Configuración de TACACS+ con la interfaz ISE Gigabit Ethernet 1

Contenido

Introducción

Este documento describe la configuración de ISE TACACS+ con interfaz Gigabit Ethernet 1, donde el router y el switch funcionan como dispositivos de red.

Antecedentes

Cisco ISE admite hasta 6 interfaces Ethernet. Sólo puede tener tres enlaces, enlace 0, enlace 1 y enlace 2. No se pueden cambiar las interfaces que forman parte de un enlace ni cambiar la

función de la interfaz en un enlace.

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos sobre estos temas:

- Conocimientos básicos sobre redes
- Cisco Identity Service Engine.

Componentes Utilizados

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

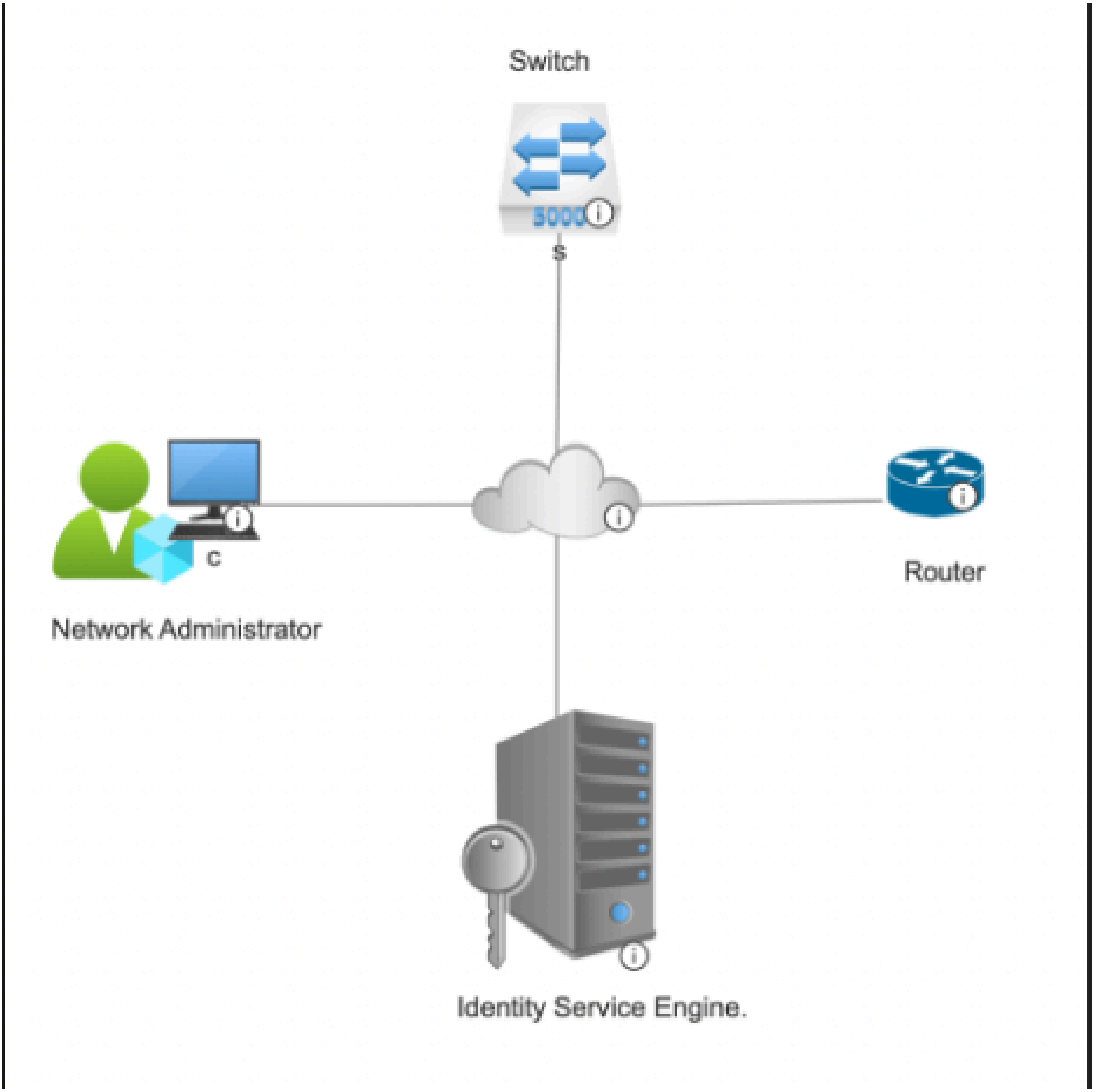
- Cisco Identity Service Engine versión 3.3
- Cisco IOS® Software Release 17.x
- Switch Cisco C9200.

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

El objetivo de la configuración es: Configure Gigabit Ethernet 1 de ISE para TACACS+ y autentique el switch y el router con TACACS+ con ISE como servidor de autenticación.

Diagrama de la red

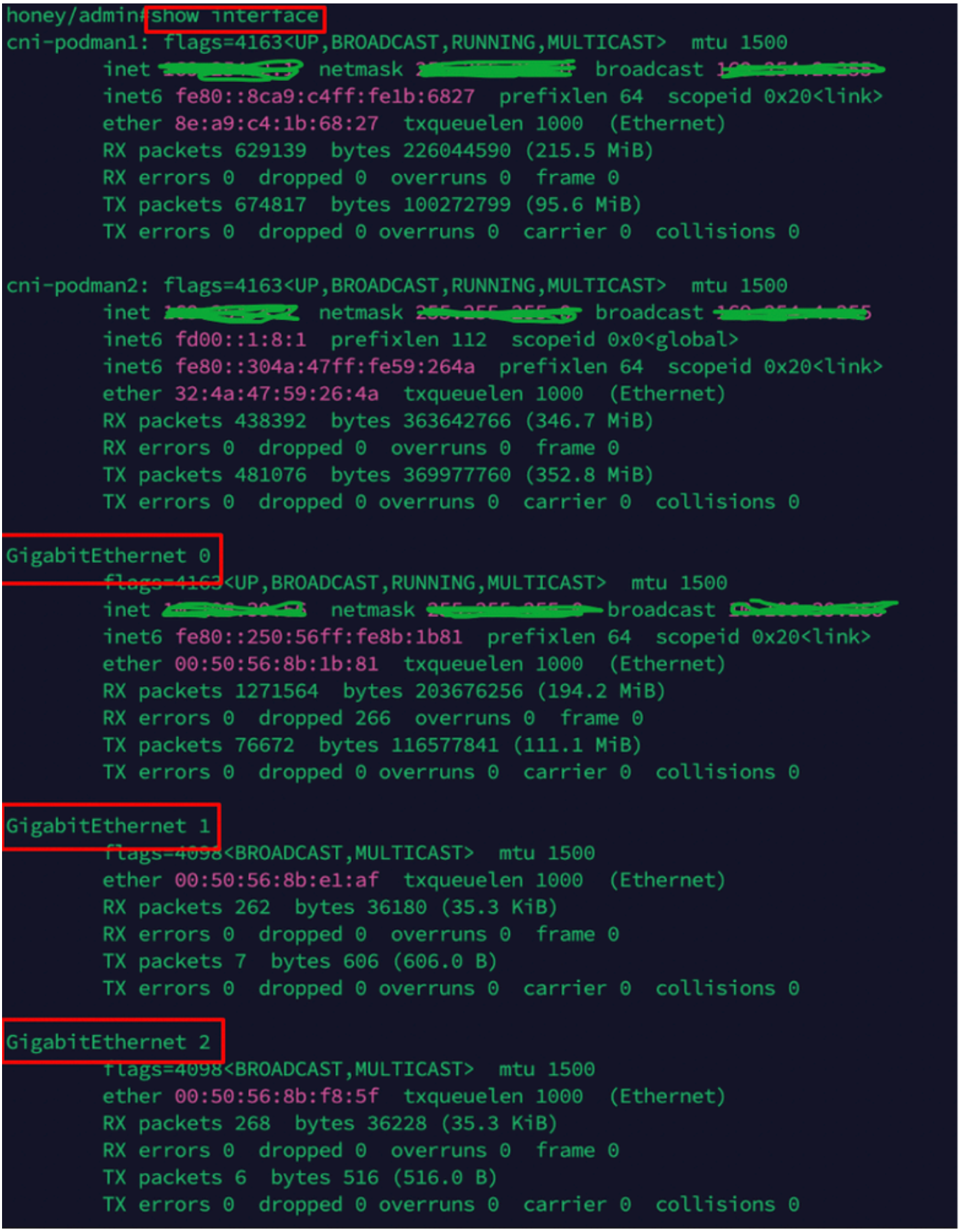


Topología de red

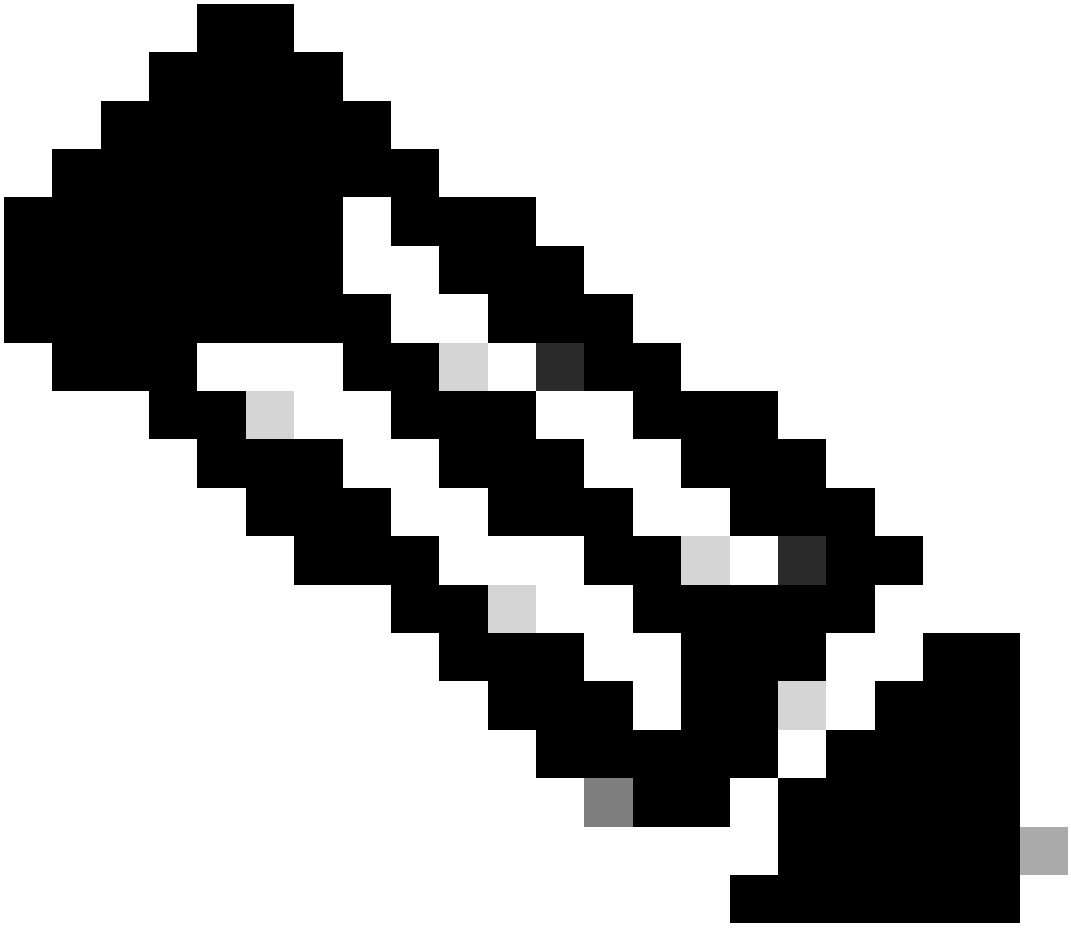
Configuración de Identity Services Engine para TACACS+

Configuración de la dirección IP para la interfaz Gigabit Ethernet 1 en ISE

1. Inicie sesión en la CLI del nodo PSN de ISE donde Device admin está habilitado y verifique las interfaces disponibles mediante el comando show interface:



Verificación de interfaces en ISE



Nota: En esta configuración, solo se configuran tres interfaces en ISE, centrándose en la interfaz Gigabit Ethernet 1. Se puede aplicar el mismo procedimiento para configurar la dirección IP para todas las interfaces. De forma predeterminada, ISE admite hasta seis interfaces Gigabit Ethernet.

---

2. Desde la CLI del mismo nodo PSN, asigne una dirección IP a la interfaz Gigabit Ethernet 1 mediante estos comandos:

hostnameofise#configure t

hostname ofiles/admin(config)#interface Gigabit Ethernet 1

hostname/admin(config-GigabitEthernet-1)# <ip address> <subnet netmask> % El cambio de la dirección IP puede hacer que se reinicien los servicios de ise

¿Desea continuar con el cambio de dirección IP?

¿Continuar? [sí,no] sí

3. Al realizar el paso 2, se reinician los servicios de nodos de ISE. Para verificar el estado de los servicios ISE, ejecute el comando show application status ise y asegúrese de que el estado de los servicios se esté ejecutando según esta captura de pantalla:

```
honey/admin#show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          1739169
Database Server                        running          102 PROCESSES
Application Server                     running          1755746
Profiler Database                      running          1746379
ISE Indexing Engine                    running          1757121
AD Connector                           running          1759148
M&T Session Database                   running          1752122
M&T Log Processor                      running          1755926
Certificate Authority Service          running          1759026
EST Service                            running          1786647
SXP Engine Service                     disabled
TC-NAC Service                         disabled
PassiveID WMI Service                  disabled
PassiveID Syslog Service               disabled
PassiveID API Service                  disabled
PassiveID Agent Service                disabled
PassiveID Endpoint Service             disabled
PassiveID SPAN Service                 disabled
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
ISE Messaging Service                  running          1743222
ISE API Gateway Database Service       running          1745409
ISE API Gateway Service                running          1750887
ISE pxGrid Direct Service              running          1874179
Segmentation Policy Service            disabled
REST Auth Service                      disabled
SSE Connector                          disabled
Hermes (pxGrid Cloud Agent)            disabled
McTrust (Meraki Sync Service)          disabled
ISE Node Exporter                      running          1760519
ISE Prometheus Service                 running          1762540
ISE Grafana Service                    running          1765779
ISE MNT LogAnalytics Elasticsearch     running          1768218
ISE Logstash Service                   running          1773207
ISE Kibana Service                     running          1774914
ISE Native IPSec Service               running          1779658
MFC Profiler                           running          1932013
```

Verificación del estado del servicio ISE

4. Verifique la dirección IP de la interfaz Gig1 mediante el comando show interface:

V

```
honey/admin#show interface
cni-podman1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::8ca9:c4ff:fe1b:6827  prefixlen 64  scopeid 0x20<link>
        ether 8e:a9:c4:1b:68:27  txqueuelen 1000  (Ethernet)
        RX packets 633876  bytes 228753800 (218.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 680052  bytes 102100762 (97.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

cni-podman2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fd00::1:8:1  prefixlen 112  scopeid 0x0<global>
        inet6 fe80::304a:47ff:fe59:264a  prefixlen 64  scopeid 0x20<link>
        ether 32:4a:47:59:26:4a  txqueuelen 1000  (Ethernet)
        RX packets 503576  bytes 516105026 (492.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 595701  bytes 383404526 (365.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 0
        flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::250:56ff:fe8b:1b81  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:8b:1b:81  txqueuelen 1000  (Ethernet)
        RX packets 1387052  bytes 213478717 (203.5 MiB)
        RX errors 0  dropped 266  overruns 0  frame 0
        TX packets 136494  bytes 261900250 (249.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 1
        flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::250:56ff:fe8b:e1af  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:8b:e1:af  txqueuelen 1000  (Ethernet)
        RX packets 5165  bytes 1072036 (1.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 2260 (2.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Verificación de la dirección IP de la interfaz ISE Gig2 desde CLI

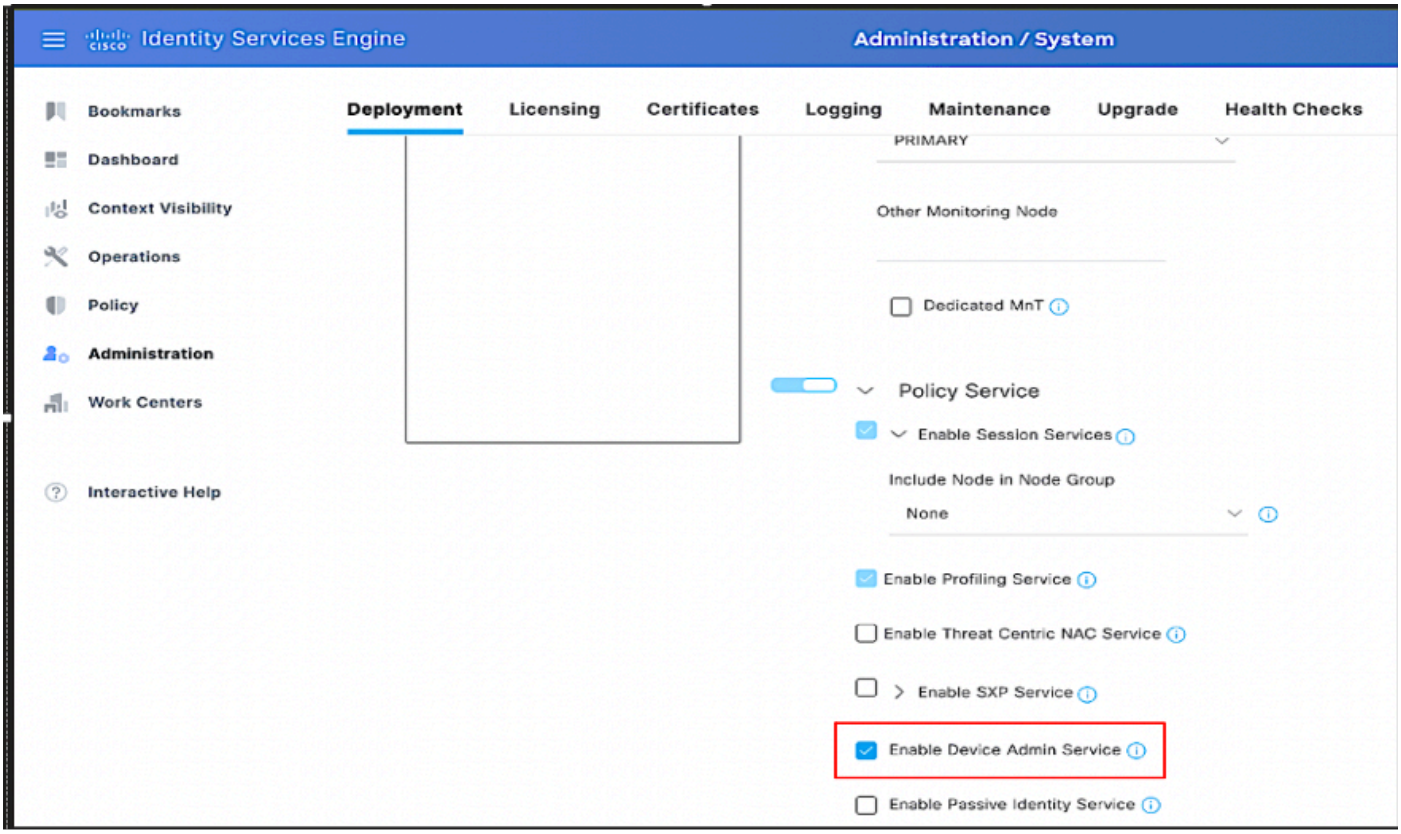
5.Verifique la tolerancia del puerto 49 en el nodo ISE mediante el comando show ports | inc 49 command:

```
honey/admin#show ports | include 49
        tcp: 127.0.0.1:8888, 169.254.4.1:49, 169.254.2.1:49, [redacted]:49, [redacted]:49,
```

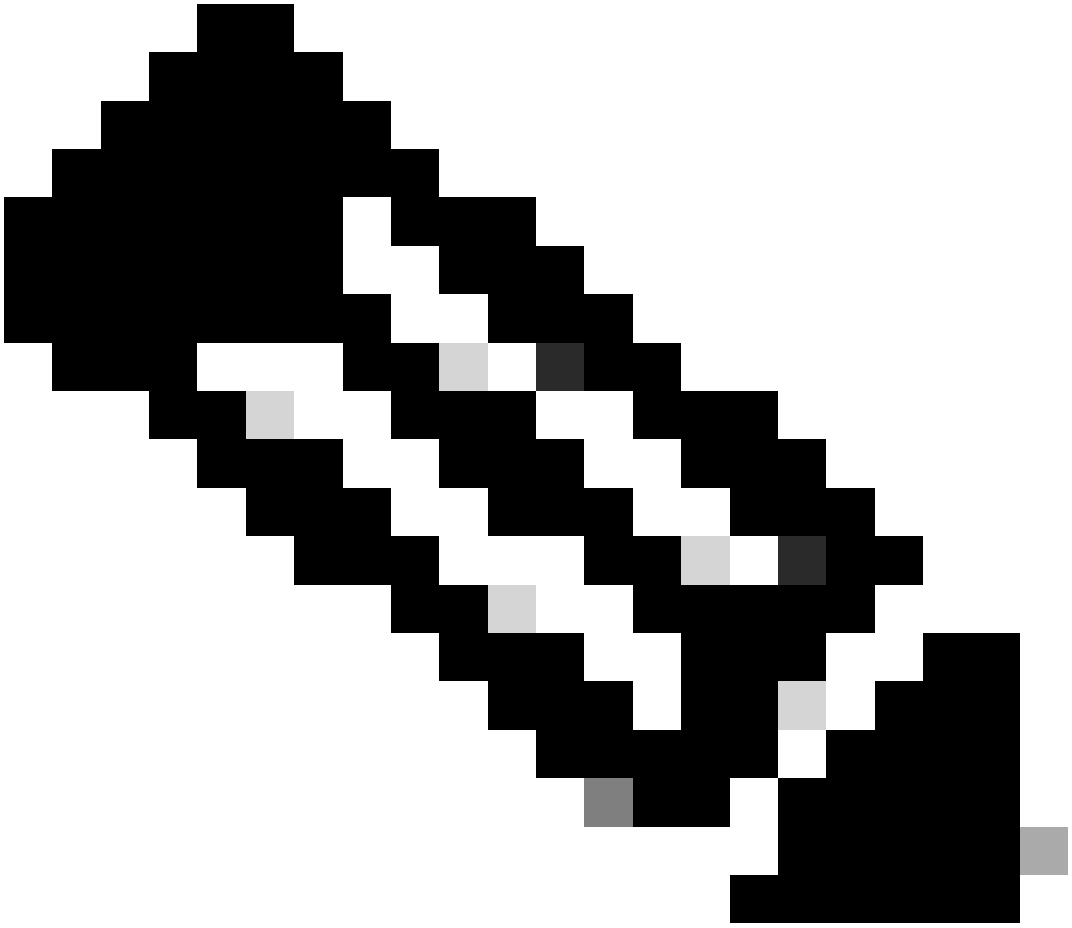
verificación de la asignación del puerto 49 en ISE

Habilitar la administración de dispositivos en ISE

Vaya a GUI de ISE > Administration > Deployment > Select the PSN node y, a continuación, marque Enable Device admin service:



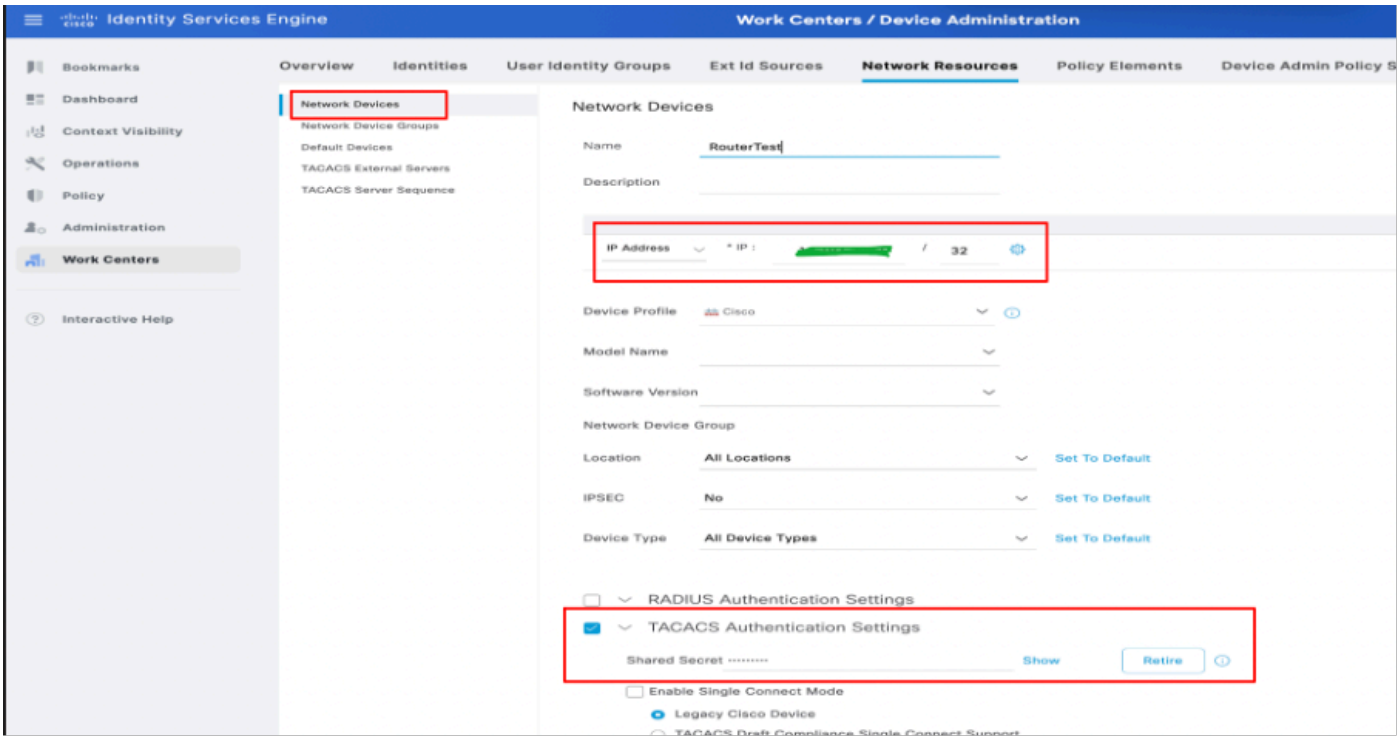
Habilitación del servicio Device Administration en ISE



Nota: Para habilitar el servicio Device Admin, se requiere una licencia Device Administration.

Agregar un dispositivo de red en ISE

1. Vaya a Centros de trabajo > Administración de dispositivos > Recursos de red > Dispositivos de red. Haga clic en Add (Agregar). Proporcione el nombre y la dirección IP. Seleccione la casilla de verificación Configuración de autenticación TACACS+ y proporcione la clave secreta compartida.



Configuración del dispositivo de red en ISE

2. Siga el procedimiento anterior para agregar todos los dispositivos de red requeridos para la autenticación TACACS.

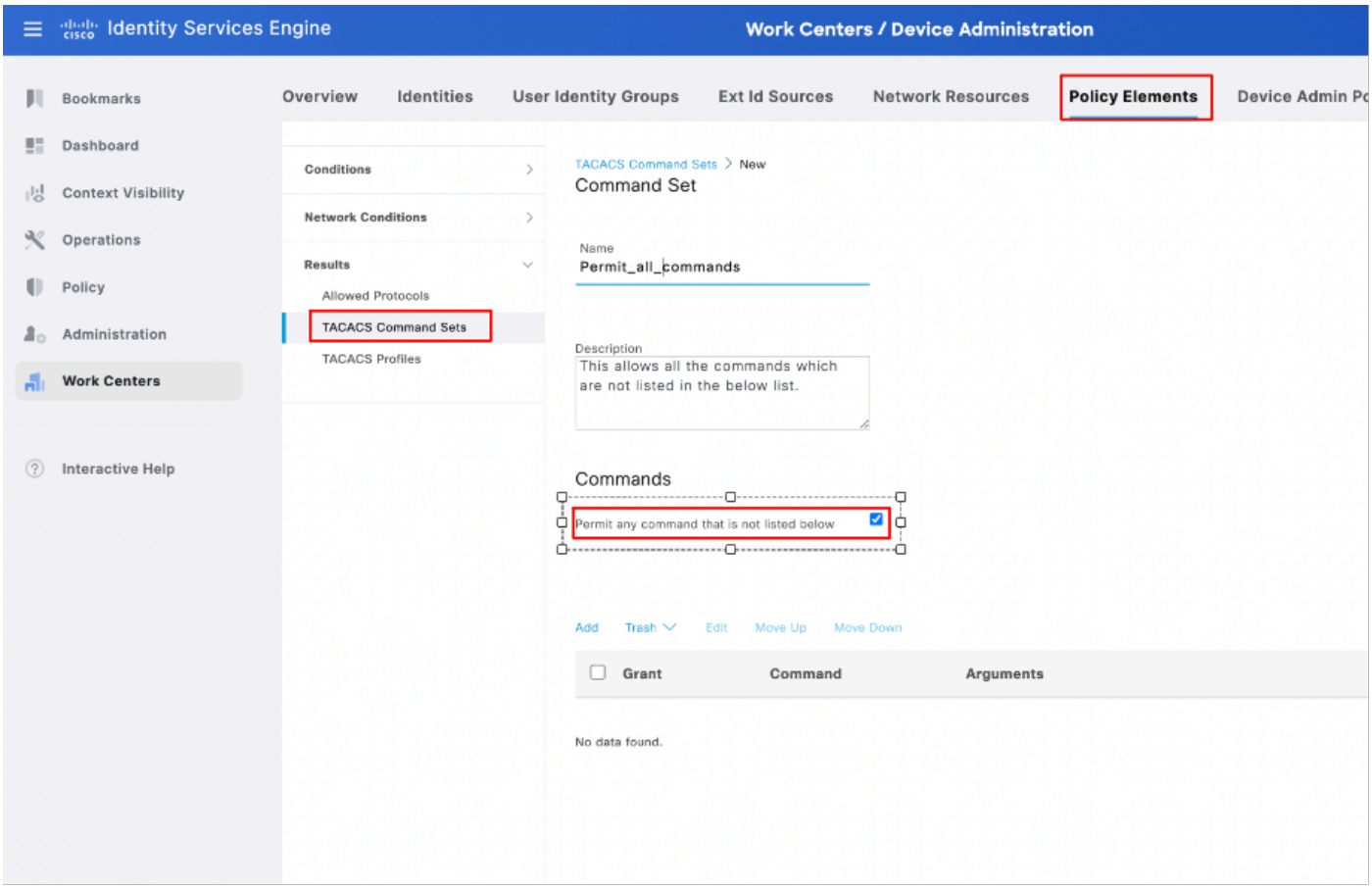
Configurar conjuntos de comandos de TACACS+

Se configuran dos conjuntos de comandos para esta demostración:

Permit_all_commands, se asigna al usuario admin y permite todos los comandos en el dispositivo.

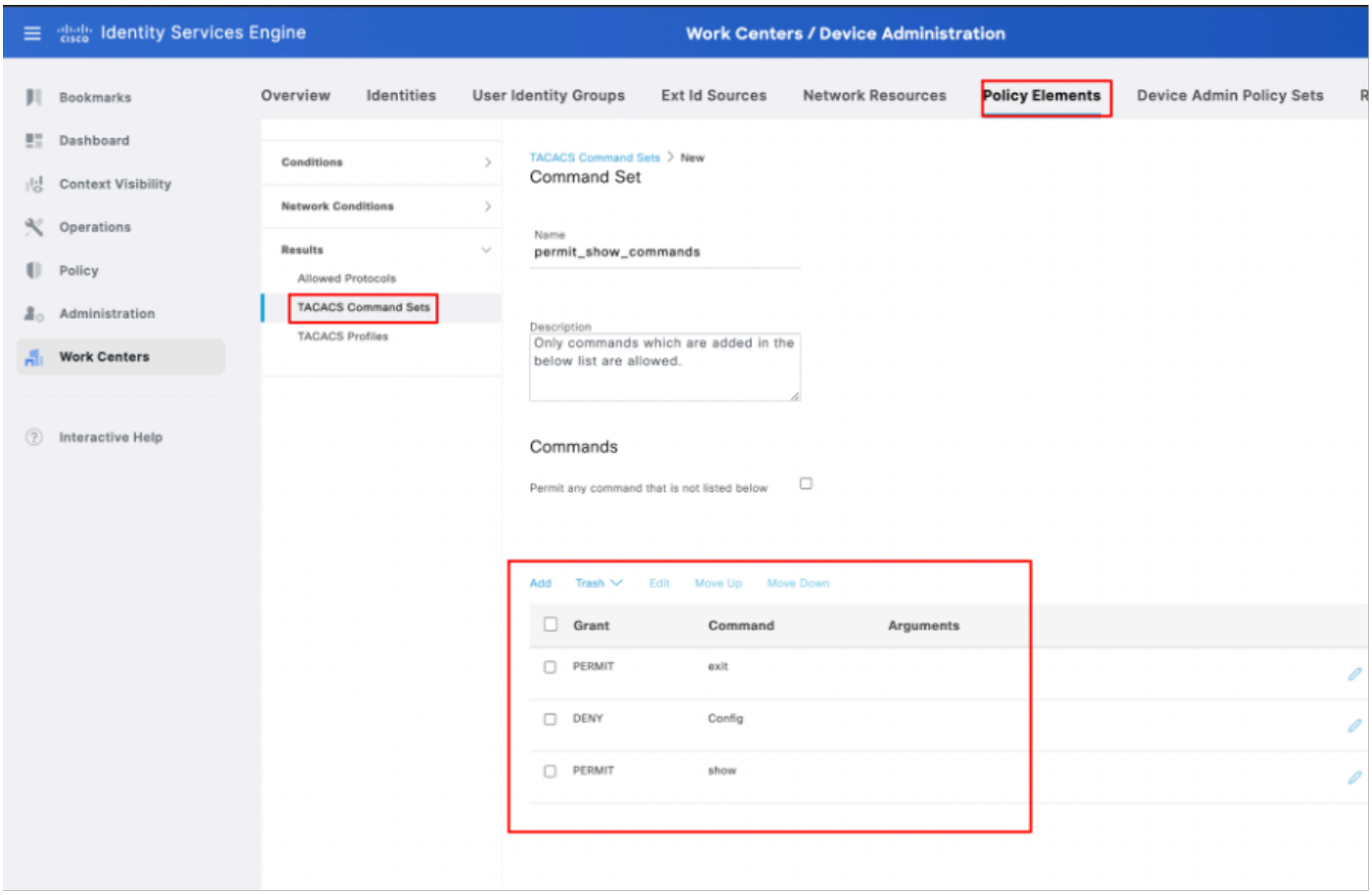
permit_show_commands, se asigna a un usuario y sólo permite comandos show

1. Navegue hasta Centros de Trabajo > Administración de Dispositivos > Resultados de Política > Juegos de Comandos TACACS. Haga clic en Agregar. Proporcione el nombre PermitAllCommands, luego elija la casilla de verificación Permitir cualquier comando que no aparezca en la lista. Haga clic en Submit (Enviar).



Configuración de conjuntos de comandos en ISE

2. Navegue hasta Centros de trabajo > Administración de dispositivos > Resultados de política > Conjuntos de comandos TACACS. Haga clic en Agregar. Proporcione el nombre PermitShowCommands, haga clic en Agregar y, a continuación, por último, permita los comandos show y exit. De forma predeterminada, si los argumentos se dejan en blanco, se incluyen todos los argumentos. Haga clic en Submit (Enviar).

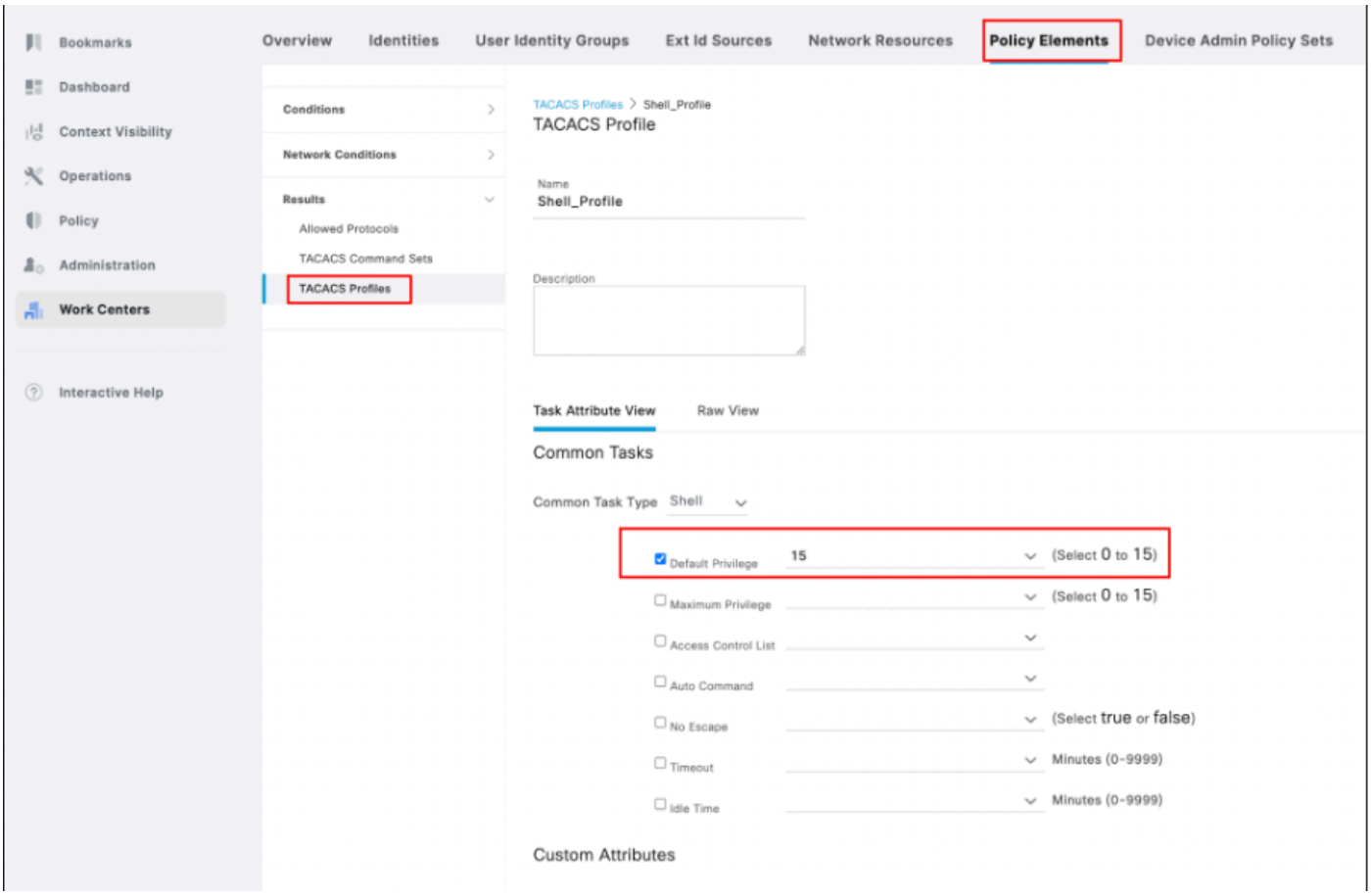


Configuración de permit_show_commands en ISE

Configuración del perfil TACACS+

Se configura un único perfil TACACS+ y la autorización de comandos se lleva a cabo a través de conjuntos de comandos.

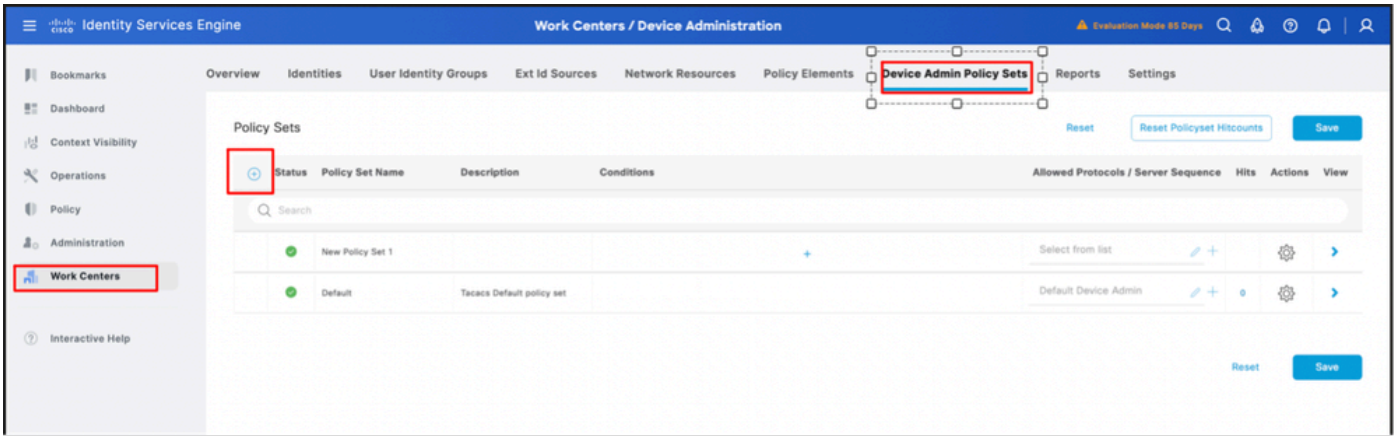
Para configurar un perfil TACACS+, navegue hasta Centros de trabajo > Administración de dispositivos > Resultados de política > Perfiles TACACS. Haga clic en Agregar, proporcione un nombre para el perfil de shell, seleccione la casilla de verificación Privilegio predeterminado e introduzca el valor 15. Finalmente, haga clic en Enviar.



Configuración del perfil TACACS en ISE

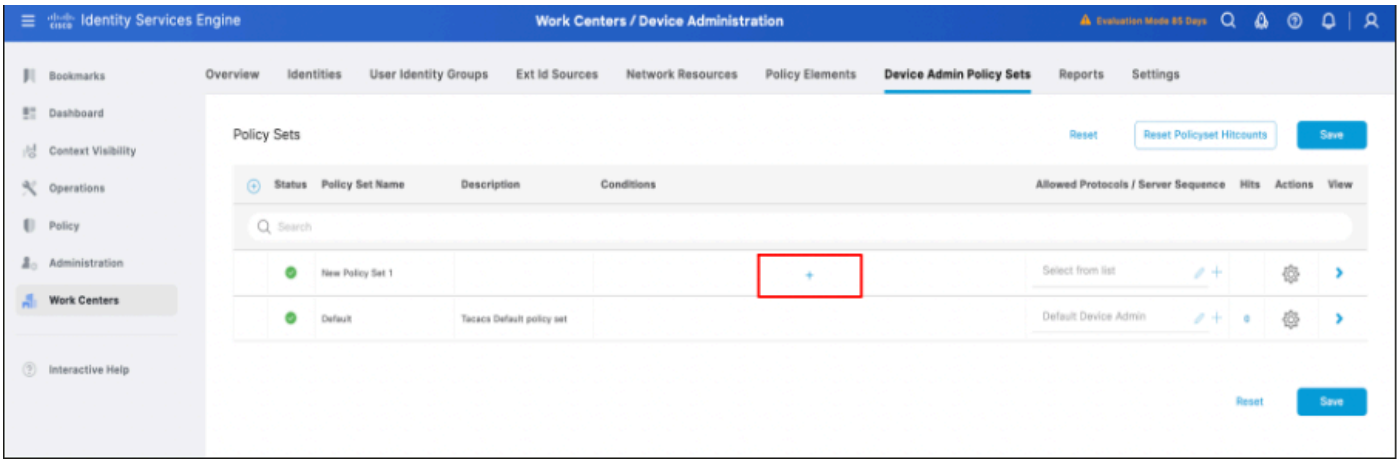
Configuración del perfil de autenticación y autorización de TACACS+

1. Inicie sesión en la GUI de ISE PAN -> Administration -> Work Centers -> Device administration -> Device admin policy sets. Haga clic en el icono + (más) para crear una nueva directiva. En este caso, el conjunto de directivas se denomina Nuevo conjunto de directivas 1.



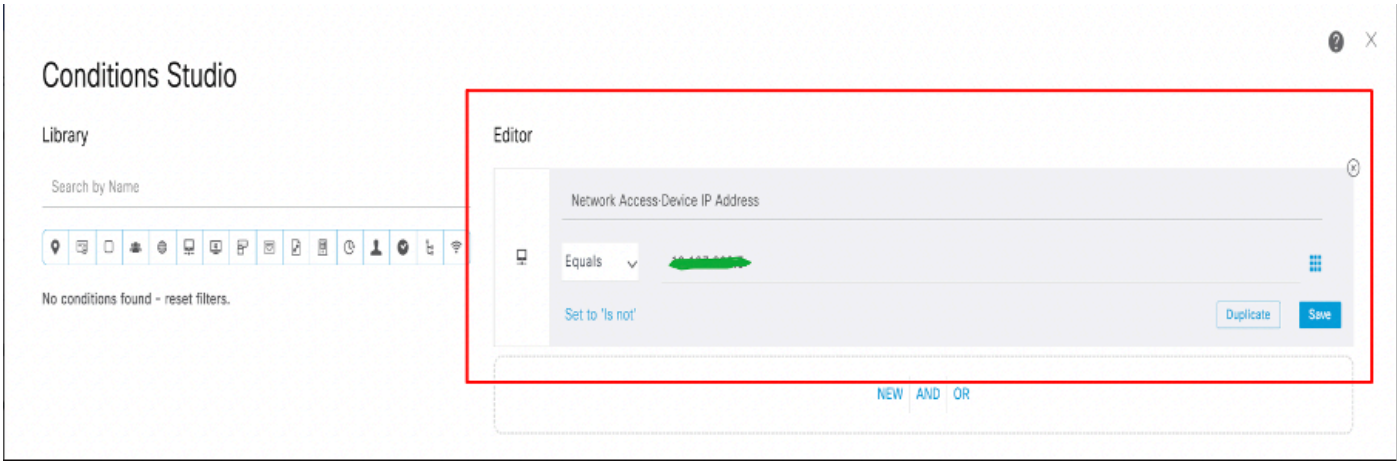
Configuración del conjunto de políticas en ISE

2. Antes de guardar el conjunto de políticas, es necesario configurar las condiciones, como se muestra en esta captura de pantalla. Haga clic en el icono + (más) para configurar las condiciones del conjunto de directivas.

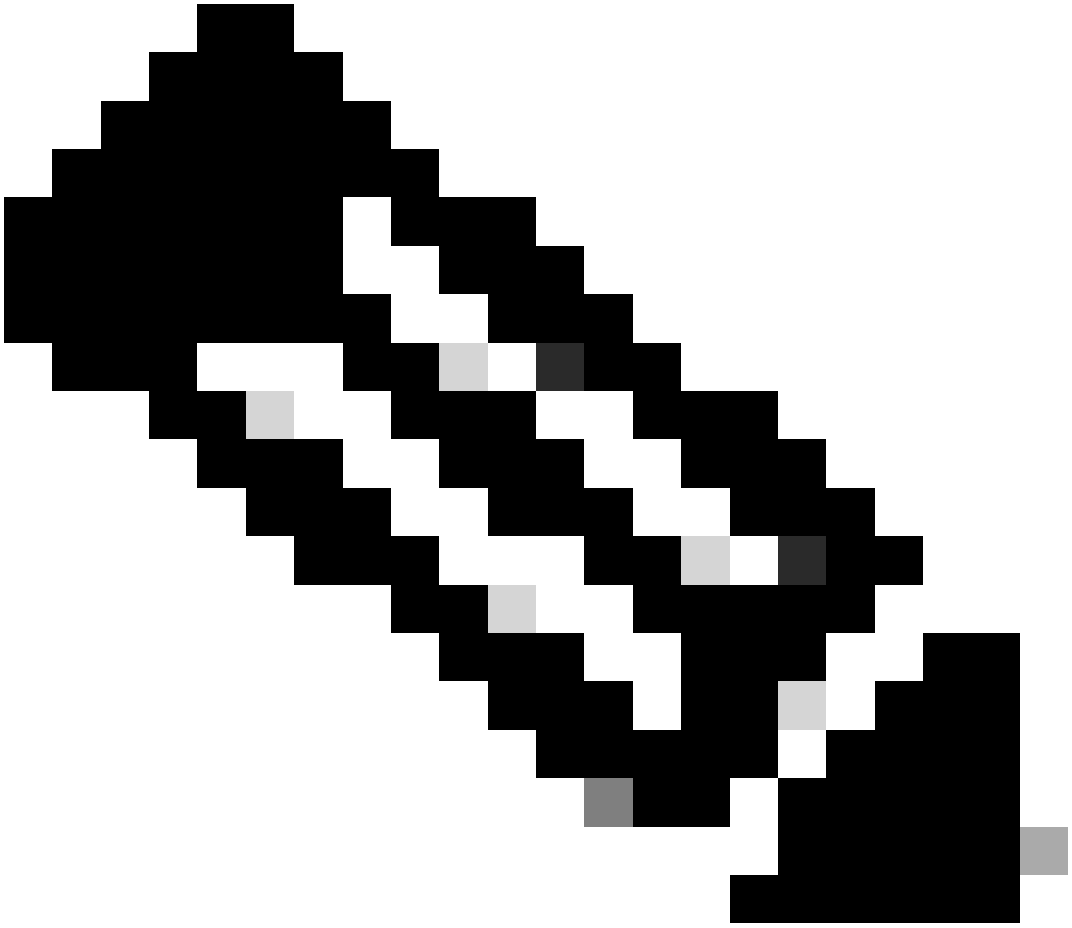


Configuración de las condiciones del conjunto de políticas en ISE

3. Después de hacer clic en el icono + (más) como se menciona en el paso 2, se abre el cuadro de diálogo de condiciones de estudio. Allí, configure las condiciones requeridas. Guarde la condición con las condiciones nuevas o existentes, desplácese. Haga clic en usar.

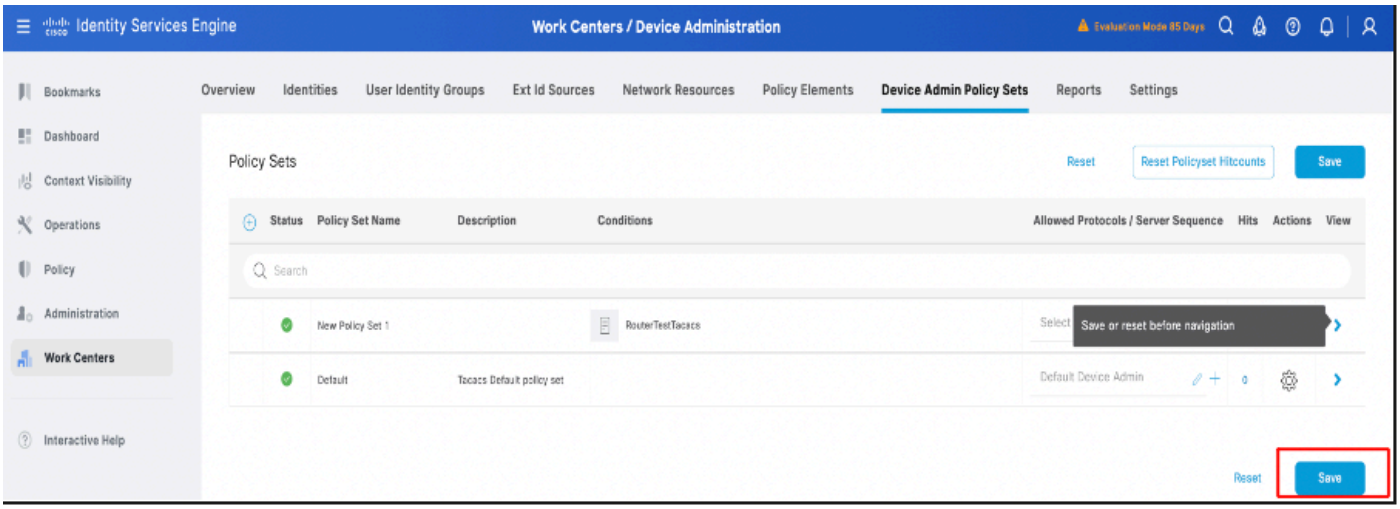


Configuración de las condiciones del conjunto de políticas en ISE



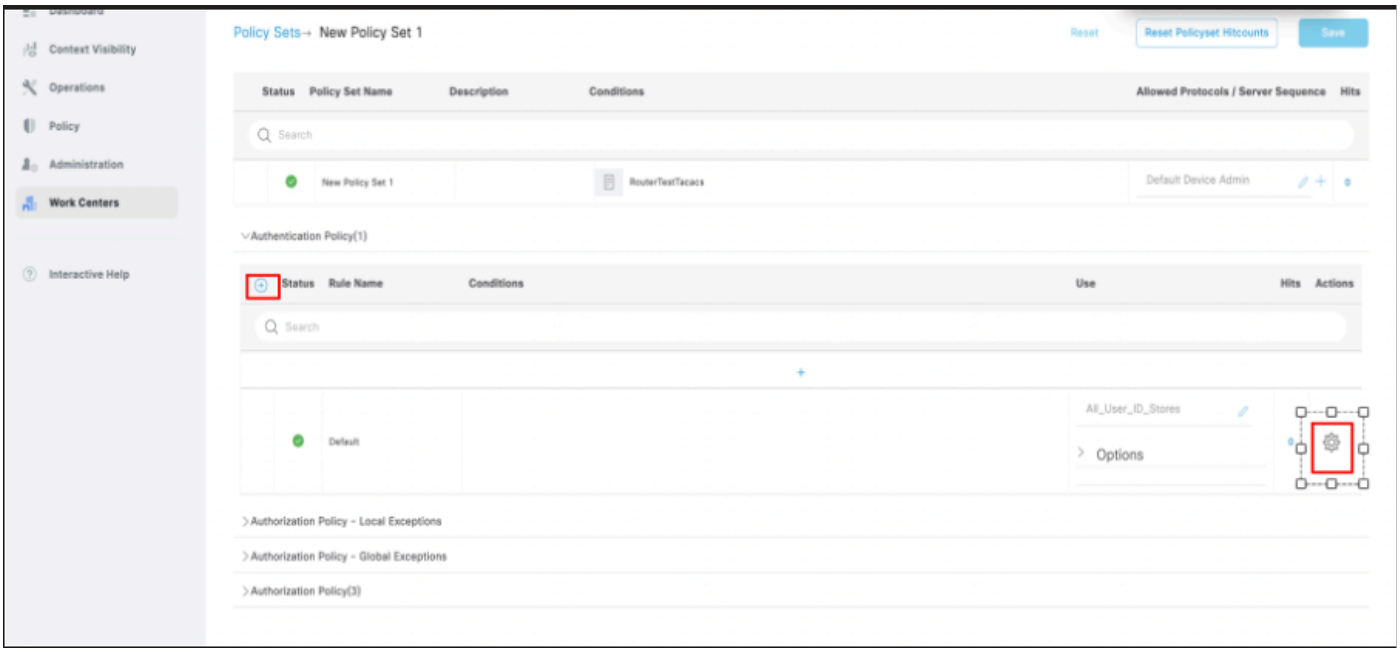
Nota: Para esta documentación, las condiciones coinciden con la IP del dispositivo de red. Sin embargo, las condiciones pueden variar según los requisitos de despliegue.

4. Después de configurar y guardar las condiciones, configure los protocolos permitidos como Default device admin. Guarde el conjunto de políticas creado haciendo clic en la opción Save .

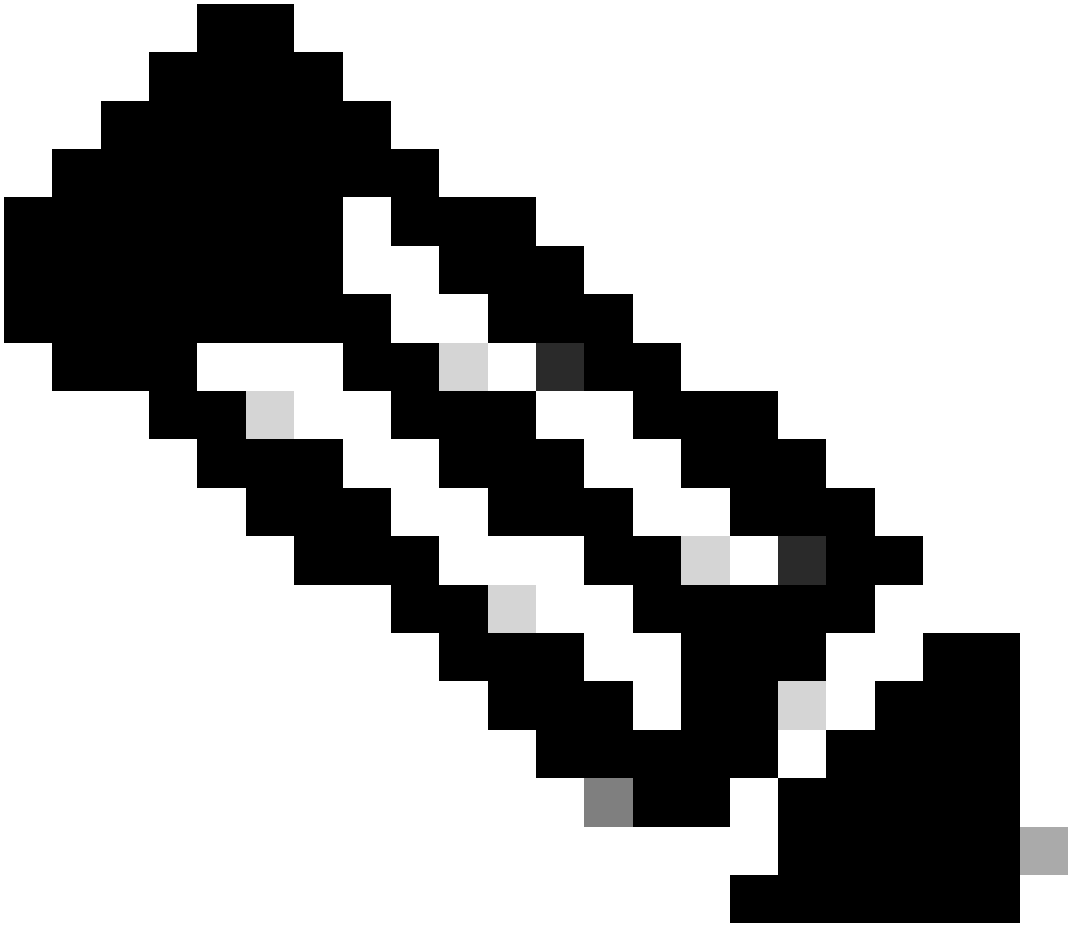


Confirmación de configuración del conjunto de políticas.

5. Expanda el Nuevo conjunto de directivas -> Directiva de autenticación (1) -> Cree una nueva directiva de autenticación haciendo clic en el icono + (más) o haciendo clic en el icono del engranaje y, a continuación, inserte una nueva fila encima.

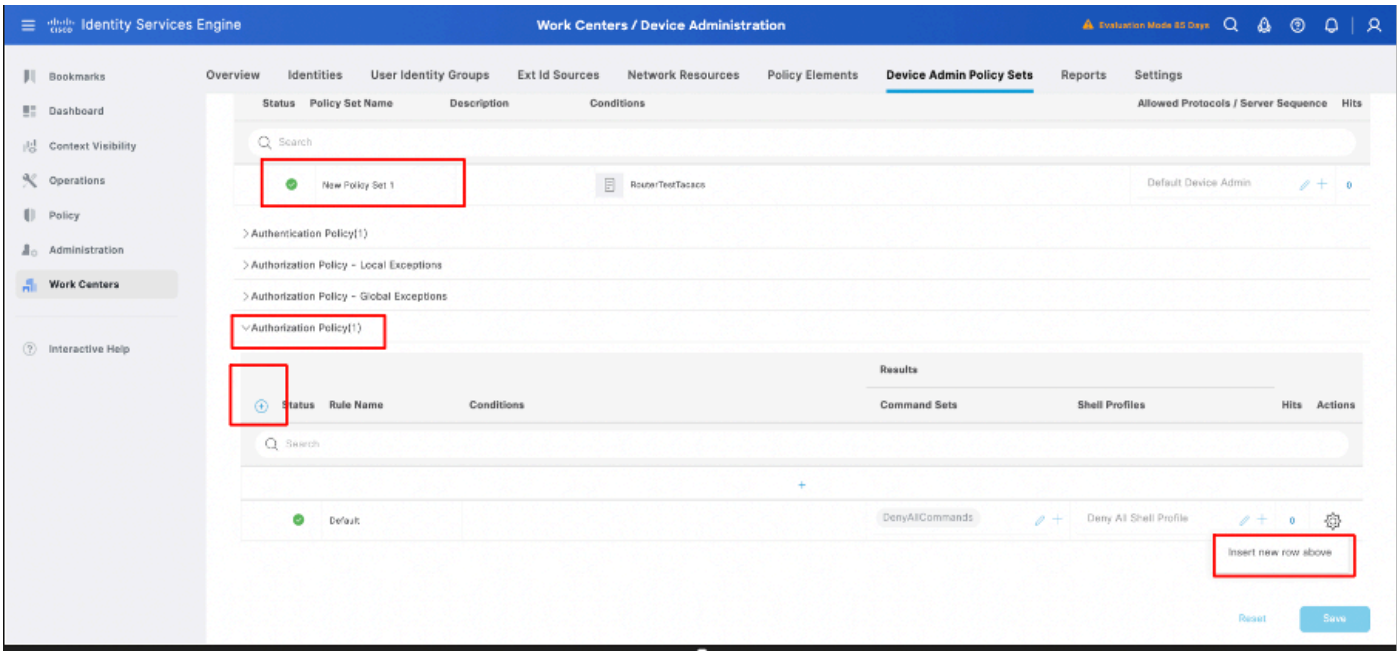


Configuración de la política de autenticación en el conjunto de políticas.



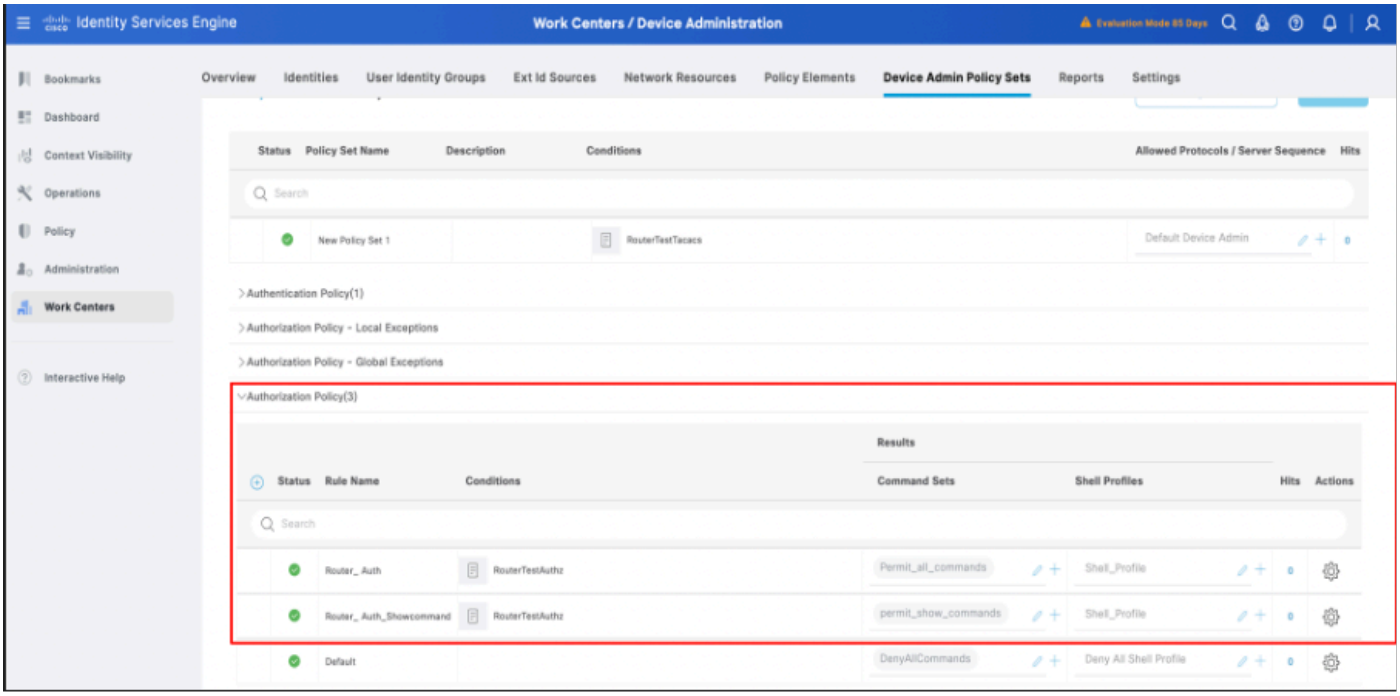
Nota: Para esta demostración, se utiliza el conjunto de políticas de autenticación predeterminado con All_User_ID_Stores. Sin embargo, el uso de los almacenes de identidad se puede personalizar según los requisitos de implementación.

6. Expanda el Nuevo conjunto de políticas -> Directiva de autorización (1). Haga clic en el icono + (más) o haga clic en el icono del engranaje. A continuación, inserte una nueva fila encima para crear una directiva de autorización.

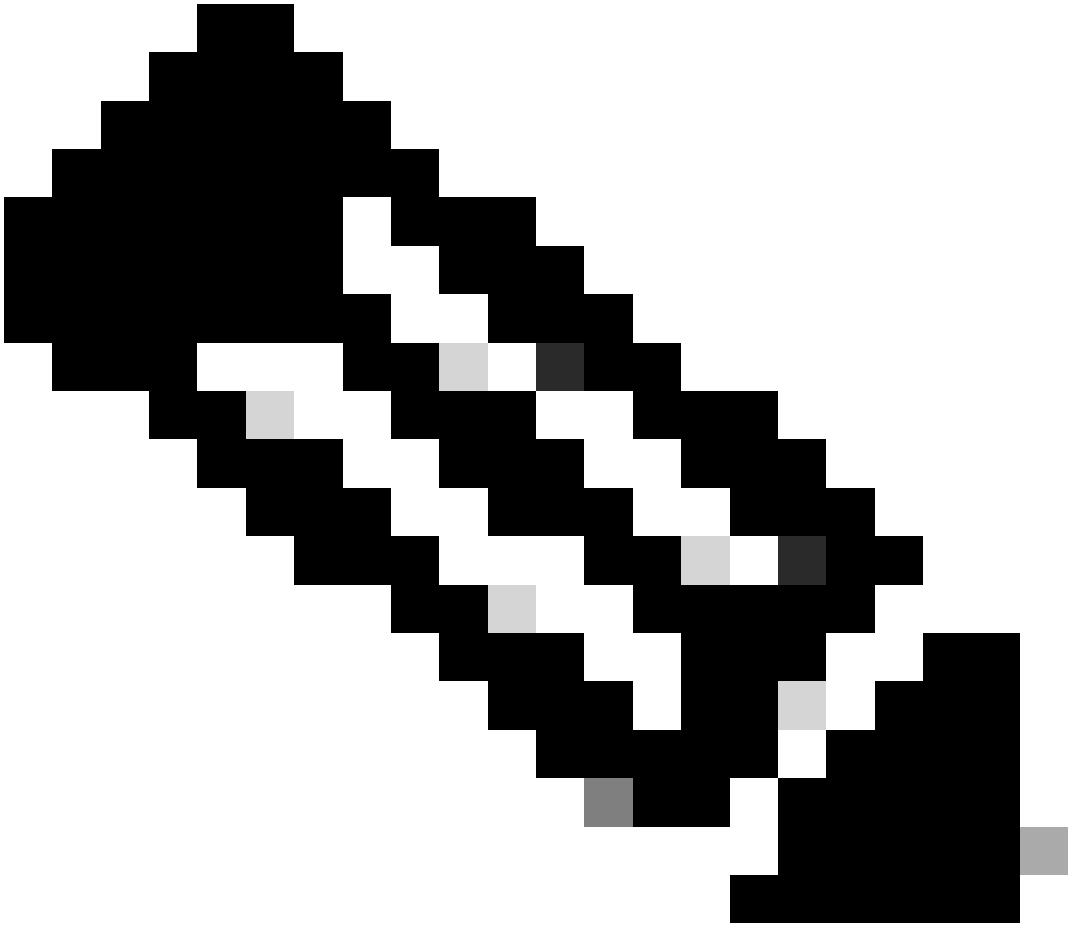


Configuración de la directiva de autorización

7. Configure la directiva de autorización con condiciones, conjuntos de comandos y perfil de shell asignados a las directivas de autorización.



Configuración completa de la política de autorización en ISE



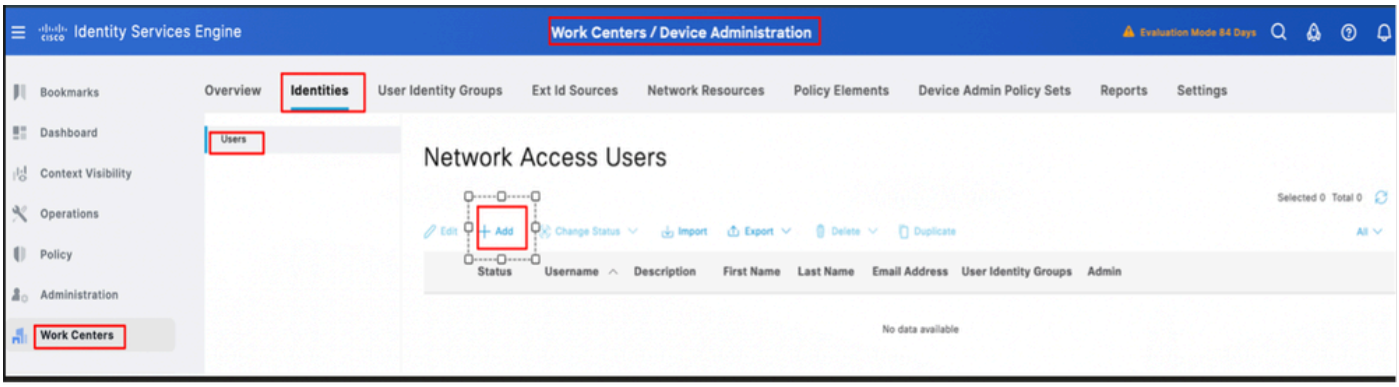
Nota: Las condiciones configuradas se ajustan al entorno de laboratorio y se pueden configurar según los requisitos de implementación.

---

8. Siga los primeros 6 pasos para configurar los conjuntos de políticas para el switch o cualquier otro dispositivo de red utilizado para TACACS+.

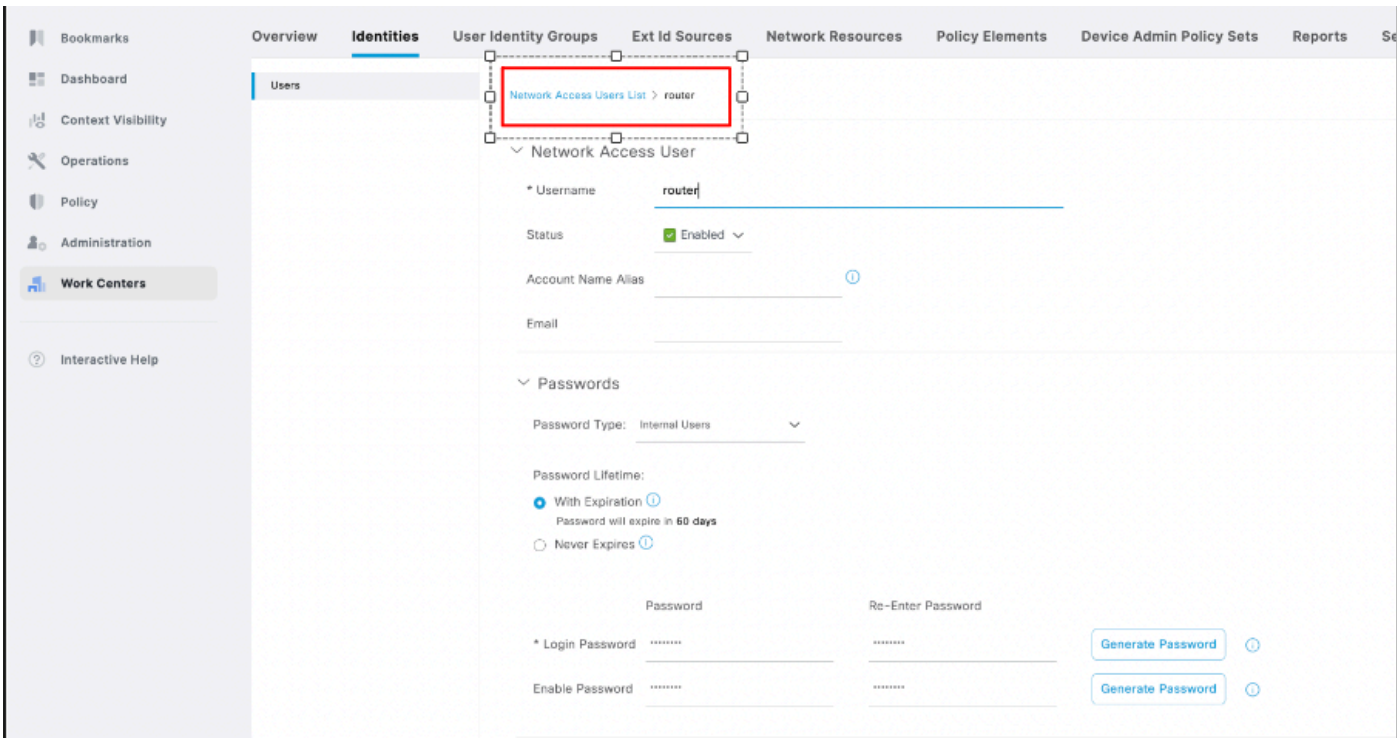
Configuración de los usuarios de acceso a la red para la autenticación TACACS de NAD en ISE

1. Vaya a Workcenters -> Device Administration -> Identities -> Users. Haga clic en el icono +(más) para crear un nuevo usuario.



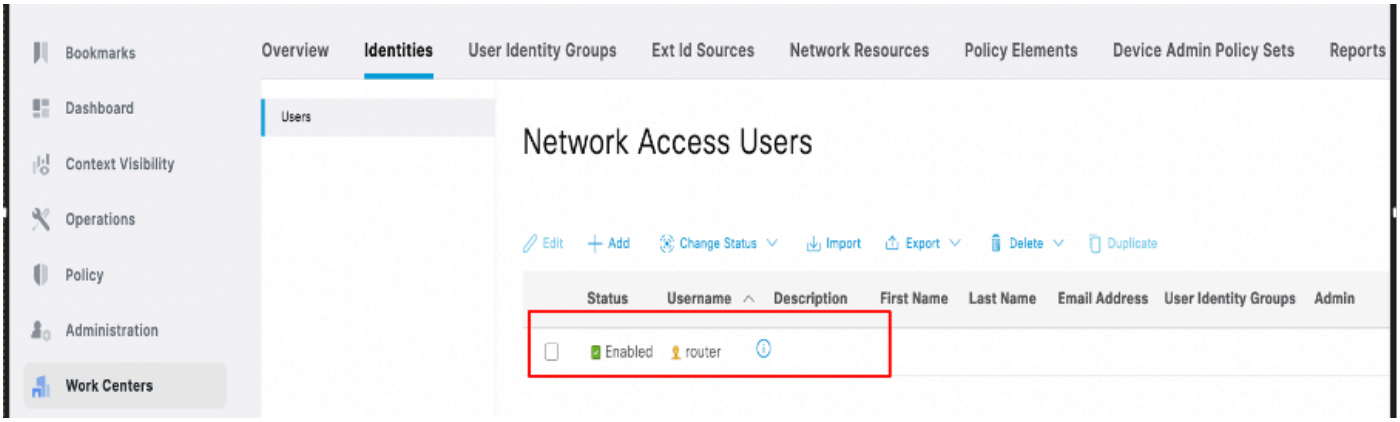
Configuración de usuarios de acceso a la red en ISE

2. Proporcione para ampliar los detalles de nombre de usuario y contraseña, asigne el usuario a un grupo de identidad de usuario (opcional) y, a continuación, haga clic en Enviar.



Configurar usuarios de acceso a la red - Continuar

3. Después de enviar la configuración de nombre de usuario en Centros de trabajo -> Identidades -> Usuarios -> Usuarios de acceso a la red , el usuario está visiblemente configurado y habilitado.



Configuración del router para TACACS+

Configuración del router Cisco IOS para autenticación y autorización TACACS+

1. Inicie sesión en la CLI del router y ejecute estos comandos para configurar TACACS en el router.

ASR1001-X(config)#aaa new-model — comando necesario para habilitar aaa en NAD

ASR1001-X(config)#aaa session-id common. : comando necesario para habilitar aaa en NAD.

ASR1001-X(config)#aaa authentication login default group tacacs+ local

ASR1001-X(config)#aaa authorization exec default group tacacs+

ASR1001-X(config)#aaa autorización red lista1 grupo tacacs+

ASR1001-X(config)servidor #tacacs ise1

ASR1001-X(config-server-tacacs)#address ipv4 <Dirección IP del servidor TACACS > . — Dirección IP G1 de la interfaz ISE.

ASR1001-X(config-server-tacacs)# key XXXXX

ASR1001-X(config)# aaa group server tacacs+ isegroup

ASR1001-X(config-sg-tacacs+)#server name ise1

ASR1001-X(config-sg-tacacs+)#ip vrf forwarding Mgmt-intf

ASR1001-X(config-sg-tacacs+)#ip tacacs source-interface GigabitEthernet0

ASR1001-X(config-sg-tacacs+)#ip tacacs source-interface GigabitEthernet1

ASR1001-X(config)#exit

2. Después de guardar las configuraciones de TACACS+ del router, verifique la configuración de TACACS+ mediante el comando show run aaa.

ASR1001-X#show run aaa

!

aaa authentication login default group isegroup local

aaa authorization exec default group isegroup

aaa authorization network list1 group isegroup

```
username admin password 0 XXXXXXX

!

servidor tacacs ise1

 address ipv4 <IP address of TACACS server>

 key XXXXX

!

!

aaa group server tacacs+ isegroup

 nombre de servidor ise1

 ip vrf forwarding Mgmt-intf

 ip tacacs source-interface GigabitEthernet1

!

!

!

aaa new-model

aaa session-id common

!

!
```

Configuración del switch para TACACS+

Configuración del Switch para Autenticación y Autorización TACACS+

1. Inicie sesión en la CLI del switch y ejecute estos comandos para configurar TACACS en el switch.

```
C9200L-48P-4X#configure t

Ingrese los comandos de configuración, uno por línea.  Finalizar con CNTL/Z.

C9200L-48P-4X(config)#aaa nuevo modelo. — comando requerido para habilitar aaa en NAD

C9200L-48P-4X(config)#aaa session-id common. — comando necesario para habilitar aaa en NAD.
```

C9200L-48P-4X(config)#aaa authentication login default group isegroup local

C9200L-48P-4X(config)#aaa authorization exec default group isegroup

C9200L-48P-4X(config)#aaa autorización lista de red1 grupo isegroup

C9200L-48P-4X(config)#tacacs servidor ise1

C9200L-48P-4X(config-server-tacacs)#address ipv4 <dirección IP del servidor TACACS> — Dirección IP de la interfaz ISE G1.

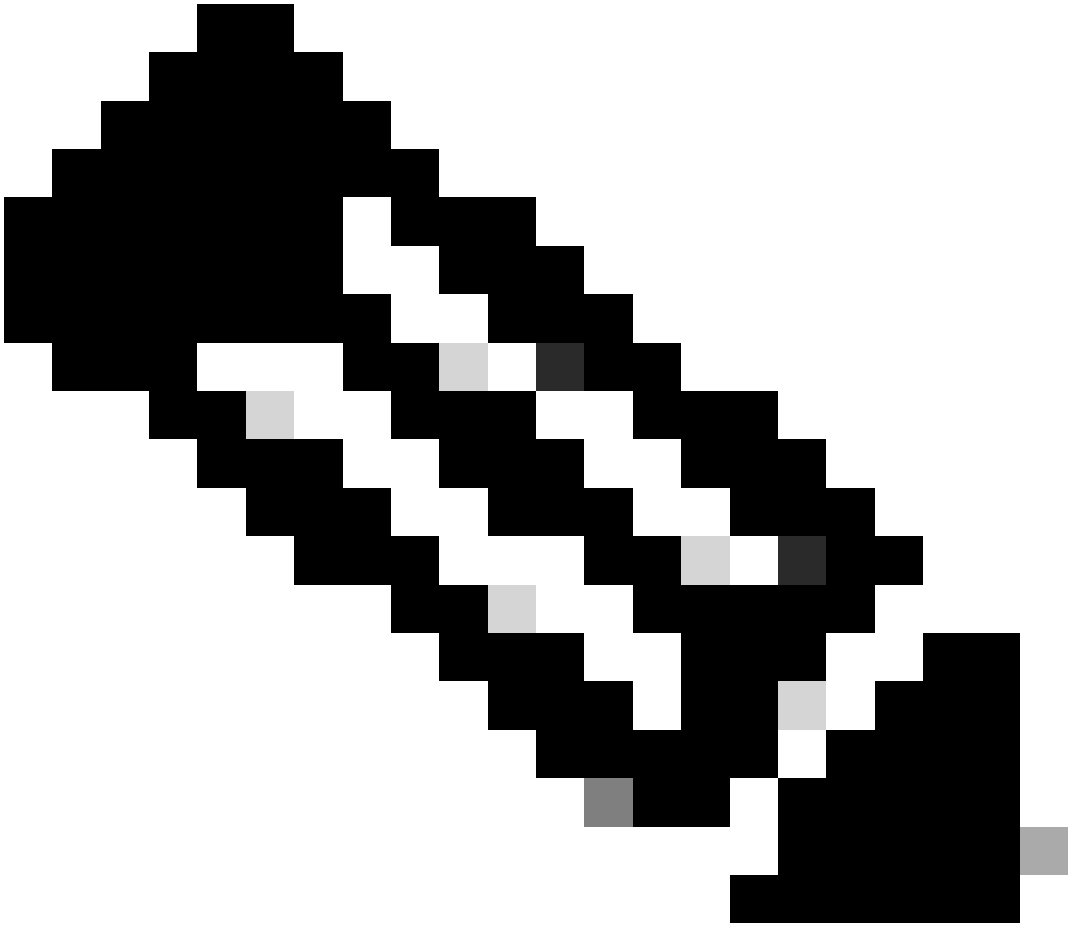
C9200L-48P-4X(config-server-tacacs)#key XXXXX

C9200L-48P(config)#aaa group server tacacs+ isegroup

C9200L-48P(config-sg-tacacs+)#server name ise1

C9200L-48P-4X(config)#exit

C9200L-48P-4X#wr mem



Nota: En la configuración de NAD TACACS+, tacacs+ es el grupo que se puede personalizar según los requisitos de implementación.

---

2. Después de guardar las configuraciones TACACS+ del switch, verifique la configuración TACACS+ mediante el comando show run aaa.

C9200L-48P#show run aaa

!

aaa authentication login default group isegroup local

aaa authorization exec default group isegroup

aaa authorization network list1 group isegroup

username admin password 0 XXXXX

```
!

!

servidor tacacs ise1

 address ipv4 <IP address of TACACS server>

 key XXXXX

!

!

aaa group server tacacs+ isegroup

 nombre de servidor ise1

!

!

!

aaa new-model

aaa session-id common

!

!
```

Verificación

Verificación desde el router

Desde la CLI del router, verifique la autenticación de TACACS+ contra ISE con la interfaz Gigabit Ethernet 1 mediante el comando test aaa group tacacsgroupname username password new.

A continuación se muestra un ejemplo de salida de Router e ISE:

Verificación del puerto 49 desde el router:

```
ASR1001-X#telnet ISE Gig 1 interface IP 49

Intentando establecer la IP de la interfaz ISE GIg 1, 49... Abierto

ASR1001-X#test aaa group isegroup router XXXX new

Enviando contraseña
```

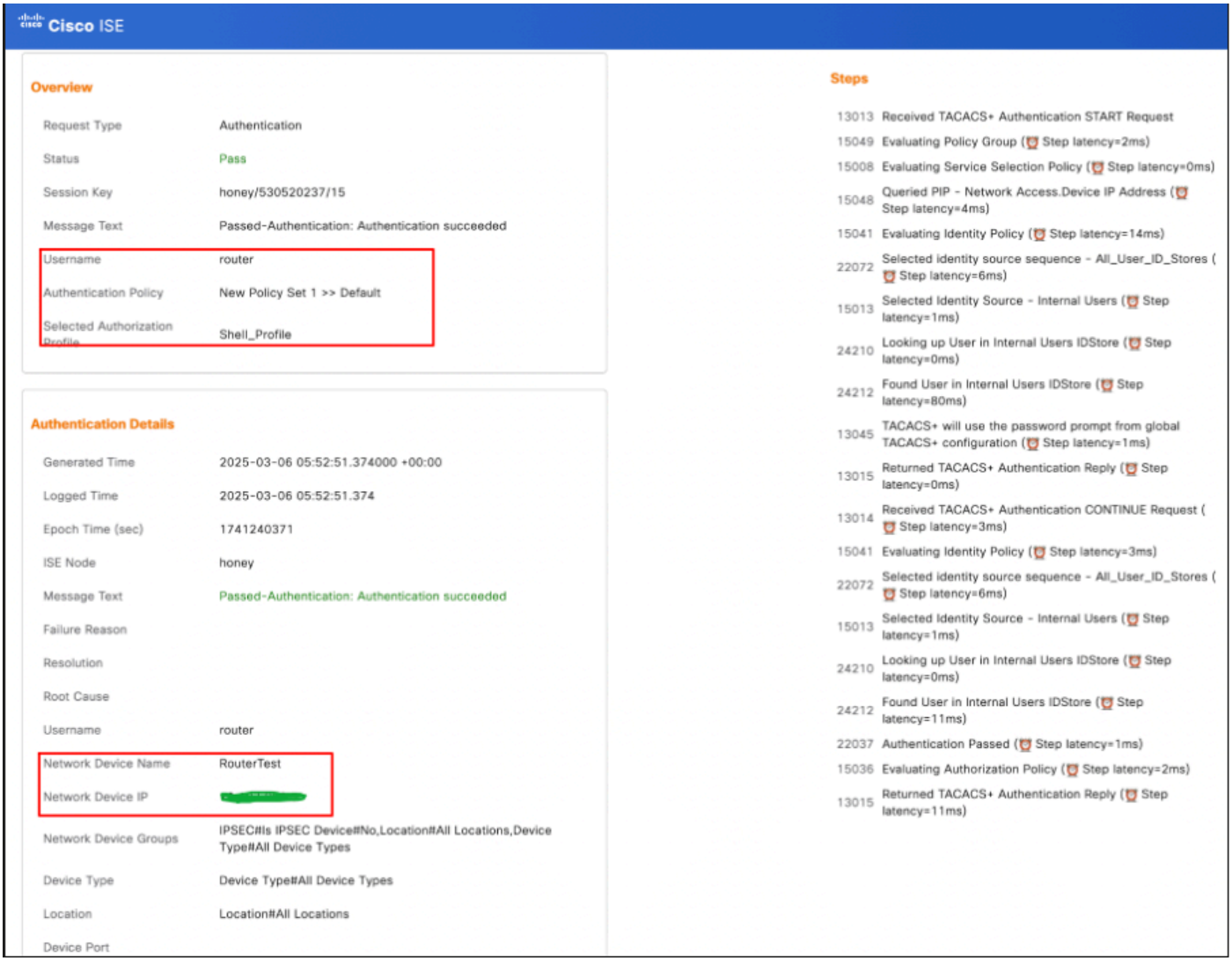
Usuario autenticado correctamente

ATRIBUTOS DE USUARIO

username 0 "router"

reply-message 0 "Contraseña:"

Para la verificación desde ISE, inicie sesión en GUI -> Operaciones -> TACACS live logs, luego filtre con la IP del router en el campo Network Device Details.



Registros en directo de TACACS desde ISE: verificación del router.

Verificación del switch

Desde la CLI del switch, verifique la autenticación de TACACS+ contra ISE con la interfaz Gigabit Ethernet 1 mediante el comando test aaa group tacacsgroupname username password newn:

Este es un ejemplo de salida de switch e ISE.

Verificación del puerto 49 desde el switch:

C9200L-48P# telnet ISE Gig1 interface IP 49

Intentando establecer la IP de la interfaz Gig1 de ISE, 49... Abierto

C9200L-48P#test aaa group isegroup switch XXXX new

Enviando contraseña

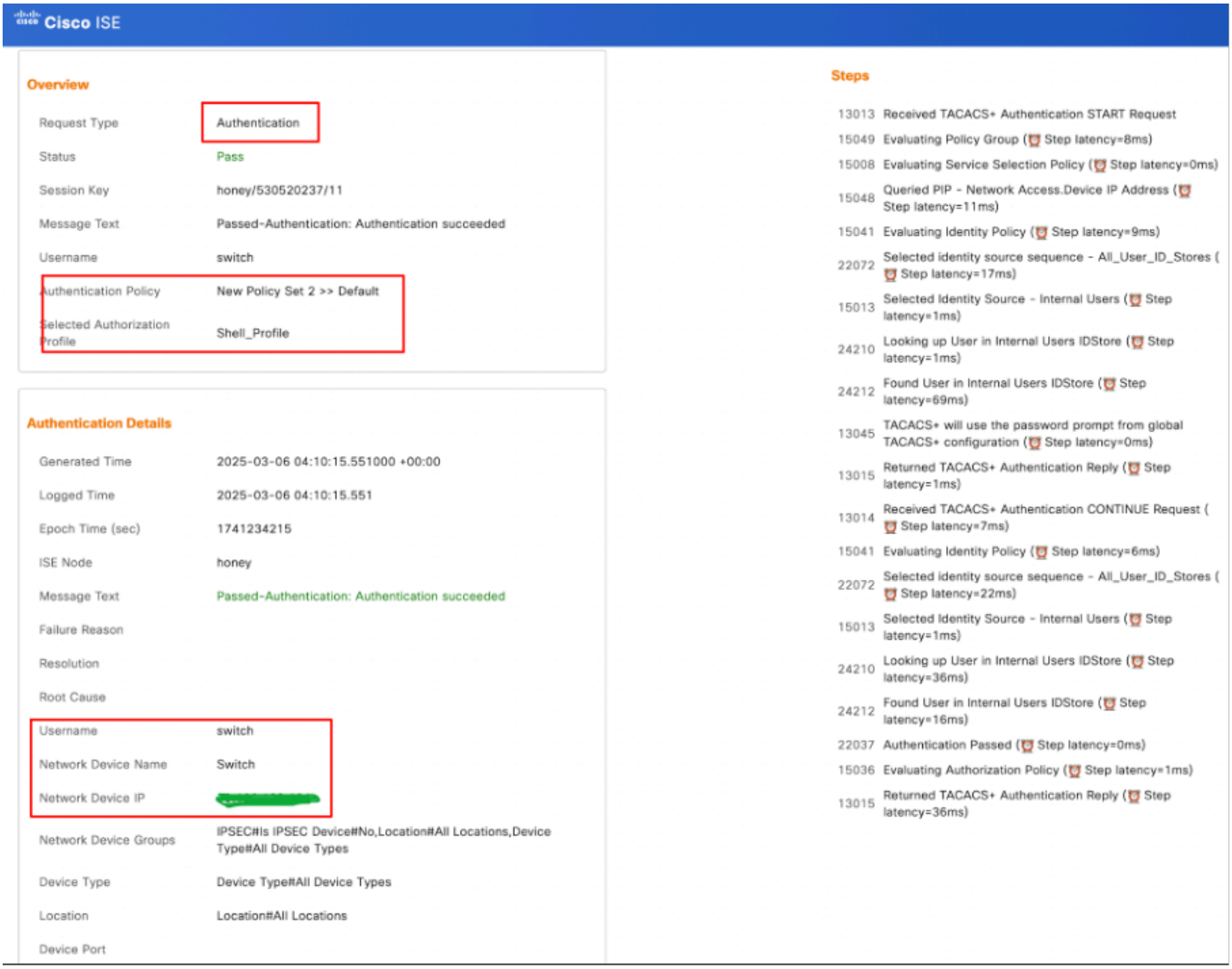
Usuario autenticado correctamente

ATRIBUTOS DE USUARIO

username 0 "switch"

reply-message 0 "Contraseña:"

Para la verificación desde ISE, inicie sesión en GUI -> Operaciones -> TACACS live logs, luego filtre con la IP del switch en el campo Detalles del dispositivo de red.



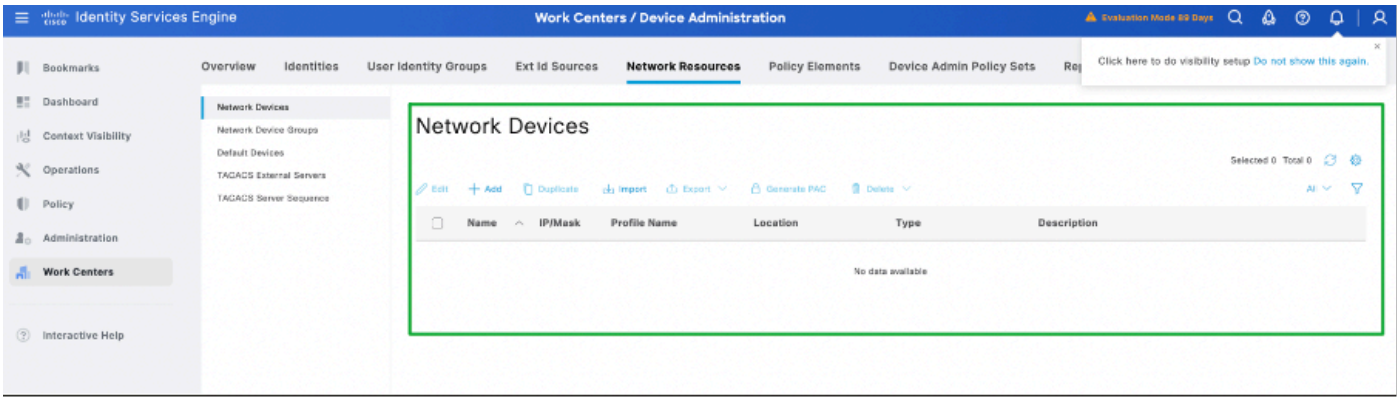
Registros en directo de TACACS desde ISE: verificación del switch.

Troubleshoot

Esta sección discute algunos de los problemas comunes encontrados relacionados con las autenticaciones TACACS+.

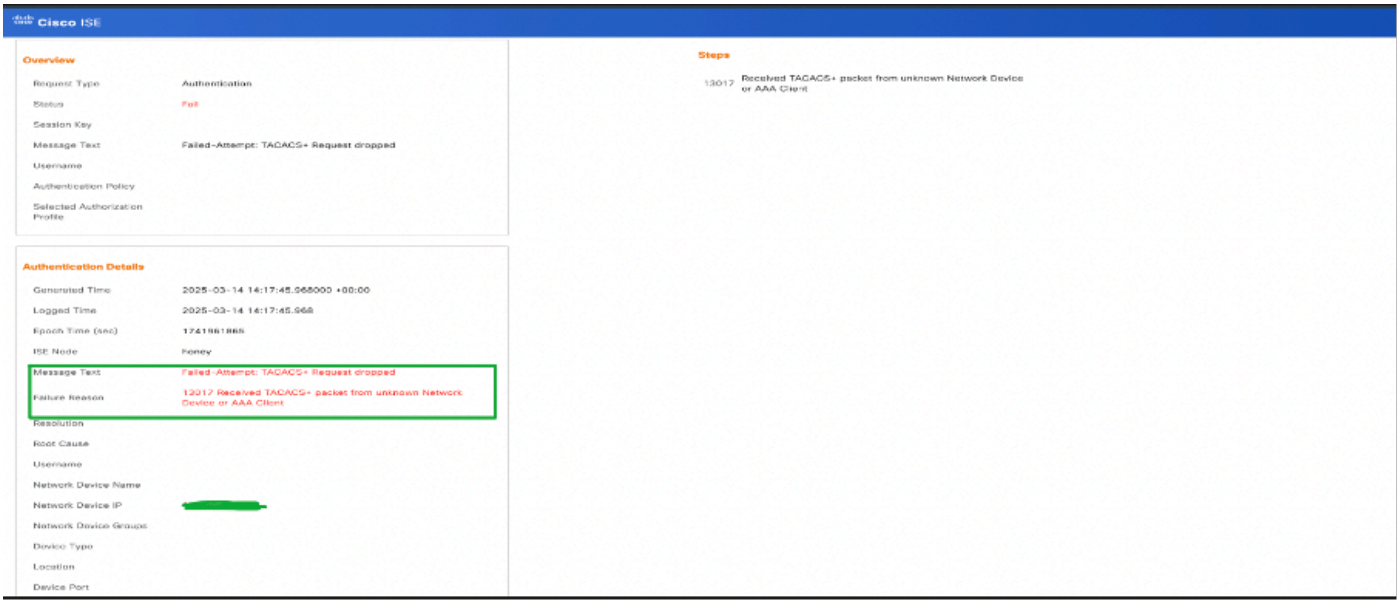
Escenario 1: La autenticación TACACS+ falla con "Error: 13017 Paquete TACACS+ recibido desde un dispositivo de red o cliente AAA desconocido".

Este escenario se produce cuando el dispositivo de red no se agrega como recursos de red en ISE. Como se muestra en esta captura de pantalla, el switch no se agrega a los recursos de red de ISE.



Situación de solución de problemas: los dispositivos de red no se agregan a ISE.

Ahora, cuando prueba la autenticación desde el switch/dispositivo de red, el paquete llega a ISE como se esperaba. Sin embargo, la autenticación falla con el error "Error : 13017 paquetes TACACS+ recibidos desde un dispositivo de red desconocido o un cliente AAA", como se muestra en esta captura de pantalla:



Registros en directo de TACACS: fallo cuando el dispositivo de red no se agrega a ISE.

Verificación desde el dispositivo de red (switch)

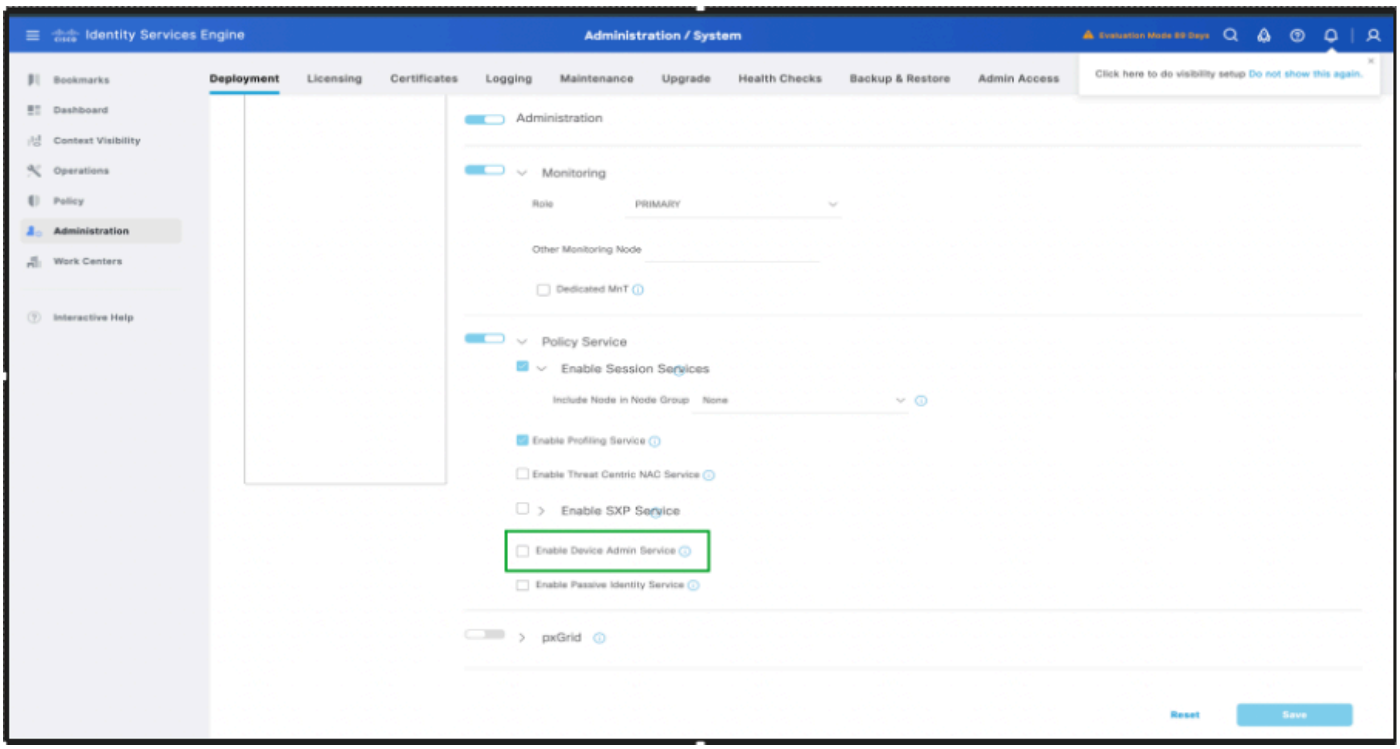
Switch#test aaa group isegroup switch XXXXXX new
Usuario rechazado

Solución: Compruebe si el switch, el router o el dispositivo de red se han agregado como el dispositivo de red en ISE. Si el dispositivo no se agrega, agregue el dispositivo de red a la lista de dispositivos de red de ISE.

Escenario 2: ISE descarta el paquete TACACS+ de forma silenciosa sin ninguna información.

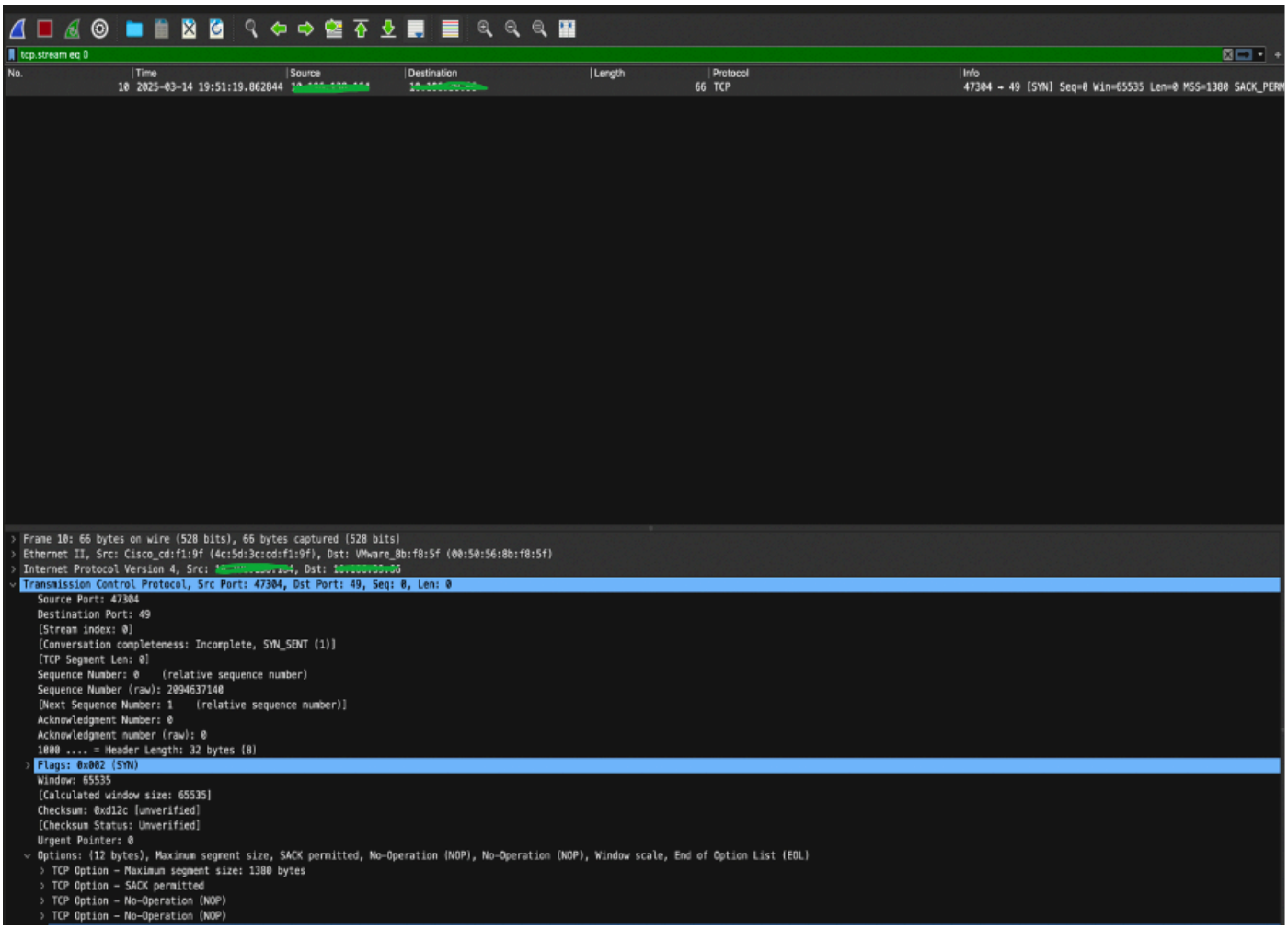
Este escenario se produce cuando Device Administration Service está deshabilitado en ISE. En esta situación, ISE descarta el paquete y no se ven registros activos aunque se inicie la autenticación desde el dispositivo de red que se agrega a los recursos de red de ISE.

Como se muestra en esta captura de pantalla, Device Administration está desactivada en ISE.



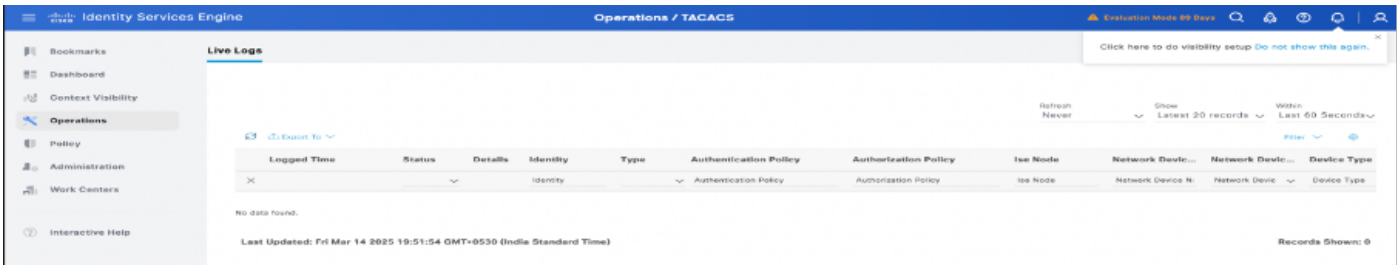
Situación: la administración de dispositivos no está habilitada en ISE.

Cuando un usuario inicia la autenticación desde el dispositivo de red, ISE descarta silenciosamente los paquetes sin ninguna información en los registros en directo e ISE no responde al paquete Syn enviado por el dispositivo de red para completar el proceso de autenticación TACACS. Consulte esta captura de pantalla:



ISE descarta paquetes en silencio durante TACACS

ISE no muestra ningún registro activo durante la autenticación.



No hay registros en directo de TACACS: verificación desde ISE

Verificación desde el dispositivo de red (switch)

Switch#
Switch#test aaa group isegroup switch XXXX new
Usuario rechazado
Switch#
* 14 de marzo 13:54:28.144: T+: Versión 192 (0xC0), tipo 1, secuencia 1, cifrado 1, SC 0
* 14 de marzo 13:54:28.144: T+: session_id 10158877 (0x9B031D), dlen 14 (0xE)
* 14 de marzo 13:54:28.144: T+: type:AUTHEN/START, priv_lvl:15 action:LOGIN ascii
* 14 de marzo 13:54:28.144: T+: svc:LOGIN user_len:6 port_len:0 (0x0) raddr_len:0 (0x0) data_len:0
* 14 de marzo 13:54:28.144: T+: usuario: switch
* 14 de marzo 13:54:28.144: T+: puerto:
* 14 de marzo 13:54:28.144: T+: rem_addr:
* 14 de marzo 13:54:28.144: T+: datos:
* 14 de marzo 13:54:28.144: T+: Paquete final

Solución: Habilitar la administración de dispositivos en ISE.

Referencia

- Solucionar problemas de autenticación de TACACS
- Guía del administrador de Cisco Identity Services Engine, versión 3.3
- VRF para servidores TACACS

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).