Configuración de TACACS+ sobre TLS 1.3 en un dispositivo IOS XR con ISE

Contenido

Introducción

Este documento describe un ejemplo de TACACS+ sobre TLS con Cisco Identity Services Engine (ISE) como servidor y un dispositivo Cisco IOS® XR como cliente.

Overview

El protocolo Terminal Access Controller Access-Control System Plus (TACACS+) Protocol [RFC8907] permite la administración centralizada de dispositivos para routers, servidores de acceso a la red y otros dispositivos conectados en red a través de uno o más servidores TACACS+. Proporciona servicios de autenticación, autorización y contabilidad (AAA), específicamente adaptados para casos prácticos de administración de dispositivos.

TACACS+ sobre TLS 1.3 [RFC8446] mejora el protocolo mediante la introducción de una capa de transporte segura, protegiendo los datos altamente confidenciales. Esta integración garantiza confidencialidad, integridad y autenticación para la conexión y el tráfico de red entre los clientes y servidores TACACS+.

Utilización de esta guía

Esta guía divide las actividades en dos partes para permitir que ISE gestione el acceso administrativo de los dispositivos de red basados en Cisco IOS XR.
· Parte 1: Configuración de ISE para la administración de dispositivos
· Parte 2: Configuración de Cisco IOS XR para TACACS+ sobre TLS

Prerequisites

Requirements

Requisitos para configurar TACACS+ sobre TLS:

- Una autoridad de certificación (CA) para firmar el certificado utilizado por TACACS+ sobre TLS para firmar los certificados de ISE y los dispositivos de red.
- El certificado raíz de la autoridad de certificación (CA).
- Los dispositivos de red e ISE tienen disponibilidad de DNS y pueden resolver nombres de host.

Componentes Utilizados

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

- Dispositivo virtual ISE VMware, versión 3.4, parche 2
- Router Cisco 8201, versión 25.3.1

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.

Licencias

Una licencia Device Administration permite utilizar los servicios TACACS+ en un nodo de Policy Service. En una implementación independiente de alta disponibilidad (HA), una licencia Device Administration permite utilizar los servicios TACACS+ en un único nodo de servicio de políticas en el par HA.

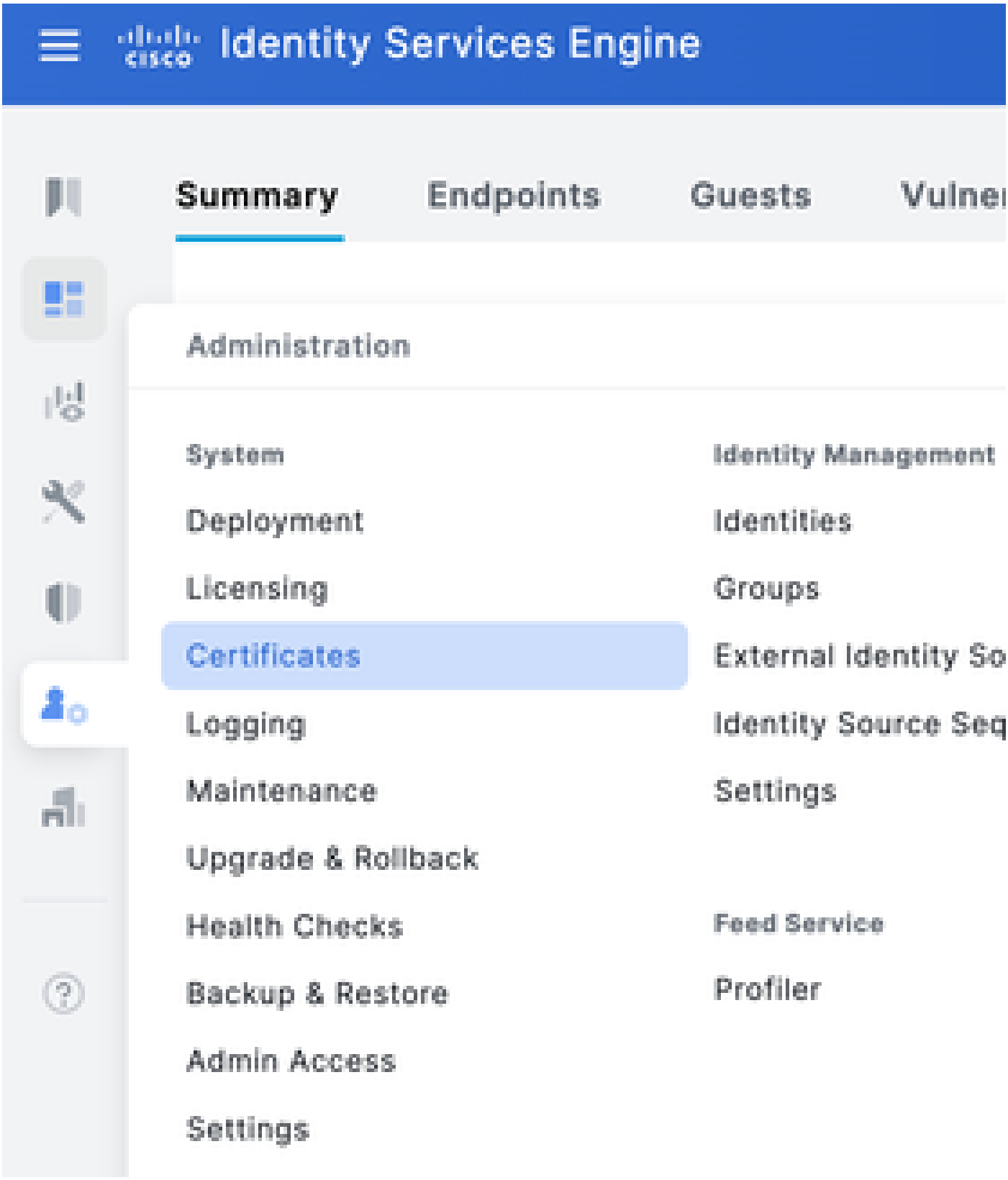
Parte 1: Configuración de ISE para la administración de dispositivos

Generar solicitud de firma de certificado para autenticación de servidor TACACS+

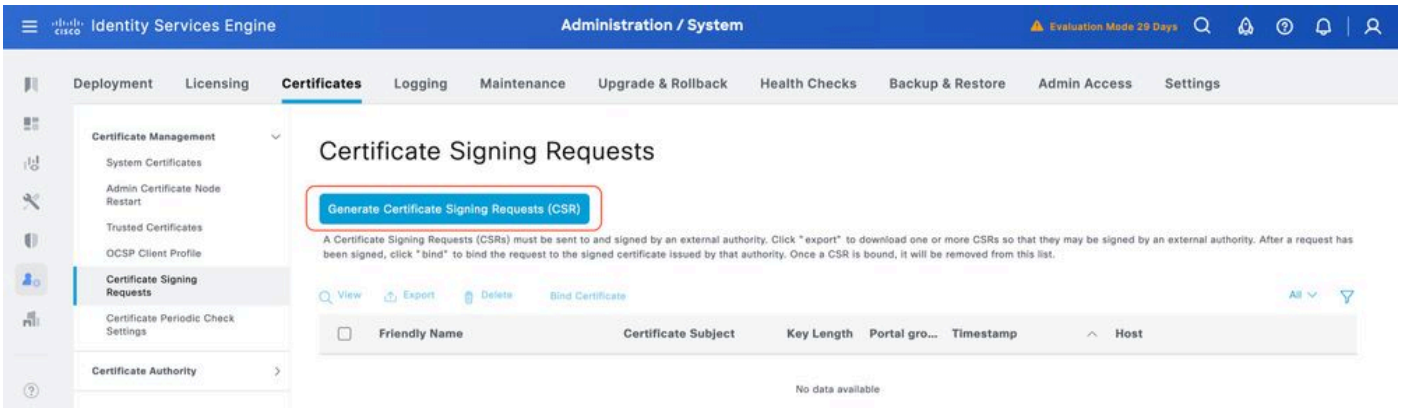
Paso 1. Inicie sesión en el portal web de administración de ISE con uno de los navegadores compatibles.

De forma predeterminada, ISE utiliza un certificado autofirmado para todos los servicios. El primer paso es generar una Solicitud de firma de certificado (CSR) para que la firme nuestra Autoridad de certificación (CA).

Paso 2. Vaya aAdministración > Sistema > Certificados.

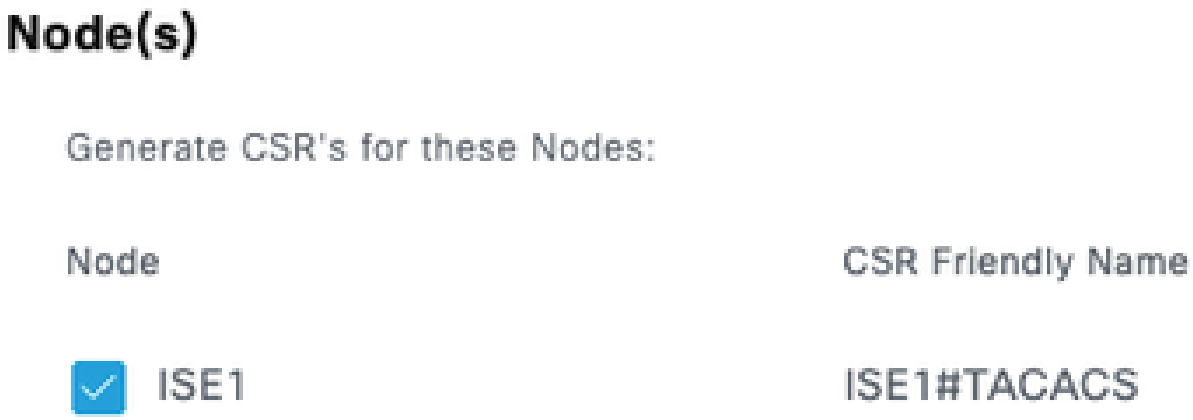


Paso 3. En Solicitudes de firma de certificado, haga clic en Generar solicitud de firma de certificado.

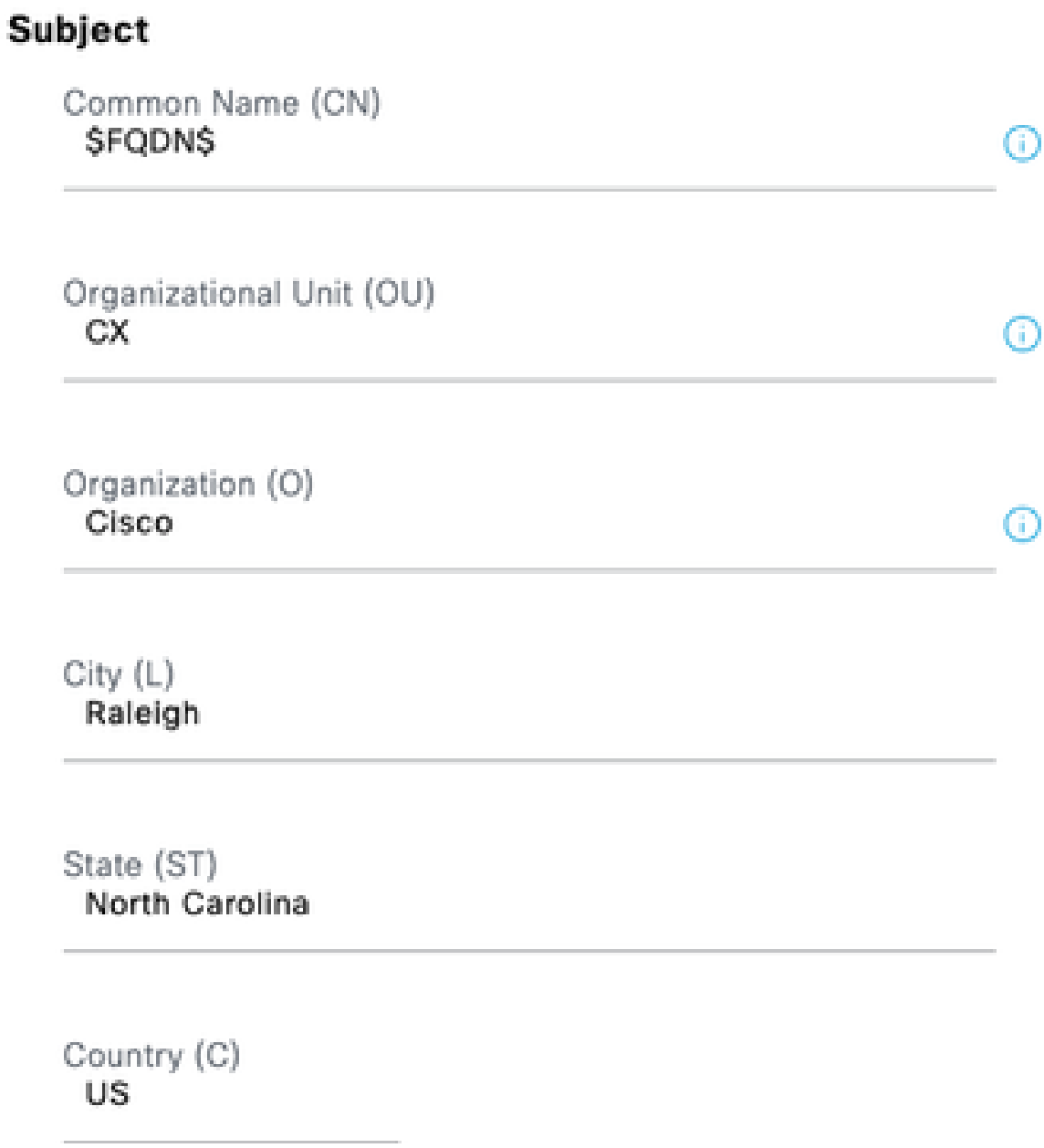


Paso 4. SeleccioneTACACS inUsage.

Paso 5. Seleccione los PSN que tienen TACACS+ habilitado.

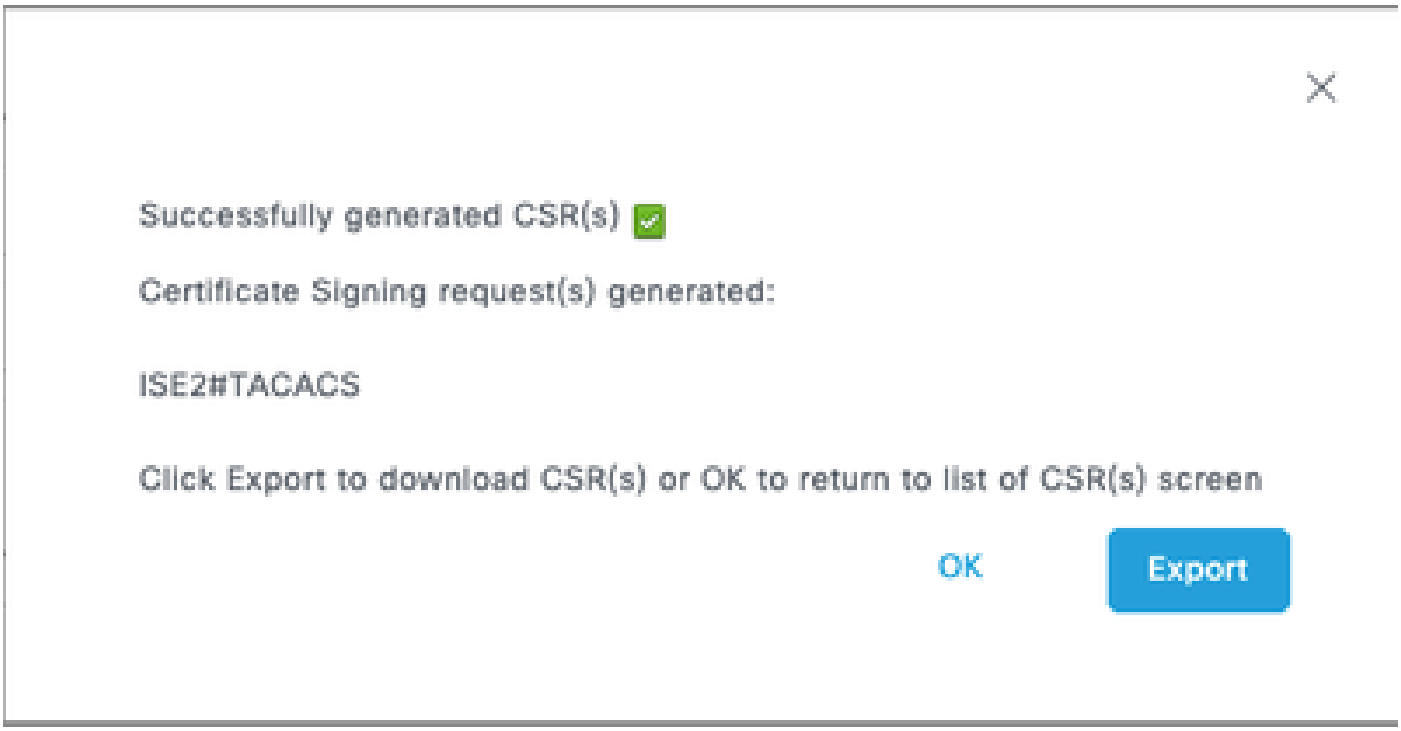


Paso 6. Rellene los campos Asunto con la información correspondiente.



Paso 7. Agregue el Nombre DNS y la Dirección IP en Nombre alternativo del sujeto (SAN).

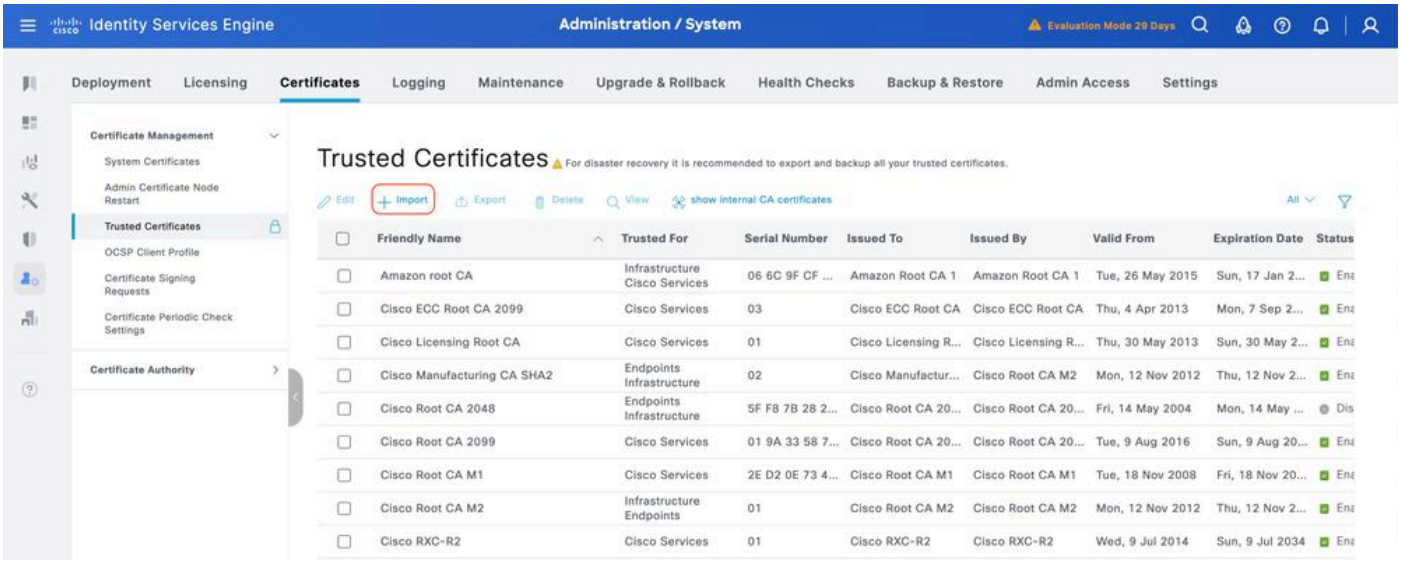
Paso 8. Haga clic en Generar y luego en Exportar.



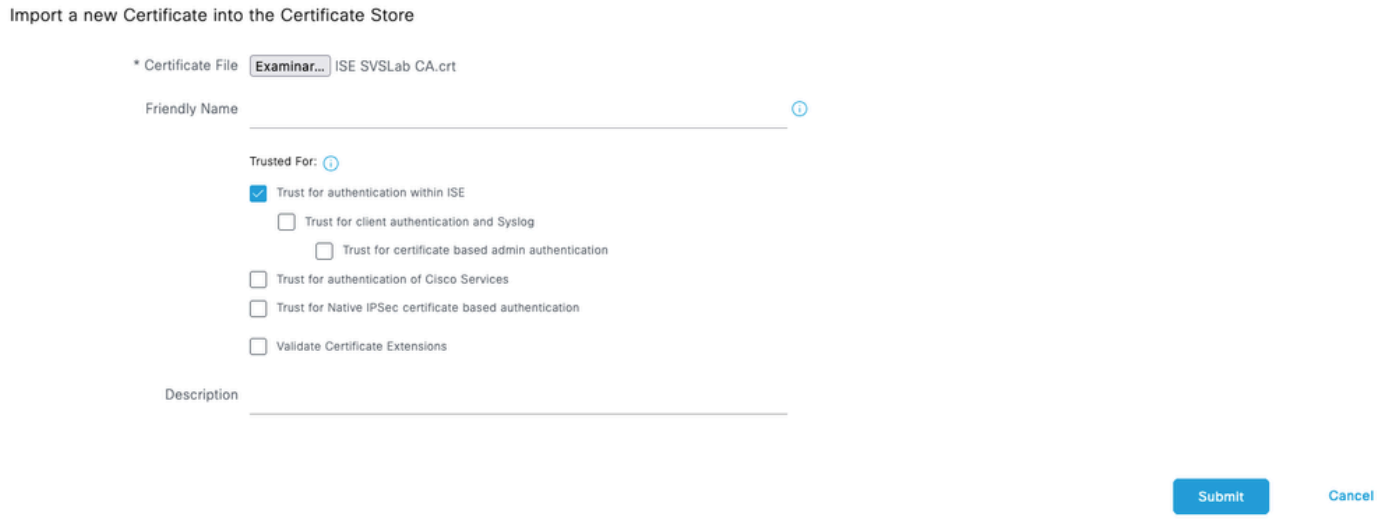
Ahora puede hacer que la autoridad certificadora (CA) firme el certificado (CRT).

Cargar certificado de CA raíz para autenticación de servidor TACACS+

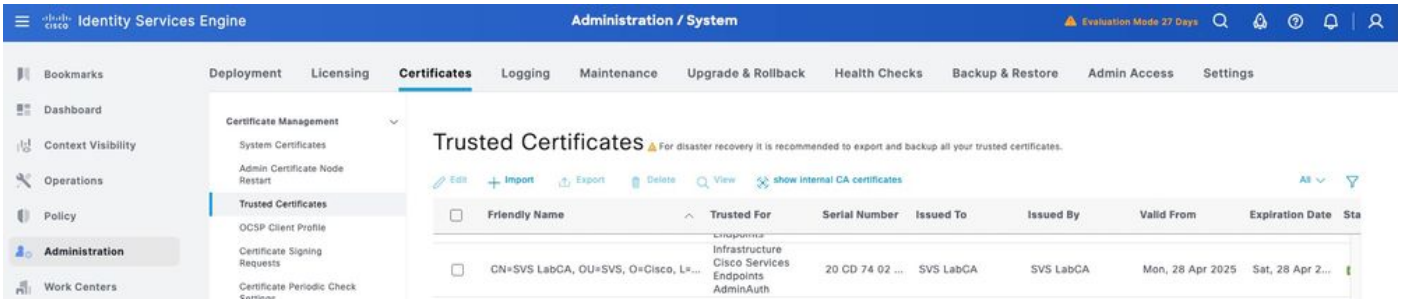
Paso 1.Vaya aAdministración > Sistema > Certificados. En Certificados de confianza, haga clic en Importar.



Paso 2. Seleccione el certificado emitido por la autoridad de certificación (CA) que firmó la solicitud de firma de certificado (CSR) de TACACS. Asegúrese de que el Confianza para la autenticación dentro de ISE está activada.



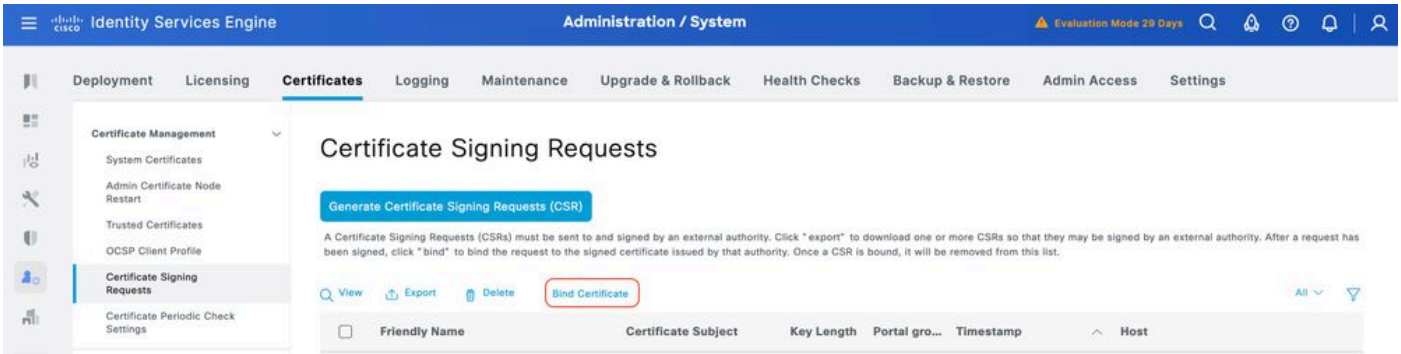
Haga clic en Enviar. El certificado debe aparecer ahora en Trusted Certificates.



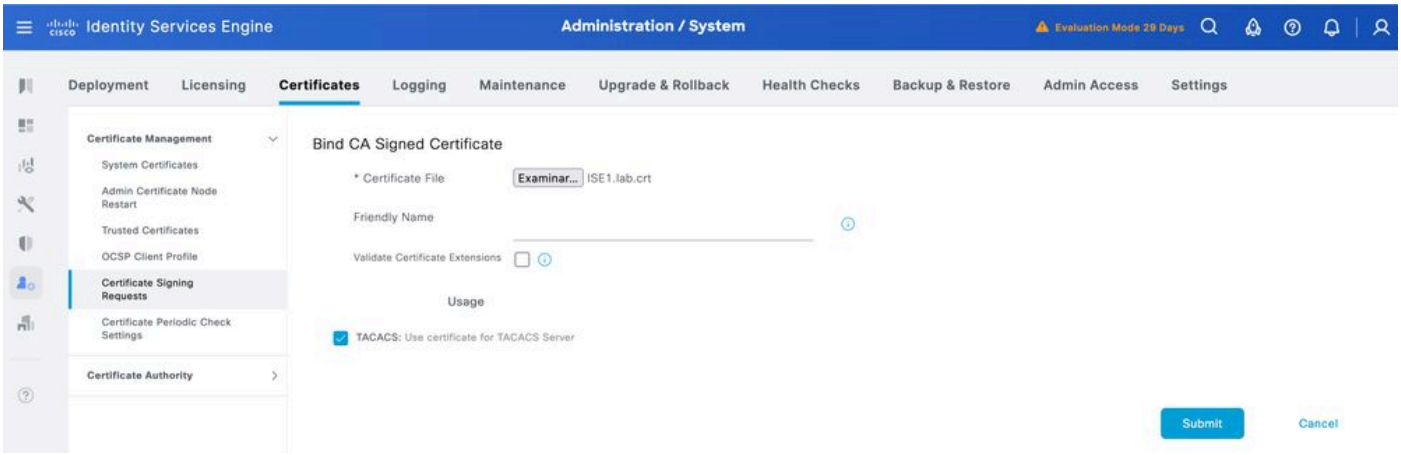
Enlazar la solicitud de firma de certificado (CSR) firmado a ISE

Una vez firmada la solicitud de firma de certificado (CSR), puede instalar el certificado firmado en ISE.

Paso 1.Vaya a Administración > Sistema > Certificados. En Solicitudes de firma de certificado, seleccione el CSR TACACS generado en el paso anterior y haga clic en Enlazar certificado.

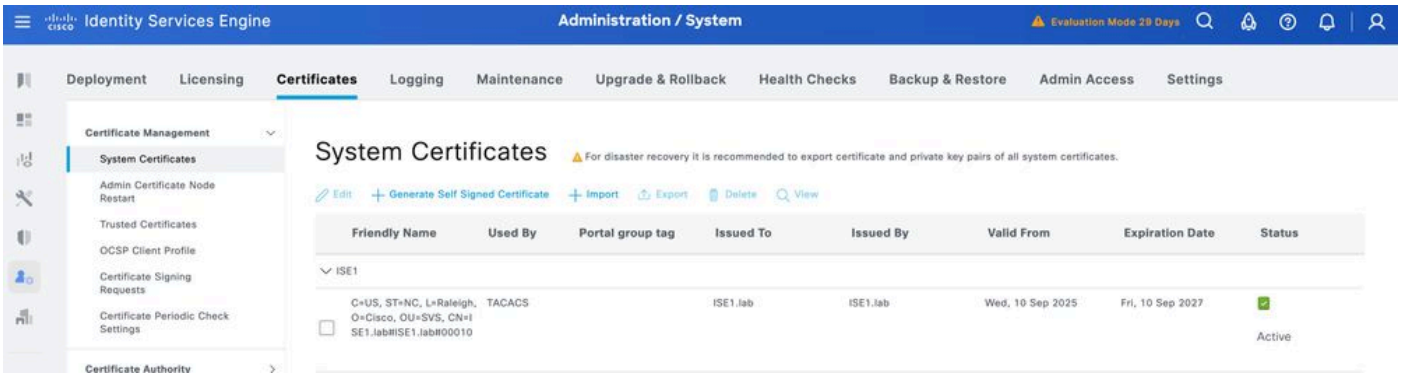


Paso 2.Seleccione el certificado firmado y asegúrese de que la casilla de verificación TACACS bajo Uso permanezca seleccionada.



Paso 3. Haga clic en Enviar. Si recibe una advertencia sobre la sustitución del certificado existente, haga clic en Sí para continuar.

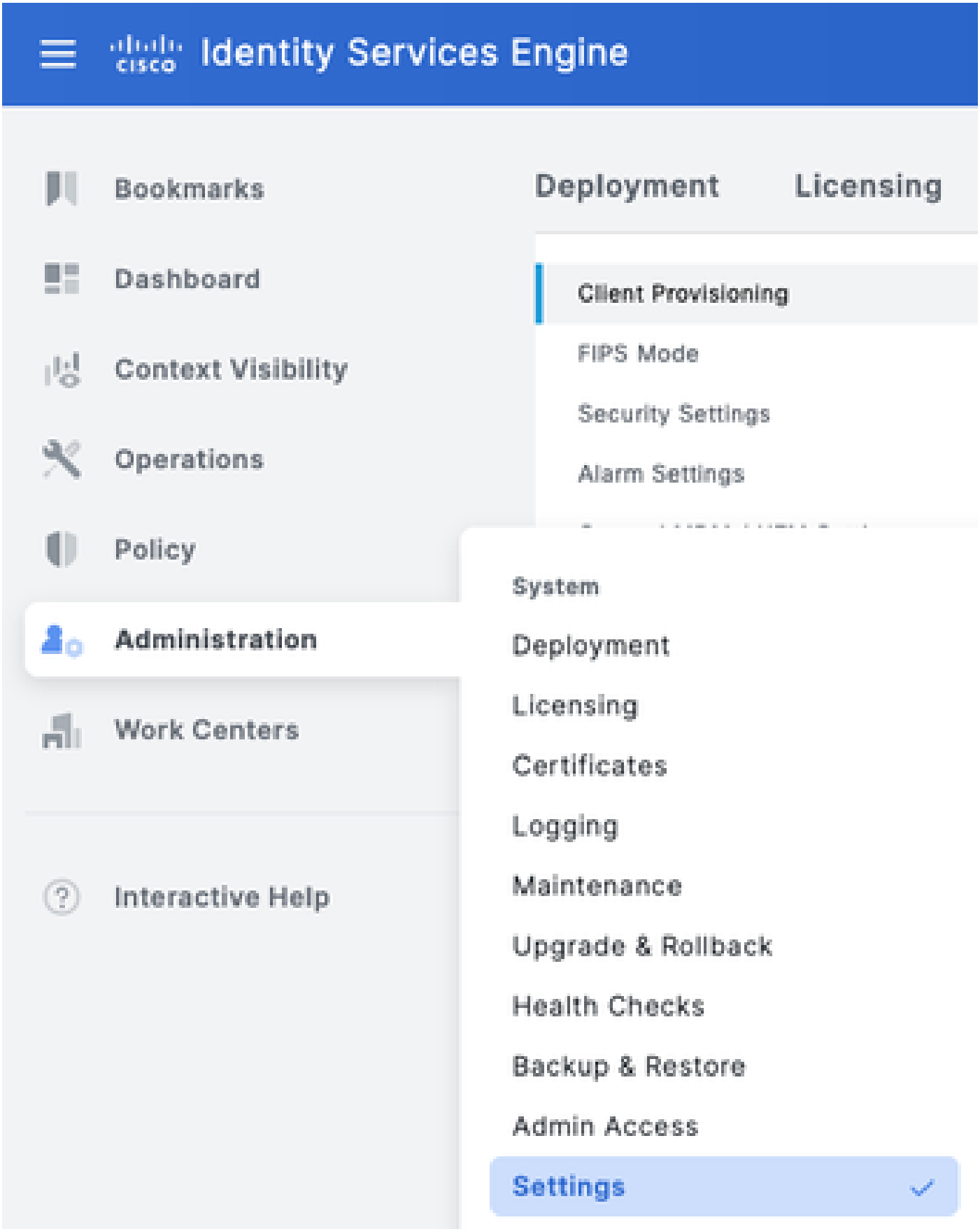
El certificado debe estar instalado correctamente. Puede verificarlo en Certificados del sistema.



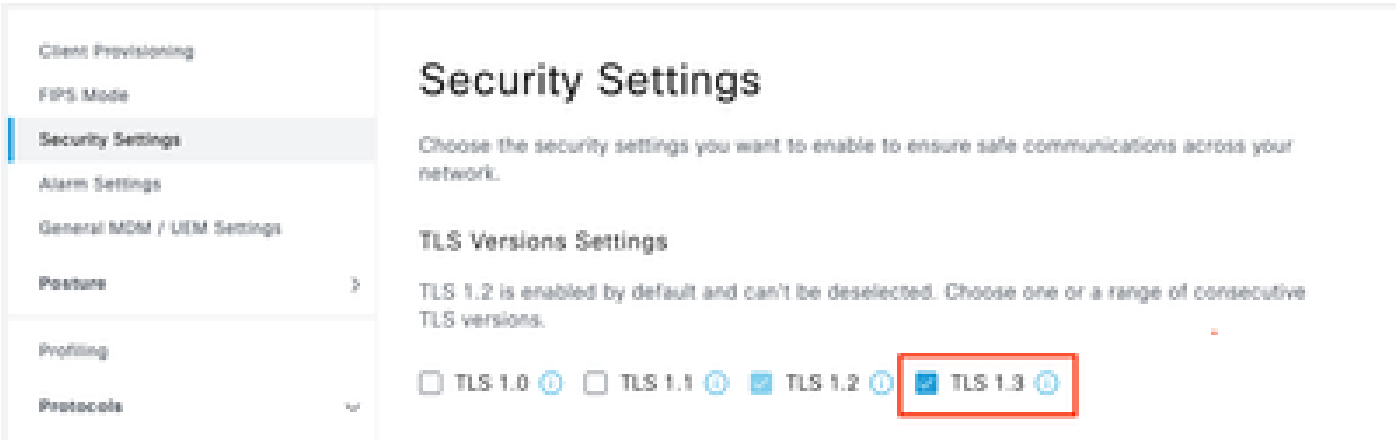
Habilitar TLS 1.3

TLS 1.3 no está habilitado de forma predeterminada en ISE 3.4.x. Debe habilitarse manualmente.

Paso 1.Vaya aAdministración > Sistema > Configuración.



Paso 2. Haga clic en Configuración de seguridad, seleccione la casilla de verificación junto a TLS1.3 en Configuración de la versión de TLS y, a continuación, haga clic en Guardar.

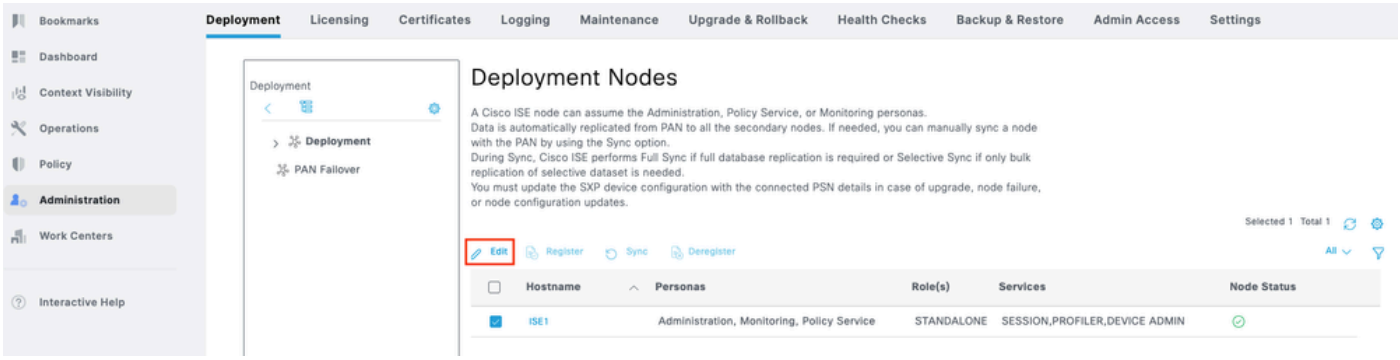


Advertencia: Al cambiar la versión de TLS, el servidor de aplicaciones de Cisco ISE se reinicia en todos los equipos de implementación de Cisco ISE.

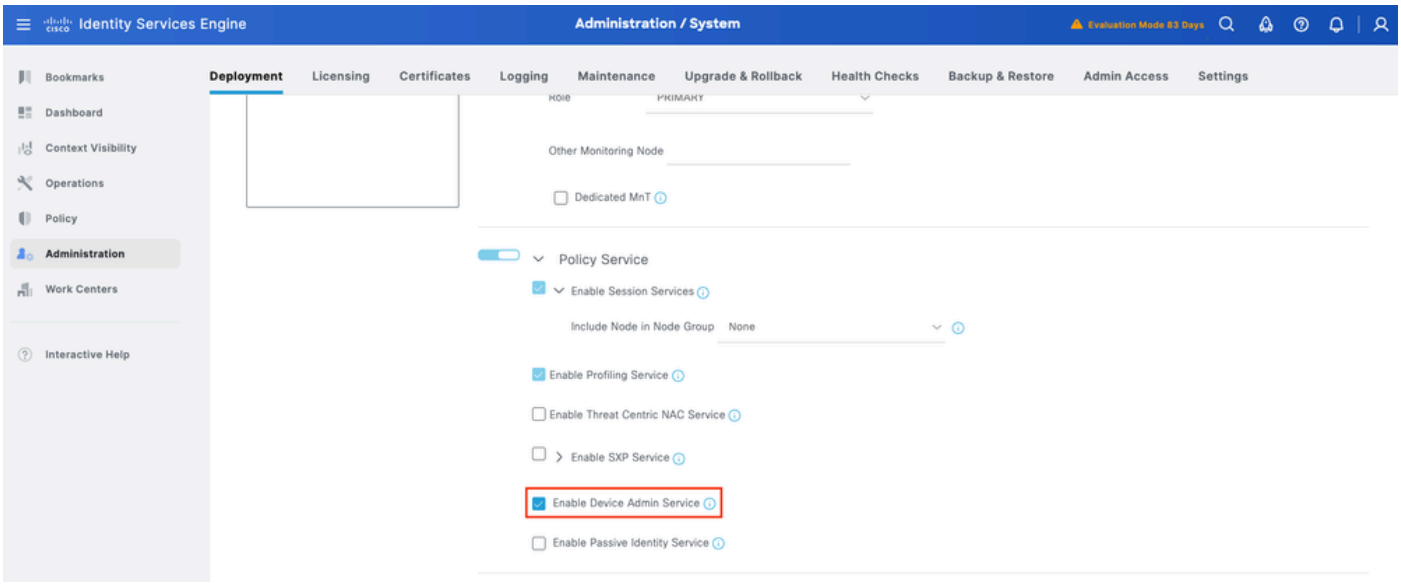
Habilitar Device Administration en ISE

El servicio Device Administration (TACACS+) no está habilitado de forma predeterminada en un nodo ISE. Para habilitar TACACS+ en un nodo PSN:

Paso 1. Vaya a Administration > System > Deployment. Active la casilla de verificación situada junto al nodo de ISE y haga clic en Editar.



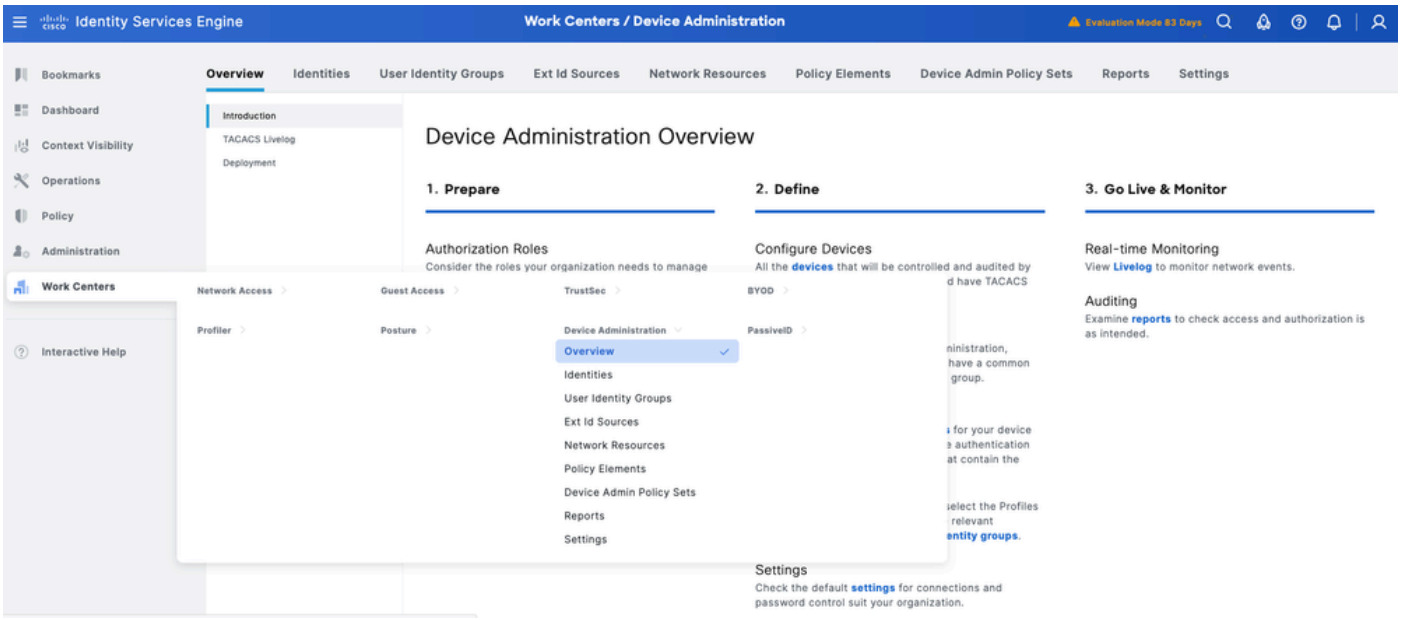
Paso 2.En GeneralSettings, desplácese hacia abajo y seleccione la casilla de verificación junto a Enable Device Admin Service.



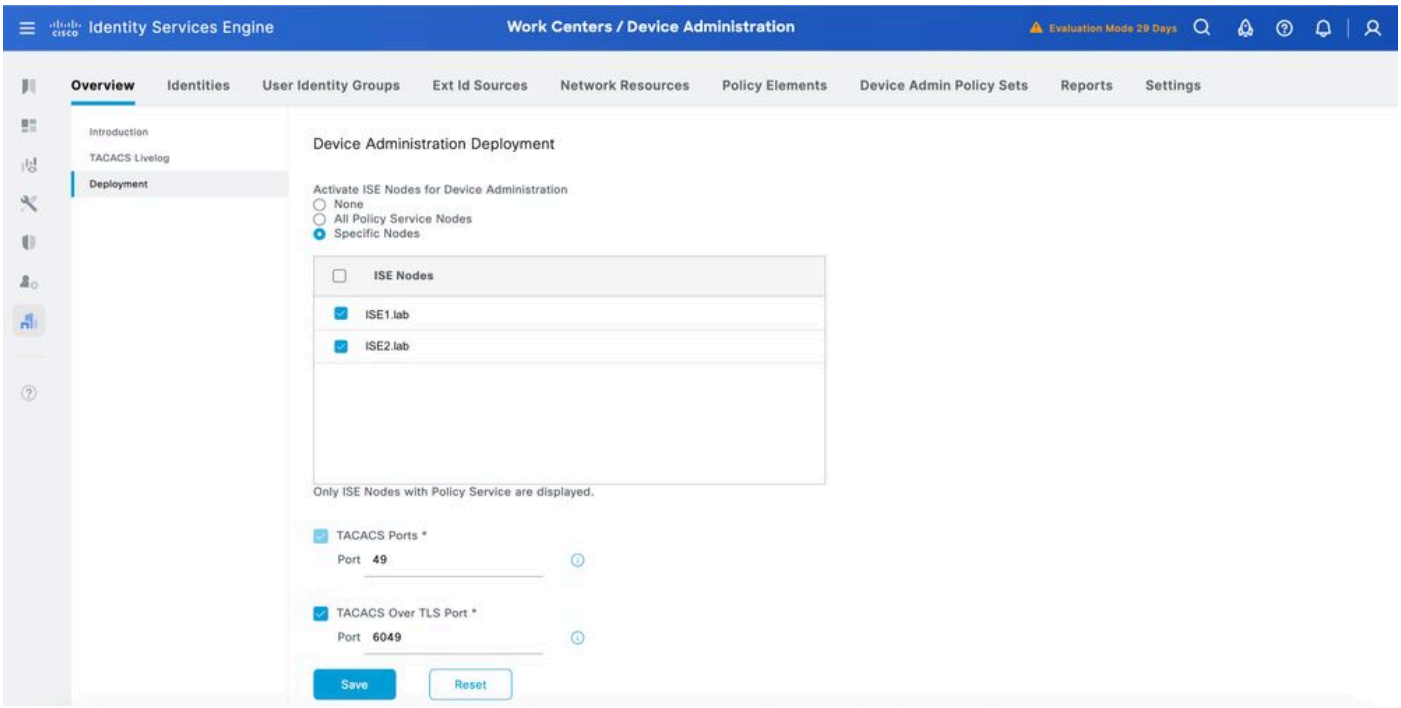
Paso 3. Guarde la configuración. El servicio Device Admin está ahora habilitado en ISE.

Habilitar TACACS sobre TLS

Paso 1.Vaya a Centros de trabajo > Administración de dispositivos > Descripción general.



Paso 2.Haga clic en Implementación. Seleccione los nodos PSN donde desea habilitar TACACS sobre TLS.

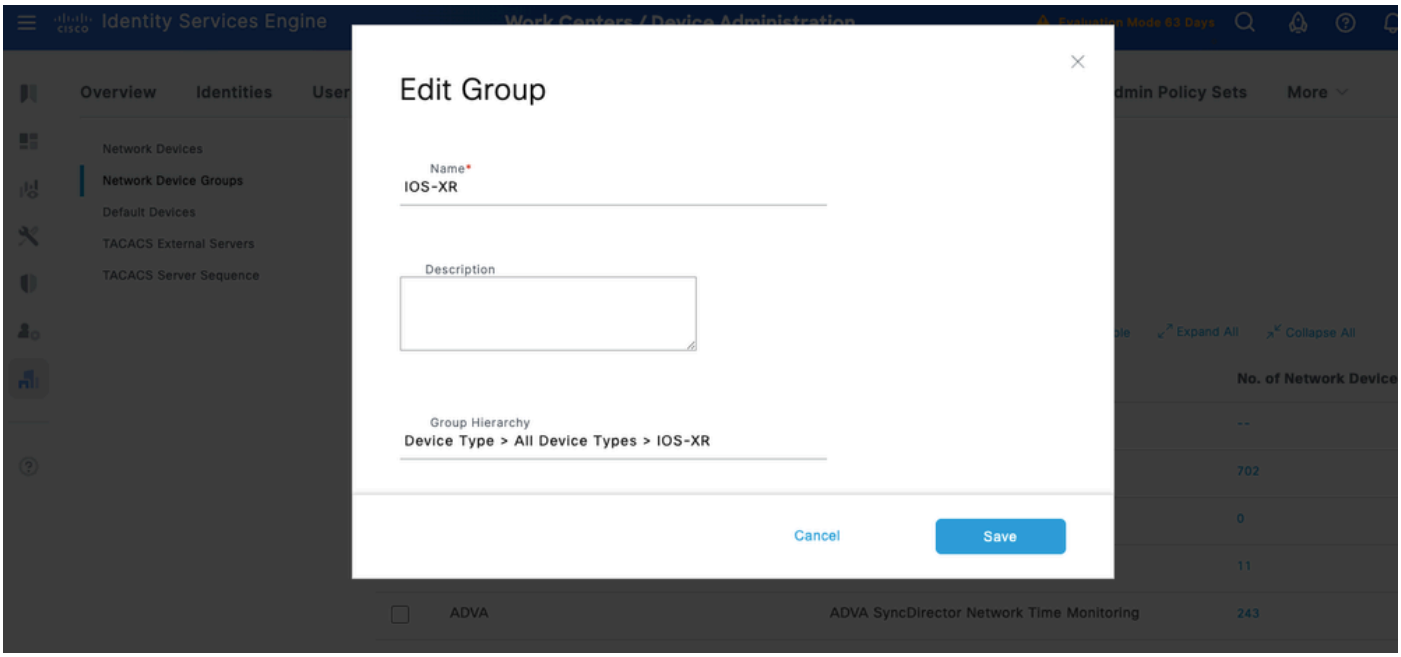


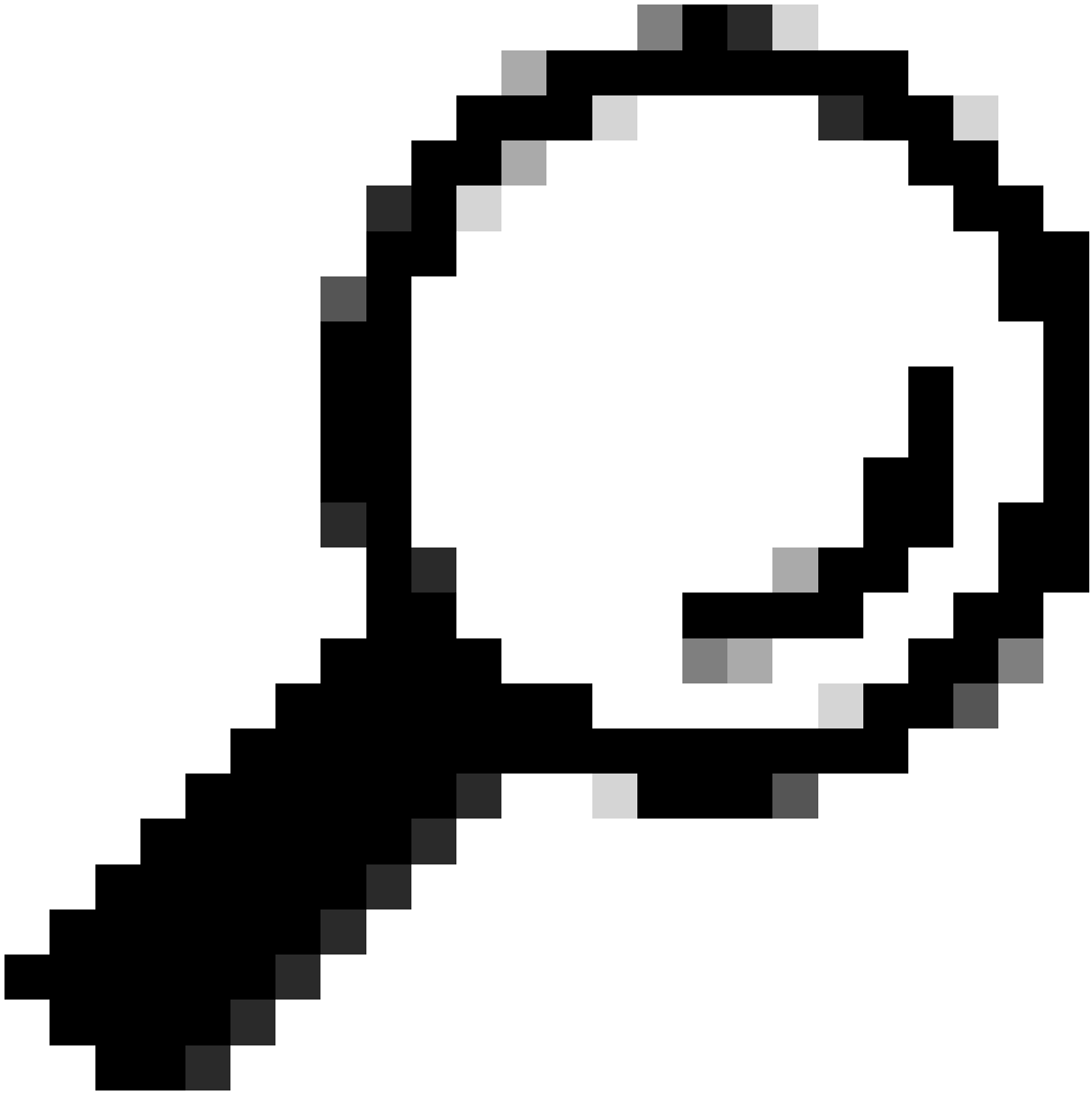
Paso 3.Mantenga el puerto predeterminado 6049 o especifique un puerto TCP diferente para TACACS sobre TLS, luego haga clic en Guardar.

Crear dispositivos de red y grupos de dispositivos de red

ISE proporciona una potente agrupación de dispositivos con varias jerarquías de grupos de dispositivos. Cada jerarquía representa una clasificación distinta e independiente de los dispositivos de red.

Paso 1.Navegue hasta Centros de trabajo > Administración de dispositivos > Recursos de red.Haga clic en Grupos de dispositivos de red y cree un grupo con el nombre IOS XR.

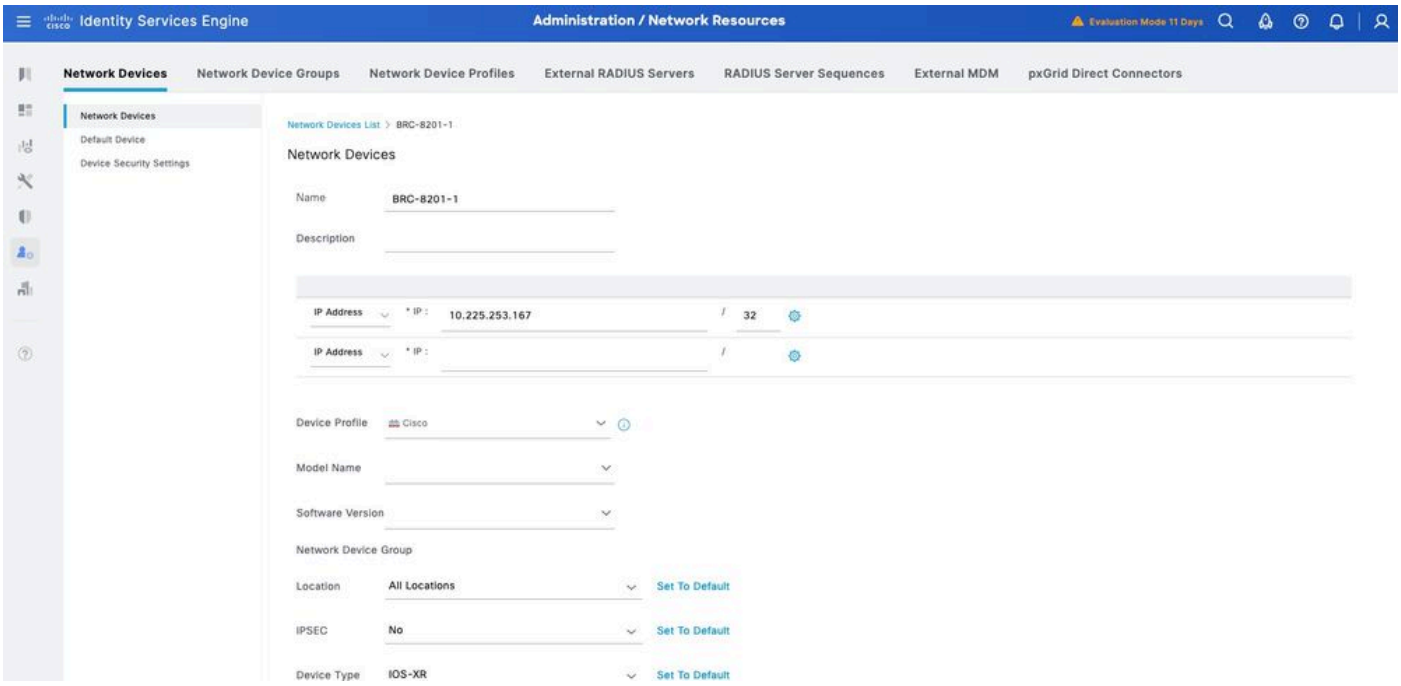

Identity Services Engine
Work Centers / Device Administration
Overview
Identities
User
Admin Policy Sets
More
Network Devices
Network Device Groups
Default Devices
TACACS External Servers
TACACS Server Sequence
Expand All
Collapse All
No. of Network Device
Edit Group
Name*
IOS-XR
Description
Group Hierarchy
Device Type > All Device Types > IOS-XR
Cancel
Save
ADVA
ADVA SyncDirector Network Time Monitoring
243



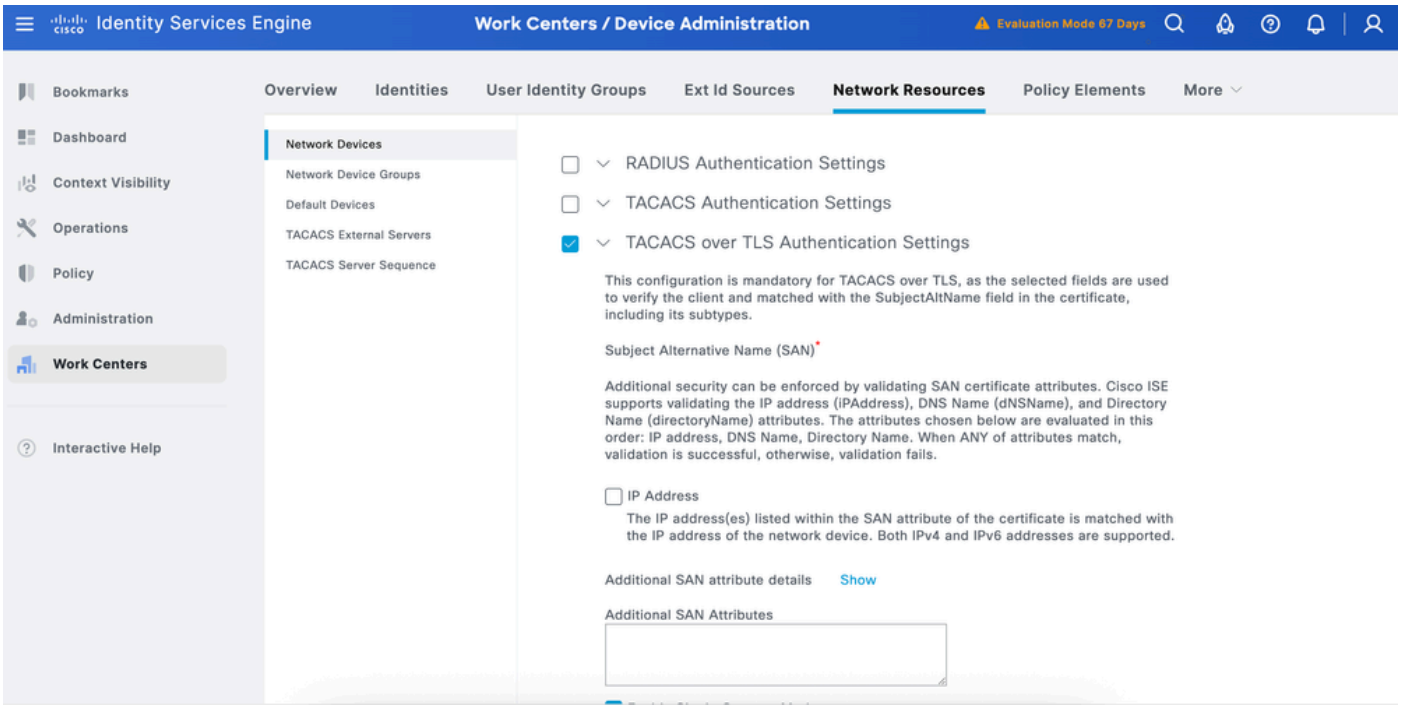
Consejo: Todos los tipos de dispositivos y todas las ubicaciones son jerarquías predeterminadas proporcionadas por ISE. Puede agregar sus propias jerarquías y definir los diversos componentes al identificar un dispositivo de red que se puede utilizar más adelante en la Condición de directiva

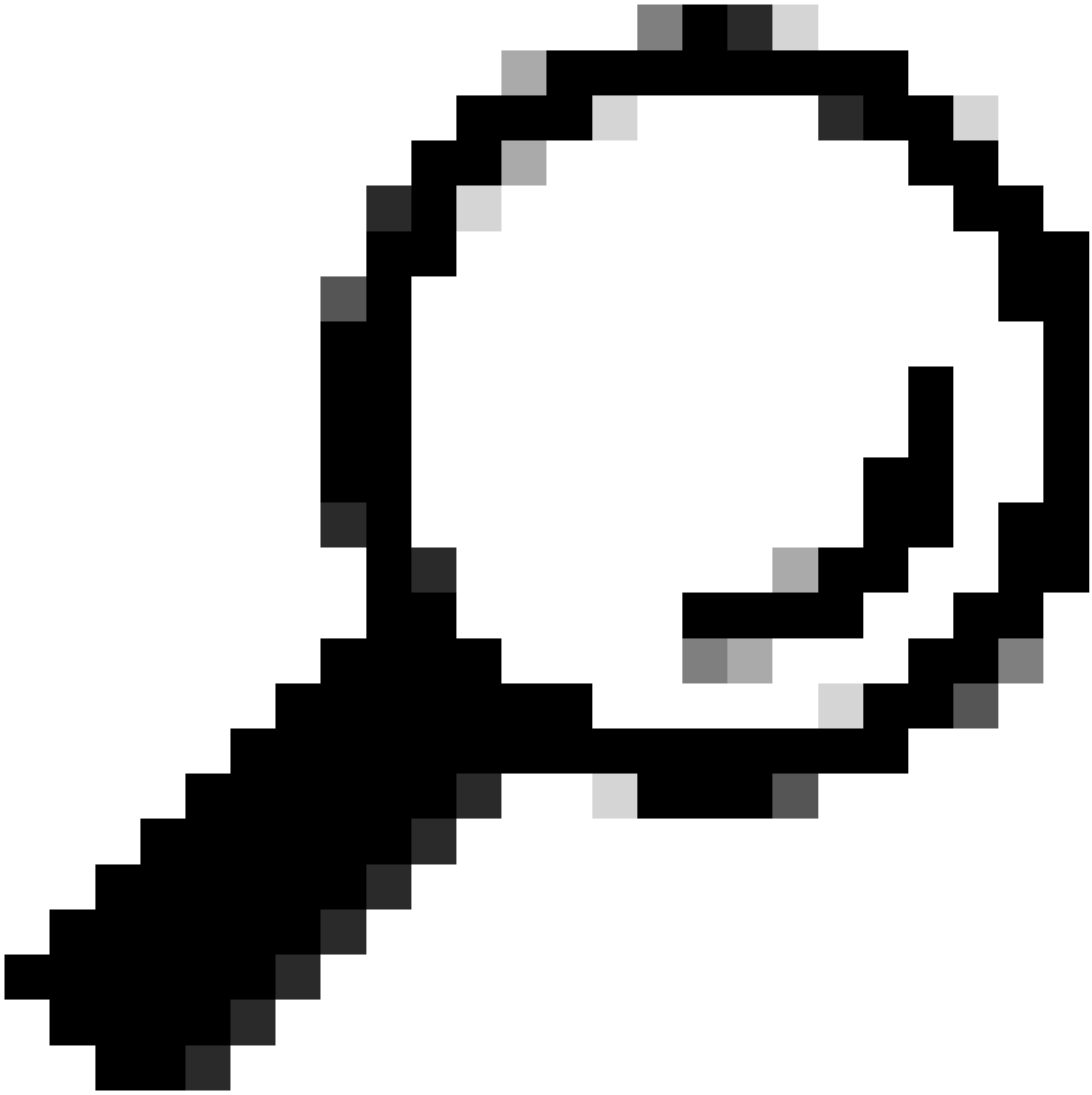
---

Paso 2. Ahora, agregue un dispositivo Cisco IOS XR como dispositivo de red. Vaya a Centros de trabajo > Administración de dispositivos > Recursos de red > Dispositivos de red. Haga clic en Agregar para agregar un nuevo dispositivo de red.



Paso 3.Introduzca la dirección IP del dispositivo y asegúrese de asignar la ubicación y el tipo de dispositivo (IOS XR) para el dispositivo. Finalmente, habilite los ajustes de autenticación de TACACS+ sobre TLS.



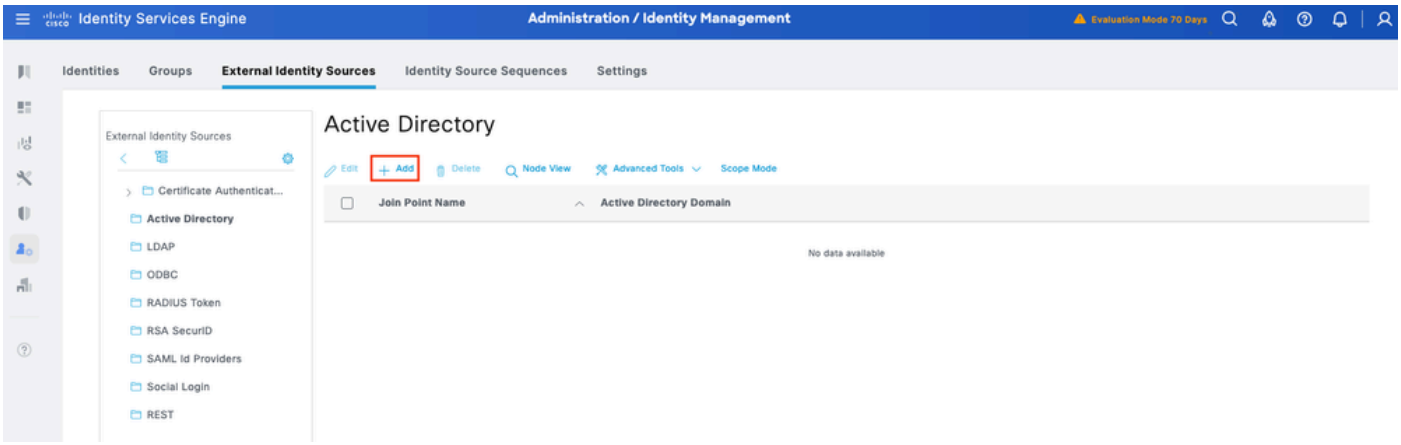


Consejo: Se recomienda habilitar el modo de conexión única para evitar reiniciar la sesión TCP cada vez que se envía un comando al dispositivo.

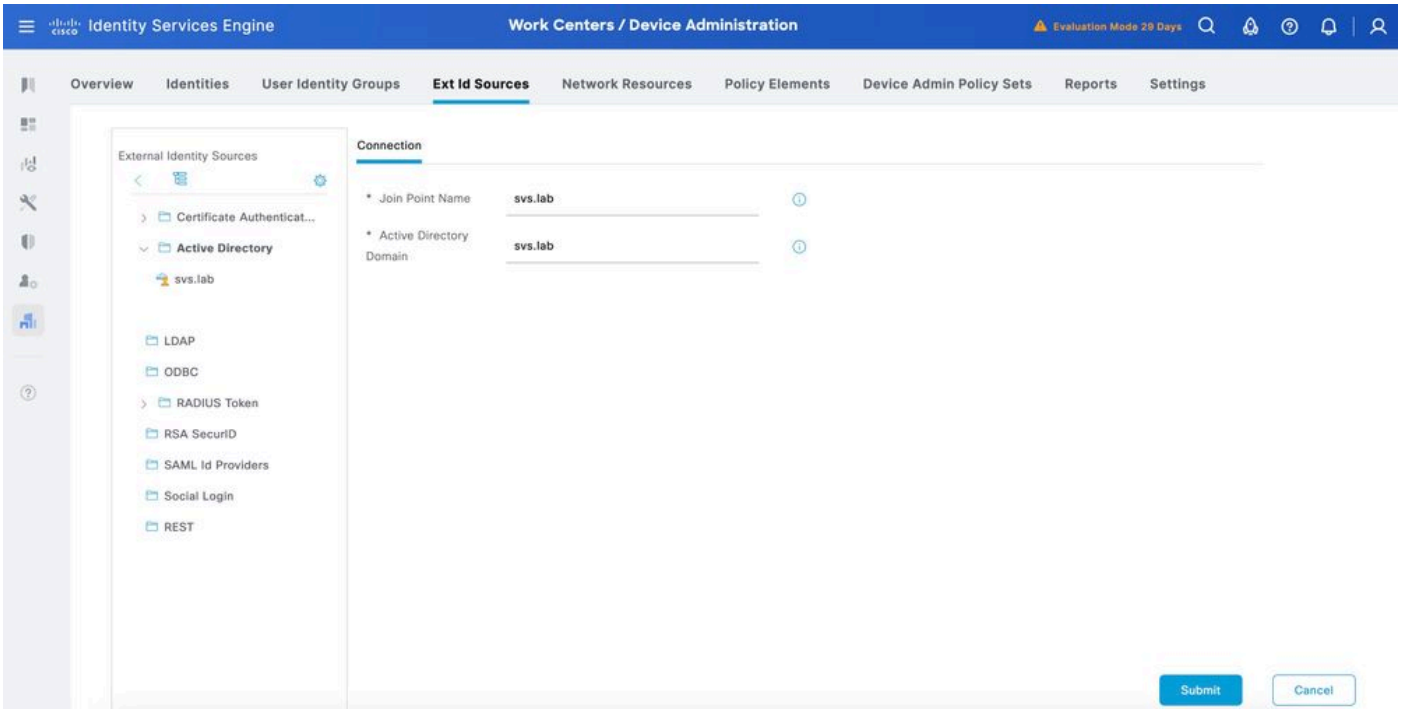
Configurar almacenes de identidad

En esta sección se define un almacén de identidades para los administradores de dispositivos, que pueden ser los usuarios internos de ISE y cualquier origen de identidad externo compatible. Aquí se utiliza Active Directory (AD), un origen de identidad externo.

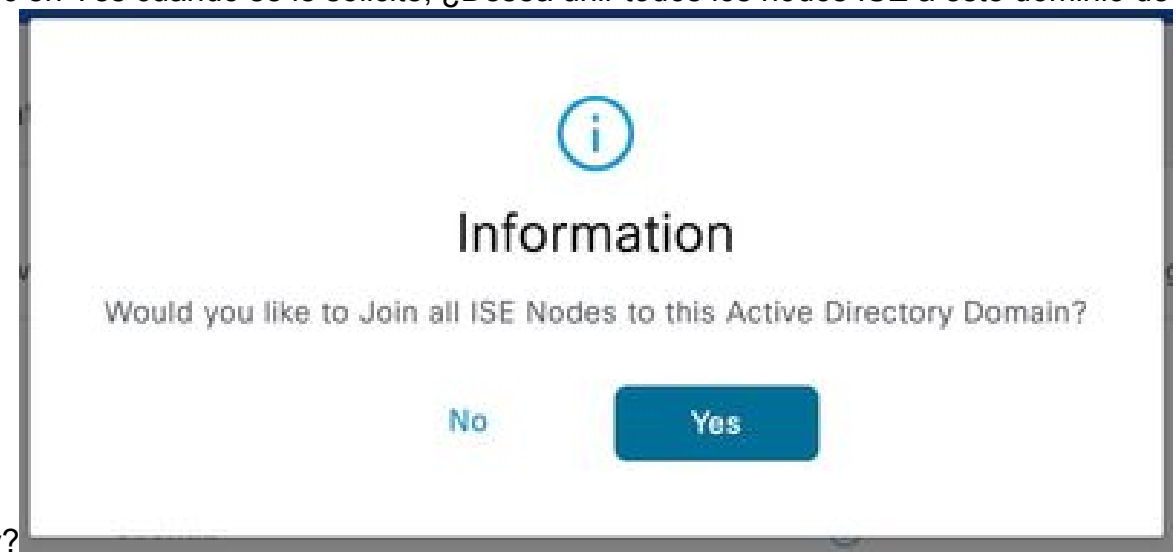
Paso 1. Vaya aAdministración > Gestión de identidad > Almacenes de identidad externos > Active Directory. Haga clic en Agregar para definir un nuevo punto de unión AD.



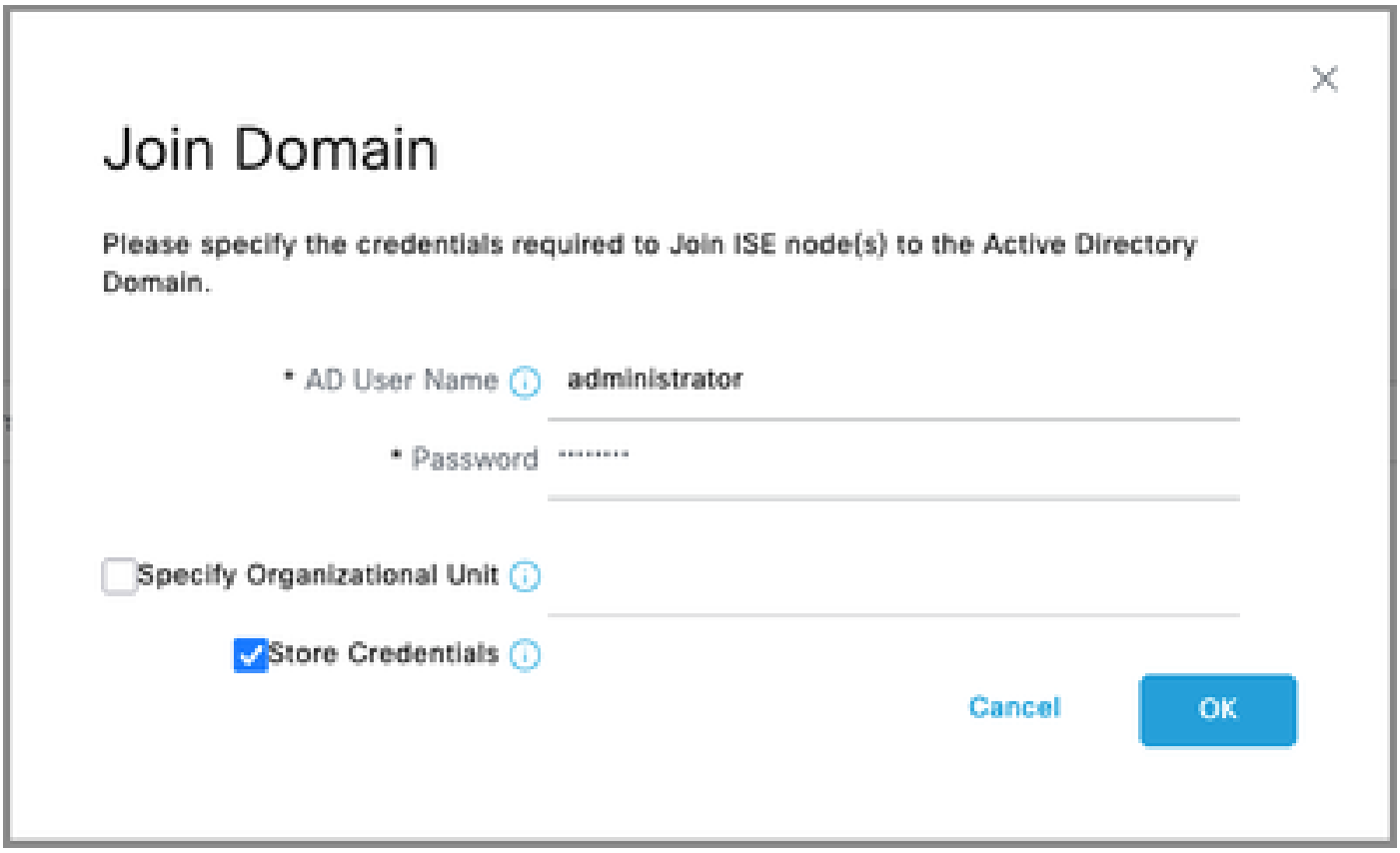
Paso 2. Especifique el nombre del punto de unión y el nombre de dominio AD y haga clic en Enviar.

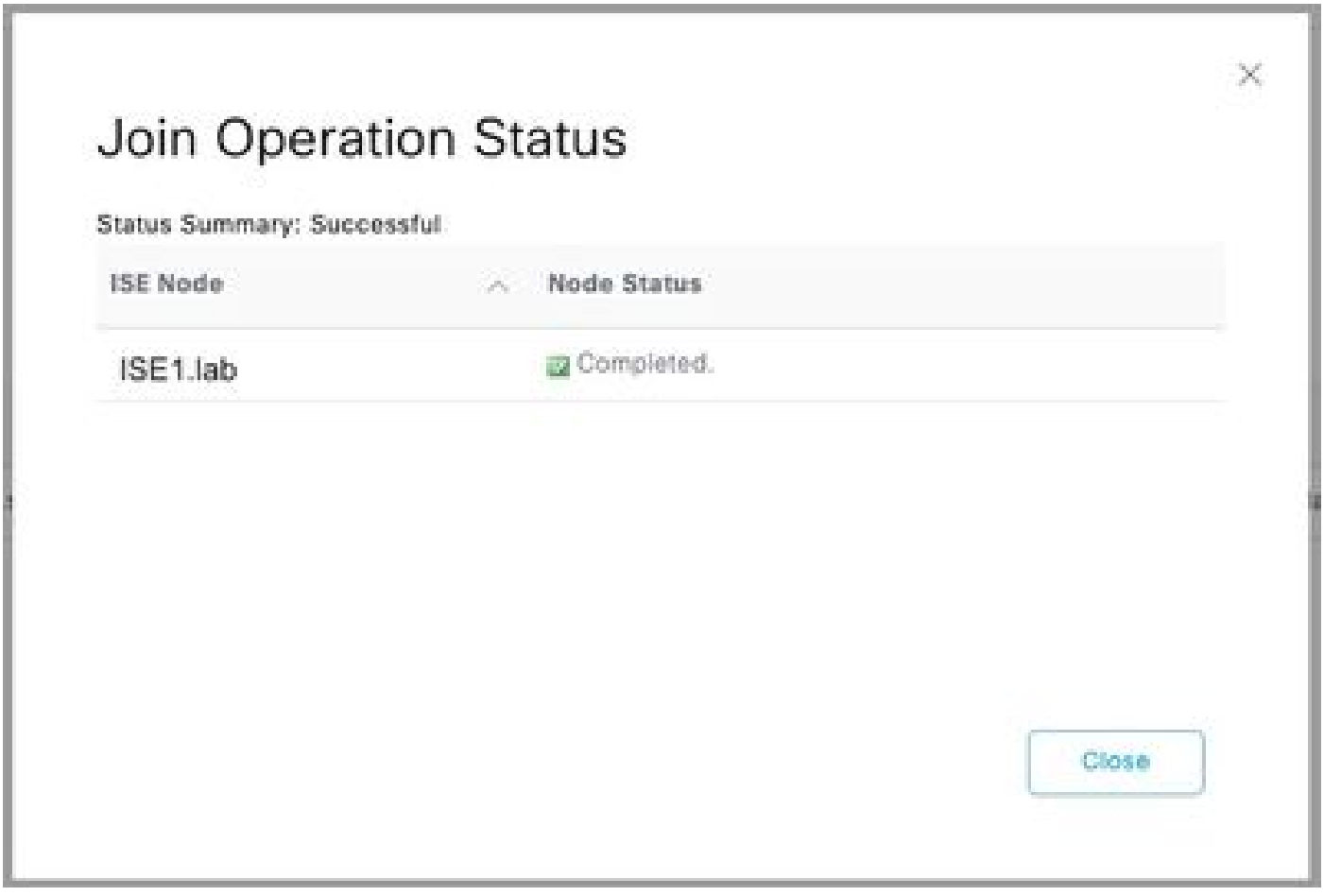


Paso 3.Haga clic en Yes cuando se le solicite, ¿Desea unir todos los nodos ISE a este dominio de Active Directory?

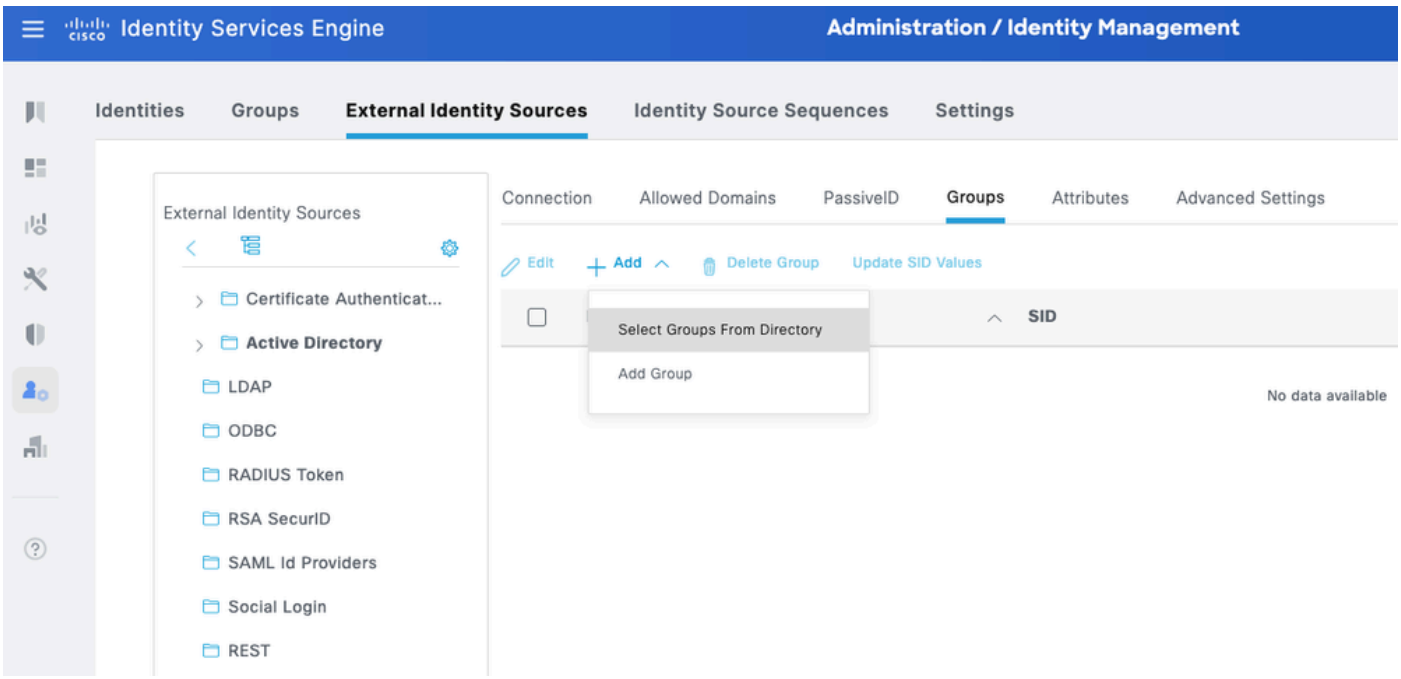


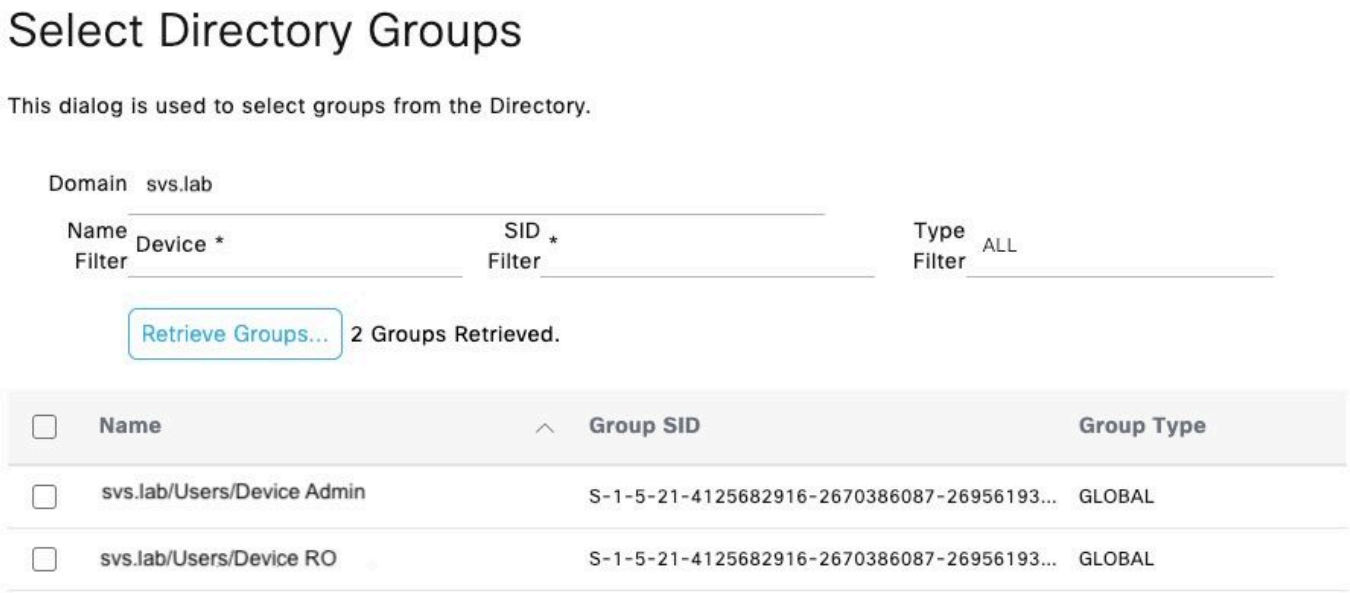
Paso 4.Introduzca las credenciales con privilegios de unión a AD y únase a ISE en AD. Compruebe el estado para verificar que funciona.

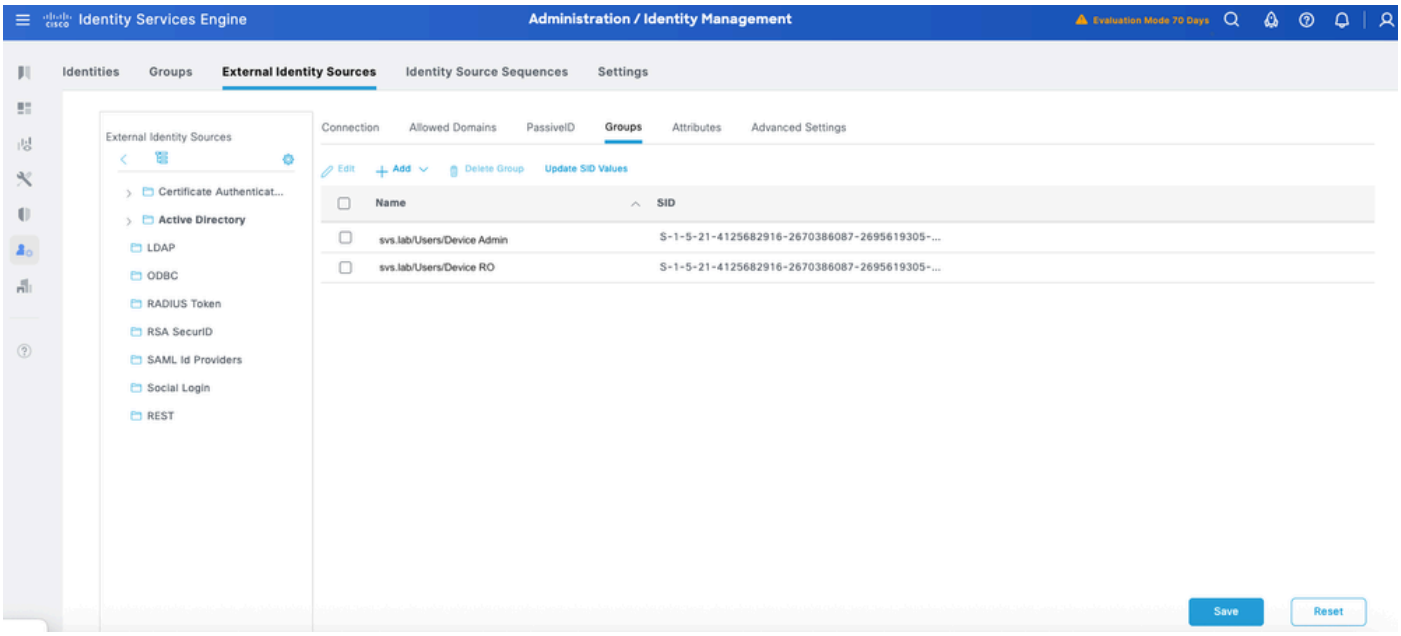




Paso 5.Navegue hasta la pestaña Groups y haga clic en Add para obtener todos los grupos necesarios según los cuales los usuarios están autorizados para el acceso del dispositivo. Este ejemplo muestra los grupos utilizados en la directiva de autorización.







Configurar perfiles TACACS+

Asigne los perfiles TACACS+ a las funciones de usuario en los dispositivos Cisco IOS XR. En este ejemplo, se definen los siguientes elementos:

- Root System Administrator (Administrador del sistema raíz): función con más privilegios en el dispositivo. El usuario con la función de administrador del sistema raíz tiene acceso administrativo total a todos los comandos del sistema y funciones de configuración.
- Operador: esta función está diseñada para usuarios que necesitan acceso de solo lectura al sistema con fines de supervisión y solución de problemas.

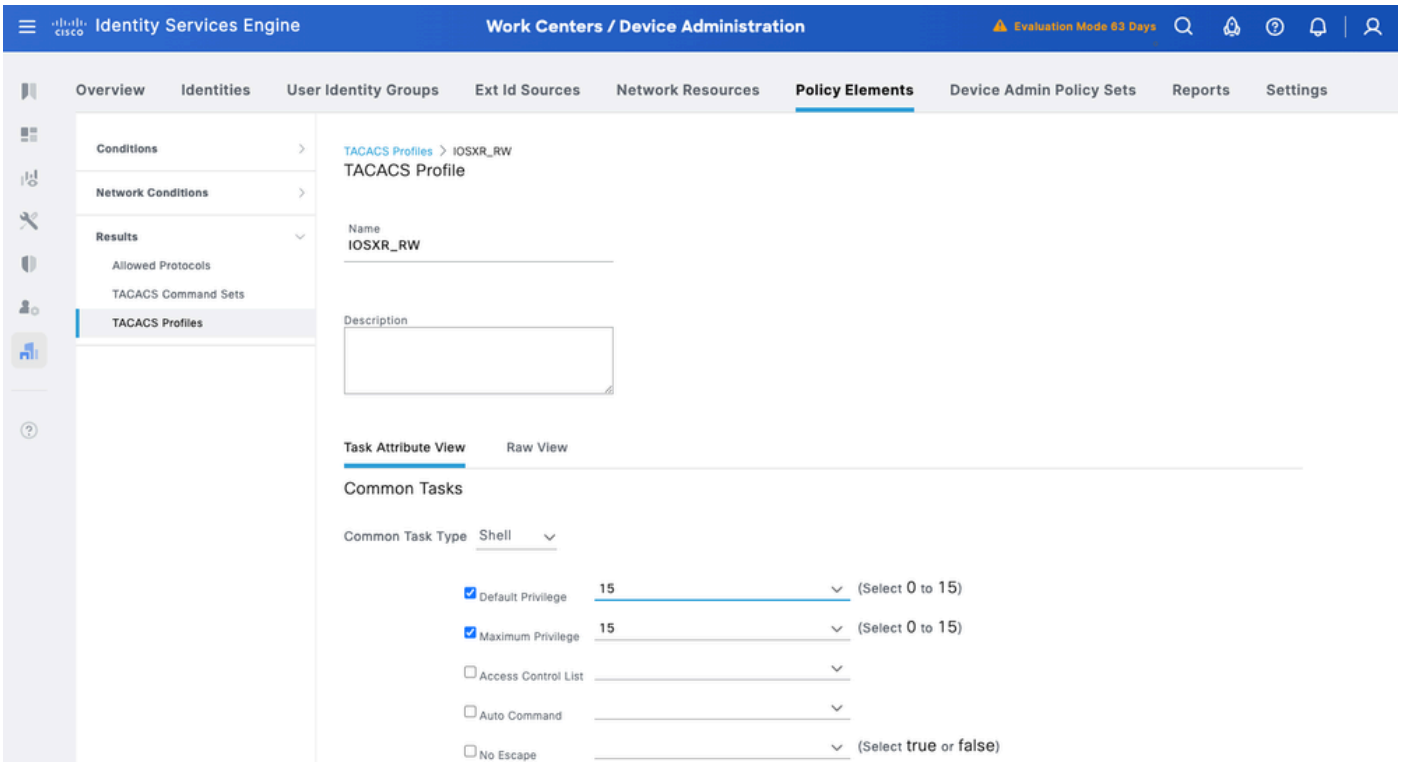
Defina dos perfiles TACACS+: IOSXR_RW e IOSXR_RO.

IOS XR_RW - Perfil del administrador

Paso 1. Navegue hasta Centros de Trabajo > Administración de Dispositivos > Elementos de Política > Resultados > Perfiles TACACS. Agregue un nuevo perfil TACACS y denomínelo IOSXR_RW.

Paso 2. Verifique y establezca el Privilegio por Defecto y el Privilegio Máximo como 15.

Paso 3. Confirme la configuración y guarde.

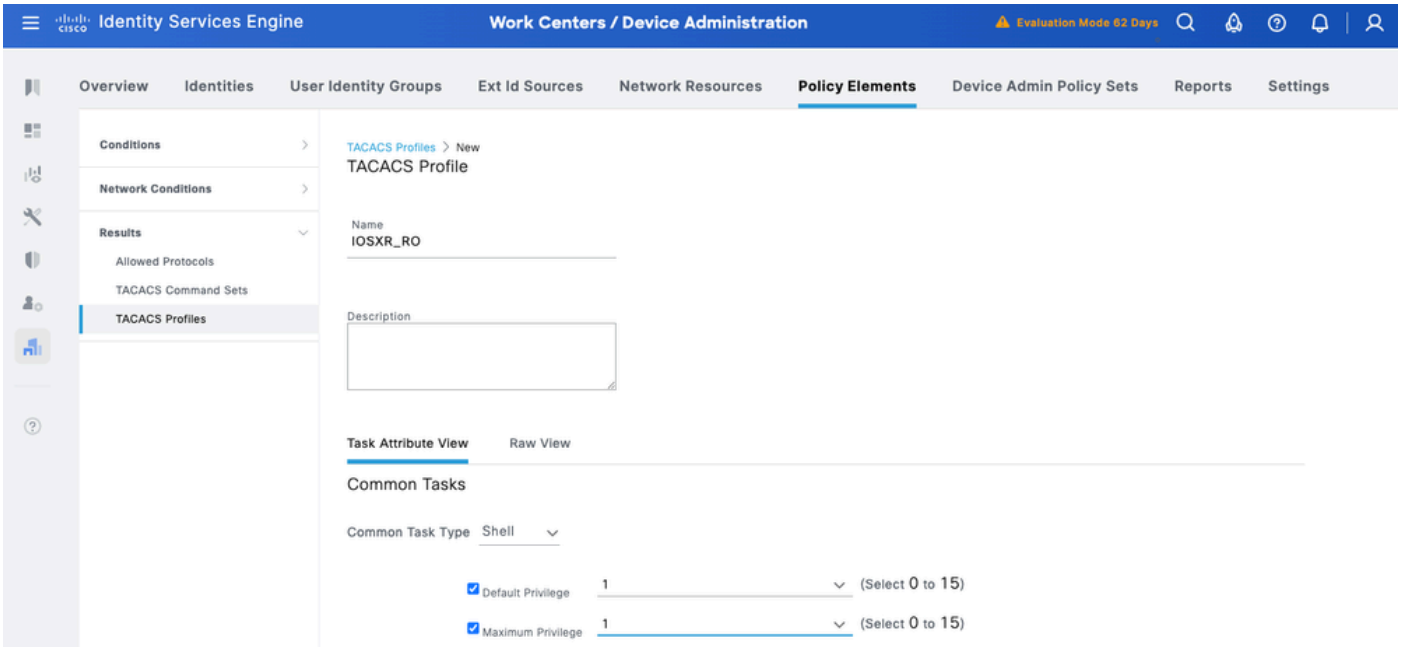


IOS XR_RO: perfil de operador

Paso 1. Navegue hasta Centros de Trabajo > Administración de Dispositivos > Elementos de Política > Resultados > Perfiles TACACS. Agregue un nuevo perfil TACACS y denomínelo IOSXR_RO.

Paso 2. Active y establezca el privilegio por defecto y el privilegio máximo como 1.

Paso 3.Confirme la configuración y guarde.



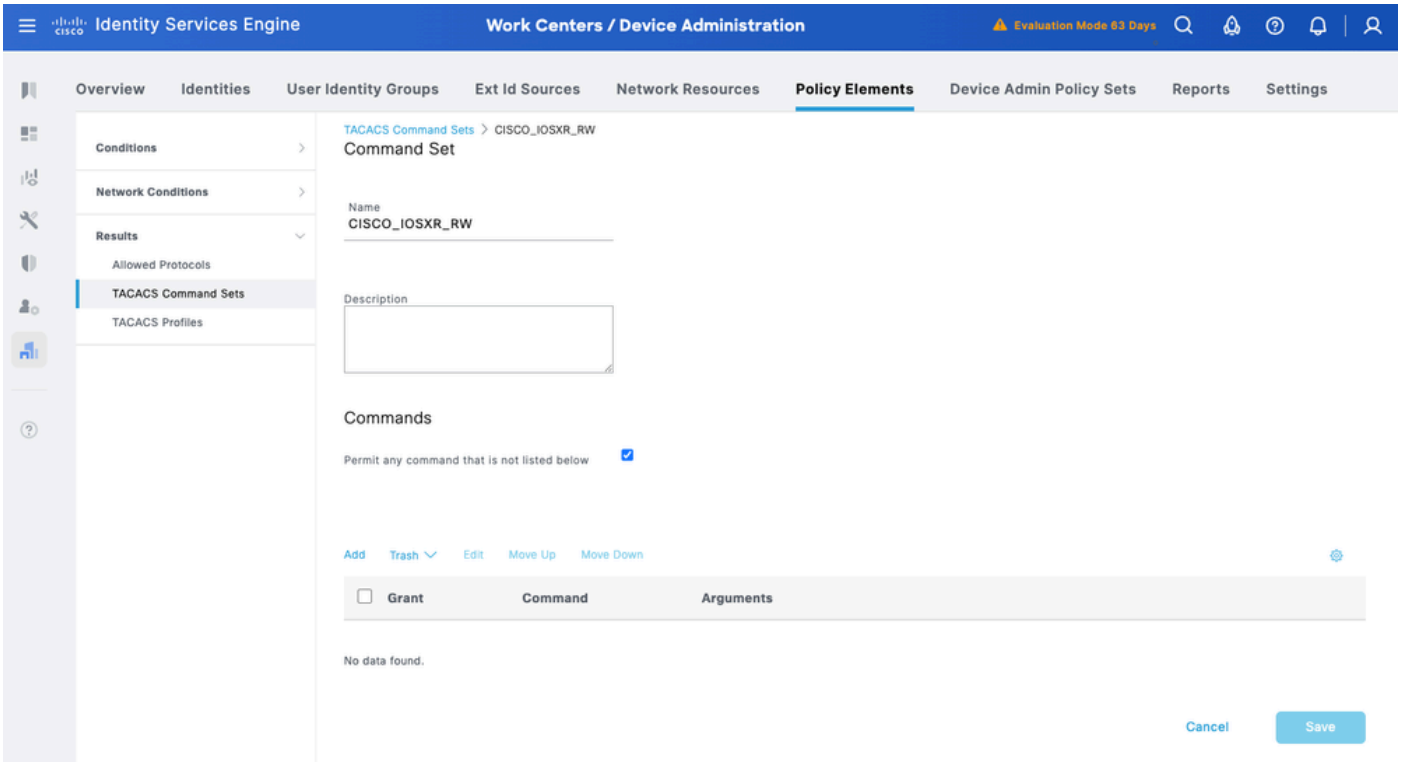
Conjuntos de comandos ConfigureTACACS+

Defina los conjuntos de comandos TACACS+: En este ejemplo, se definen CISCO_IOSXR_RW y CISCO_IOSXR_RO.

CISCO IOS XR RW - Conjunto de comandos del administrador

Paso 1. Navegue hasta Centros de Trabajo > Administración de Dispositivos > Elementos de Política > Resultados > Conjuntos de Comandos TACACS. Agregue un nuevo Juego de Comandos TACACS y denomínelo CISCO_IOSXR_RW.

Paso 2. Marque la casilla de verificación Permitir cualquier comando que no aparezca debajo (esto permite cualquier comando para el rol de administrador) y haga clic en Guardar.



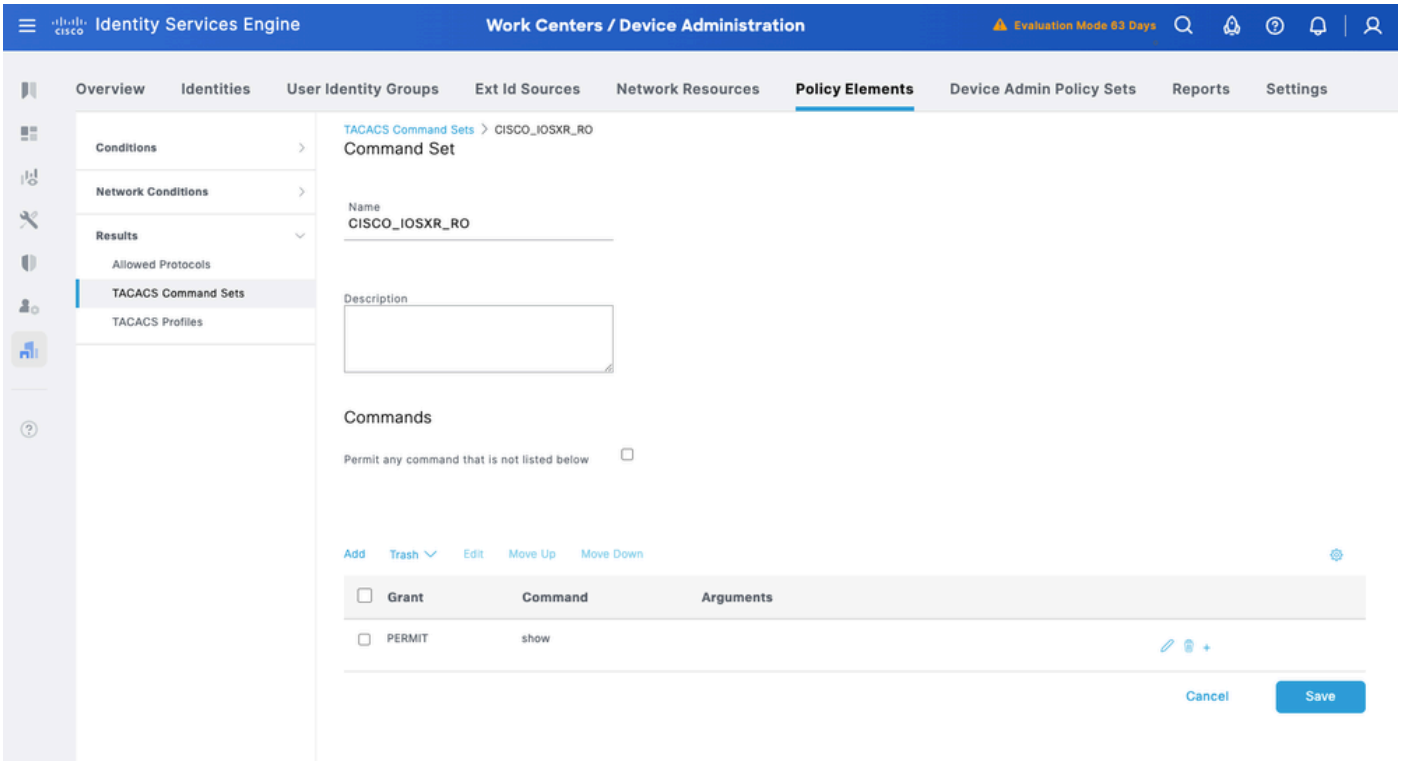
CISCO IOS XR RO - Conjunto de comandos del operador

Paso 1. Desde la interfaz de usuario de ISE, navegue hasta Centros de trabajo > Administración de dispositivos > Elementos de política > Resultados > Conjuntos de comandos TACACS. Agregue un nuevo conjunto de comandos TACACS y asígnele el nombre CISCO_IOSXR_RO.

Paso 2. En la sección Comandos, agregue un nuevo comando.

Paso 3. Seleccione Permiso de la lista desplegable para la columna Otorgar e ingrese show en la columna Comando; y haga clic en la flecha de verificación.

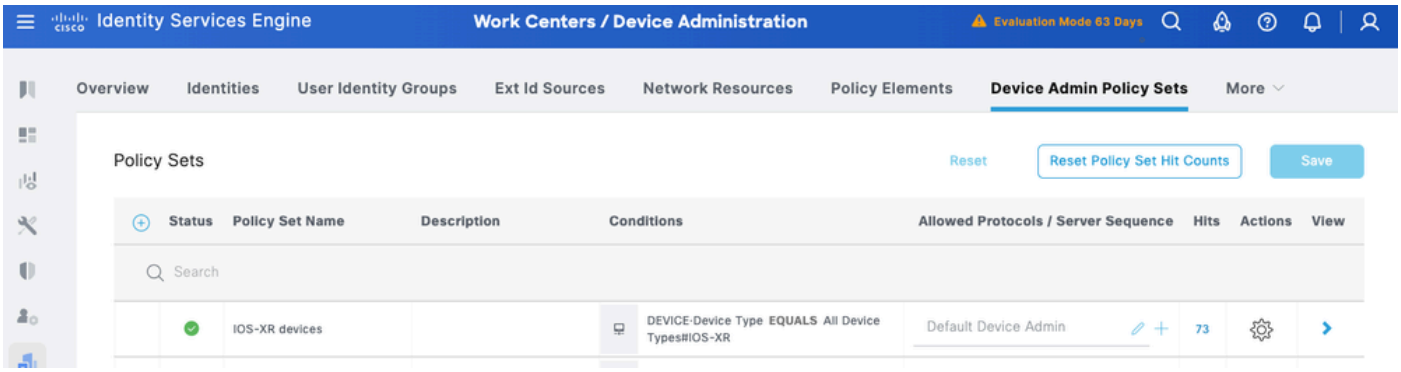
Paso 4. Confirme los datos y haga clic en Guardar.



Configurar conjuntos de políticas de administración de dispositivos

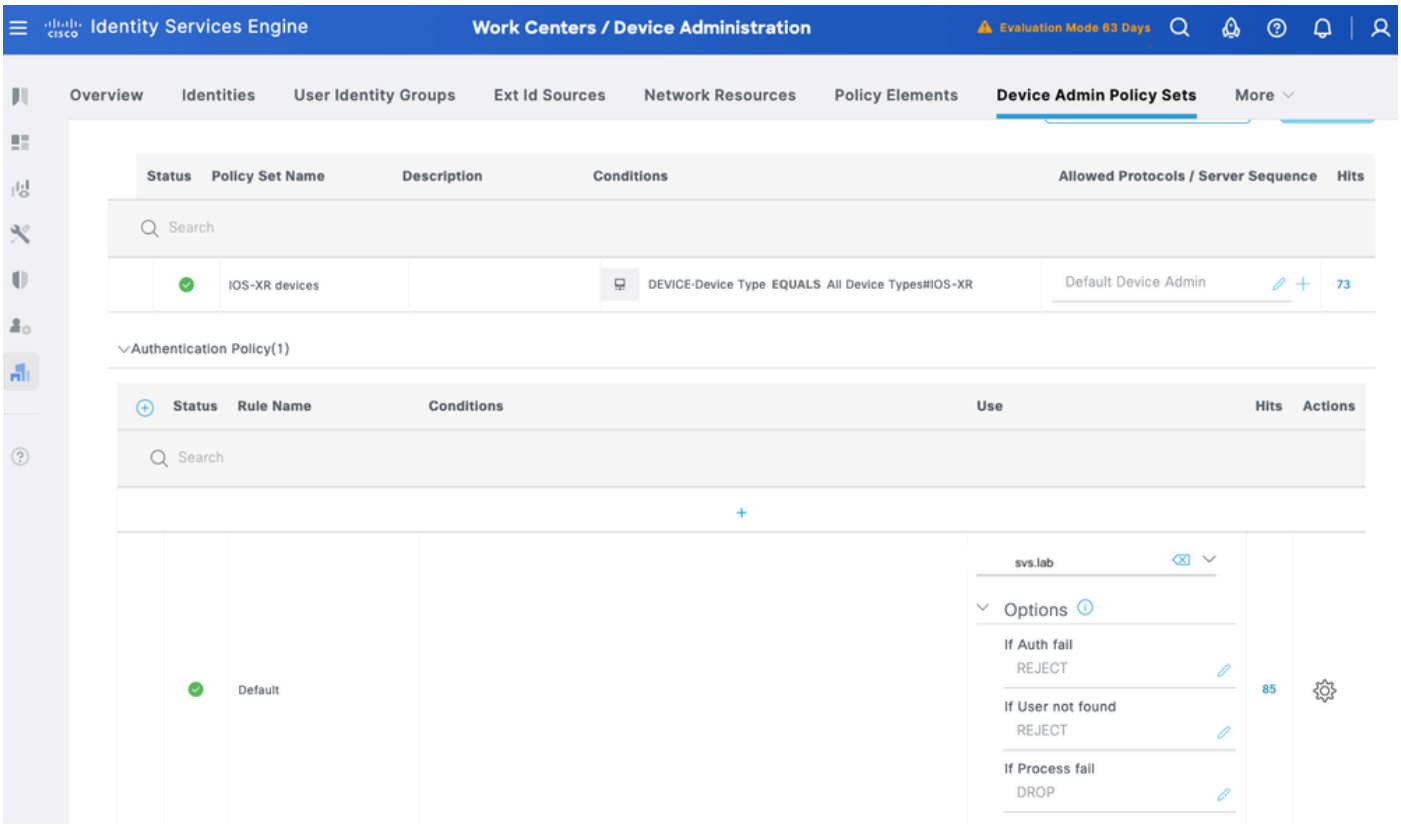
Los conjuntos de directivas están habilitados de forma predeterminada para la administración de dispositivos. Los conjuntos de políticas pueden dividir las políticas según los tipos de dispositivos para facilitar la aplicación de perfiles TACACS.

Paso 1.Vaya a Centros de trabajo > Administración de dispositivos > Conjuntos de políticas de administración de dispositivos. Agregue un nuevo conjunto de políticas para dispositivos IOS XR. En la condición especifique DEVICE:Device Type EQUALS All Device Types#IOS XR. En Allowed Protocols, seleccione Default Device Admin.



Paso 2. Haga clic en Guardar y haga clic en la flecha derecha para configurar este conjunto de políticas.

Paso 3. Cree la Política de Autenticación. Para la autenticación, se utiliza AD como almacén de ID. Deje las opciones predeterminadas bajo If Auth fail, If User not foundy If Process fail.

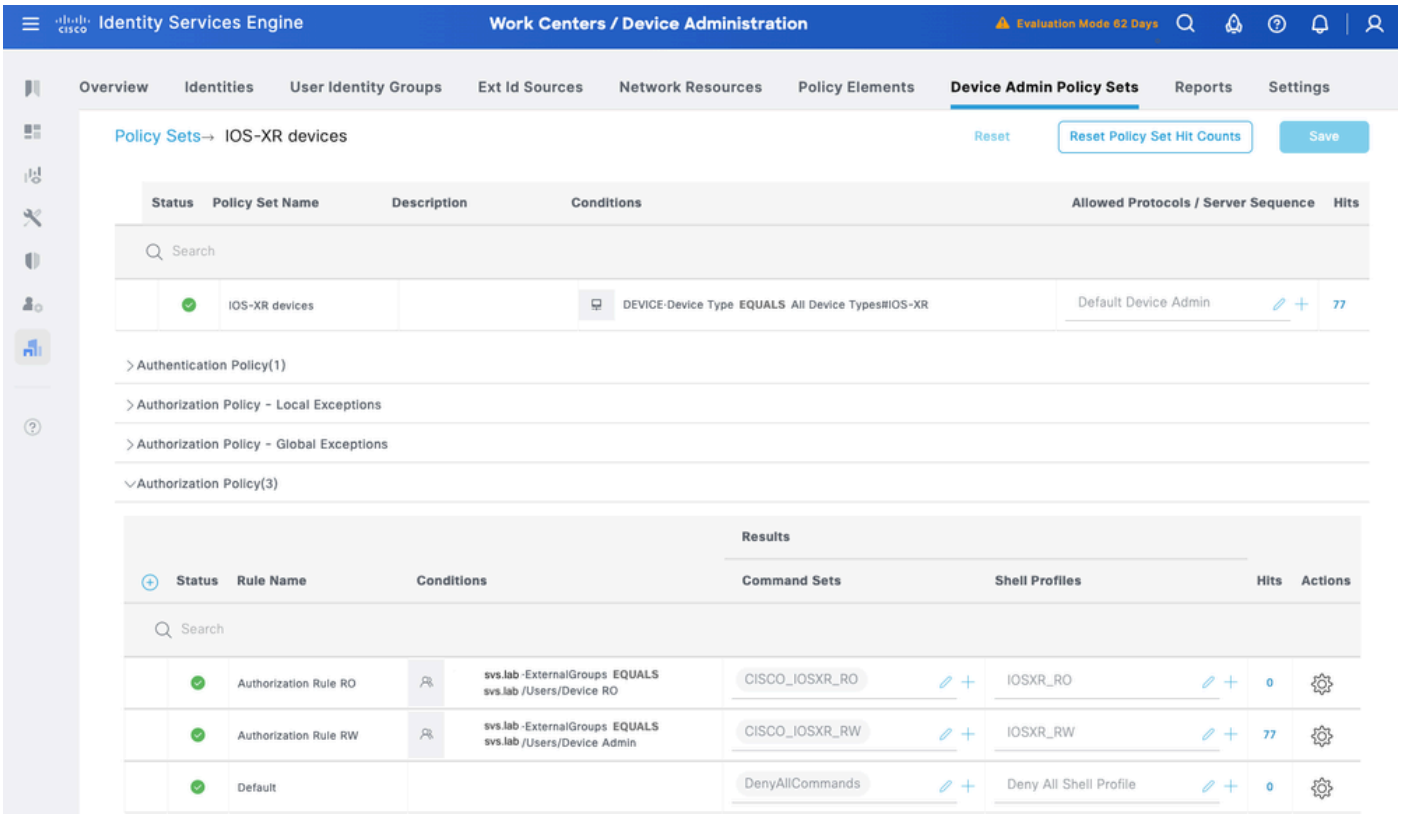


Paso 4. Defina la Política de Autorización.

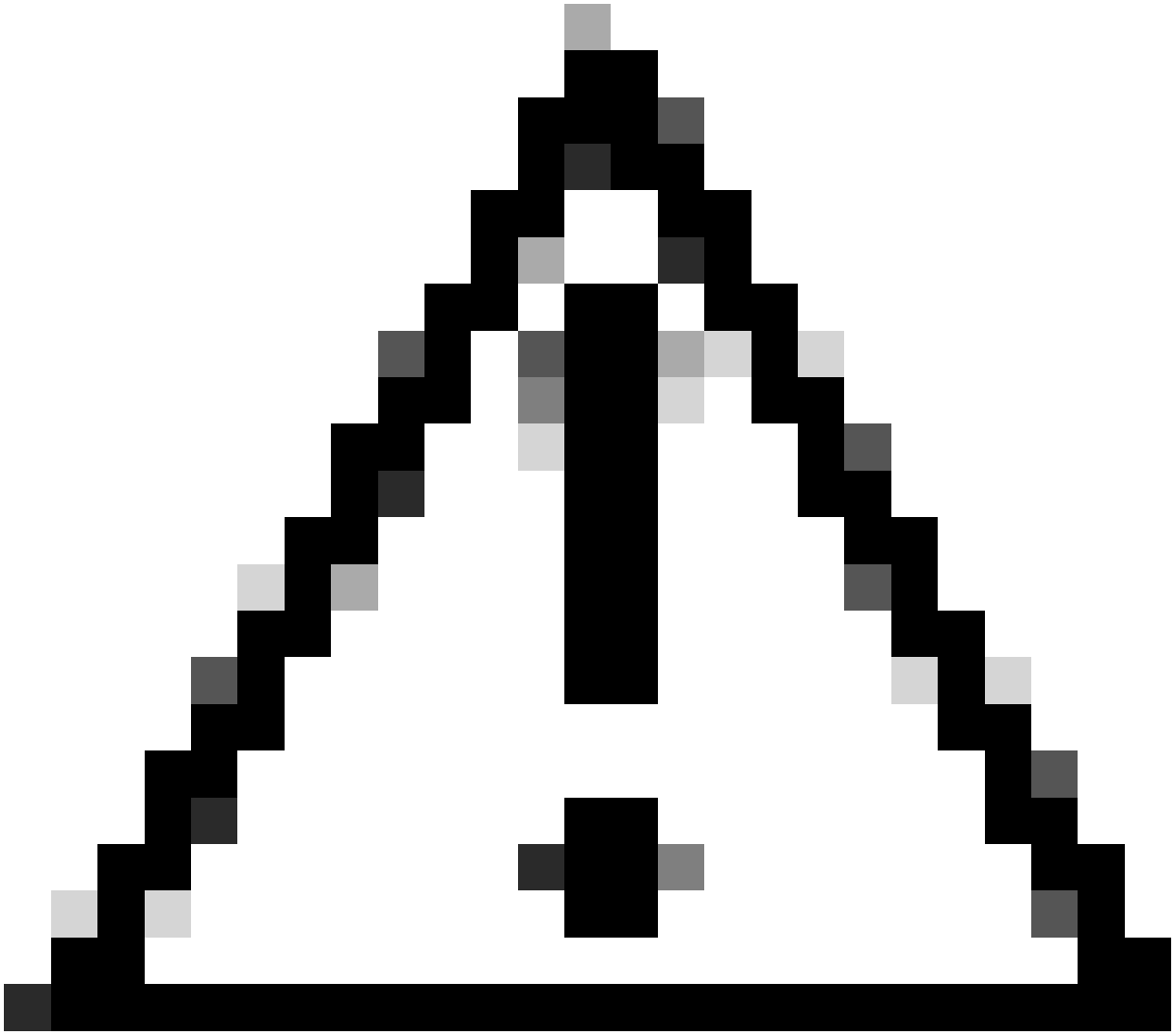
Cree la directiva de autorización basada en grupos de usuarios de Active Directory (AD).

Por ejemplo:

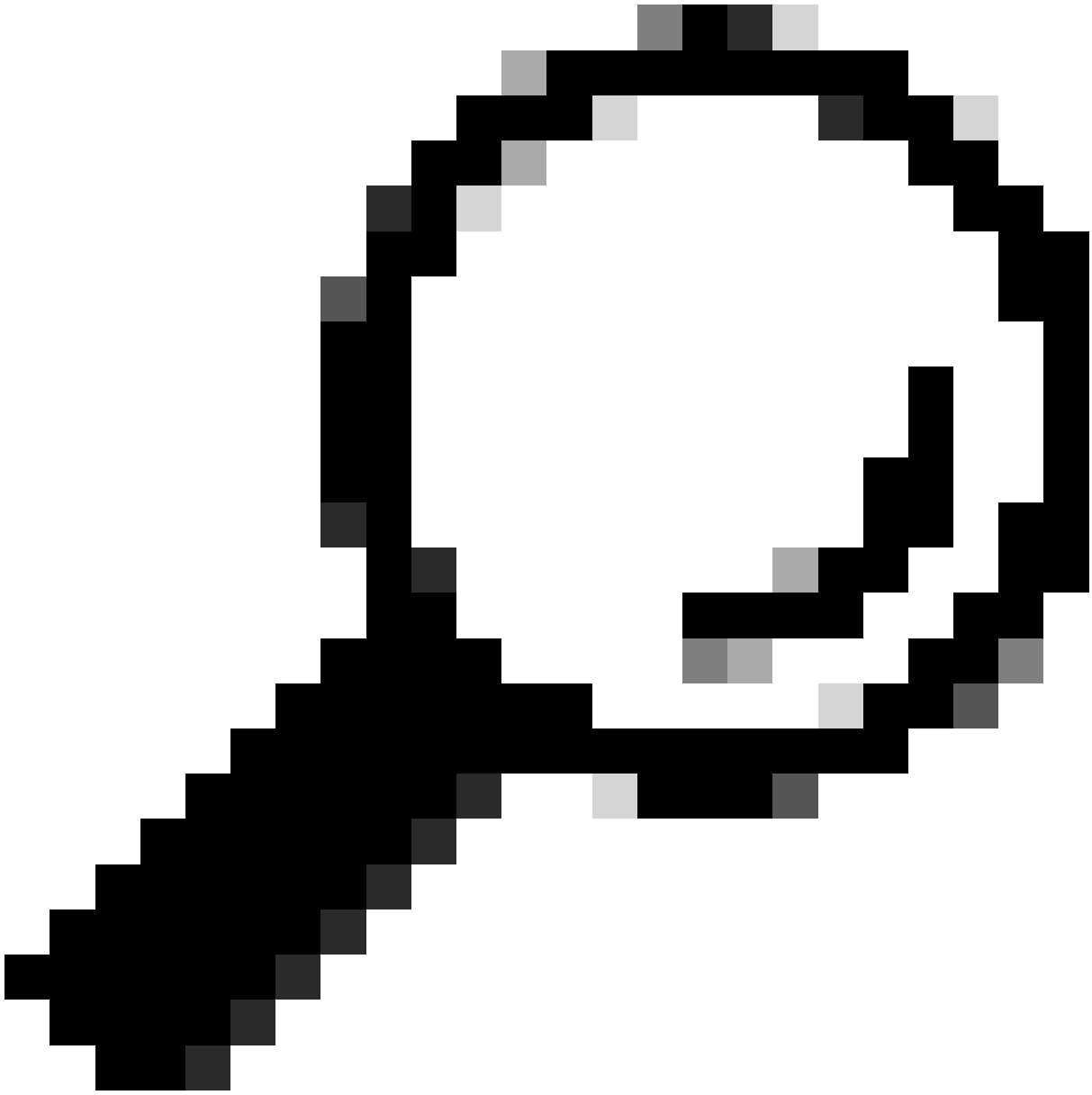
- A los usuarios del grupo AD Device RO se les asigna el conjunto de comandos CISCO_IOSXR_RO y el perfil de shell IOSXR_RO.
- A los usuarios del grupo AD Device Admin se les asigna el conjunto de comandos CISCO_IOSXR_RW y el perfil de shell de IOSXR_RW.



Parte 2 - Configuración de Cisco IOS XR para TACACS+ sobre TLS 1.3



Precaución: Asegúrese de que la conexión de la consola es accesible y funciona correctamente.



Consejo: Se recomienda configurar un usuario temporal y cambiar los métodos de autenticación y autorización AAA para utilizar las credenciales locales en lugar de TACACS mientras se realizan cambios de configuración, para evitar que se bloquee el dispositivo.

Configuraciones iniciales

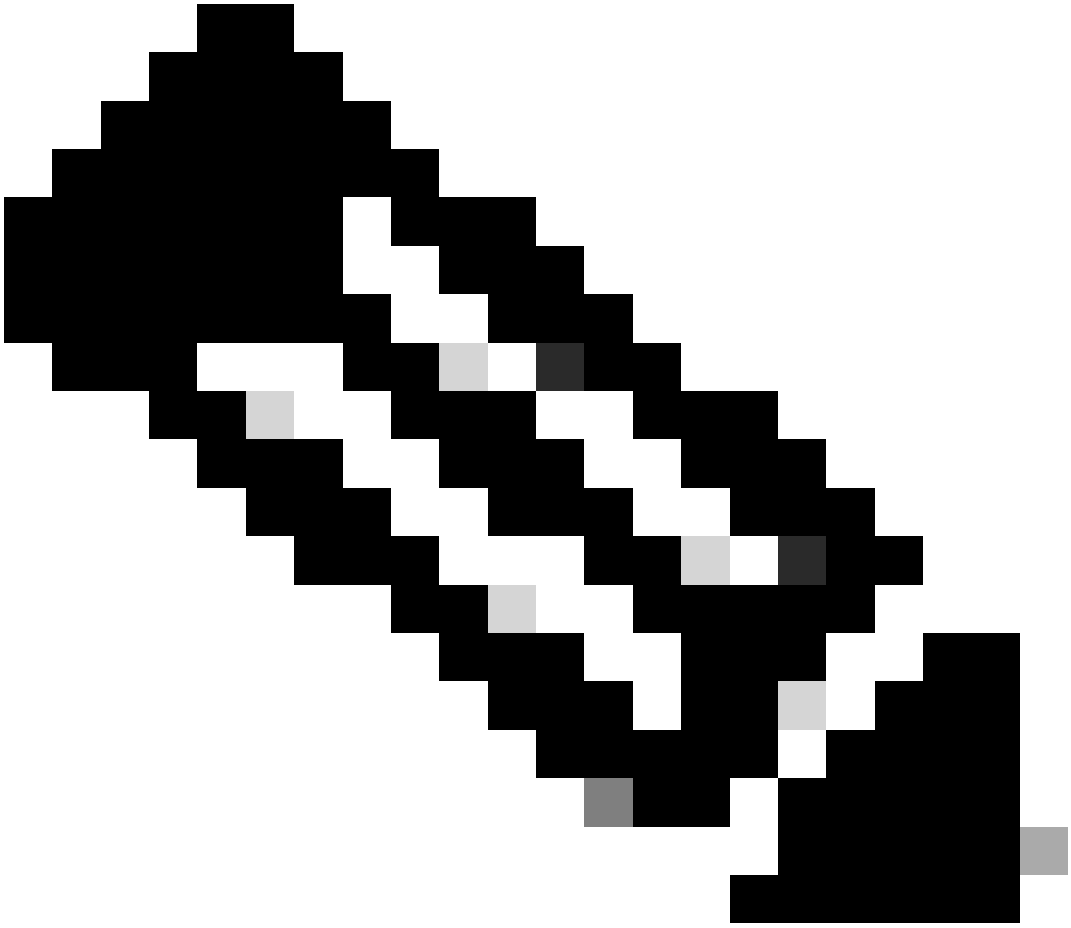
Paso 1. Asegúrese de que el servidor de nombres (DNS) está configurado y de que el router puede resolver correctamente los nombres de dominio frecuentemente cualificados (FQDN), especialmente el FQDN del servidor ISE.

```
domain vrf mgmt name svs.lab
domain vrf mgmt name-server 10.225.253.247
```

```
no domain vrf mgmt lookup disable

RP/0/RP0/CPU0:BRC-8201-1#ping vrf mgmt ise1.svs.lab
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.225.253.209 timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Paso 2. Borre los certificados y los puntos de confianza antiguos o no utilizados. Asegúrese de que no haya certificados y puntos de confianza antiguos. Si ve alguna entrada antigua, elimínela o elimínela.

```
show crypto ca trustpoint
show crypto ca certificates

(config)# no crypto ca trustpoint <tp-name>
# clear crypto ca certificates <tp-name>
```



Nota: Puede crear manualmente un nuevo par de claves RSA y adjuntarlo en trustpoint. Si no crea uno, se utiliza el par de claves predeterminado. Actualmente no se admite la definición de pares de claves ECC en trustpoint.

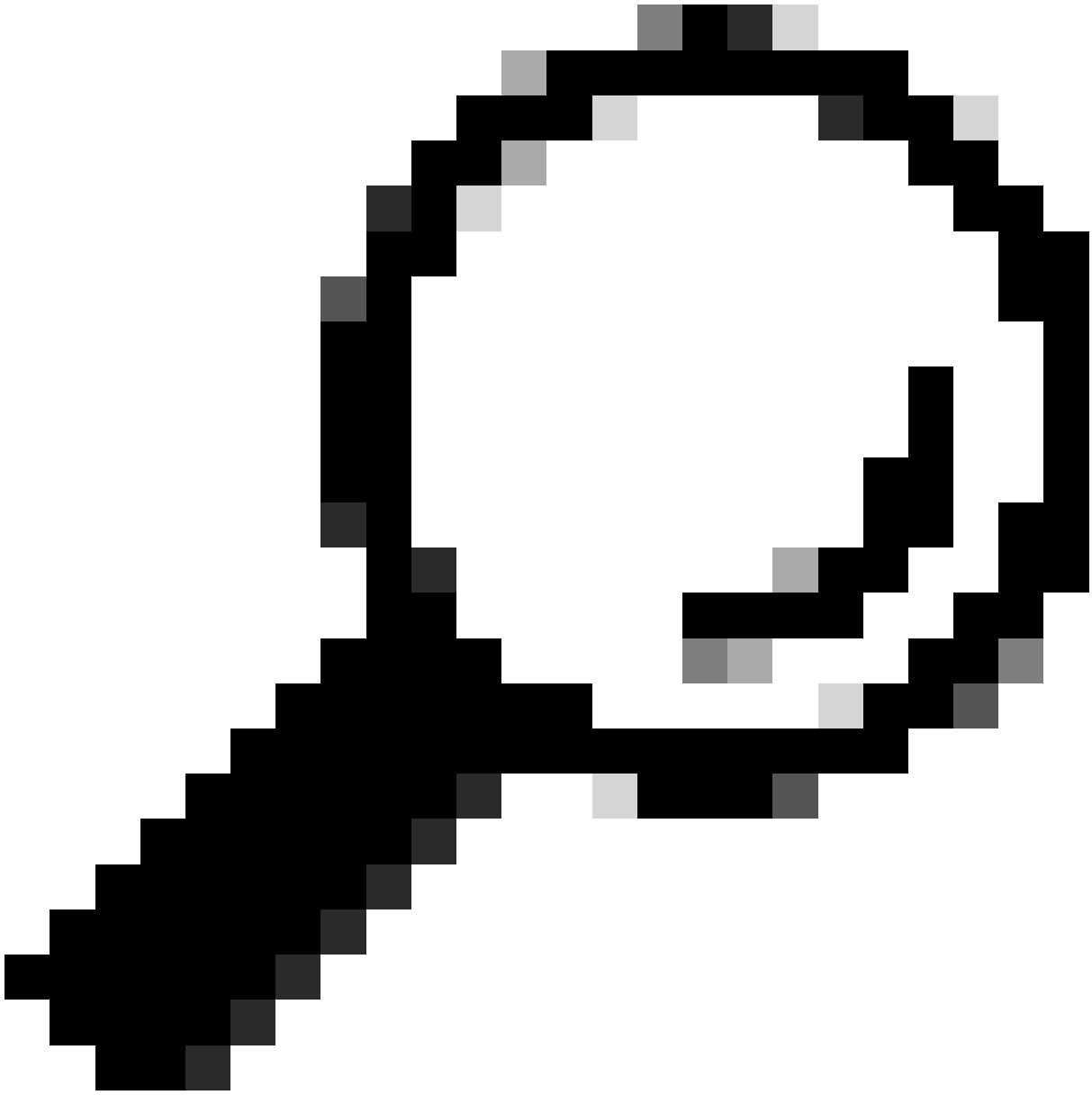
Configurar Trustpoint

Paso 1. Configuración de par de claves (opcional).

```
<#root>

RP/0/RP0/CPU0:BRC-8201-1(config)#

crypto key generate rsa

          4096
```

```
RP/0/RP0/CPU0:BRC-8201-1(config)#
crypto ca trustpoint


RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
rsakeypair
```

Paso 2. Crear punto de confianza.

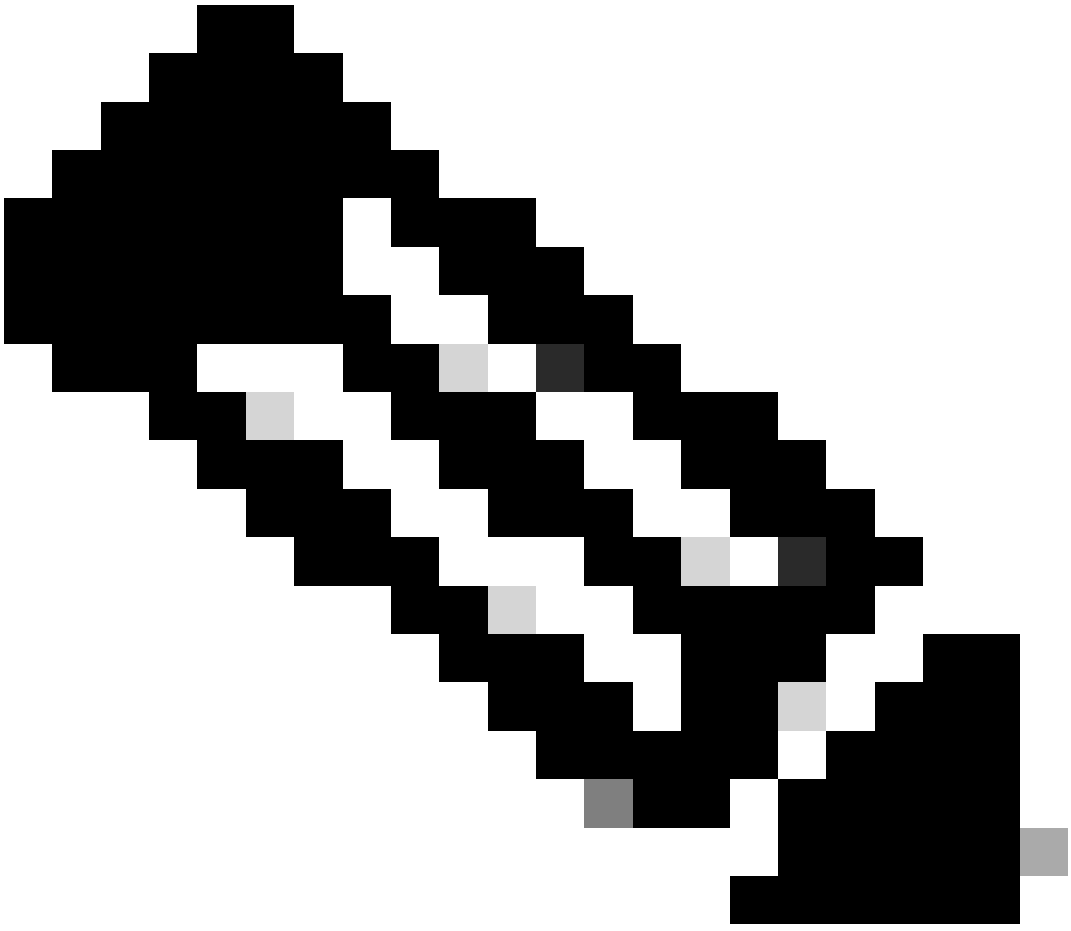


Consejo: La configuración de DNS para el nombre alternativo del sujeto es opcional (si se habilita en ISE), pero se recomienda.

<#root>

```
RP/0/RP0/CPU0:BRC-8201-1(config)#
crypto ca trustpoint svs

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
vrf mgmt

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
crl optional
```

```
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
subject-name C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=brc-8201-1.svs.lab

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
subject-alternative-name IP:10.225.253.167,DNS:brc-8201-1.svs.lab

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
enrollment url terminal
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
rsakeypair svs-4096

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
commit
```



Nota: Si necesita utilizar una coma en O u OU, puede utilizar una barra diagonal inversa (\) antes de la coma. Por ejemplo: O=Cisco Systems\, Inc.

Paso 3. Autentique Trustpoint instalando el certificado de CA.

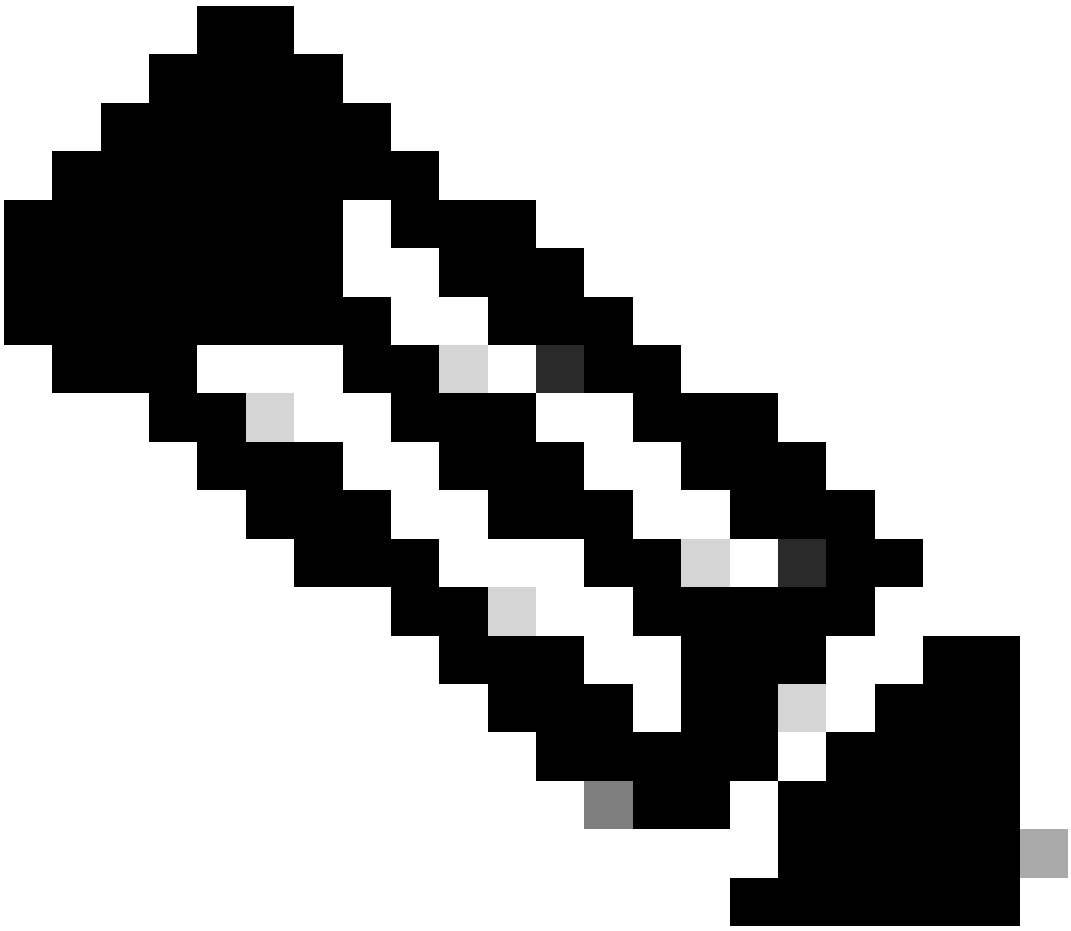
<#root>

```
RP/0/RP0/CPU0:BRC-8201-1#

crypto ca authenticate svs



Enter the base64/PEM encoded certificate/certificates.
Please note: for multiple certificates use only PEM.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIFlDCCA3ygAwIBAgIIIM1OAsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
QOEwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUGA1UECBMOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBAcTB1JhbGVpZ2gxDjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTVlMxEjAQBgNVBAMTCVNWUyBMYWJDQTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZUOyn2vIn6gKbx3M7vaRq
2YjwZlzSH6EkEvxnJTy+kksiFD33GyHQepk7vfp4NFU5OtQ4HC7t/AOv9grDa3QW
VwvV4MBbJhFM3s0J/ejgDYcMZhIAaPyOZo5WLboOkXEiKjPLatkXojB8FVrhLF3O
jMBSqwa4/Wlniy5S+7s4FFxsCf2OCOWfBAsnrs0tatIIhmcnx+VLJP7MRm8fOw4m
mutNo7IhbJSrgAFXmjlbBjMmgspObULo/wxMHdTbtPBf11HRHTkNIo3qyO4UADL2
WpoGhgT/FaxxBo2UBcnYVaP+jjRE0NYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7BOe8oDNKU6gXlojKyLP/gC7j8AePO3ir+KZui8
b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
gJ+kQXe7QtT/u6m1MrtjE3gAEVpL334rTIxy9hpKZIkB86t2ZA3JX8CLsbCa13sA
z1XCoONX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTAO1xh6OI4QnK+MNQKpTjt/E4
ydHlOrrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVLl783nTc9wYptQEPi5sw
83g9EMgKV0ARIiVUa/qlAgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAYb4
QgEBBAQDAgAHMBkGCWCGSAGG+EIBDQQMFgpTVlMgTGFiIENBMA0GCSqGSIb3DQEB
CwUAA4ICAQAIT3O8oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oKOdGayi
iSEkSSX9qyfLfINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXRX67X+v
O+ja6zTQqjO6lqJhmrSkyFbYf/ZTpe4d1OzJsZjNsNOr8bF9nOA/7qNZLp3Z3cpU
PUOKdbiSvRqnPw3e8TfITVmAzcx8COI2SrYFMSUazolVBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIEOf5ay1PKURO/8aj/B7aluJapXkmnj5qPeGhNOpB
Q9r14reov4so2EspkXS7CrH9yGfpIyTprokz1UvZBZ8vloI7YZmjFmem+5rT6Gnk
eU/lX7nV61SYG5W5K+I8uaKuyBHOMn7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggzlPOdsS/i6Lo7ypYXOeB9HgVDCkzQsLXQuHGj/2WsgPgdRcjkvnyURk4Jx+Ib
xDrmo7e0XPpSW4l72a6Kl8CR3U2Cr4wsuvndPEq/qd2NRSBWffF0XE/AJHQG7STT
HaXLU9r2Ko6O3oecu8ysGTwLlIt/9T1/FOb0xZRugWcpJrVoTgDGuA==
-----END CERTIFICATE-----


quit


   Serial Number : AB:CD:87:FD:41:12:C3:FE:FD:87:D5
   Subject:
      CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
   Issued By :
      CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
```

```
   Validity Start : 17:05:00 UTC Mon Apr 28 2025
   Validity End : 17:05:00 UTC Sat Apr 28 2035
RP/0/RP0/CPU0:May 9 14:52:20.961 UTC: pki_cmd[66362]: %SECURITY-PKI-6-LOG_INFO_DETAIL : Fingerprint: 2A
   SHA1 Fingerprint:
      0EB181E95A3ED7803BC5A8059A854A95C83AC737
Do you accept this certificate? [yes/no]:
```

yes

```
RP/0/RP0/CPU0:May 9 14:52:23.437 UTC: cepki[153]: %SECURITY-CEPKI-6-INFO : certificate database updated
```



Nota: Si tiene un sistema de CA subordinada, debe importar los certificados de CA raíz y CA secundaria. Utilice el mismo comando con Sub CA en la parte superior y Root CA en la inferior.

Paso 4. Generar solicitud de firma de certificado (CSR).

<#root>

```
RP/0/RP0/CPU0:BRC-8201-1#
```

crypto ca enroll svs

```
Fri May 9 14:52:44.030 UTC
% Start certificate enrollment ...
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
% For security reasons your password will not be saved in the configuration.
% Please make a note of it.
```

Password:

Re-enter Password:

```
% The subject name in the certificate will include: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=10.225.253.167
% The subject name in the certificate will include: BRC-8201-1.svs.lab
% Include the router serial number in the subject name? [yes/no]:
```

yes

```
% The serial number in the certificate will be: 4090843b
% Include an IP address in the subject name? [yes/no]:
```

yes

```
Enter IP Address[]
```

10.225.253.167

```
Fingerprint: 36354532 38324335 43434136 42333545
Display Certificate Request to terminal? [yes/no]:
```

yes

```
Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
MIIDQTCCAikCAQAwcjELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAk5DMQwwCgYDVQQH
DANSVFAxDjAMBgNVBAoMBUNpc2NvMQwwCgYDVQQLDANTVlMxFzAVBgNVBAMMDjEw
LjIyNS4yNTMuMTY3MREwDwYDVQQFEwg0MDkwODQzYjCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBALwx9w4DnTtrloDH9iOZxPvEDARwN0t4WrPEjaQclZUA
6ax6Cxq/0JlQiUf2+eQv+4rKZqAZ1xDhiaiMGqETnO0LKpwmtx10IqXL7UYMHHwF
9vRII52zomkWA8a63Wx66UkExaXoeXaf5HkLoqDu68X83U7LPvMe1sMwvmq7Rmy2
DAu30HB/JfYlQCHmTVFz3M5fBt86xx4t1nxTFU/4lRWMC73UdL5YdKJLjMpBT2tN
E3piZ+kL4p1c9U4RIBkU8/G4drzFbGvHCIkWkwI0cb1X2HgtbVQdCXTAwJDmr2O9
zd2ZCa5enTbOKHbNXuHjpy0k8MewKOV2muwxVcQbej8CAwEAAaCBiTAYBgkqhkiG
9w0BCQcxCxMJQzFzY28uMTIzMG0GCSqGSIb3DQEJDjFgMF4wDgYDVR0PAQH/BAQD
AgWgMCAGA1UdJQEB/wQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAJBgNVHRMEAjAA
MB8GA1UdEQQYMBaCDjEwLjIyNS4yNTMuMTY3hwQK4f2nMA0GCSqGSIb3DQEBBQUA
A4IBAQBBXOeWF5ZUz7O1GFjuQHBBDgYb+3lhFOxbYm9psIWfv1uwjkKoL297tGHv
Iux7nMyrDVkSJ81i5BSTdd9FE6AbSFswjlYpO+IxkUM971Ejwg2rj+jABDR7I8SU
O6YO6mS9x2ZJYqImeq8xwIr19Hi+7tyaLe6apfTIljdgVxB+XyzOFJMckIO5US3j
T/3aw/115RcXerdrh36oMUHEepUjIx/15u9s1c7e1mxACoQE6f9OA+fdg2zYtOME
Z6VAw64cY+YF6iLbYv7c4lizO5Zj2NJbUKpeqijkFAkY/1rIxTHypzH/p2ma4zuS
46a+kLXsVHZ716ZMB3WrUzB2ZNOO
```

```
-----END CERTIFICATE REQUEST-----
---End - This line not part of the certificate request---
Redisplay enrollment request? [yes/no]:
```

no

Paso 5. Importe el certificado firmado por la CA.

<#root>

```
RP/0/RP0/CPU0:BRC-8201-1#
```

crypto ca import svs certificate

```
Fri May 9 15:00:35.426 UTC


Enter the base64/PEM encoded certificate/certificates.
Please note: for multiple certificates use only PEM.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIE3zCCAsegAwIBAgIINL1NAUzx14UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
QOEwHhcNMjUwNTA5MTQ1NzAwWhcNMjYwNTA5MTQ1NzAwWjByMQswCQYDVQQGEwJV
UzELMAkGA1UECAwCTkMxDDAKBgNVBAcMA1JUUDEOMAwGA1UECgwFQ2lzY28xDDAK
BgNVBAsMA1NWUzEXMBUGA1UEAwwOMTAuMjI1LjI1My4xNjcxETAPBgNVBAUTCDQw
OTA4NDNiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvDH3DgOdO2uW
gMf2I5nE+8QMBHA3S3has8SNpByVlQDprHoLGr/QmVCJR/b55C/7ispmoBnXEOGJ
qIwaoROc7QsqnCa3HXQipcvtRgwcfAX29EgjnbOiaRYDxrrdbHrpSQTFpeh5dp/k
eQuioO7rxfzdTss+8x7WwzC+artGbLYMC7fQcH8l9iVAIeZNUXPczl8G3zrHHi3W
fFMVT/iVFYwLvdROvlhOokuMykFPaOOTemJn6QvinVz1ThEgGRTz8bh2vMVsa8cI
iRaTAjRxvVfYeC1tVBOJdMDAkOavY73N3ZkJrl6dNs4ods1e4eOnLSTwx7Ao5Xaa
7DFVxBt6PwIDAQABo4GAMH4wHgYJYIZIAYb4QgENBBEWD3hjYSBjZXJOaWZpY2FO
ZTAOBgNVHQ8BAf8EBAMCBaAwIAYDVR0lAQH/BBYwFAYIKwYBBQUHAwEGCCsGAQUF
BwMCMAkGA1UdEwQCMAAwHwYDVR0RBBgwFoIOMTAuMjI1LjI1My4xNjeHBArh/acw
DQYJKoZIhvcNAQELBQADggIBAARpS5bEck+ojO121O6WxedDQ8VduObBtrnOH+Nt
94EA1co7HEe4USf1FiASAX7rNveLpY3ICmLh+tQZYTZrQ93tb9mMTZg7exqN89ZU
VlXoB2UOTri5Kl0/+izEGgyNq42/ytAP8YOO7HR/2jf7gfhoRvwcR5QNOEHv4o6l
Zma5Xio1sBbkA7JB2mpzzZg4ZjsyV8lRGXxxgyt1mwNmb7EiAc8lodRcgyp7FNh3
F/k9cMMMr5lM4Ysvoltx1k9AeLjzb2syv5/fG6QuOZdWwTaaQhOY2h/cVDiV97wg
ODlmEfdSv6QrxQSujZr22RzVyKKHltuiV2B74pthUuGRBtfHS5XFy7uTTbfGX8M6
ZJw8rX1SADr8tDplrf1ZIrPmv3ZPP7woTB22yWzydOuse+5IalbOw7OtwN4t/IIw
8CJu6HfnDXLDPZOjsC8steffrSlopwGccp3j6aZKPFz+I/Purb44a9WxEWa2TA7H
+rloynBcGMetOHxVLnptlsC7Q4mN/MDXeGyW+OTNCirNEG/gqcu+dn9EnNKkE2WV
oF537Ow+uNHoK8Bdt8mqadUT4OoUSqY8ArVOBomO5tzbemreVPmQAZ/IahZ7TqKo
3dGNonTAfFTESM1iujQ81iRKsikDHySnwcCM2nilCKZrhVq5IB8NK6jKRJZOeQAX
vMt1
-----END CERTIFICATE-----
```

quit

```
Serial Number : C2:F4:AB:34:02:D2:76:74:65:34:FE:D5
Subject:
serialNumber=4090843b,CN=10.225.253.167,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
Issued By :
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
```

```
Validity Start : 14:57:00 UTC Fri May 09 2025
Validity End : 14:57:00 UTC Sat May 09 2026
SHA1 Fingerprint:
21E4DA0B02181D08B6E51F0CC754BCE5B815C792
```

Verifique que el certificado de identidad del router esté inscrito.

<#root>

```
RP/0/RP0/CPU0:BRC-8201-1#
```

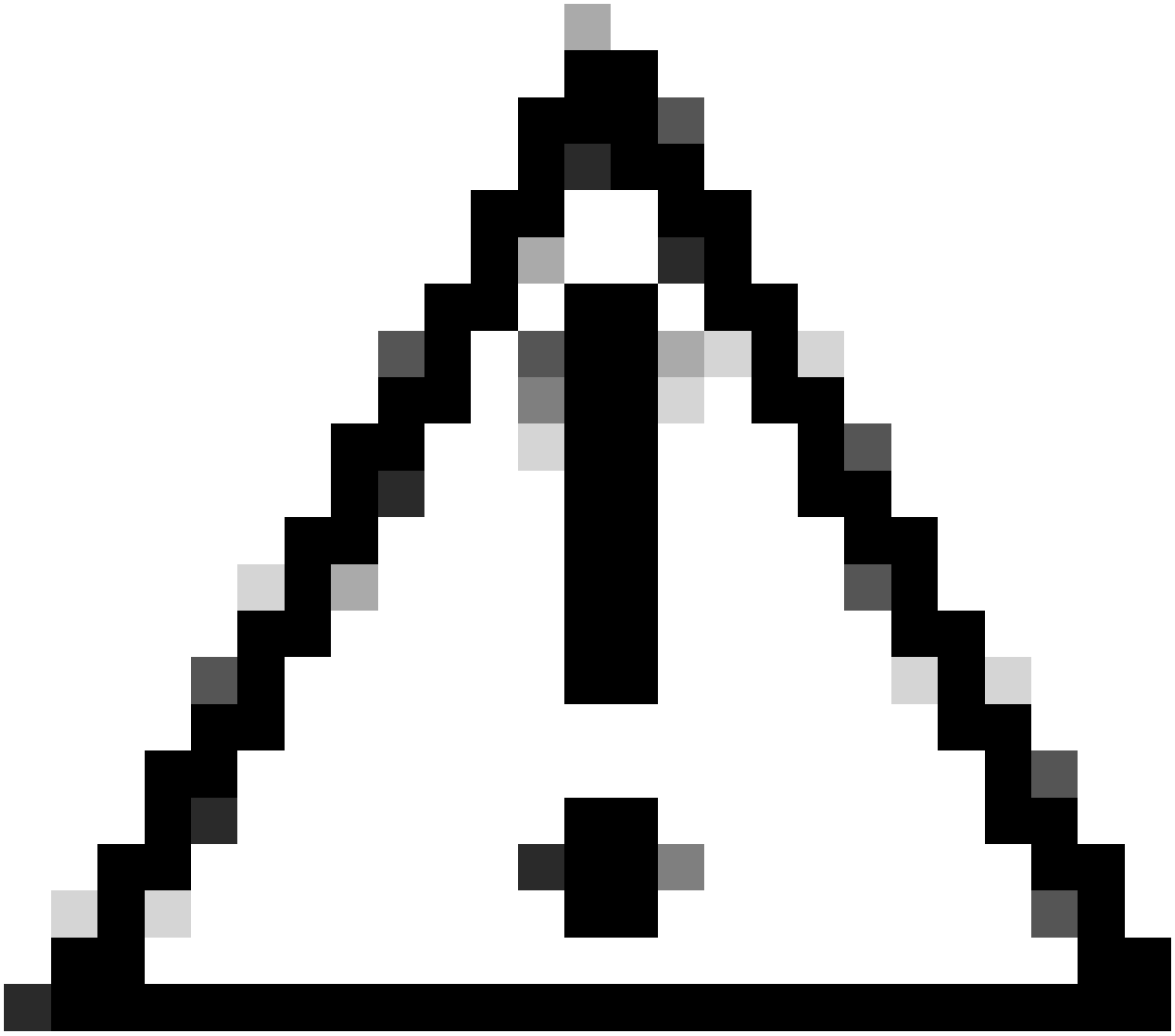
show crypto ca trustpoint svs detail

```
Trustpoint        :svs-new
================================================================
KeyPair Label: the_default
CRL:optional
enrollment: terminal
subject name: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=brc-8201-1.svs.lab

RP/0/RP0/CPU0:BRC-8201-1#
```

show crypto ca certificates svs

```
Wed May 14 14:55:58.173 UTC

Trustpoint       : svs-new
================================================
CA certificate
  Serial Number  : 20:01:20:1F:B6:9D:C3:FE:43:78:FF:64
  Subject:
        CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
  Issued By      :
        CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
  Validity Start : 17:05:00 UTC Mon Apr 28 2025
  Validity End   : 17:05:00 UTC Sat Apr 28 2035
  SHA1 Fingerprint:
         0EB181E95A3ED7803BC5A8059A854A95C83AC737
Router certificate
  Key usage      : General Purpose
  Status         : Available
  Serial Number  : FD:AC:20:1F:B6:9D:C3:FE:98:43:ED
  Subject:
        serialNumber=4090843b,CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
  Issued By      :
        CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
  Validity Start : 19:59:00 UTC Fri May 09 2025
  Validity End   : 19:59:00 UTC Sat May 09 2026
  SHA1 Fingerprint:
         AC17E4772D909470F753BDBFA463F2DF522CC2A6
Associated Trustpoint: svs
```

Configuración de TACACS y AAA con TLS



Precaución: Realice los cambios de configuración mediante la consola con credenciales locales.

Paso 1. Configuración del servidor TACACS+.

```
tacacs source-interface MgmtEth0/RP0/CPU0/0 vrf mgmt
tacacs-server host 10.225.253.209 port 49
  key 7 072C705F4D0648574453

aaa group server tacacs+ tacacs2
 server 10.225.253.209
 vrf mgmt
```

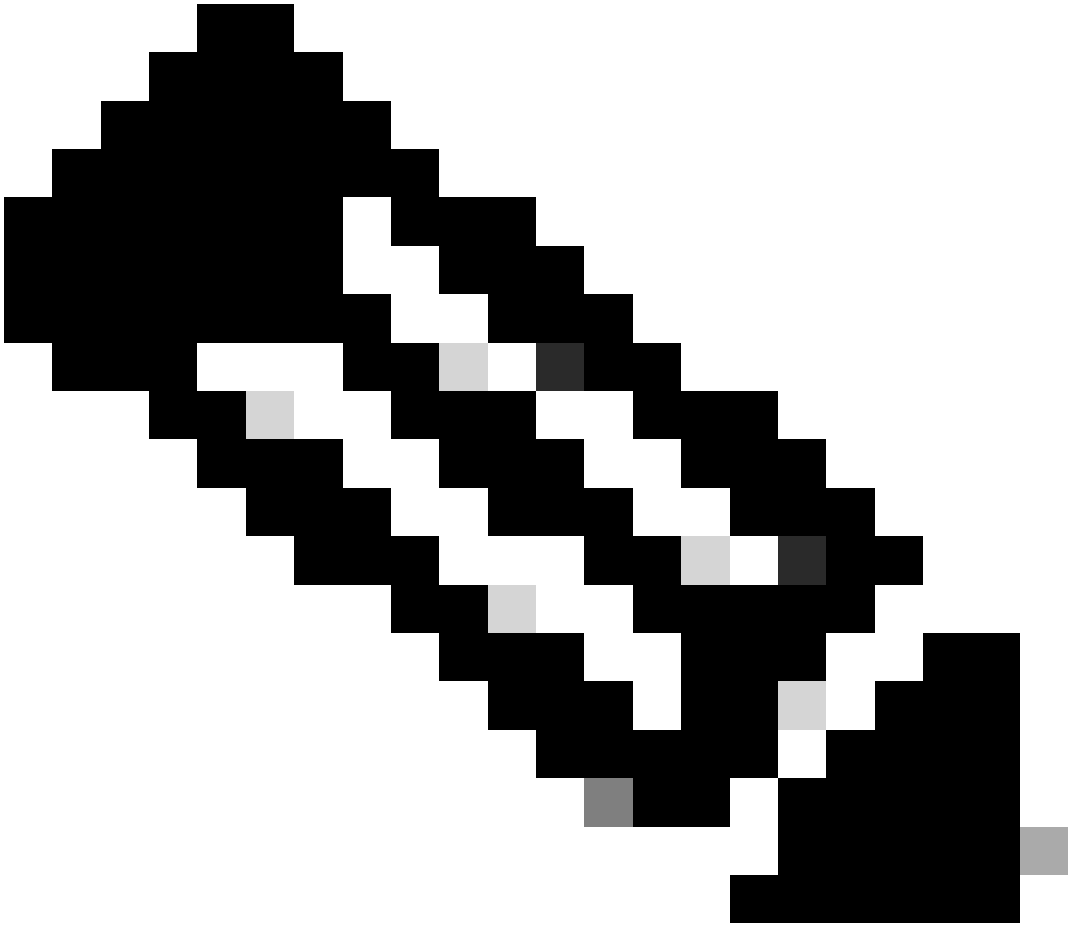
Paso 2. Configure el grupo AAA.

```
aaa group server tacacs+ tac_tls_sc
 vrf mgmt
 server-private 10.225.253.209 port 6049
  timeout 10
  tls
   trustpoint svs
  !
  single-connection
```

Paso 2. Configure AAA.

```
aaa accounting exec default start-stop group tac_tls_sc
aaa accounting system default start-stop group tac_tls_sc
aaa accounting network default start-stop group tac_tls_sc
aaa accounting commands default stop-only group tac_tls_sc
aaa authorization exec default group tac_tls_sc local
aaa authorization commands default group tac_tls_sc none
aaa authentication login default group tac_tls_sc local
```

Renovación de certificados



Nota: No es necesario eliminar el punto de confianza de la configuración de TACACS+ durante la renovación.

Paso 1. Compruebe las fechas de validez del certificado actual.

```
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates svs-new
Thu Aug 14 15:13:37.465 UTC

Trustpoint : svs-new
================================================
CA certificate
  Serial Number : 30:A2:10:14:C9:5E:B0:E0:07:CE:0A:24:16:69:90:ED:D1:34:B5:9B
  Subject:
        CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Issued By :
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 22:13:17 UTC Thu Jun 26 2025
  Validity End : 22:13:16 UTC Tue Jun 25 2030
```

```
  CRL Distribution Point

http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=m9uBlQsZDYy6wxomiFWB5GvOAZM

  SHA1 Fingerprint:
        EA8FB276563B927FCAF0174D9FD1C58F3E8B5FF2
Trusted Certificate Chain
  Serial Number : 1F:A6:6E:2E:F8:AB:CE:B4:9C:B8:07:5A:9F:2B:32:02:B4:56:5C:96
  Subject:
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Issued By :
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 22:13:17 UTC Thu Jun 26 2025
  Validity End : 22:13:16 UTC Sun Jun 24 2035
  SHA1 Fingerprint:
        E225647FF9BDA176D2998D5A3A9770270F37D2A7
Router certificate
  Key usage : General Purpose
  Status : Available
  Serial Number : 7A:13:EB:C0:6A:8D:66:68:09:0B:32:C7:0C:D8:05:BD:81:72:9B:4E
  Subject:
        CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
  Issued By :
        CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 16:38:36 UTC Wed Jul 30 2025
  Validity End : 16:38:35 UTC Thu Jul 30 2026
  CRL Distribution Point

http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=X4as2q+6I9Bd4QglQa8g1xoH8GY
  SHA1 Fingerprint:
        B562F3CF507CE7F97893F28BC896794CFF6995C1
Associated Trustpoint: svs-new
```

Paso 2. Eliminar certificado de punto de confianza existente.

```
RP/0/RP0/CPU0:BRC-8201-1#clear crypto ca certificates KF_TP
Thu Aug 14 15:25:26.286 UTC
certificates cleared for trustpoint KF_TP
RP/0/RP0/CPU0:Aug 14 15:25:26.577 UTC: cepki[382]: %SECURITY-CEPKI-6-INFO : certificate database update
RP/0/RP0/CPU0:BRC-8201-1#
RP/0/RP0/CPU0:BRC-8201-1#
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates KF_TP
Thu Aug 14 15:25:37.270 UTC
RP/0/RP0/CPU0:BRC-8201-1#
```

Paso 3. Vuelva a autenticar e inscriba el punto de confianza como se describe en los pasos bajo Configuración de Punto de Confianza.

Paso 4. Compruebe que se actualizan las fechas de validez del certificado.

```
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates KF_TP
Thu Aug 14 15:31:28.309 UTC
```

```
Trustpoint : KF_TP
================================================
CA certificate
  Serial Number : 30:A2:10:14:C9:5E:B0:E0:07:CE:0A:24:16:69:90:ED:D1:34:B5:9B
  Subject:
CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Issued By :
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 22:13:17 UTC Thu Jun 26 2025
  Validity End : 22:13:16 UTC Tue Jun 25 2030

  CRL Distribution Point

http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=m9uBlQsZDYy6wxomiFWB5GvOAZM
  SHA1 Fingerprint:
        EA8FB276563B927FCAF0174D9FD1C58F3E8B5FF2
Trusted Certificate Chain
  Serial Number : 1F:A6:6E:2E:F8:AB:CE:B4:9C:B8:07:5A:9F:2B:32:02:B4:56:5C:96
  Subject:
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Issued By :
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 22:13:17 UTC Thu Jun 26 2025
  Validity End : 22:13:16 UTC Sun Jun 24 2035
  SHA1 Fingerprint:
        E225647FF9BDA176D2998D5A3A9770270F37D2A7
Router certificate
  Key usage : General Purpose
  Status : Available
  Serial Number : 1F:B0:AE:44:CF:8E:24:62:83:42:2F:34:BF:D0:82:07:DF:E4:49:0B
  Subject:
        CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
  Issued By :
        CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 15:17:29 UTC Thu Aug 14 2025
  Validity End : 15:17:28 UTC Fri Aug 14 2026

  CRL Distribution Point

http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=X4as2q+6I9Bd4QglQa8g1xoH8GY
  SHA1 Fingerprint:
        D3CE0AEB51C5E8009F626A1A9FD633FB9AFA96DE
Associated Trustpoint: KF_TP
```

Verificación

Verifique la Configuración.

```
show crypto ca certificates [detail]
show crypto ca trustpoint detail
show tacacs details
```

Depuración para TACACS+

```
debug tacacs tls
```

Debug TLS

```
debug ssl error
debug ssl events
```

Pruebe el usuario remoto antes de configurar la autenticación AAA.

<#root>

test aaa group tacacs2

```
user has been authenticated
```

Resolución de problemas

Borrar los certificados (se eliminan todos los certificados asociados a un punto de confianza).

```
clear crypto ca certificate <trustpoint name>
```

Reinicio del proceso TACACS (si es necesario)

```
process restart tacacsd
```

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).