Configuración de la autorización de comandos de autenticación TACACS+ de ISE 2.0

Contenido

Introducción

Este documento describe cómo configurar la autenticación TACACS+ y la autorización de comandos según la pertenencia al grupo de Microsoft Active Directory (AD).

Antecedentes

Para configurar la autenticación TACACS+ y la autorización de comandos según la pertenencia a grupos de Microsoft Active Directory (AD) de un usuario con Identity Service Engine (ISE) 2.0 y versiones posteriores, ISE utiliza AD como almacén de identidades externo para almacenar recursos como usuarios, equipos, grupos y atributos.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- El router Cisco IOS está completamente operativo
- Conectividad entre router e ISE.
- El servidor ISE es de arranque y tiene conectividad con Microsoft AD

Componentes Utilizados

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

- Cisco Identity Service Engine 2.0
- Software Cisco IOS® versión 15.4(3)M3
- Microsoft Windows Server 2012 R2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

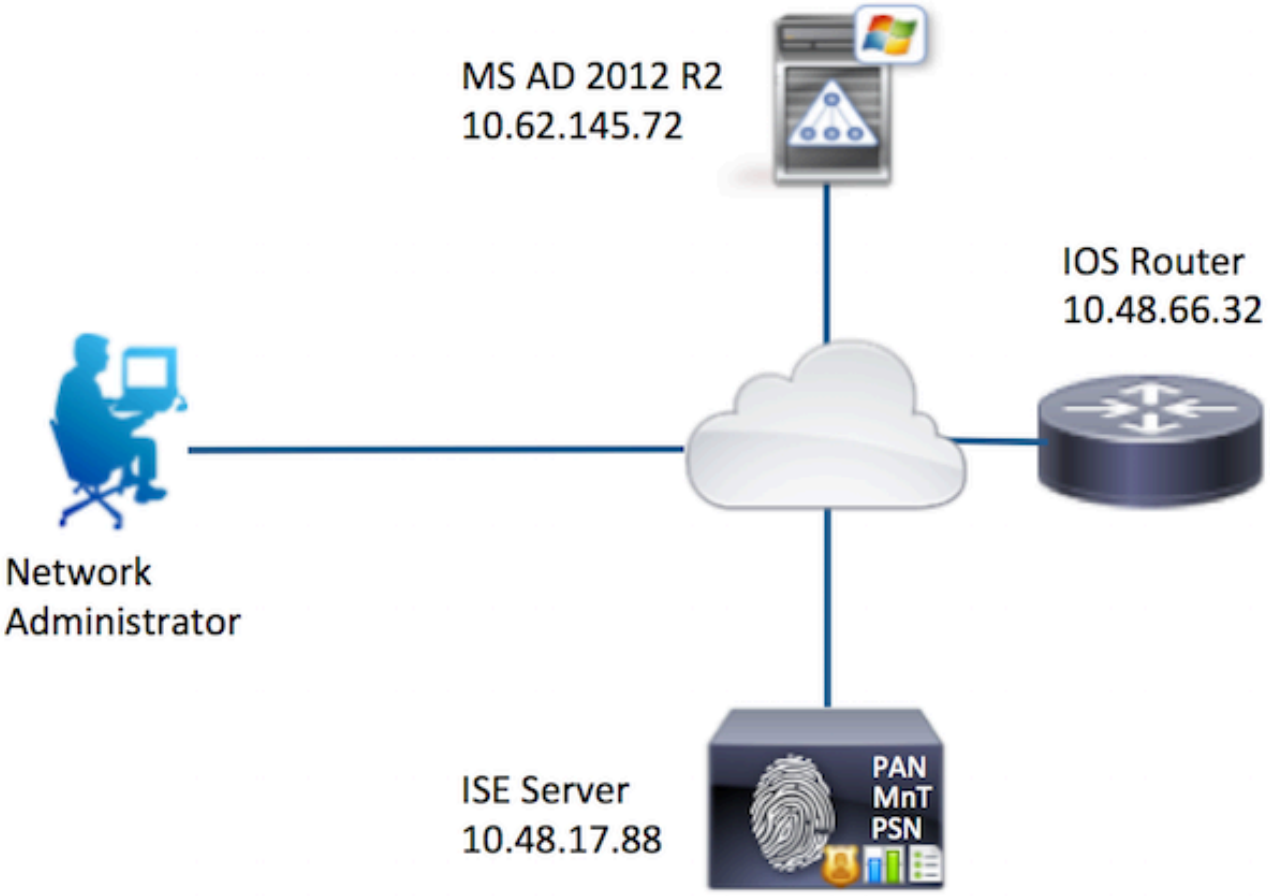
Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Configurar

El objetivo de la configuración es:

- Autenticar usuario telnet mediante AD
- Autorice al usuario telnet para que se coloque en el modo EXEC privilegiado después del login
- Verifique y envíe cada comando ejecutado a ISE para su verificación

Diagrama de la red

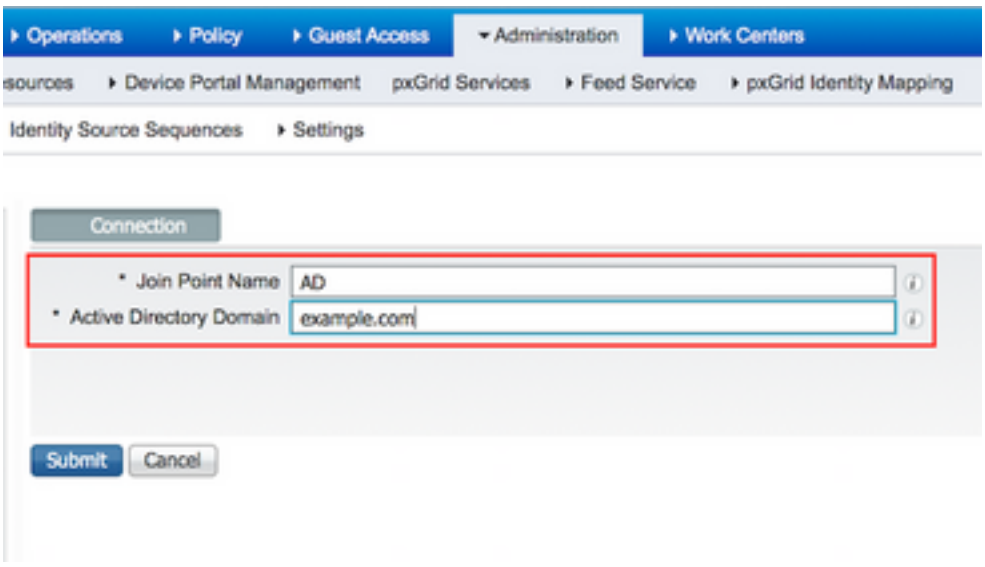


Configuraciones

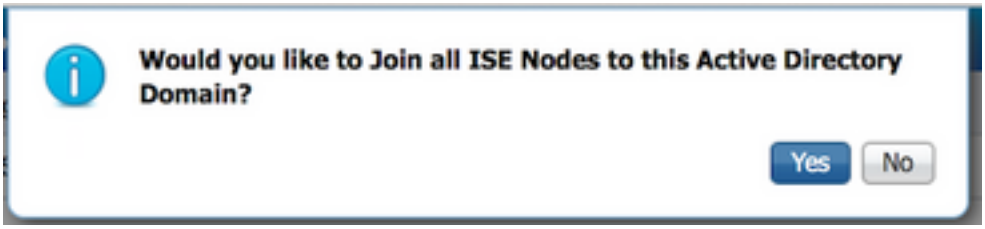
Configuración de ISE para autenticación y autorización

Incorporación de ISE 2.0 a Active Directory

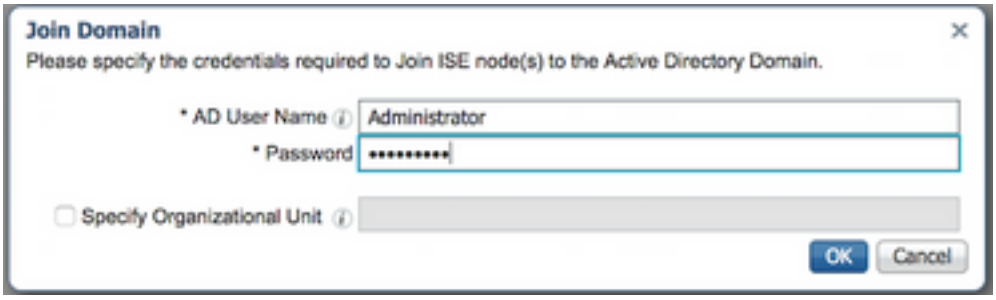
1. Vaya a **Administration > Identity Management > External Identity Stores > Active Directory > Add**. Proporcione el nombre del punto de unión, el dominio de Active Directory y haga clic en **Enviar.**



2. Cuando se le solicite que una todos los nodos ISE a este dominio de Active Directory, haga clic en **Sí.**



3. Proporcione el nombre de usuario y la contraseña de AD y haga clic en **Aceptar**.

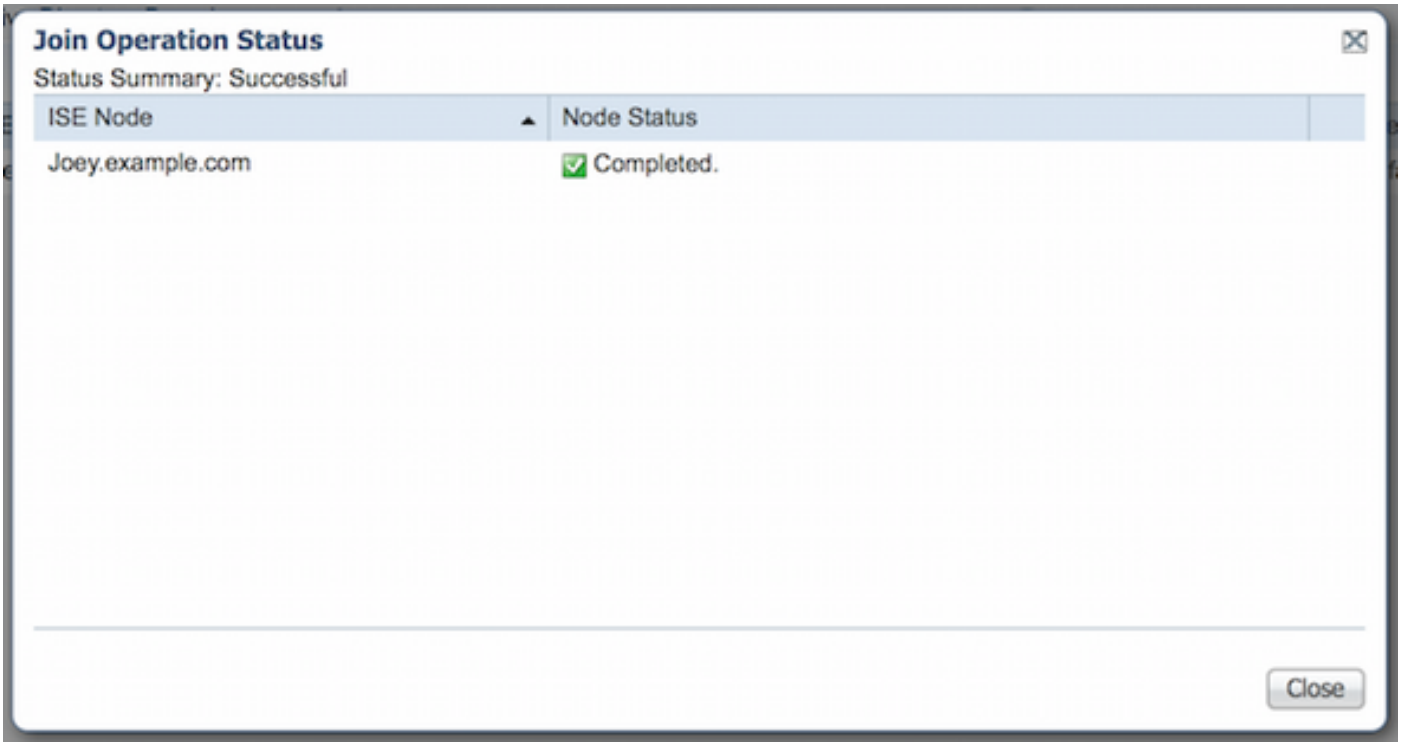


La cuenta de AD necesaria para el acceso al dominio en ISE puede tener cualquiera de estas características:

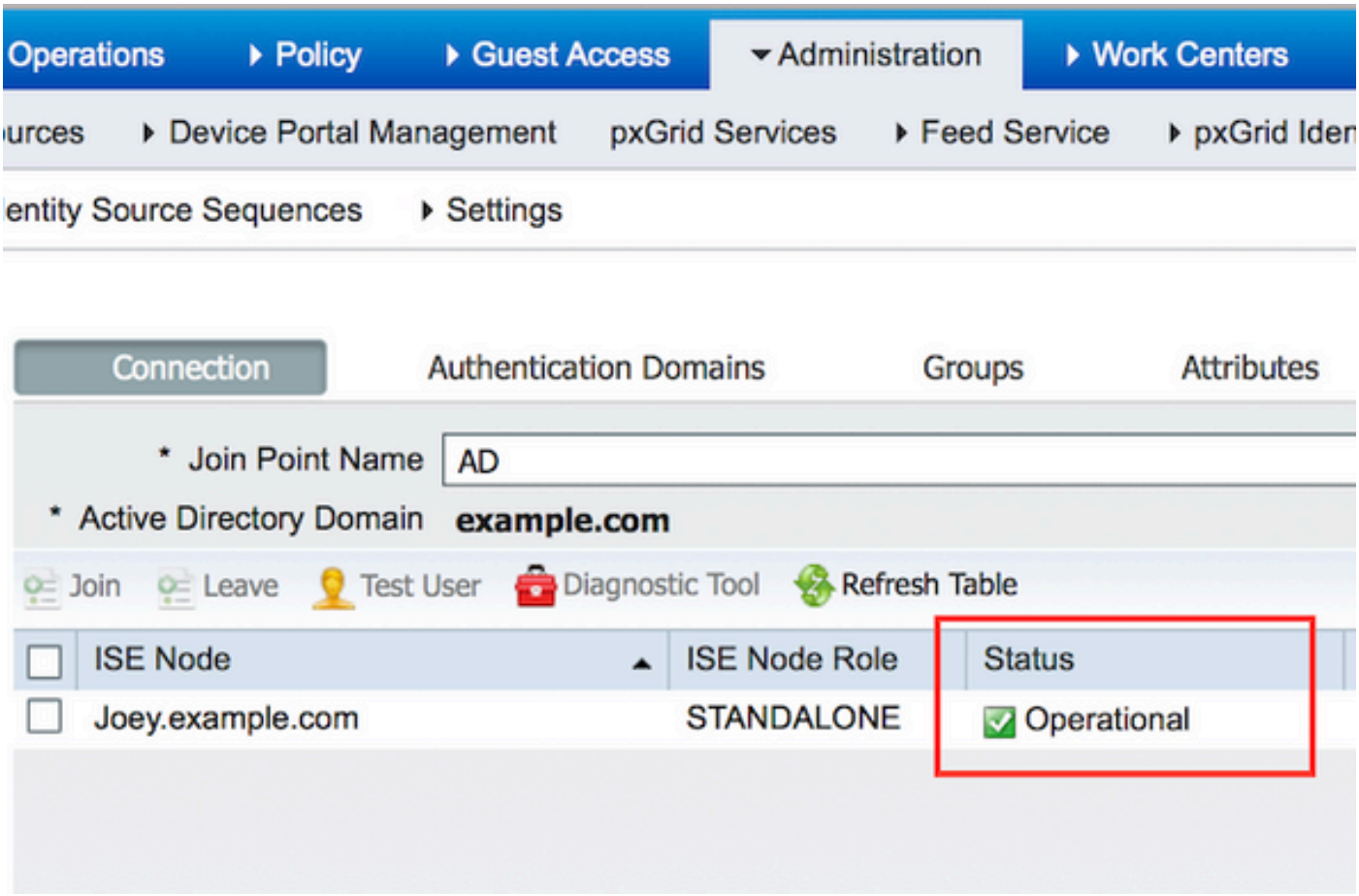
- Agregar estaciones de trabajo al derecho de usuario del dominio correspondiente
- Crear objetos de equipo o Eliminar objetos de equipo en el contenedor de equipos correspondiente donde se crea la cuenta del equipo ISE antes de que se una al equipo ISE en el dominio

Nota: Cisco recomienda deshabilitar la política de bloqueo para la cuenta ISE y configurar la infraestructura AD para enviar alertas al administrador si se utiliza una contraseña incorrecta para esa cuenta. Cuando se introduce una contraseña incorrecta, ISE no crea ni modifica su cuenta de equipo cuando es necesario y, por lo tanto, posiblemente deniegue todas las autenticaciones.

4. Revise El Estado De La Operación. El estado del nodo debe aparecer como completado. Haga clic en Close (Cerrar).



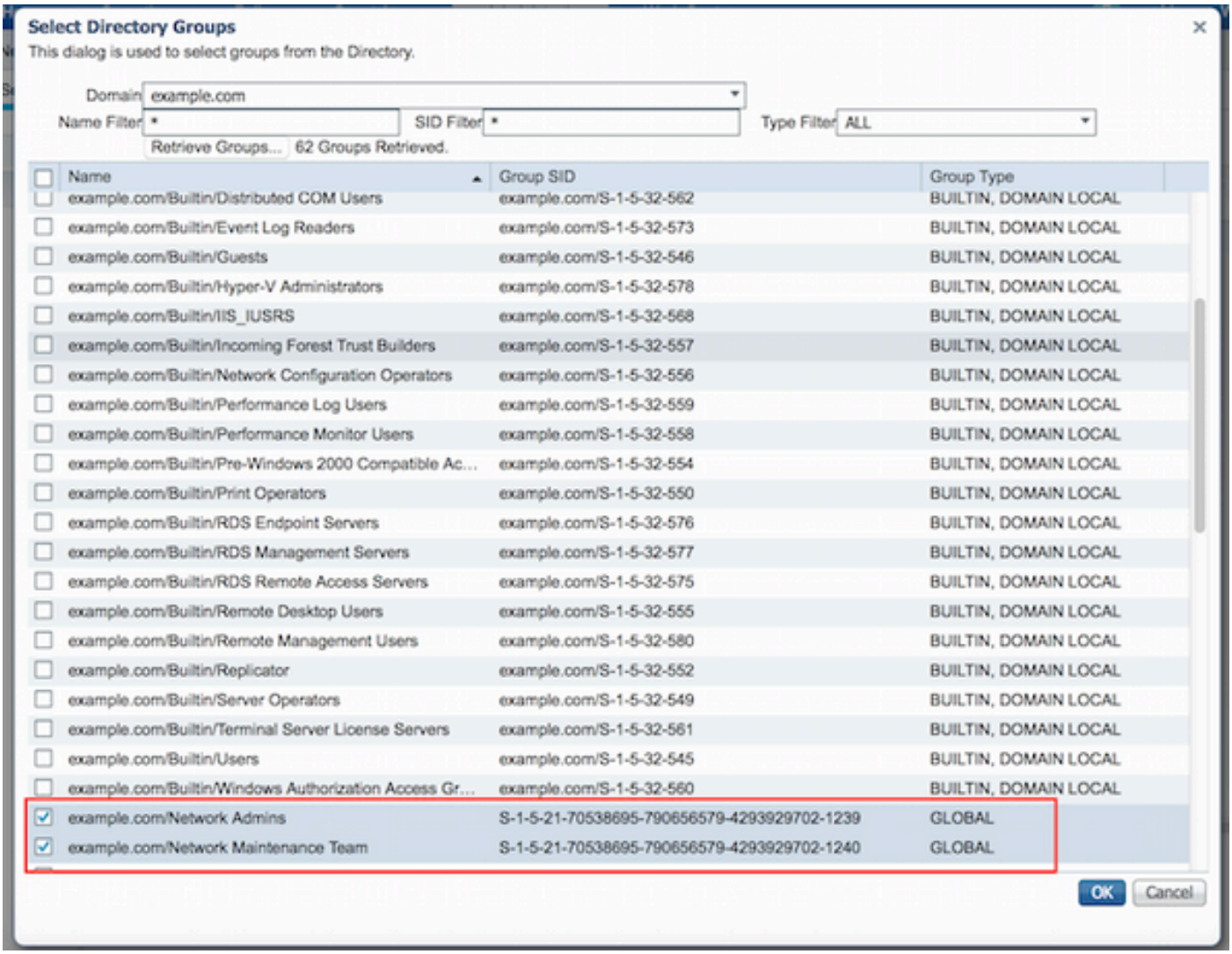
5. El estado de AD es operativo.



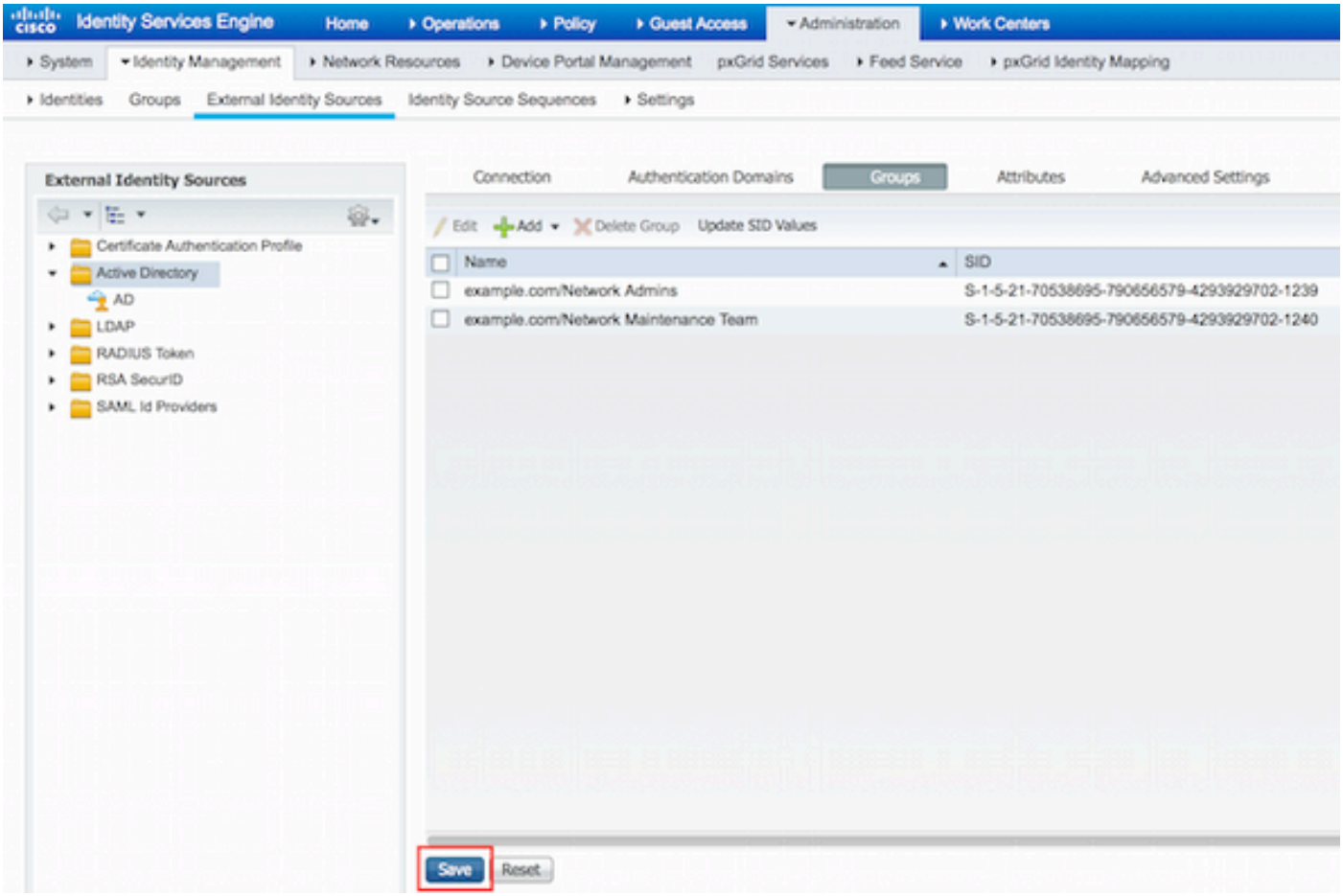
6. Vaya a **Grupos > Agregar > Seleccionar grupos del directorio > Recuperar grupos.** Seleccione las casillas de verificación **Network Admins** AD Group y **Network Maintenance Team** AD Group, como se muestra en esta imagen.

Nota: El usuario admin es miembro del grupo AD de administradores de red. Este usuario tiene privilegios de acceso completos. Este usuario es miembro del grupo AD del equipo de

mantenimiento de red. Este usuario sólo puede ejecutar comandos show.

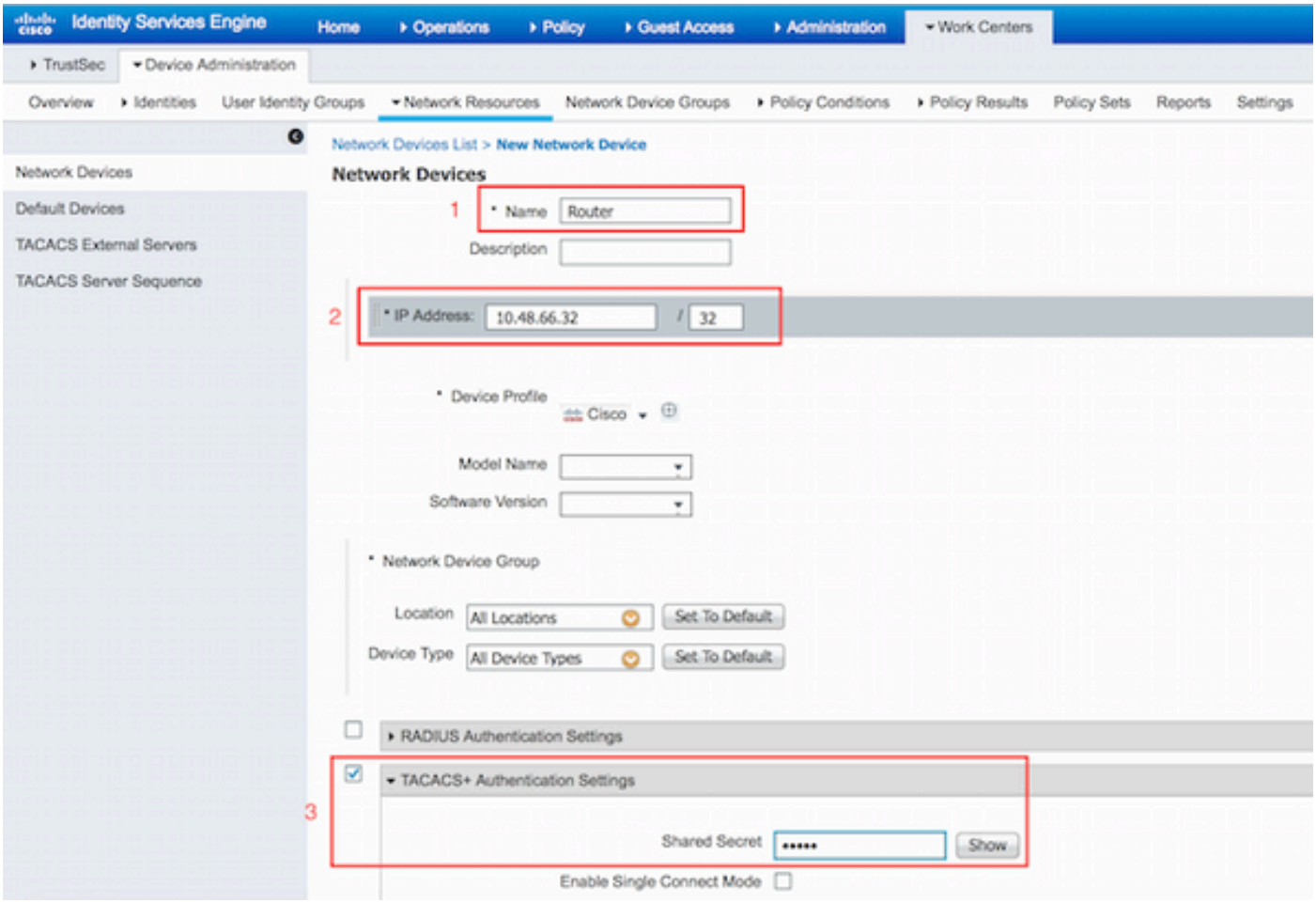


7. Haga clic en **Guardar** para guardar los grupos de AD recuperados.



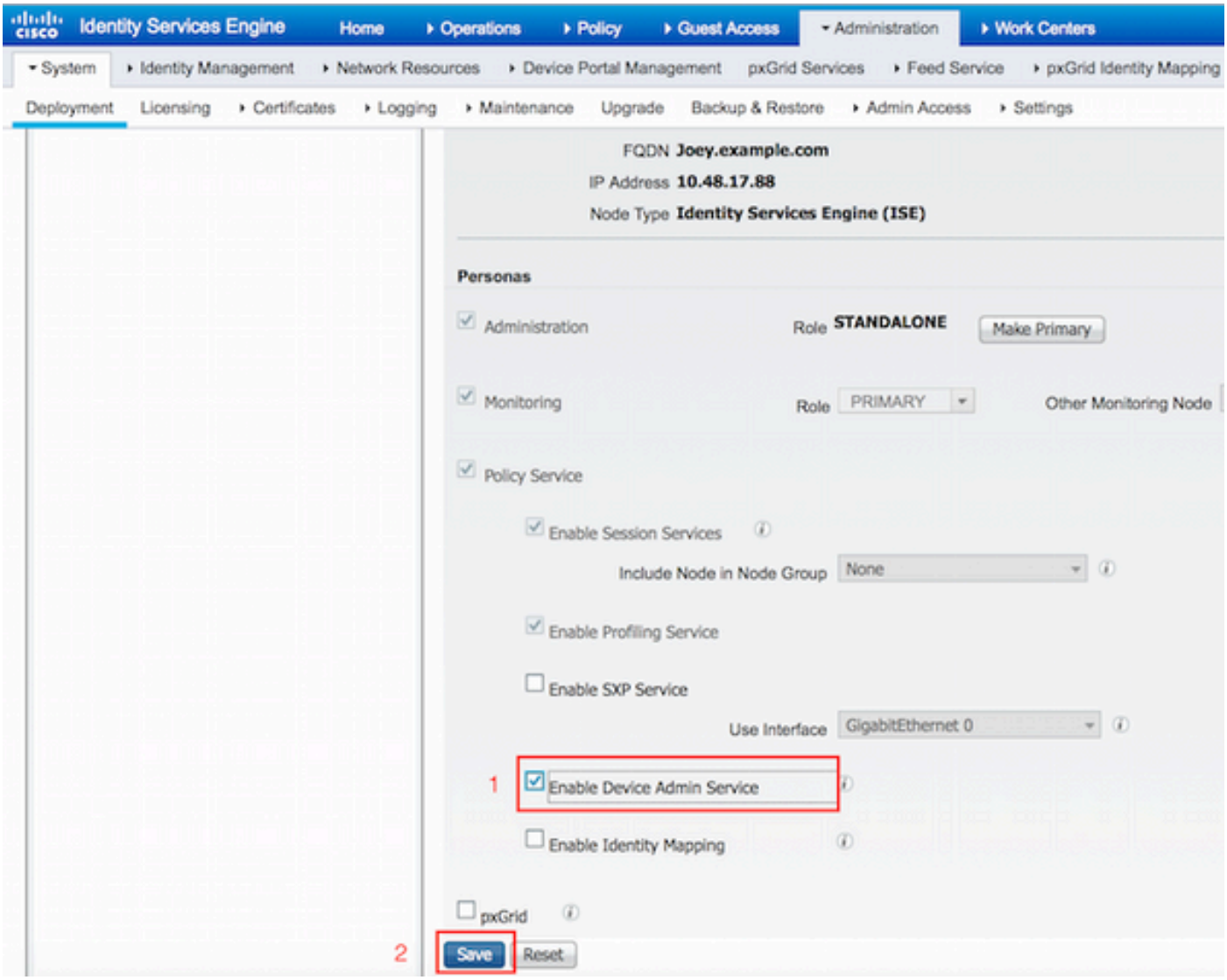
Agregar dispositivo de red

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



Habilitar servicio de administración de dispositivos

Vaya a **Administration > System > Deployment.** Seleccione el nodo necesario. Seleccione la casilla de verificación **Enable Device Admin Service** y haga clic en **Save.**

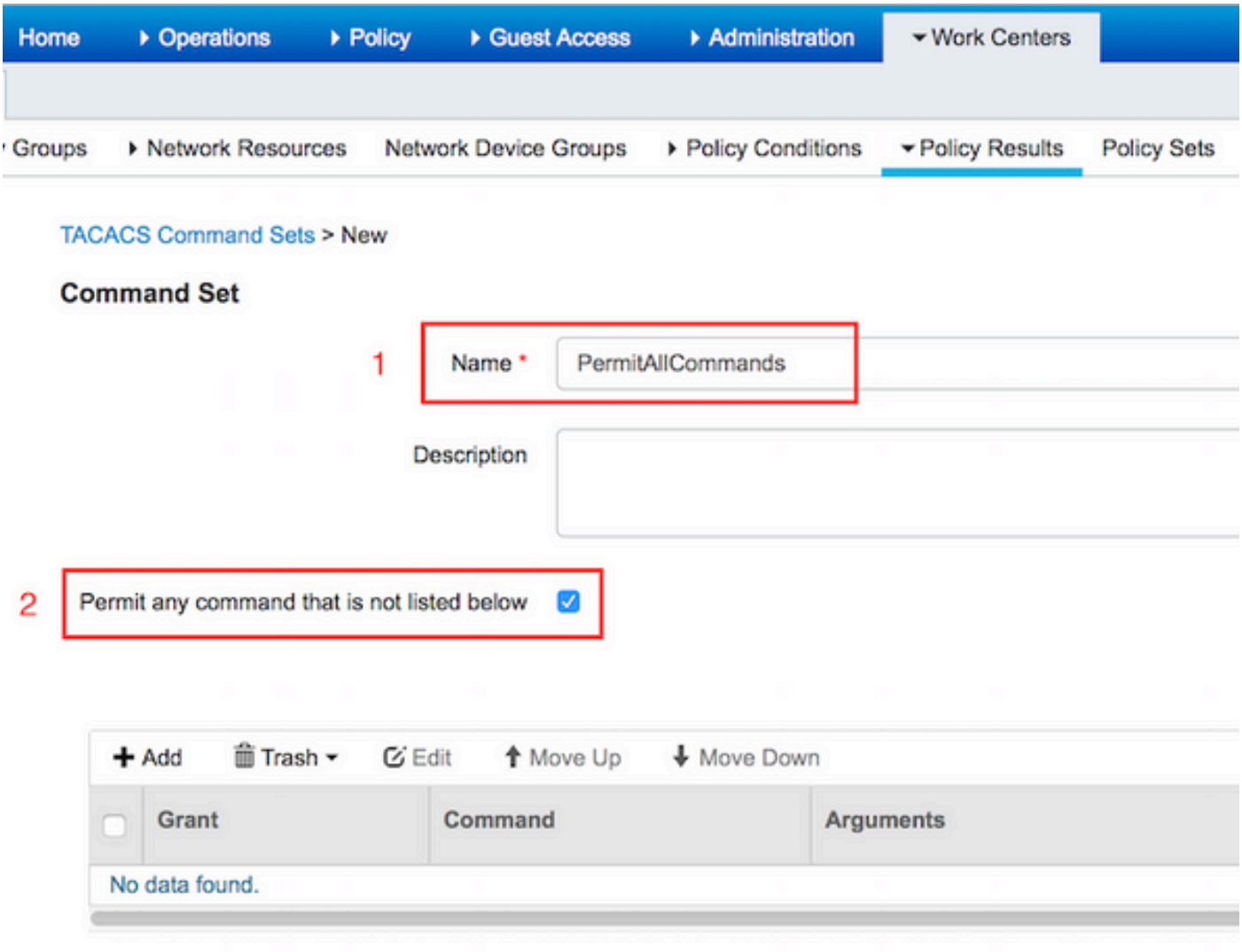


Nota: Para TACACS debe tener instaladas licencias independientes.

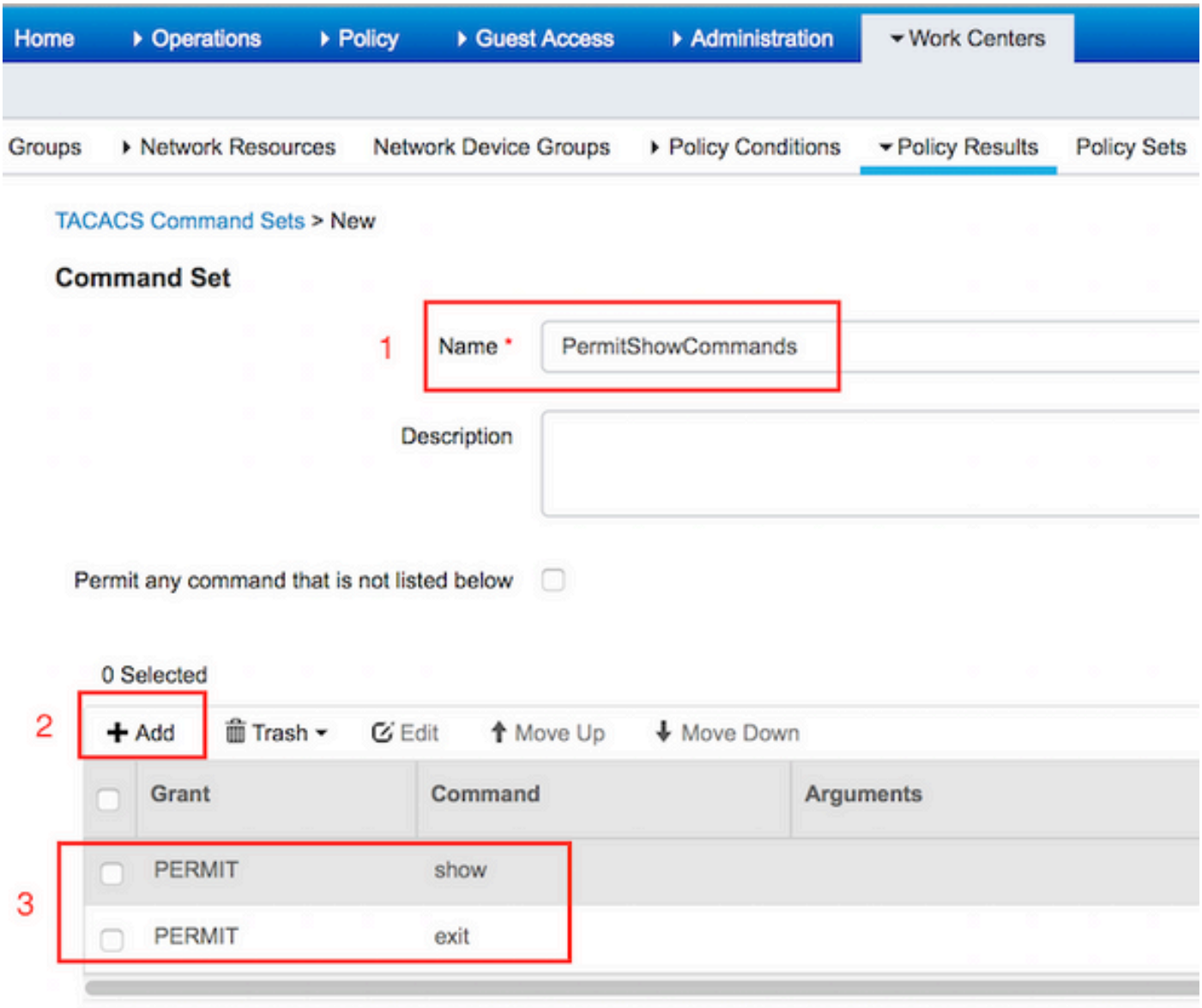
Configurar conjuntos de comandos TACACS

Se configuran dos conjuntos de comandos. First **PermitAllCommands** para el usuario admin que permite todos los comandos en el dispositivo. Second **PermitShowCommands** para el usuario user que sólo permite comandos show.

1. Vaya a **Centros de trabajo > Administración de dispositivos > Resultados de política > Conjuntos de comandos TACACS.** Haga clic en Add (Agregar). Proporcione el nombre **PermitAllCommands**, elija la casilla de verificación **Permitir cualquier comando** que no aparezca en la lista y haga clic en **Enviar.**

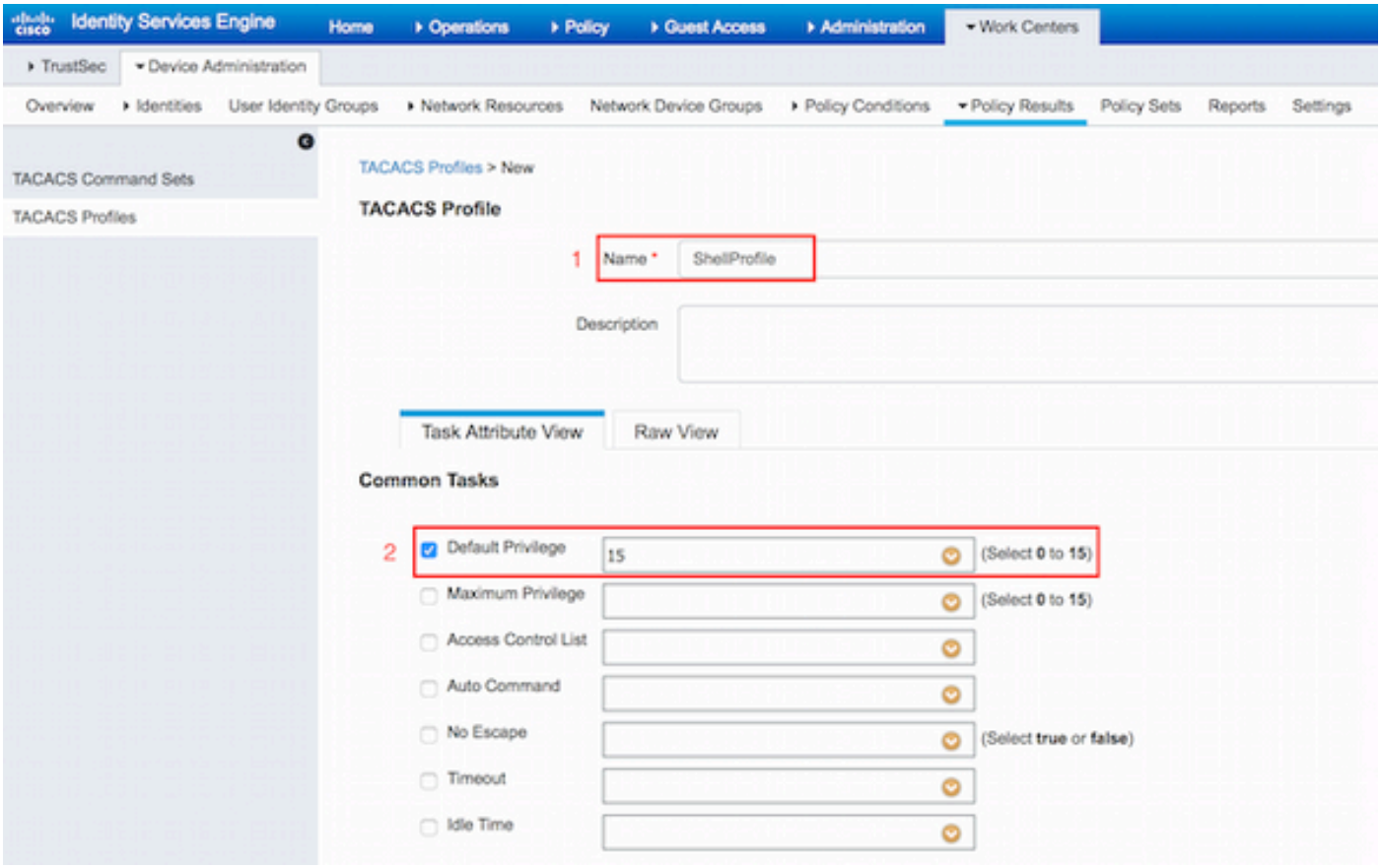


2. Vaya a **Centros de trabajo > Administración de dispositivos > Resultados de política > Conjuntos de comandos TACACS.** Haga clic en Add (Agregar). Proporcione los comandos Name **PermitShowCommands**, haga clic en los comandos **Add** y permit **show** y **exit**. De forma predeterminada, si Arguments se deja en blanco, se incluirán todos los argumentos. Haga clic en Submit (Enviar).



Configurar perfil TACACS

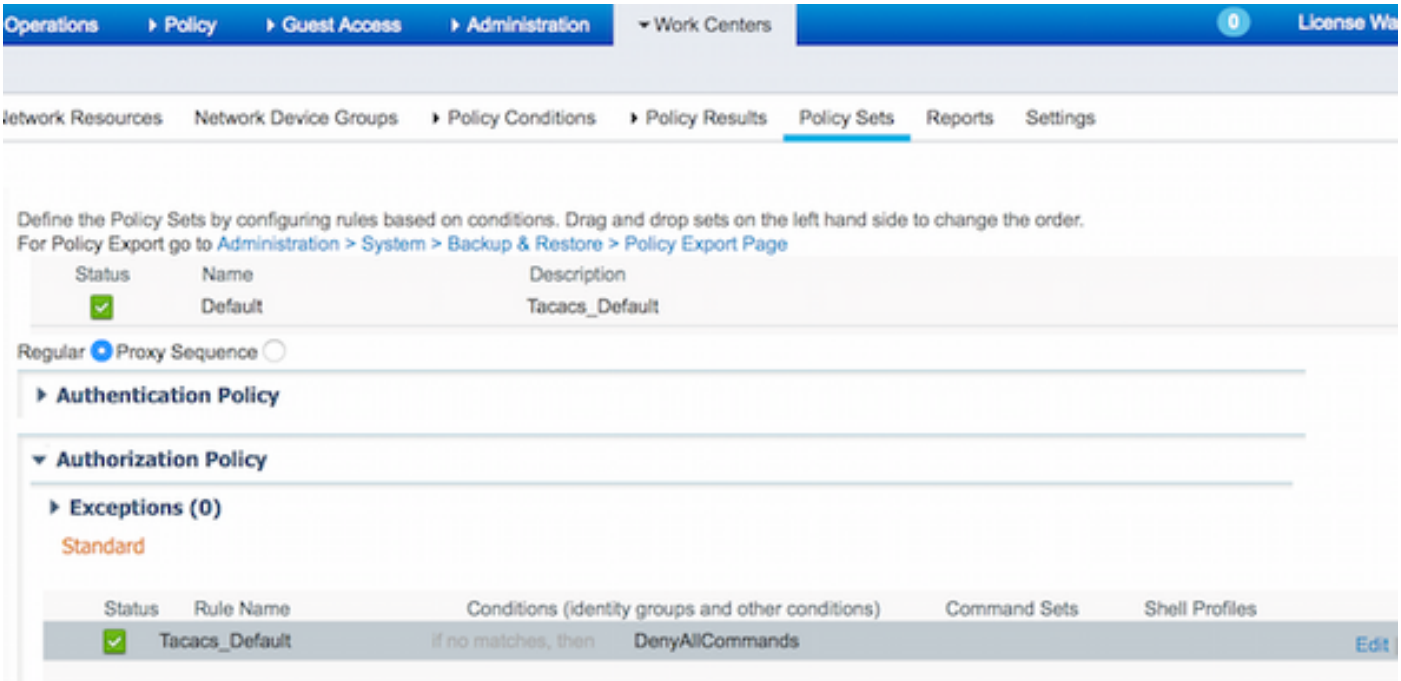
Se ha configurado un único perfil TACACS. El perfil TACACS es el mismo concepto que el perfil Shell en ACS. La aplicación real de los comandos se realiza mediante conjuntos de comandos. Vaya a **Centros de trabajo > Administración de dispositivos > Resultados de política > Perfiles TACACS.** Haga clic en Add (Agregar). Proporcione Name ShellProfile, active la casilla de verificación **Default Privilege** e introduzca el valor de 15. Haga clic en **Submit**.



Configurar política de autorización TACACS

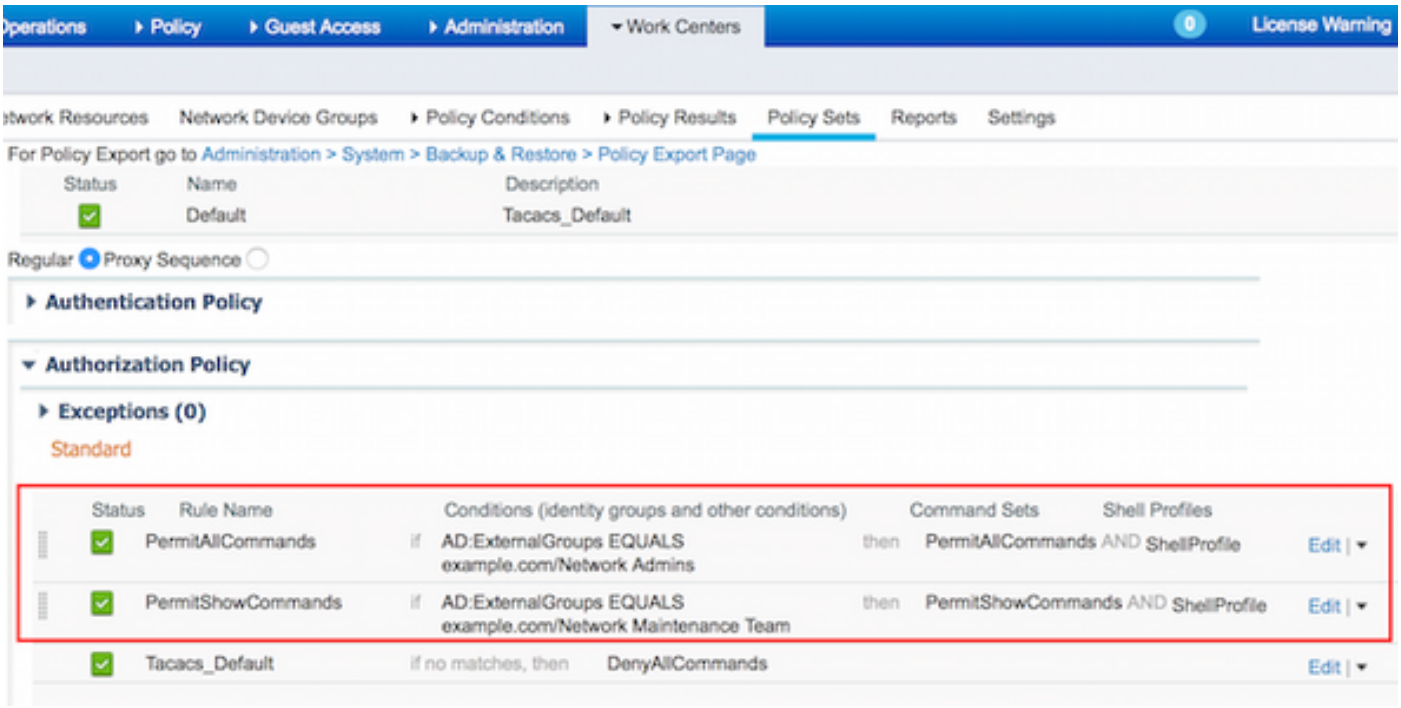
La política de autenticación de forma predeterminada señala a All_User_ID_Stores, que incluye AD, por lo que no se modifica.

Vaya a **Centros de trabajo > Administración de dispositivos > Conjuntos de políticas > Predeterminado > Política de autorización > Editar > Insertar nueva regla arriba.**



Se configuran dos reglas de autorización; La primera regla asigna el perfil TACACS ShellProfile y el comando Set PermitAllCommands en función de la pertenencia al grupo AD de administradores

de red. La segunda regla asigna el perfil TACACS ShellProfile y el comando Set PermitShowCommands en función de la pertenencia al grupo AD del equipo de mantenimiento de red.



Configuración del router Cisco IOS para autenticación y autorización

Complete estos pasos para configurar el router Cisco IOS para la autenticación y la autorización.

1. Cree un usuario local con privilegios completos para el respaldo con el comando **username** como se muestra aquí.

```
username cisco privilege 15 password cisco
```

2. Activar aaa new-model. Defina el ISE del servidor TACACS y colóquelo en el grupo ISE_GROUP.

```
aaa new-model

tacacs server ISE
 address ipv4 10.48.17.88
 key cisco
aaa group server tacacs+ ISE_GROUP
 server name ISE
```

Nota: La clave del servidor coincide con la definida anteriormente en el servidor ISE.

3. Pruebe la disponibilidad del servidor TACACS con el comando test **aaa** como se muestra.

```
Router#test aaa group tacacs+ admin Krakow123 legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.
```

El resultado del comando anterior muestra que el servidor TACACS es accesible y que el usuario se ha autenticado correctamente.

4. Configure el login y habilite las autenticaciones y luego utilice las autorizaciones exec y command como se muestra.

```
aaa authentication login AAA group ISE_GROUP local
aaa authentication enable default group ISE_GROUP enable
aaa authorization exec AAA group ISE_GROUP local
aaa authorization commands 0 AAA group ISE_GROUP local
aaa authorization commands 1 AAA group ISE_GROUP local
aaa authorization commands 15 AAA group ISE_GROUP local
aaa authorization config-commands
```

> **Nota:** La lista de métodos creada se denomina AAA, que se utiliza posteriormente, cuando se asigna a la línea vty.

5. Asigne listas de métodos a la línea vty 0 4.

```
line vty 0 4
 authorization commands 0 AAA
 authorization commands 1 AAA
 authorization commands 15 AAA
 authorization exec AAA
 login authentication AAA
```

Verificación

Verificación del router Cisco IOS

1. Establezca una conexión Telnet con el router Cisco IOS como administrador que pertenece al grupo de acceso completo en AD. El grupo Network Admins es el grupo en AD que está asignado a los comandos ShellProfile y PermitAllCommands establecidos en ISE. Intente ejecutar cualquier comando para garantizar el acceso completo.

```
Username:admin
Password:

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#encryption aes
Router(config-isakmp)#exit
Router(config)#exit
Router#
```

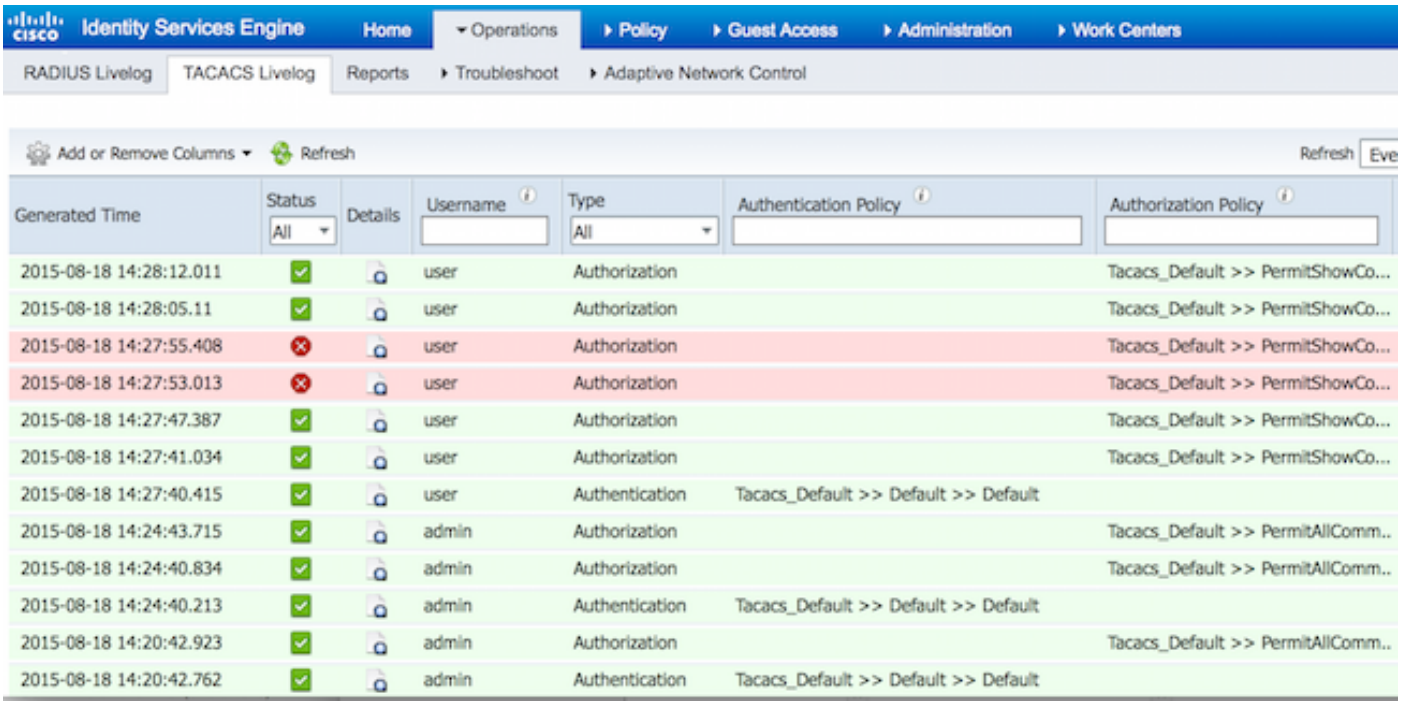
2. Telnet al router Cisco IOS como usuario que pertenece al grupo de acceso limitado en AD. El grupo Equipo de mantenimiento de red es el grupo en AD que está asignado al conjunto de comandos ShellProfile y PermitShowCommands en ISE. Intente ejecutar cualquier comando para asegurarse de que sólo se pueden ejecutar los comandos show.

```
Username:user
Password:

Router#show ip interface brief | exclude unassigned
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         10.48.66.32     YES NVRAM  up                    up
```

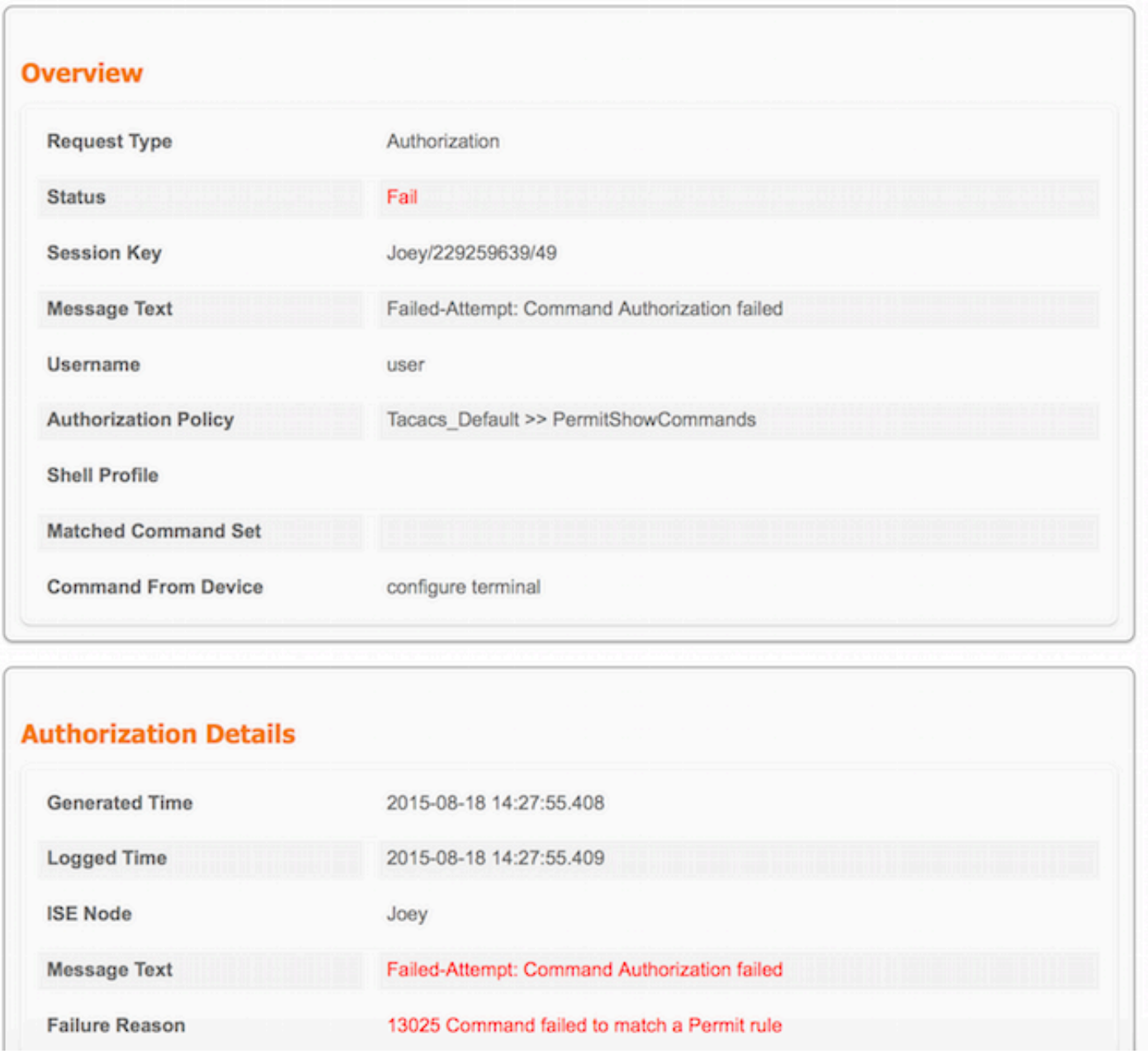
```
Router#ping 8.8.8.8
Command authorization failed.

Router#configure terminal
Command authorization failed.

Router#show running-config | include hostname
hostname Router
Router#
```

Verificación de ISE 2.0

1. Vaya a **Operaciones > Livellog TACACS.** Asegúrese de ver los intentos realizados.



2. Haga clic en los detalles de uno de los informes rojos. Se puede ver el comando fallido ejecutado anteriormente.



Overview

Request Type	Authorization
Status	Fail
Session Key	Joey/229259639/49
Message Text	Failed-Attempt: Command Authorization failed
Username	user
Authorization Policy	Tacacs_Default >> PermitShowCommands
Shell Profile	
Matched Command Set	
Command From Device	configure terminal

Authorization Details

Generated Time	2015-08-18 14:27:55.408
Logged Time	2015-08-18 14:27:55.409
ISE Node	Joey
Message Text	Failed-Attempt: Command Authorization failed
Failure Reason	13025 Command failed to match a Permit rule

Troubleshoot

Error: El comando 13025 no pudo coincidir con una regla de permiso

Compruebe los atributos SelectedCommandSet para comprobar que la directiva de autorización ha seleccionado los conjuntos de comandos esperados.

Información Relacionada

Soporte Técnico y Documentación - Cisco Systems

Notas de la versión de ISE 2.0

Guía de instalación de hardware de ISE 2.0

Guía de actualización a ISE 2.0

Guía de la herramienta de migración de ACS a ISE

Guía de integración de Active Directory de ISE 2.0

Guía del administrador del motor ISE 2.0

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).