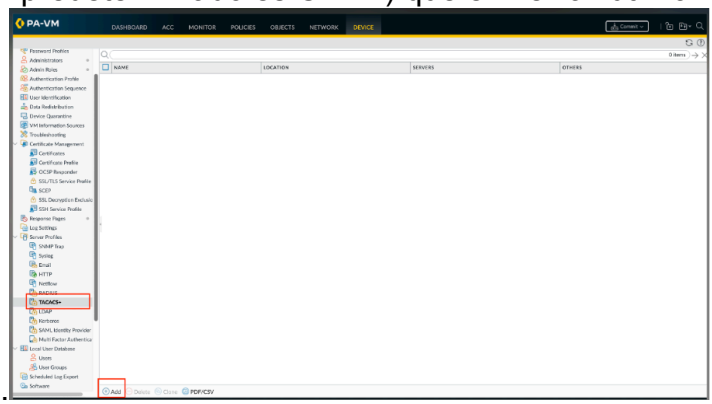
Configurar

Sección 1: Configuración de Palo Alto Firewall para TACACS+

Paso 1. Agregue un perfil de servidor TACACS+.

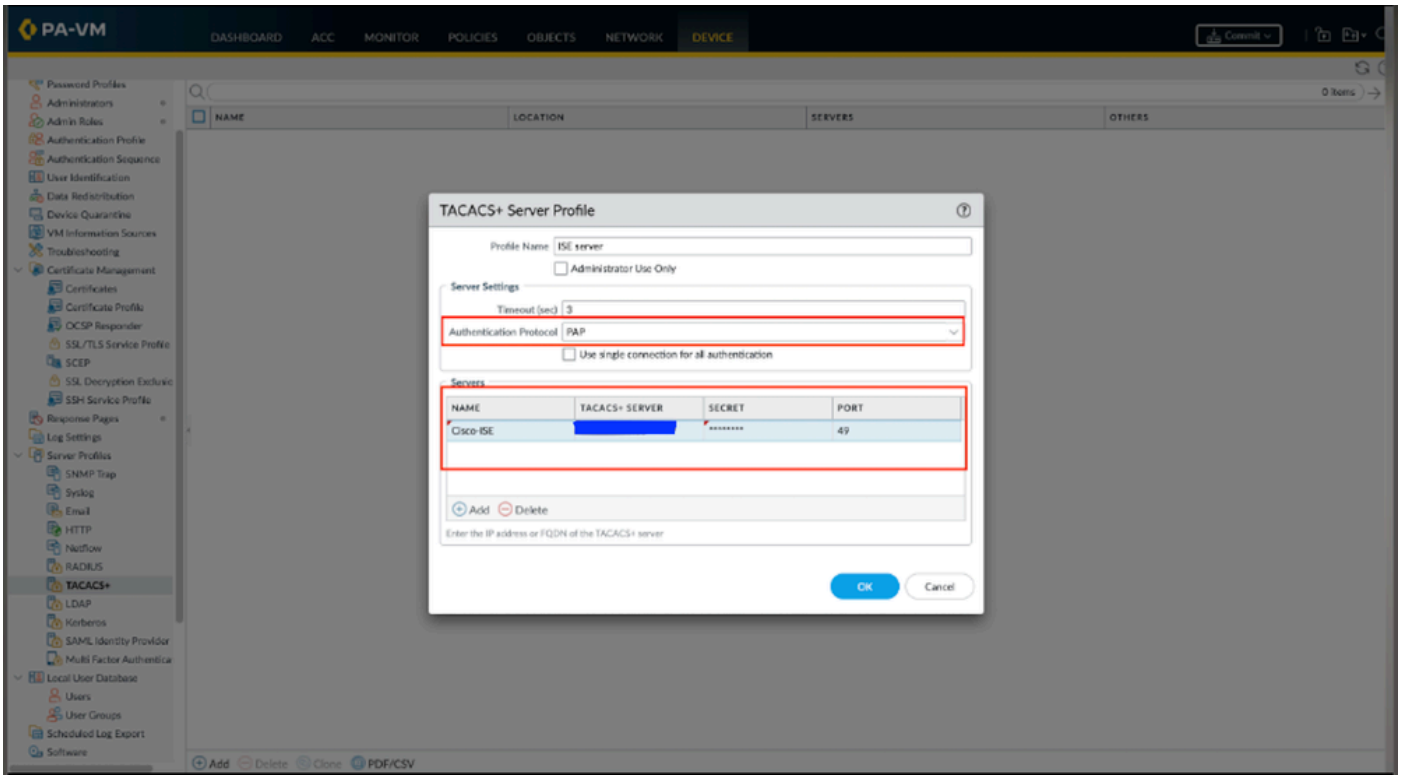
El perfil define cómo el firewall se conecta al servidor TACACS+.

1. Seleccione Device > Server Profiles > TACACS+ or Panorama > Server Profiles > TACACS+ en Panorama y Add a profile.
2. Introduzca un nombre de perfil para identificar el perfil de servidor.
3. (Opcional) Seleccione Administrator Use Only para restringir el acceso a los administradores.
4. Introduzca un intervalo de tiempo de espera en segundos tras el cual se agotará el tiempo de espera de una solicitud de autenticación (el valor predeterminado es 3; es de 1 a 20).
5. Seleccione el protocolo de autenticación (el predeterminado es CHAP) que el firewall utiliza para autenticarse en el servidor TACACS+.



6. Agregue cada servidor TACACS+ y realice estos pasos:
    1. Un Nombre para identificar el servidor.
    2. La dirección IP o FQDN del servidor TACACS+. Si utiliza un objeto de dirección FQDN para identificar el servidor y posteriormente cambia la dirección, debe confirmar el cambio para que la nueva dirección del servidor surta efecto.
    3. Secreto y Confirmar secreto para cifrar nombres de usuario y contraseñas.
    4. El puerto del servidor para las solicitudes de autenticación (el valor predeterminado es 49). Haga clic en Aceptar para guardar el perfil de servidor.

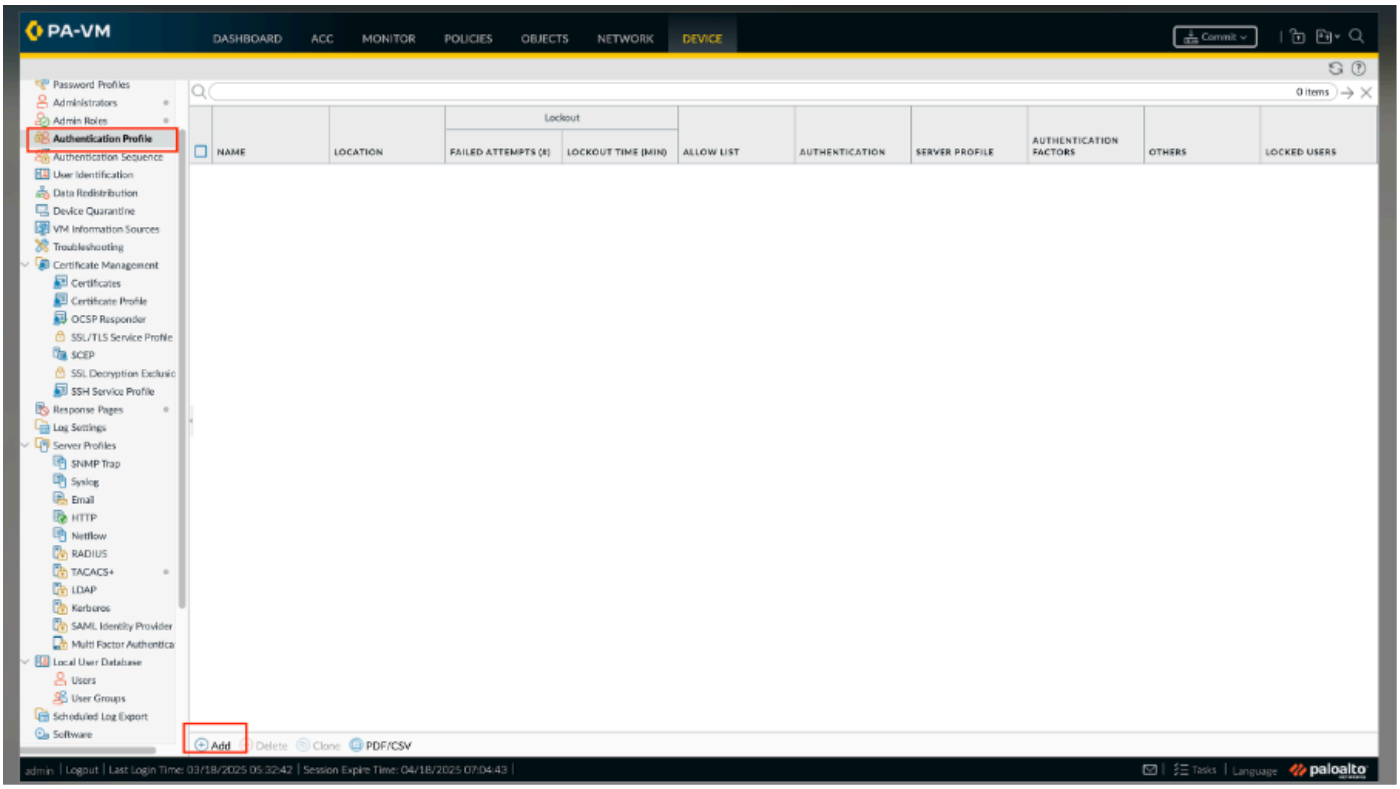
7. Haga clic en Aceptar para guardar el perfil de servidor.

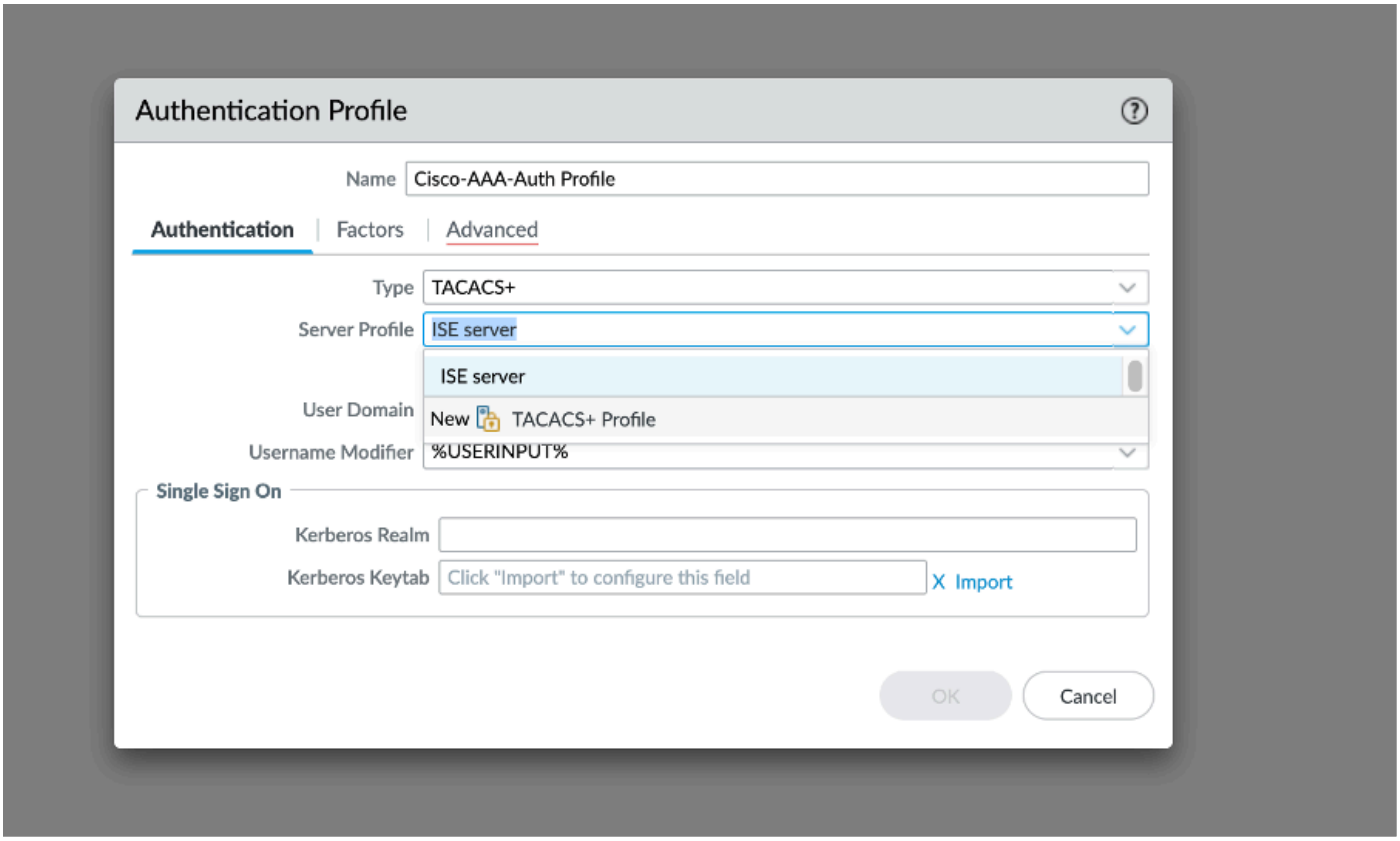


Paso 2. Asigne el perfil de servidor TACACS+ a un perfil de autenticación.

El perfil de autenticación define las opciones de autenticación que son comunes a un conjunto de usuarios.

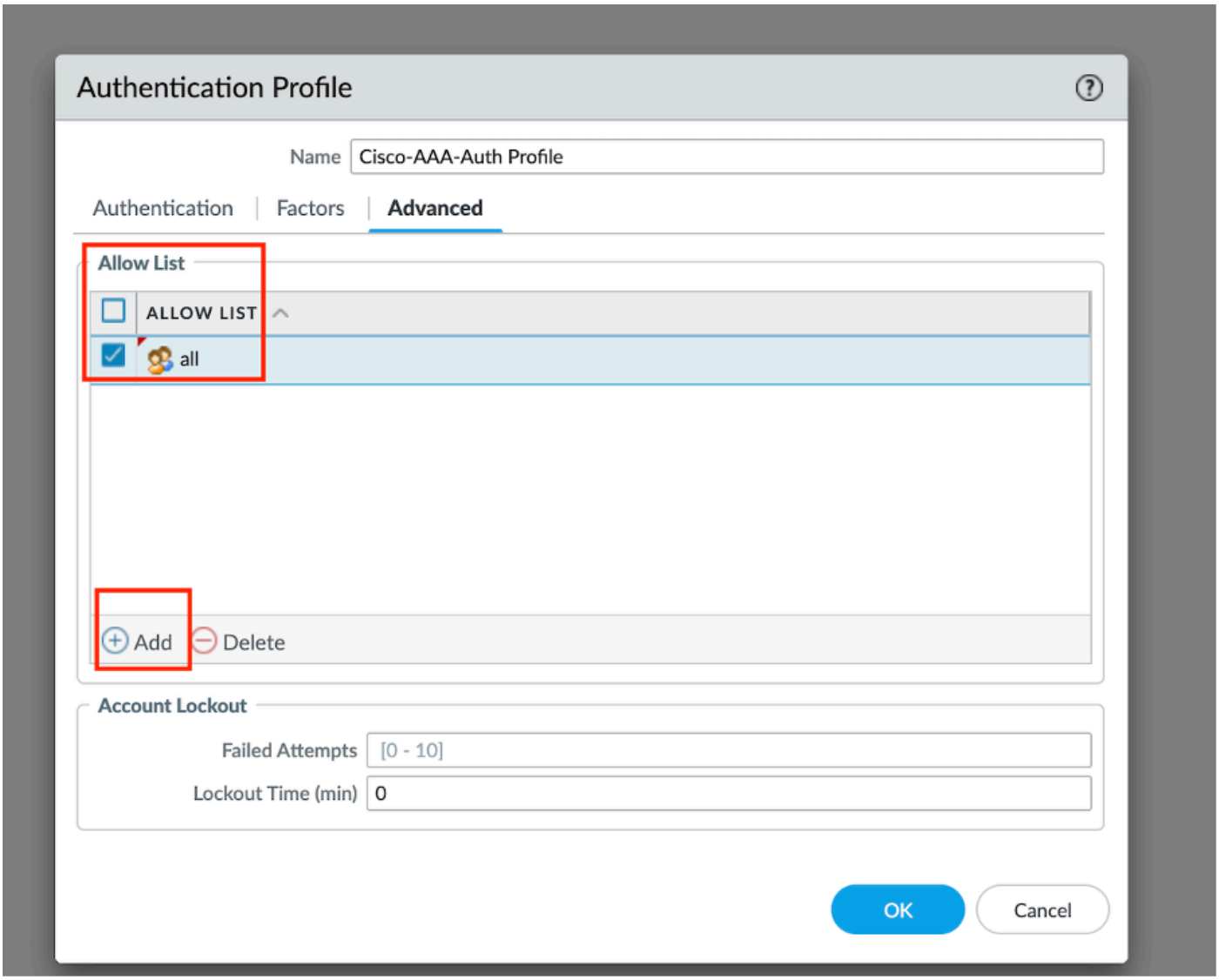
1. Seleccione Device > Authentication Profile y Add a profile.
    1. Introduzca un nombre para identificar el perfil
    2. Establezca el Tipo en TACACS+.
    3. Seleccione el perfil de servidor que ha configurado.
    4. Seleccione Recuperar grupo de usuarios de TACACS+ para recopilar información de grupo de usuarios de VSA definidos en el servidor TACACS+.





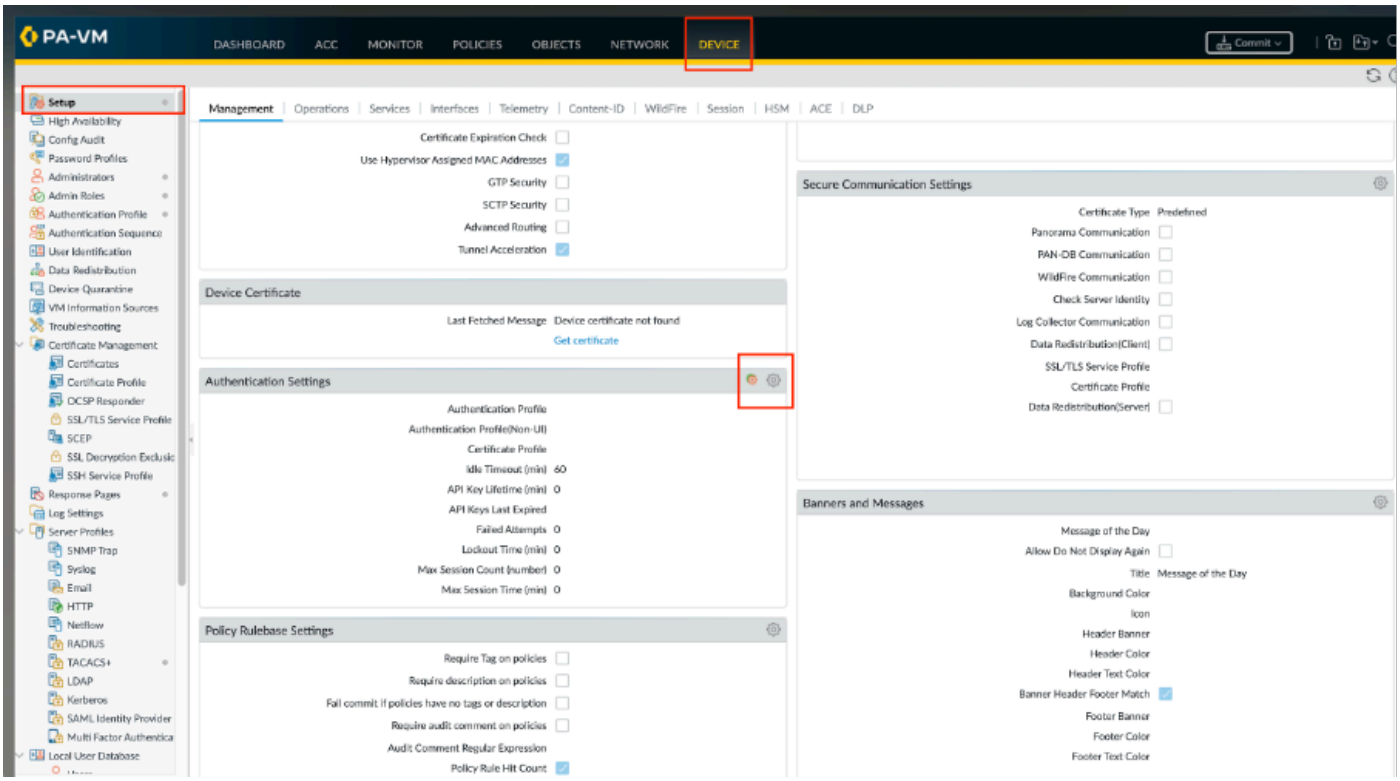
El firewall hace coincidir la información del grupo mediante los grupos especificados en la Lista de permitidos del perfil de autenticación.

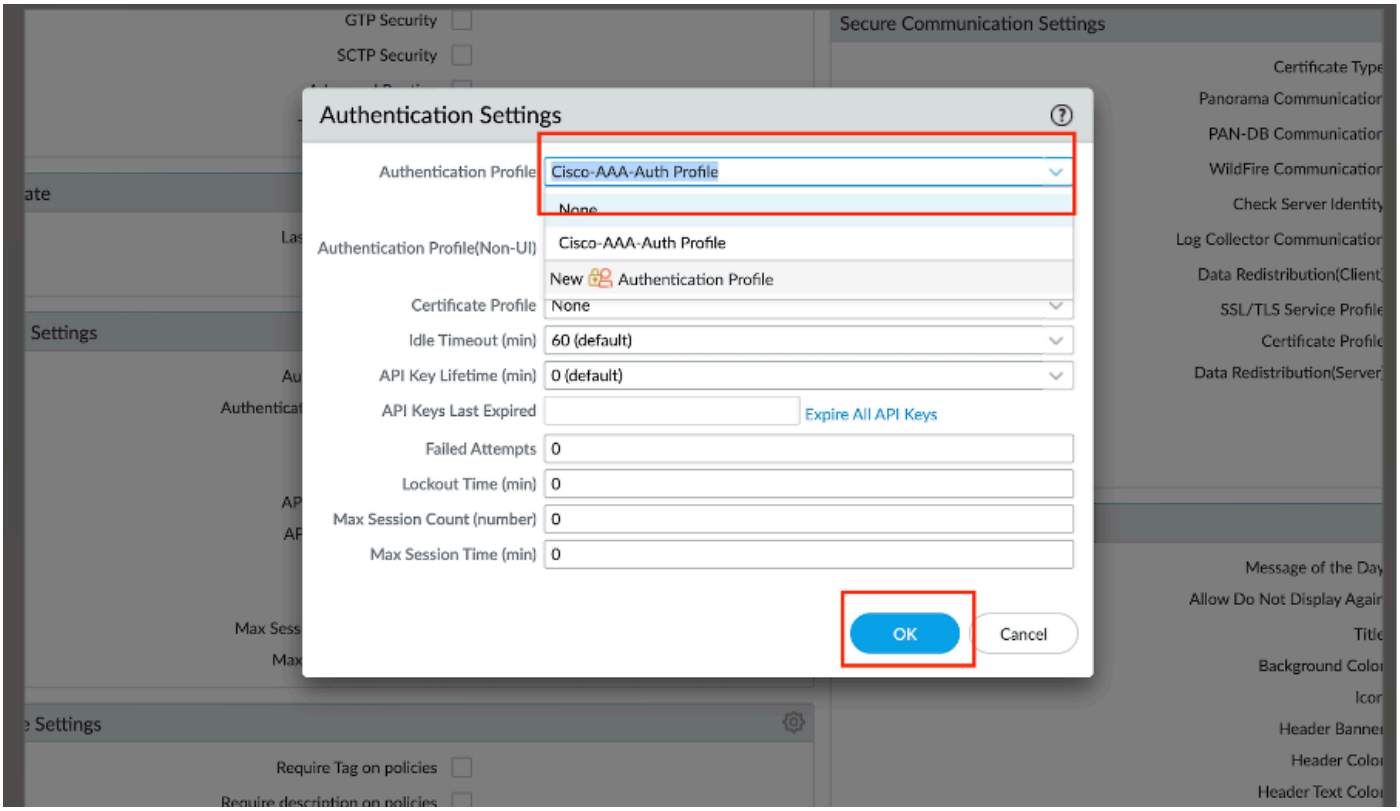
1. Seleccione Advanced y en la Lista de permitidos, Add los usuarios y grupos que pueden autenticarse con este perfil de autenticación.
2. Haga clic en Aceptar para guardar el perfil de autenticación.



Paso 3. Configure el firewall para utilizar el perfil de autenticación para todos los administradores.

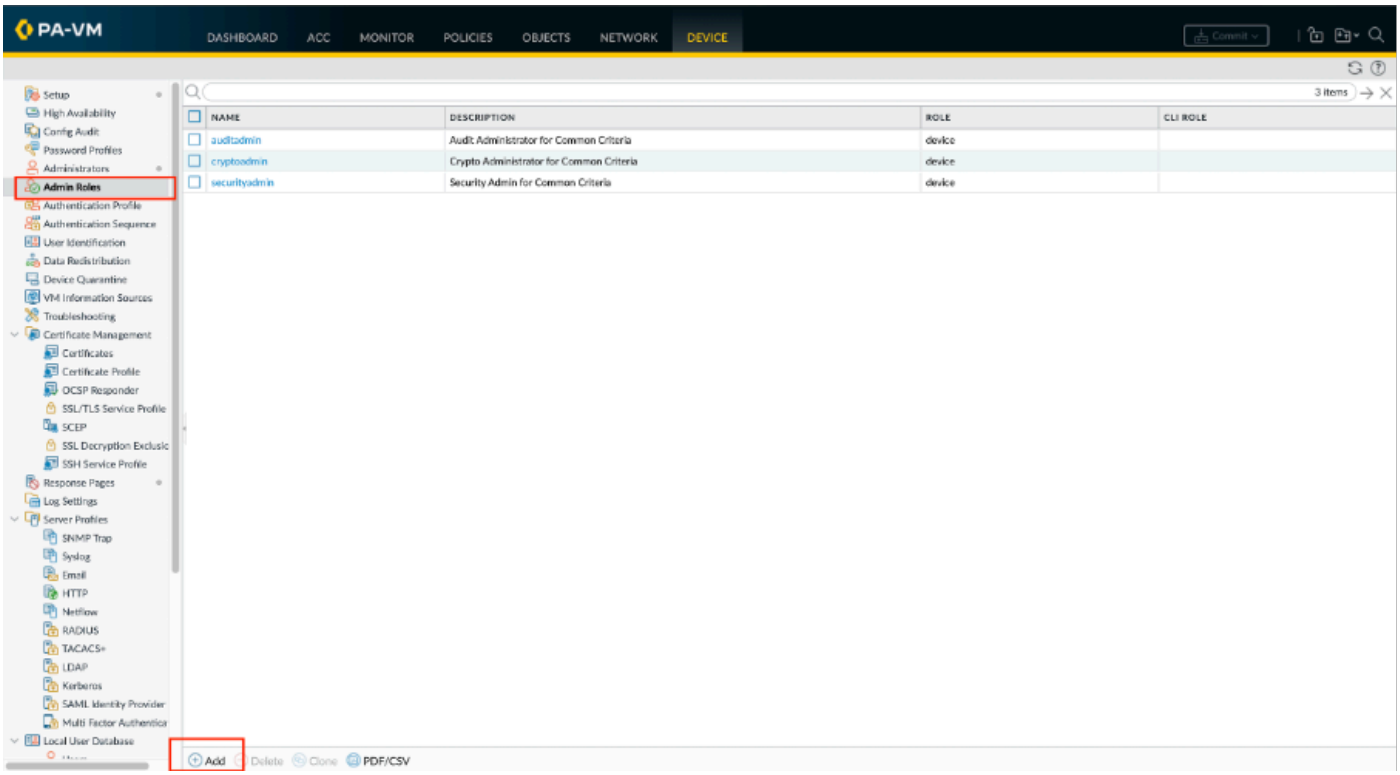
1. Seleccione Device > Setup > Management y edite los ajustes de autenticación.
2. Seleccione el perfil de autenticación que configuró y haga clic en Aceptar.



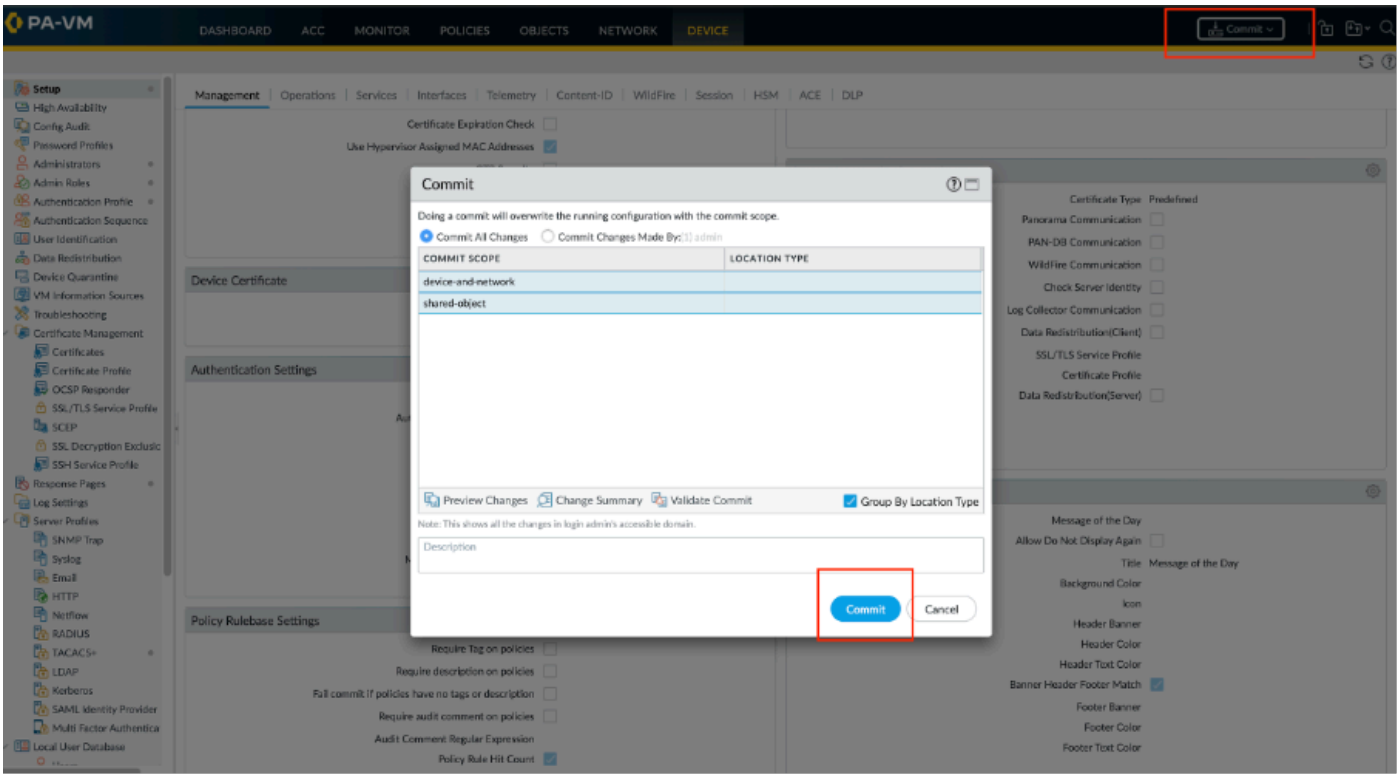


Paso 4. Configure un perfil de rol de administrador.

Seleccione Device > Admin Roles y haga clic en Add. Introduzca un nombre para identificar el rol.



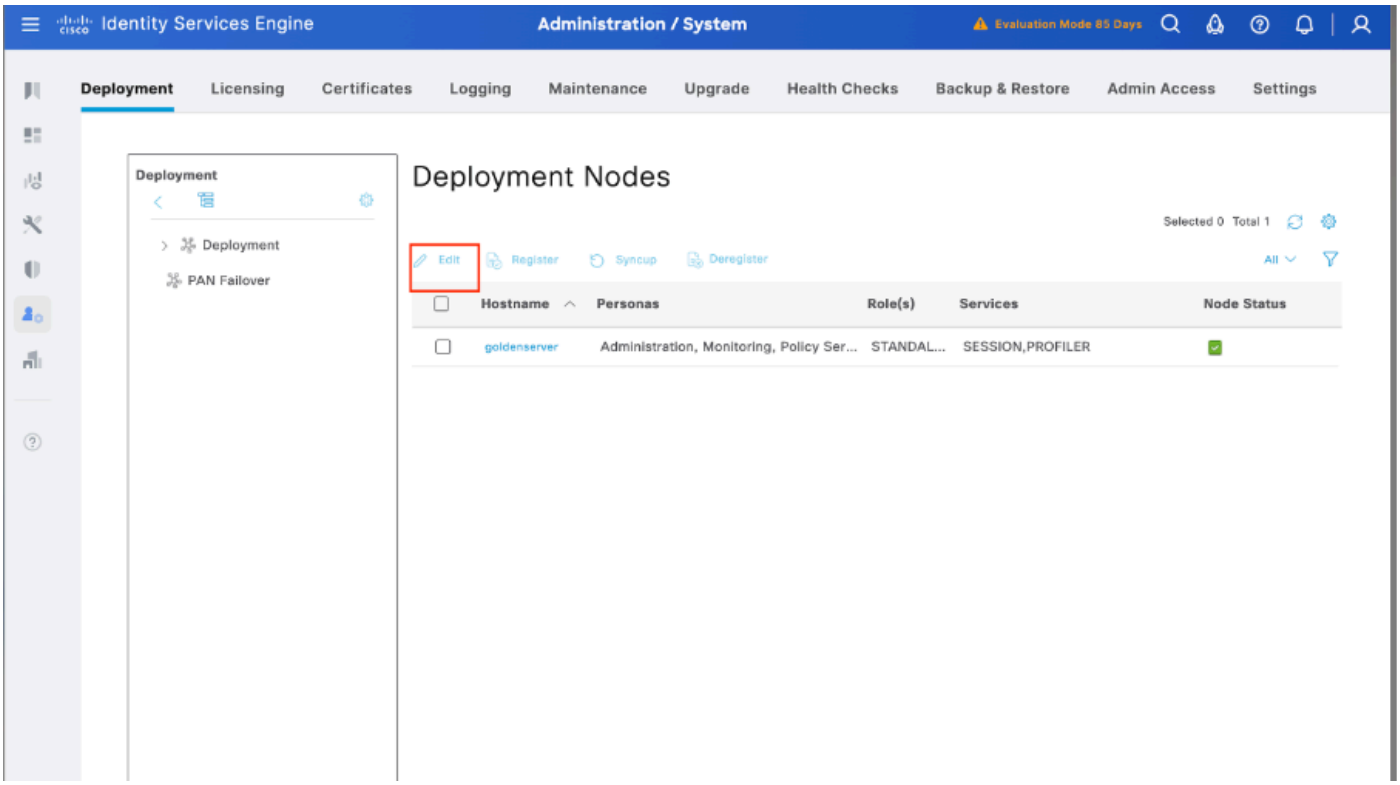
Paso 5. Realice los cambios para activarlos en el firewall.



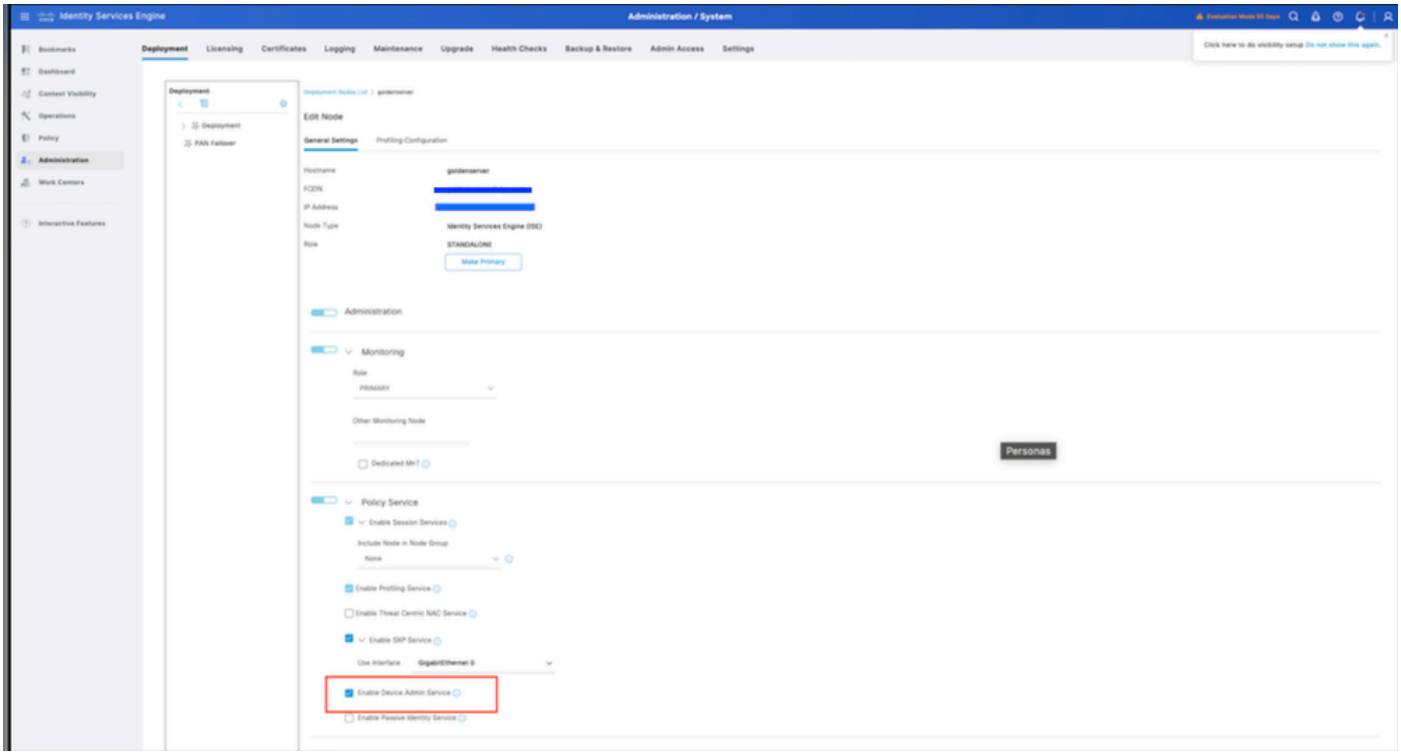
Sección 2: Configuración de TACACS+ en ISE

Paso 1. El paso inicial es verificar si Cisco ISE cuenta con las capacidades necesarias para gestionar la autenticación TACACS+. Para ello, confirme que el nodo de servicios de directivas (PSN) deseado tiene activada la función Device Admin Service. Vaya a Administration > System > Deployment, seleccione el nodo adecuado donde ISE procesa la autenticación TACACS+ y haga

clic en Edit para revisar su configuración.

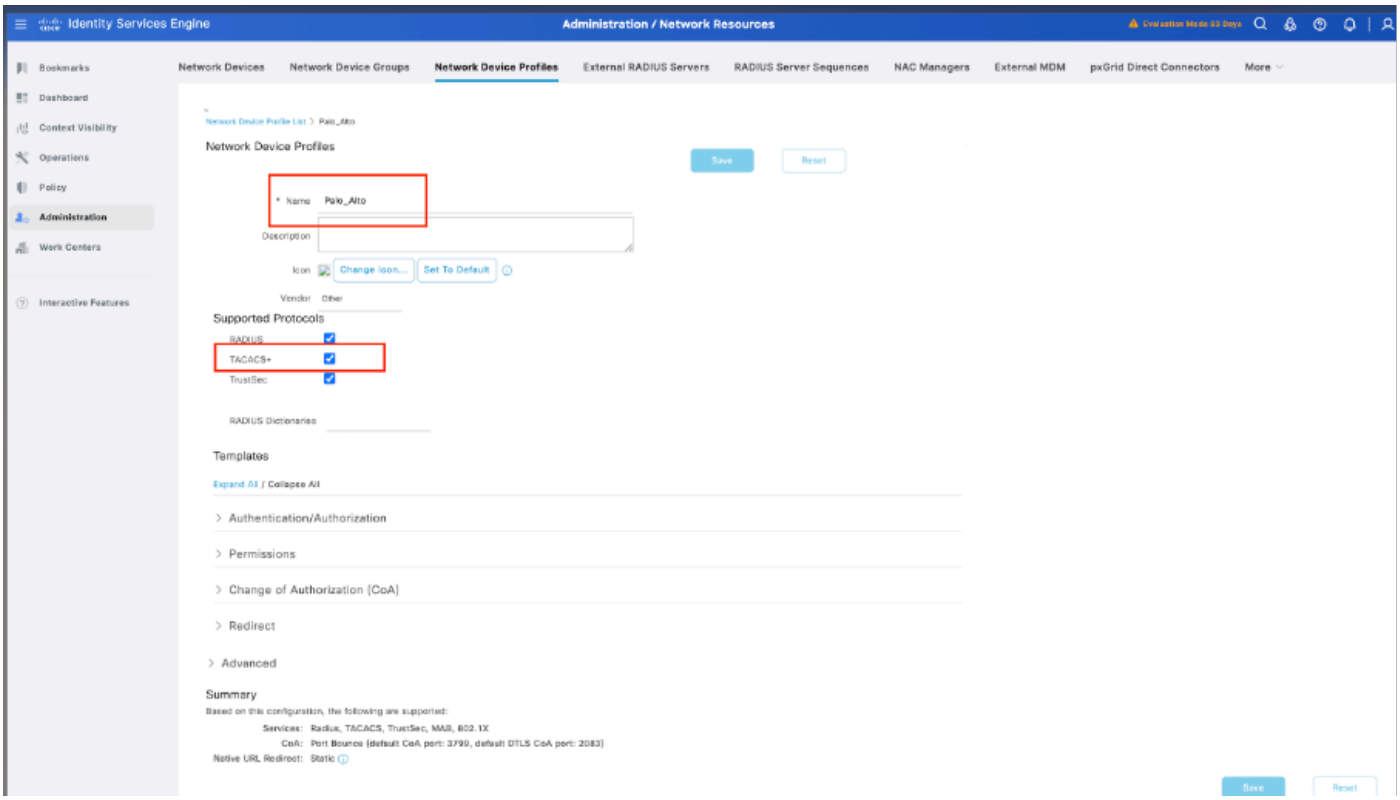


Paso 2. Desplácese hacia abajo para localizar la función Device Administration Service. Tenga en cuenta que para activar esta función es necesario que el usuario del servicio de políticas esté activo en el nodo, junto con las licencias TACACS+ disponibles en la implementación. Seleccione la casilla de verificación para activar la función y, a continuación, guarde la configuración.



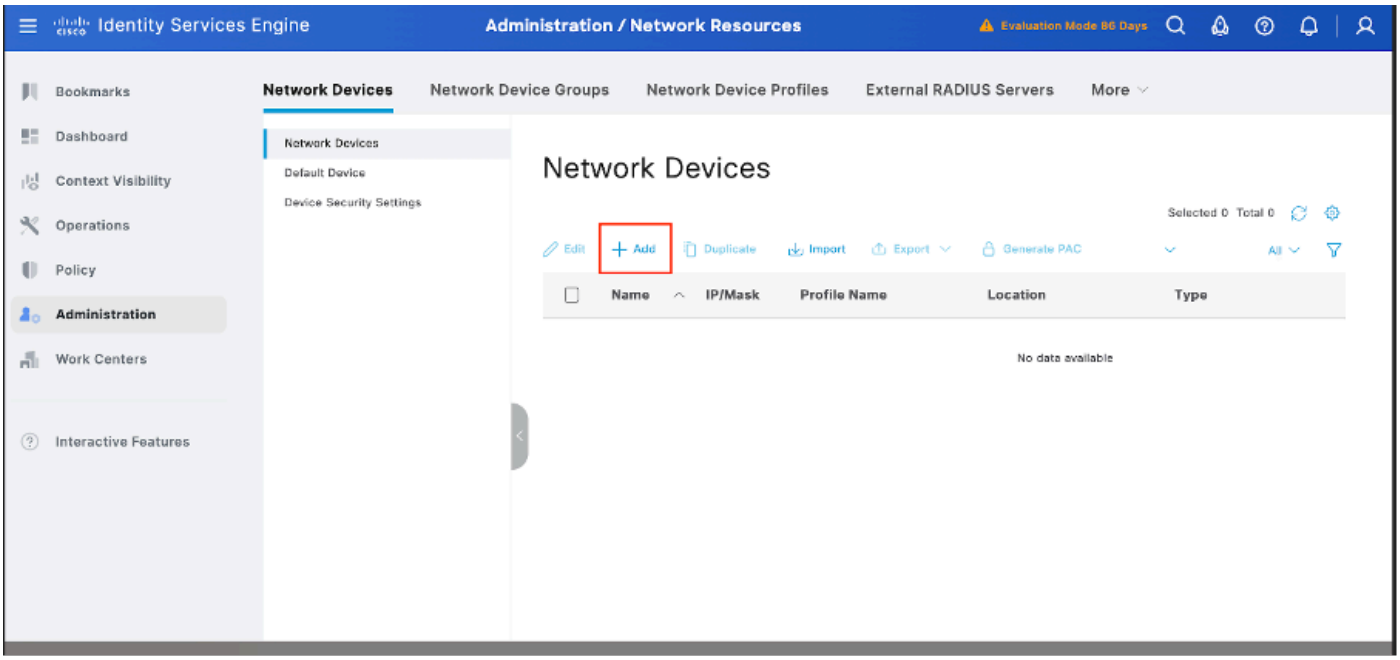
Paso 3. Configuración del perfil de dispositivo de red de Palo Alto para Cisco ISE.

Vaya a Administration > Network Resources > Network device profile. Haga clic en Agregar y mencione el nombre (Palo Alto) y habilite TACACS+ en los protocolos soportados.



Paso 4. Agregue Palo Alto como dispositivo de red.

1. Vaya a Administración > Recursos de red > Dispositivos de red > +Agregar.



2. Haga clic en Agregar e ingrese estos detalles:

Nombre: Palo Alto

IP Address: <IP de Palo-Alto>

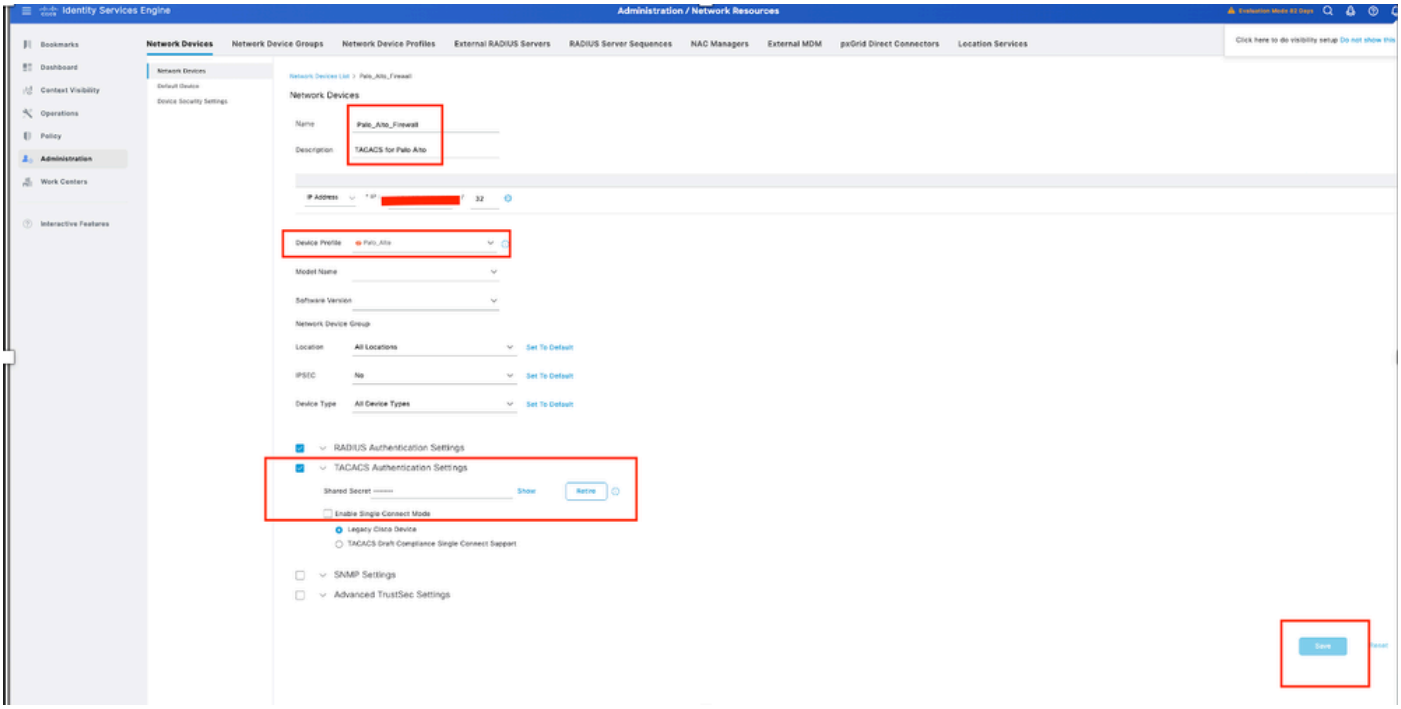
Perfil de dispositivo de red: select Palo Alto

Configuración de autenticación TACACS:

Habilitar autenticación TACACS+

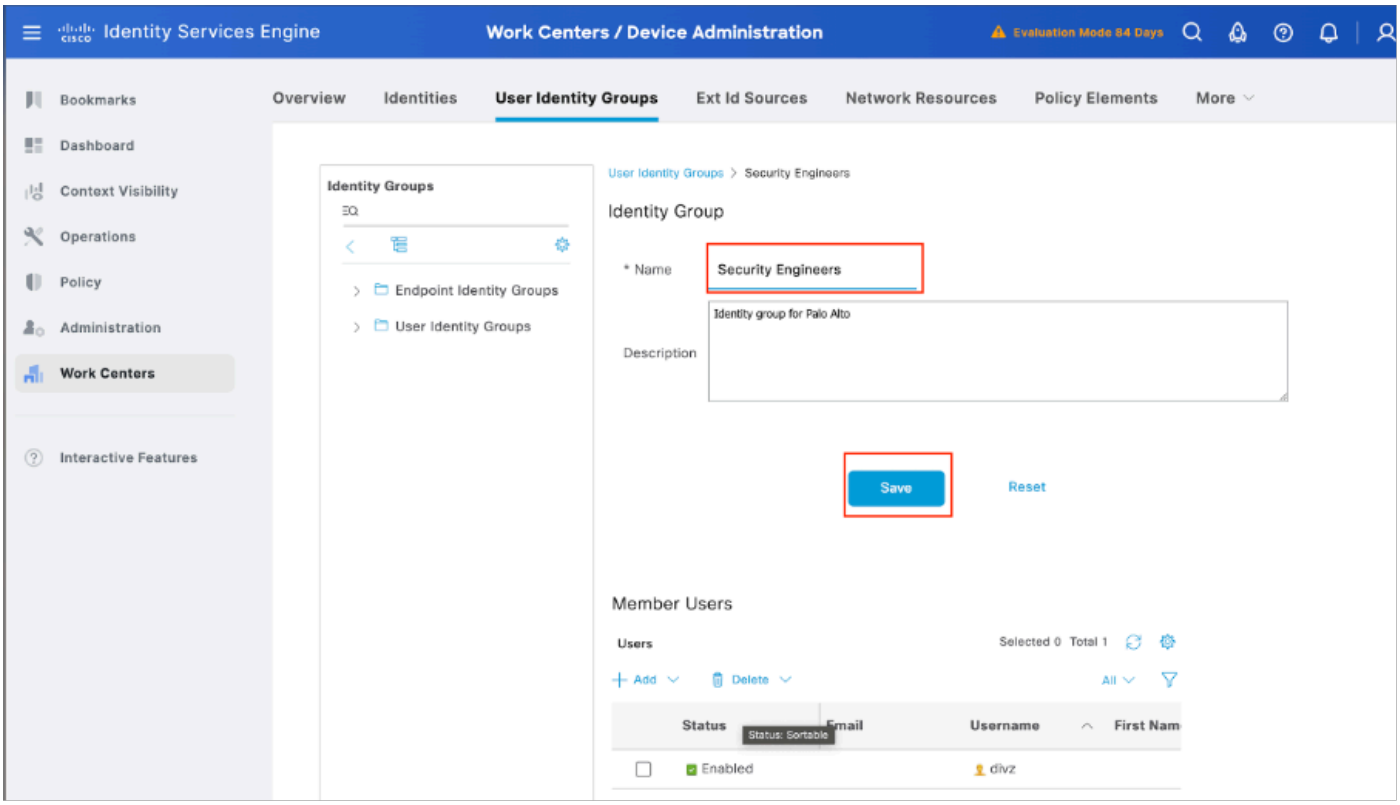
Introduzca la clave secreta compartida (debe coincidir con la configuración de Palo Alto)

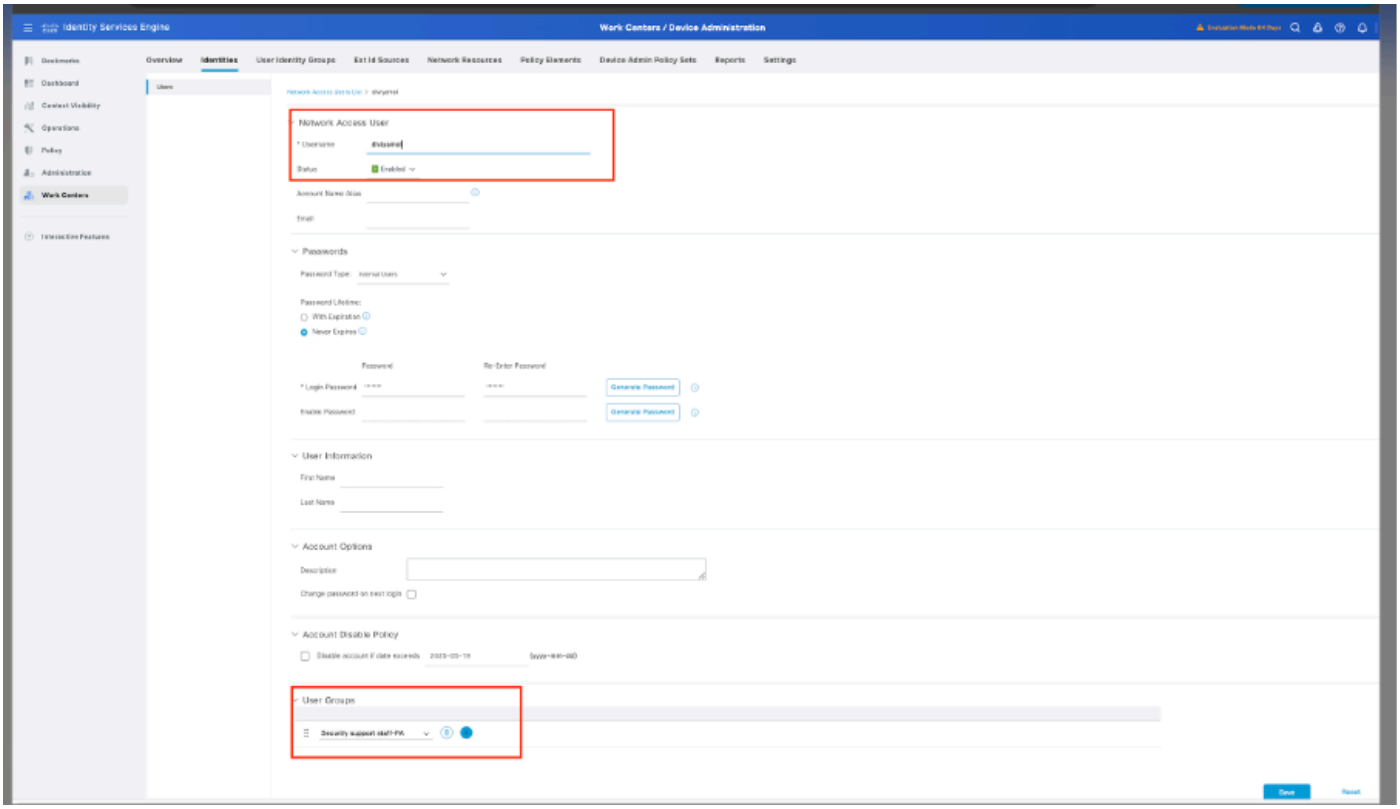
Click Save.

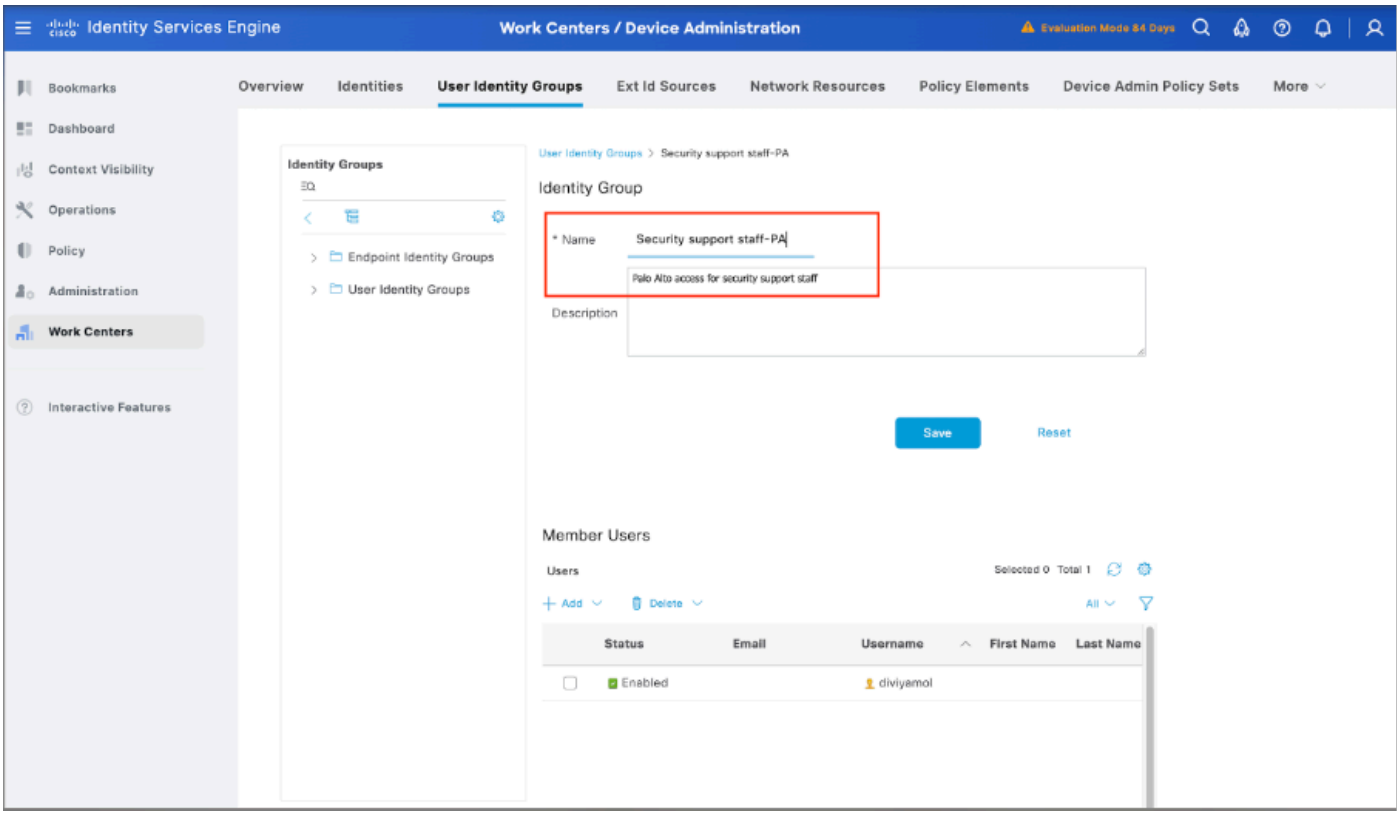


Paso 5. Crear grupos de identidad de usuarios.

Navegue hasta Centros de trabajo > Administración de dispositivos > Grupos de identidades de usuario, luego haga clic en Agregar y especifique el nombre para el grupo de usuarios.


Identity Services Engine
Work Centers / Device Administration
Evaluation Mode 84 Days
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Features
Overview
Identities
User Identity Groups
Ext Id Sources
Network Resources
Policy Elements
More
Identity Groups
Endpoint Identity Groups
User Identity Groups
User Identity Groups > Security Engineers
Identity Group
* Name
Security Engineers
Description
Identity group for Palo Alto
Save
Reset
Member Users
Users
Selected 0 Total 1
Add
Delete
All
Status
Email
Username
First Nam
Status: Sortable
Enabled
divz

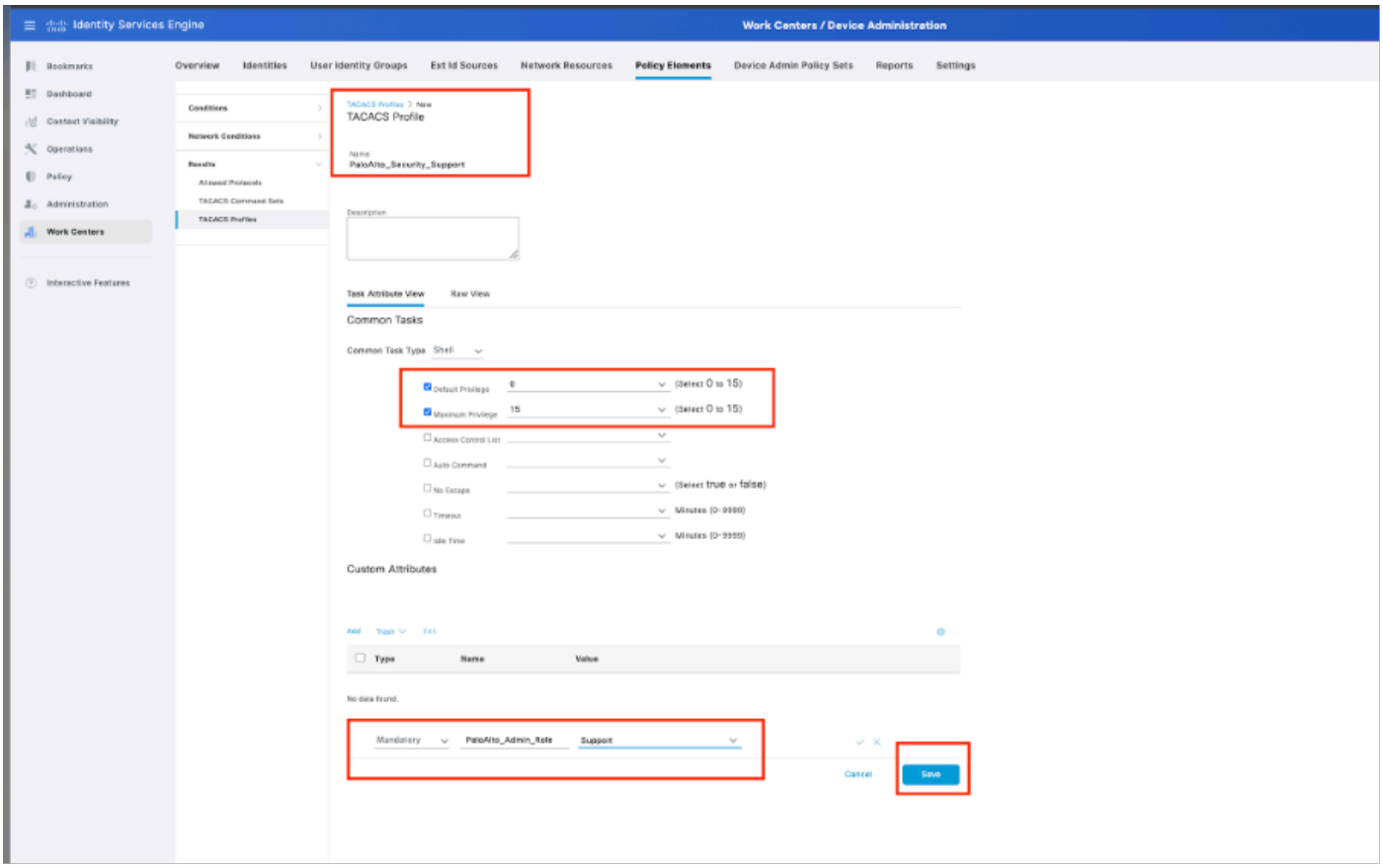

Identity Services Engine
Work Centers / Device Administration
Network Access User
Passwords
User Information
Account Options
Account Disable Policy
User Groups

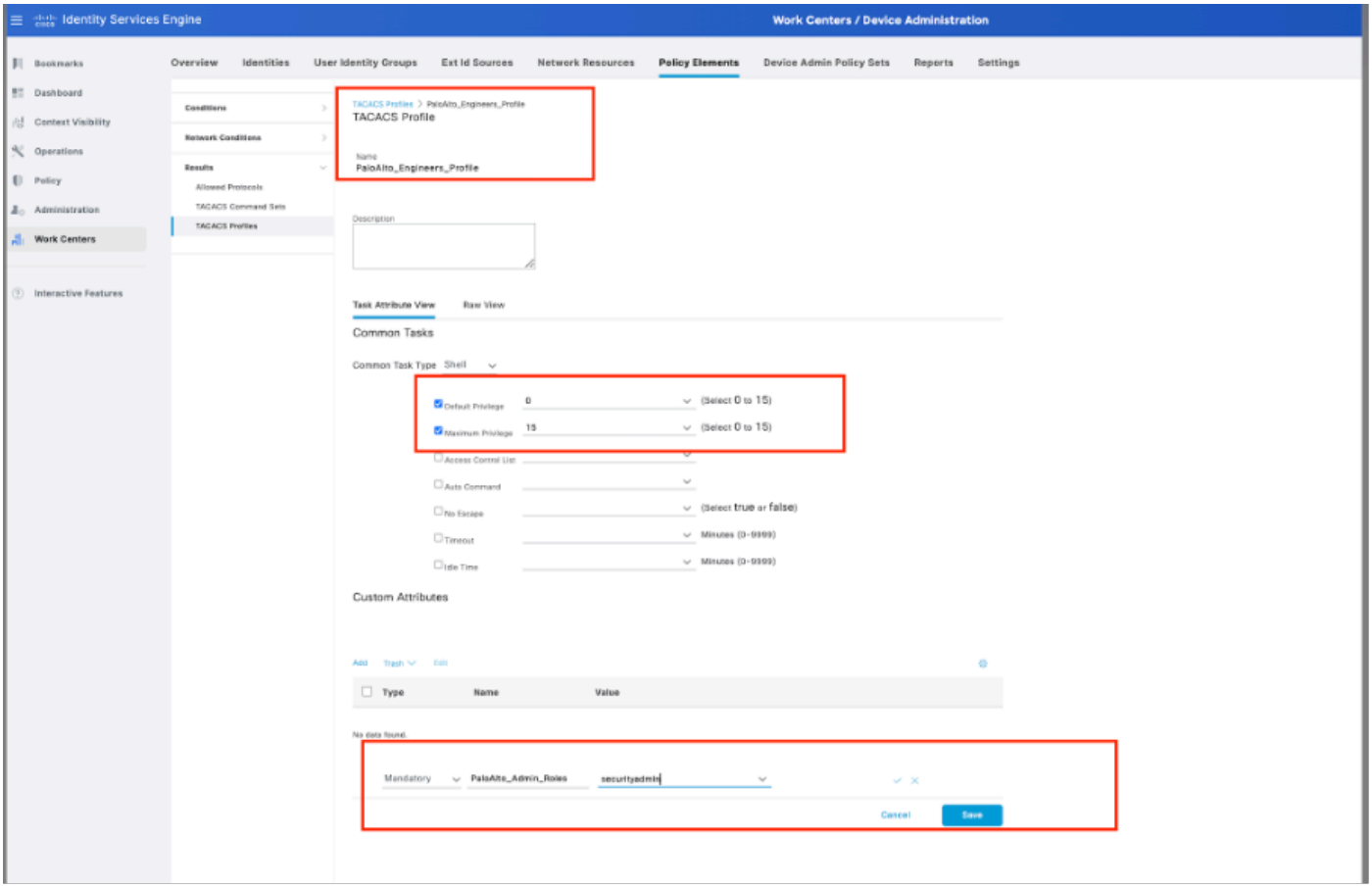


Paso 6. Configure Un Perfil TACACS.

Lo siguiente que debe hacer es configurar un perfil TACACS, que es donde puede configurar parámetros como el nivel de privilegio y el tiempo de espera. Vaya a Centros de trabajo > Administración de dispositivos -> Elementos de política -> Resultados -> Perfiles TACACS.

Haga clic en Agregar para crear un nuevo perfil TACACS. Dé un buen nombre al perfil.





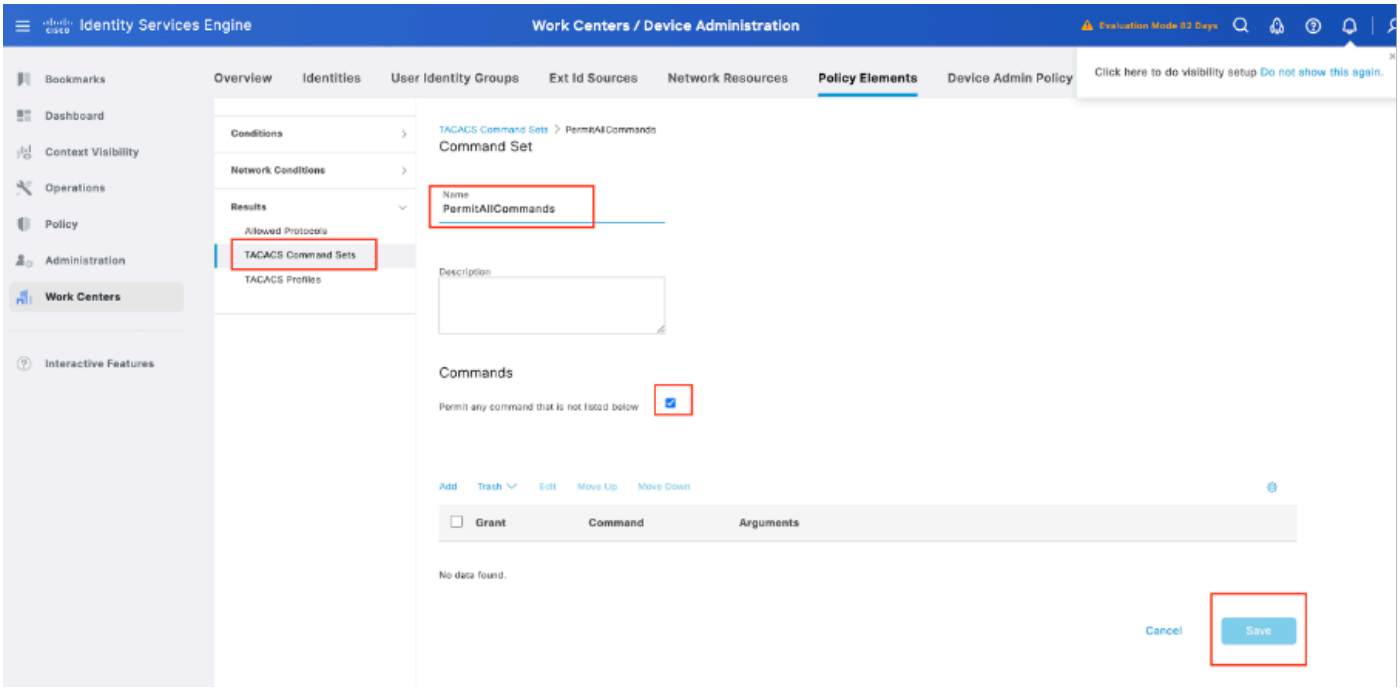
Paso 6. Configure los Conjuntos de Comandos TACACS.

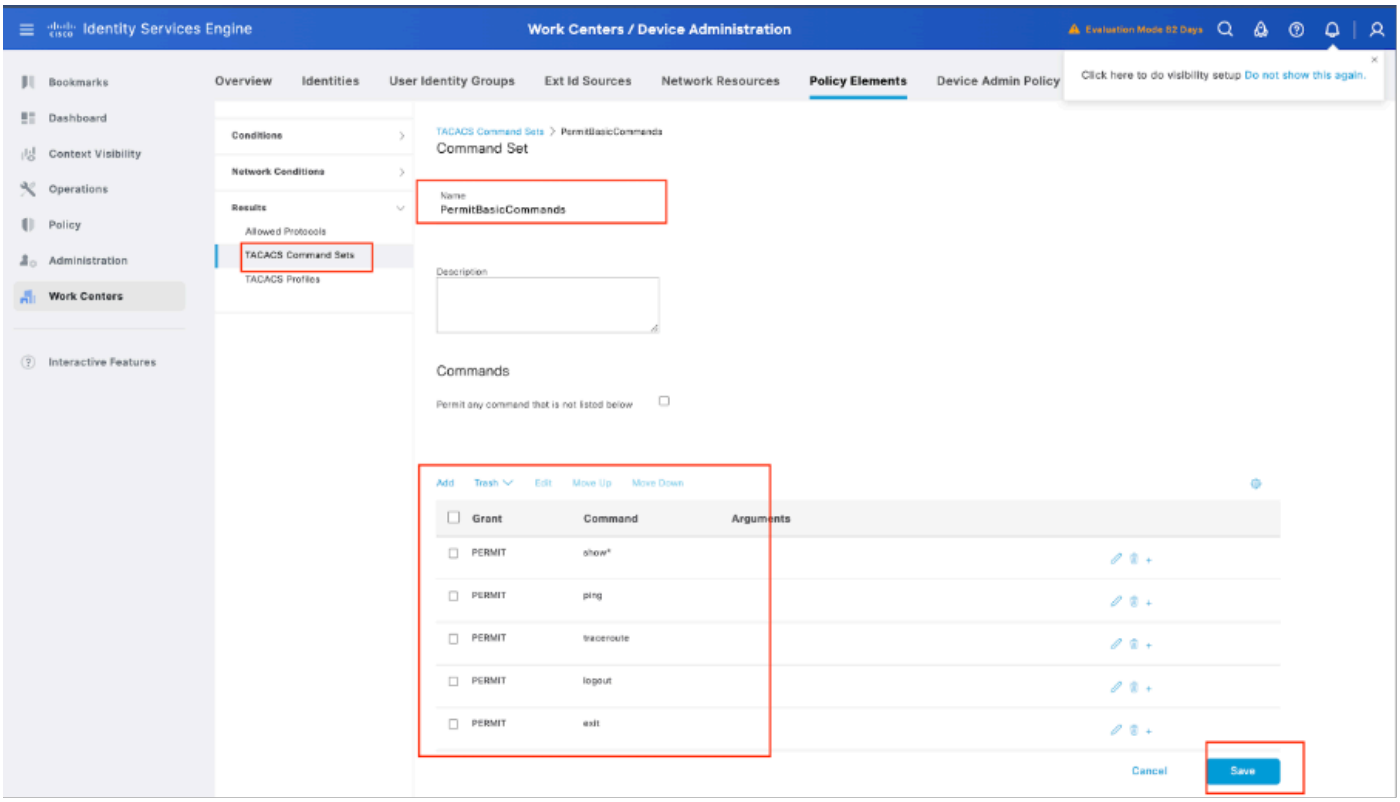
Ahora, es el momento de configurar qué comandos pueden utilizar los usuarios. Dado que puede

otorgar a ambos casos de uso el Nivel de Privilegio 15, que da acceso a todos los comandos disponibles, utilice los Conjuntos de Comandos TACACS para limitar los comandos que se pueden utilizar.

Vaya a Centros de trabajo > Administración de dispositivos > Elementos de política > Resultados -> Conjuntos de comandos TACACS. Haga clic en Agregar para crear un nuevo conjunto de comandos TACACS y denominarlo PermitAllCommands. Aplique este conjunto de comandos TACACS para el soporte de seguridad.

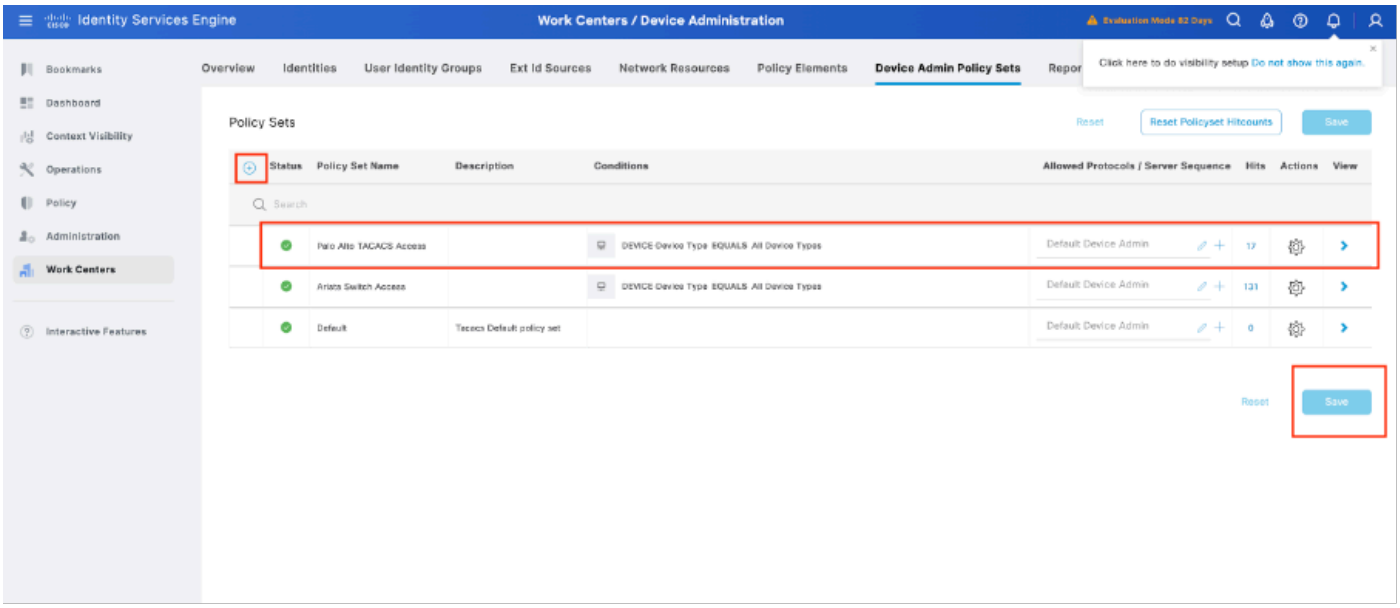
Lo único que necesita configurar en este conjunto de comandos TACACS es marcar la casilla Permit any command that is not listed below.





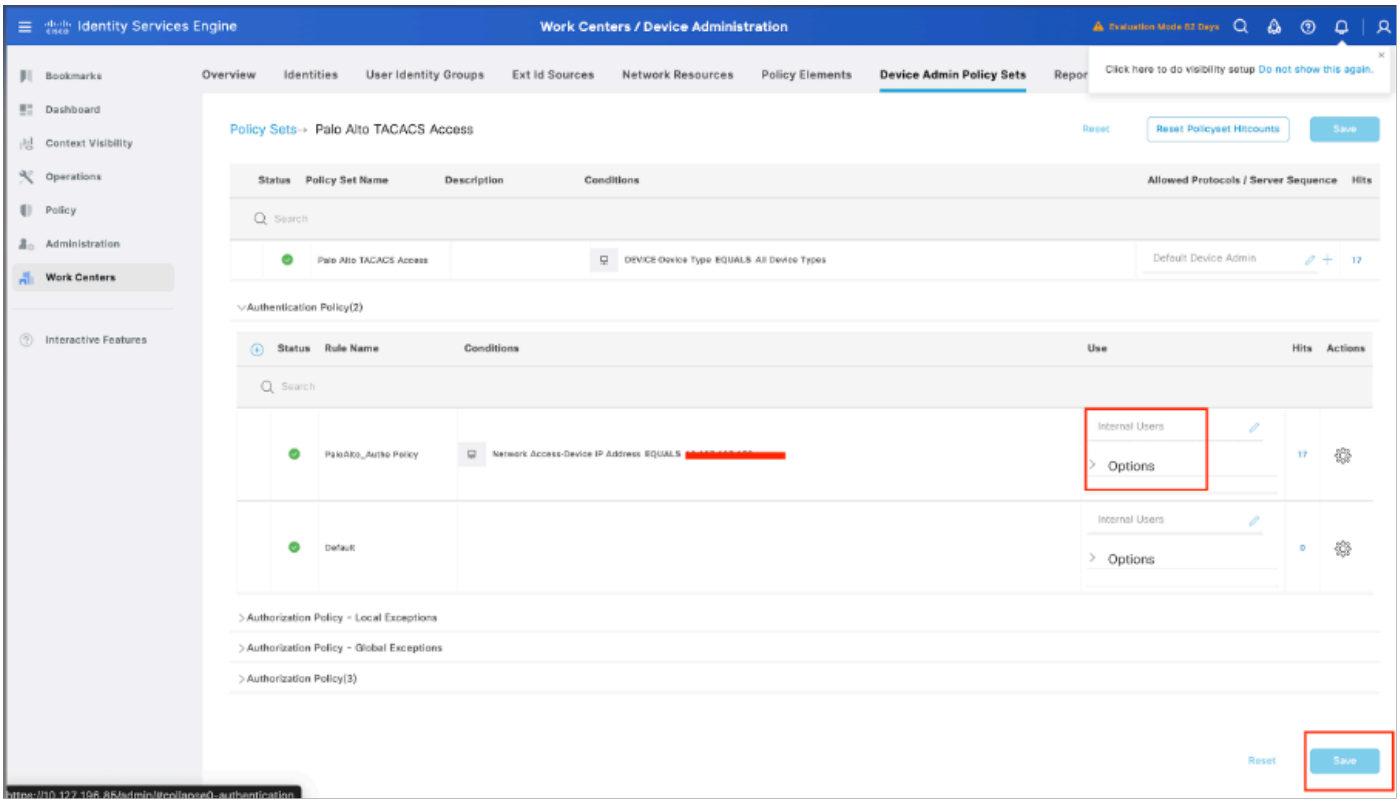
Paso 7. Cree un conjunto de políticas de administración de dispositivos para utilizarlo en Palo Alto. Navegue por el menú Centros de trabajo > Administración de dispositivos > Conjuntos de políticas de administración de dispositivos, y haga clic en el icono Agregar +.

Paso 8. Dé un nombre a este nuevo conjunto de políticas, agregue condiciones en función de las características de las autenticaciones TACACS+ que se estén realizando desde el firewall de Palo Alto y seleccione Protocolos permitidos > Administrador de dispositivos predeterminado. Guarde la configuración.

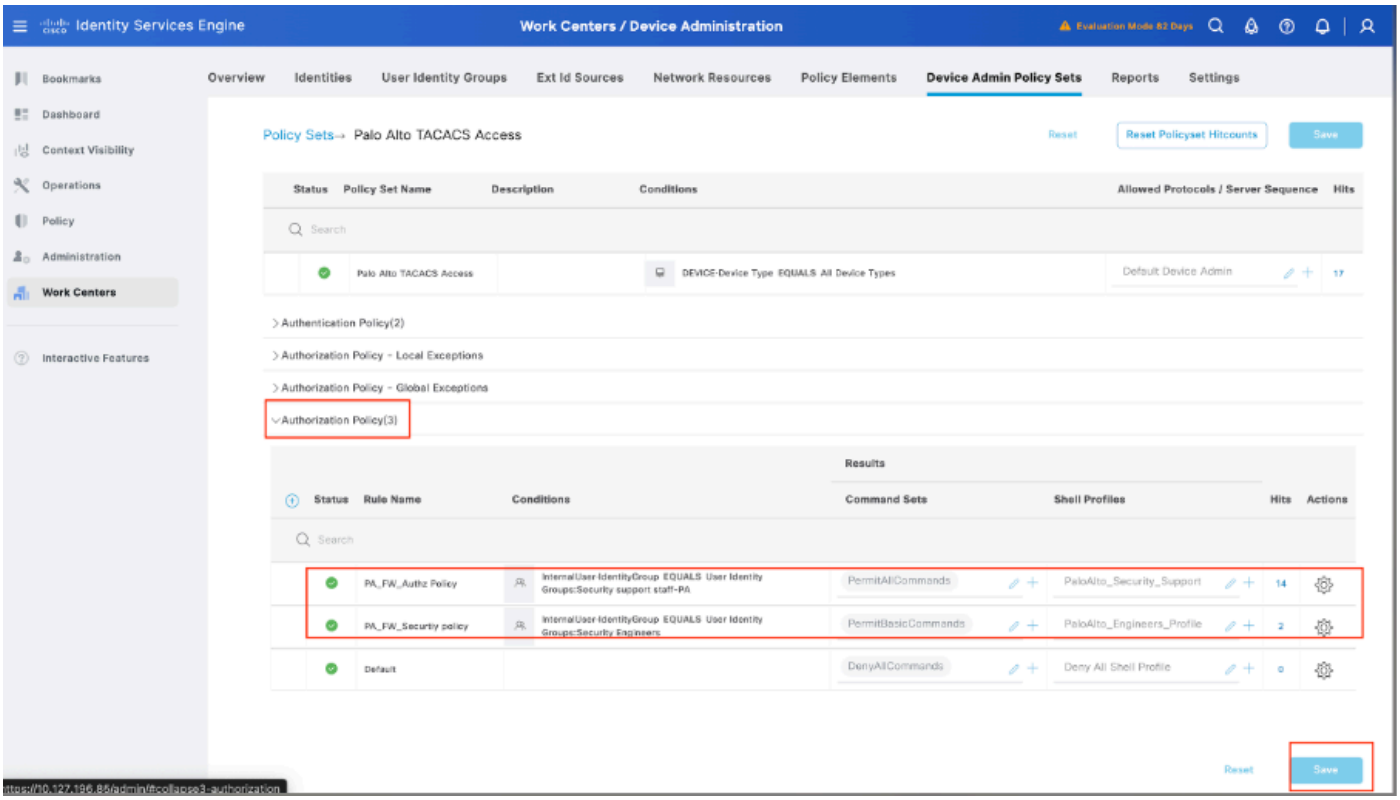


Paso 9. Seleccione la opción > view y, a continuación, en la sección Authentication Policy (Política de autenticación), seleccione el origen de identidad externo que Cisco ISE utiliza para consultar el nombre de usuario y las credenciales para la autenticación en el firewall de Palo Alto. En este

ejemplo, las credenciales corresponden a los usuarios internos almacenados en ISE.



Paso 10. Desplácese hacia abajo hasta la sección denominada Authorization Policy (Directiva de autorización) hasta la directiva Default (Predeterminada), seleccione el icono de engranaje y, a continuación, inserte una regla arriba.



Paso 11. Asigne un nombre a la nueva regla de autorización, agregue condiciones relativas al usuario que ya se ha autenticado como miembro del grupo y, en la sección Perfiles de shell,

agregue el perfil TACACS que configuró anteriormente y guarde la configuración.

Verificación

Revisión de ISE

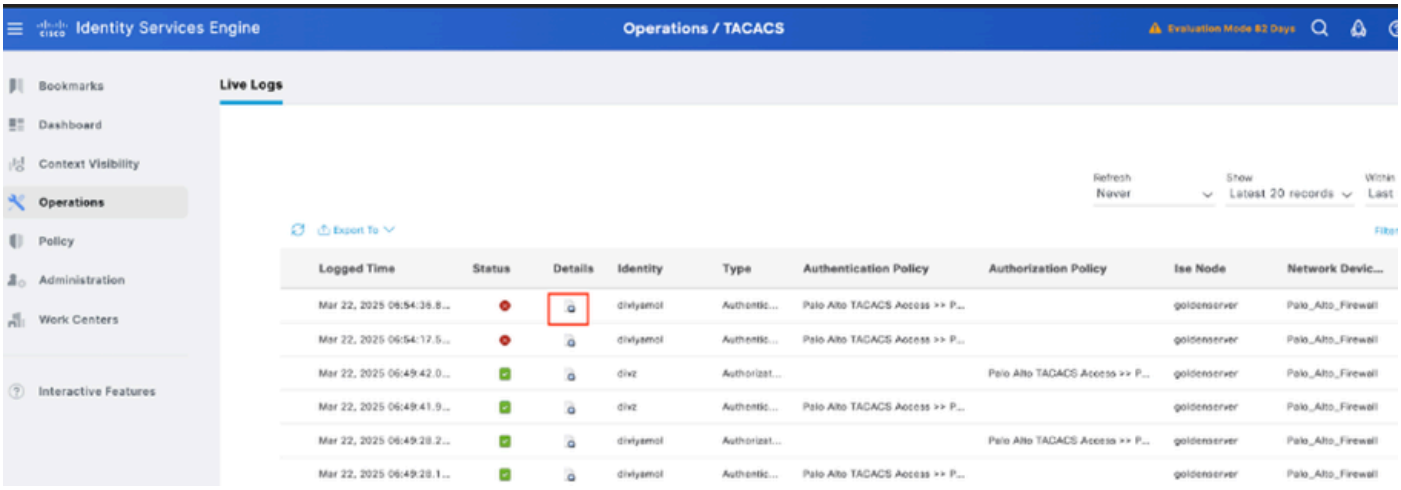
Paso 1. Revise si la capacidad de servicio de TACACS+ se está ejecutando, esto se puede registrar:

- GUI: Revise si el nodo aparece con el servicio DEVICE ADMIN en Administration -> System -> Deployment.
- CLI: Ejecute el comando show ports | incluir 49 para confirmar que hay conexiones en el puerto TCP que pertenecen a TACACS+

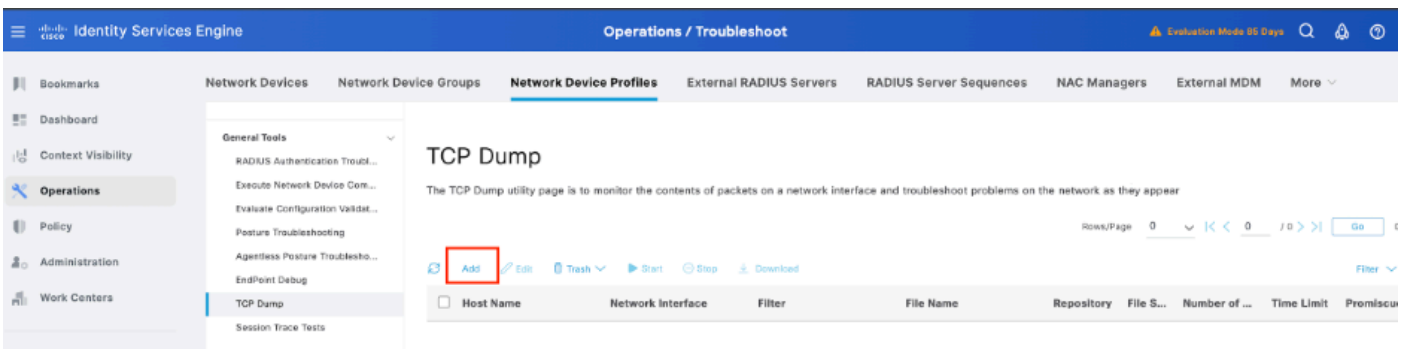
```
goldenserver/admin#show ports | include 49
tcp: [redacted]
```

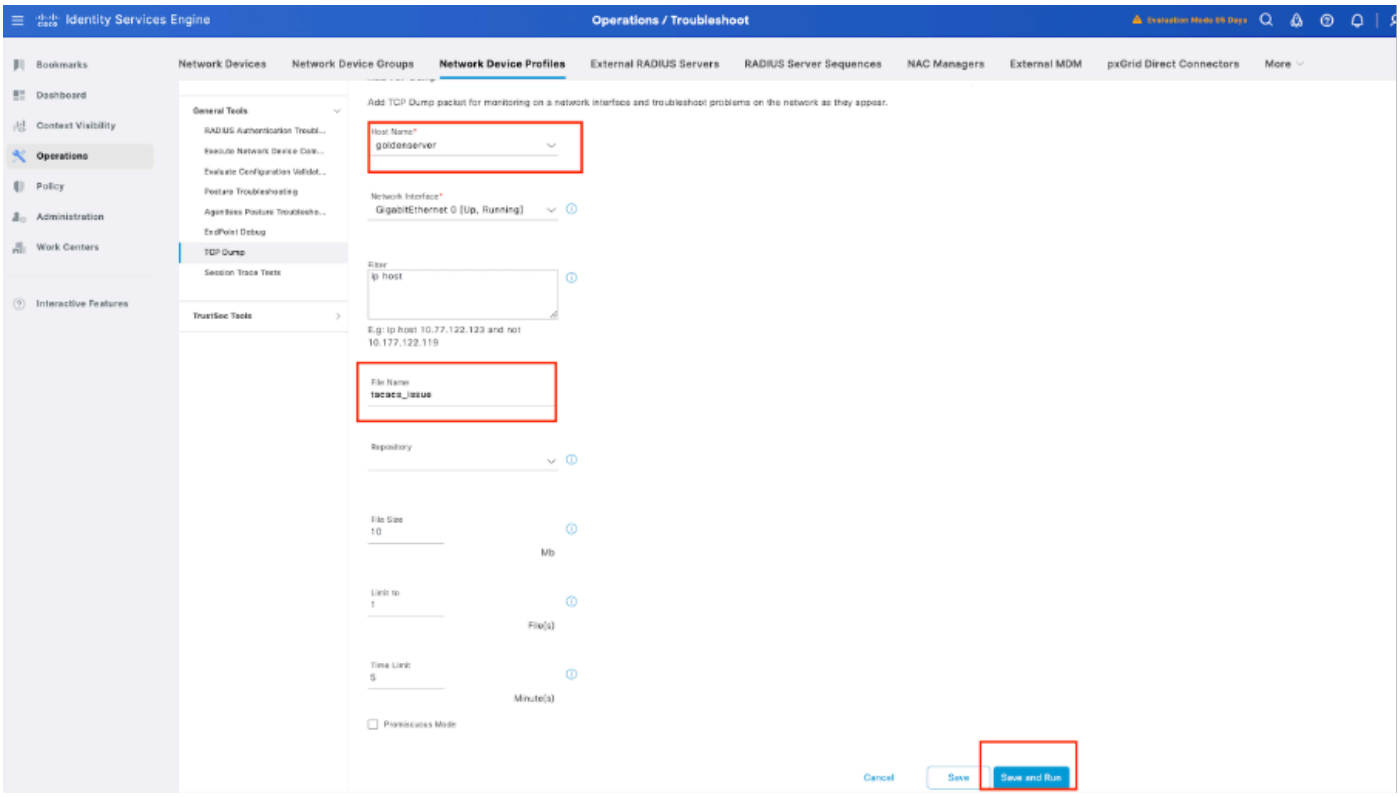
Paso 2. Confirme si hay registros en vivo relacionados con intentos de autenticación TACACS+ : esto se puede verificar en el menú Operations -> TACACS -> Live logs.

Dependiendo del motivo del fallo, puede ajustar la configuración o abordar la causa del fallo.

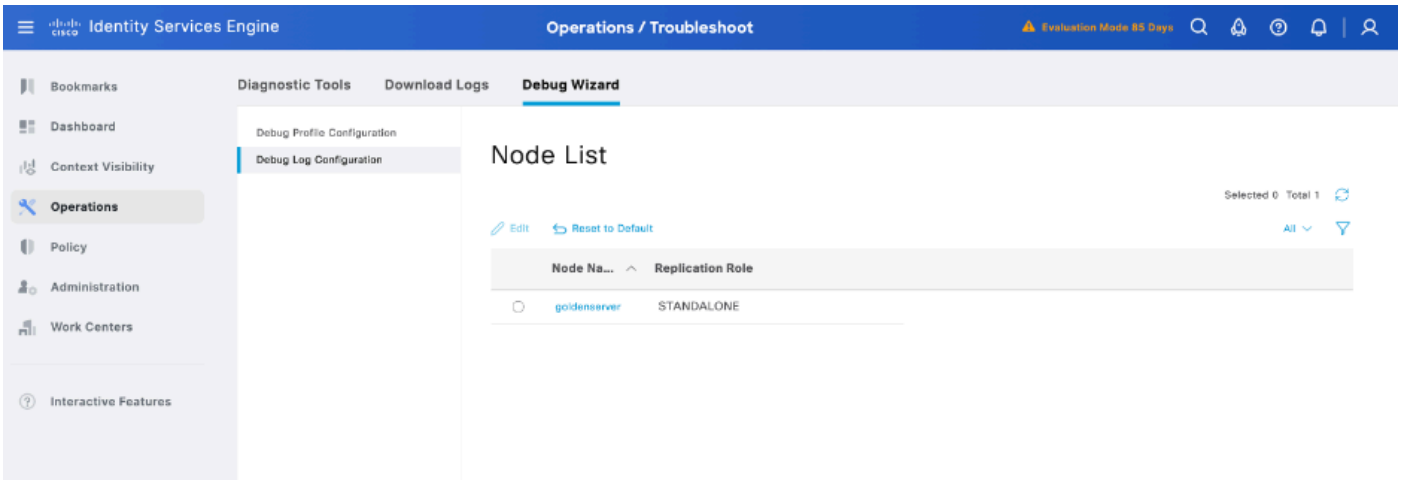


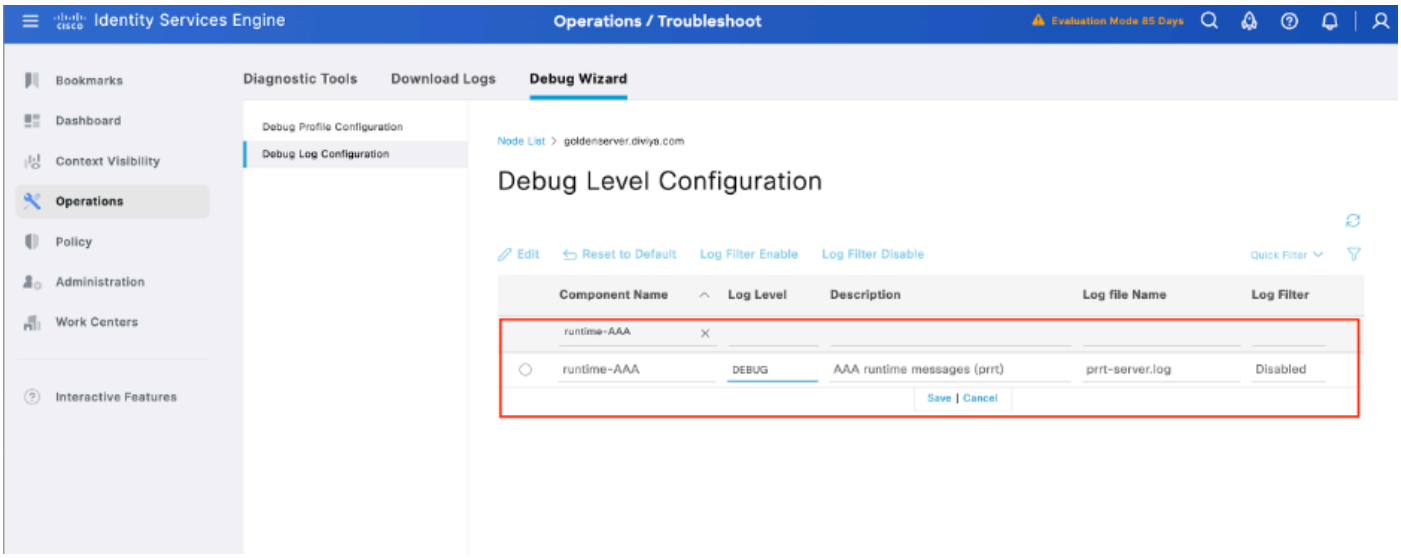
Paso 3. En caso de que no vea ningún registro en vivo, continúe con la captura de paquetes y navegue hasta el menú Operaciones > Solución de problemas > Herramientas de diagnóstico > Herramientas generales > Volcado TCP , seleccione Agregar.





Paso 4. Habilite el componente runtime-AAA en debug dentro de PSN desde donde se realiza la autenticación en Operaciones > Troubleshooting > Debug Wizard > Debug log configuration, seleccione el nodo PSN , luego seleccione next en el botón de edición .





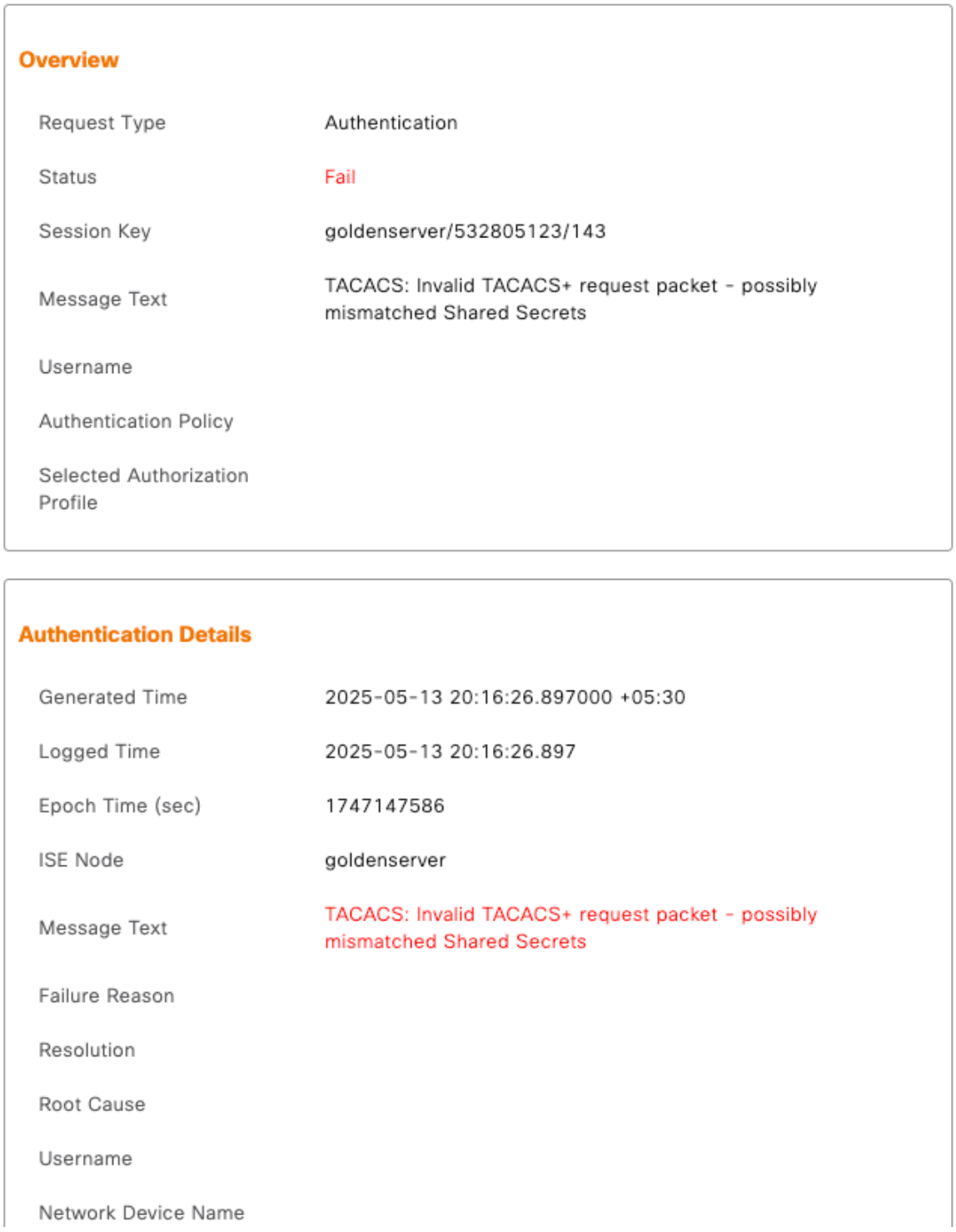
Identifique el componente runtime-AAA, establezca su nivel de registro en debug, reproduzca el problema y analice los registros para una investigación adicional.

Resolución de problemas

TACACS: Paquete de solicitud TACACS+ no válido: posiblemente secretos compartidos no coincidentes

Problema

La autenticación TACACS+ entre Cisco ISE y el firewall de Palo Alto (o cualquier dispositivo de red) falla con el mensaje de error:
"Paquete de solicitud TACACS+ no válido; posiblemente secretos compartidos no coincidentes"



Esto evita los intentos de inicio de sesión administrativos exitosos y puede afectar el control de acceso del dispositivo a través de la autenticación centralizada.

Posibles Causas

- Una discordancia en el secreto compartido configurado en Cisco ISE y el firewall o dispositivo de red de Palo Alto.
- Configuración incorrecta del servidor TACACS+ en el dispositivo (como dirección IP, puerto o protocolo incorrecto).

Solución

Hay varias posibles soluciones para este problema:

1. Compruebe la clave secreta compartida:

- En Cisco ISE:
  Vaya a Administration > Network Resources > Network Devices , seleccione el dispositivo afectado y confirme el secreto compartido.

- En el firewall de Palo Alto:
  Vaya a Device > Server Profiles > TACACS+, y asegúrese de que el secreto compartido coincida exactamente, incluyendo mayúsculas y minúsculas y caracteres especiales.

2. Compruebe la configuración del servidor TACACS+:

- Asegúrese de que la dirección IP y el puerto correctos (el predeterminado es el 49) de Cisco ISE están configurados en el perfil TACACS+ del firewall.

- Confirme que el tipo de protocolo es TACACS+ (no RADIUS).

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).