Configuración de TACACS+ sobre TLS 1.3 en un dispositivo IOS XE 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® XE 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 XE.
· Parte 1: Configuración de ISE para la administración de dispositivos
· Parte 2 - Configuración de Cisco IOS XE 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
- Software Cisco IOS XE, versión 17.15+

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.

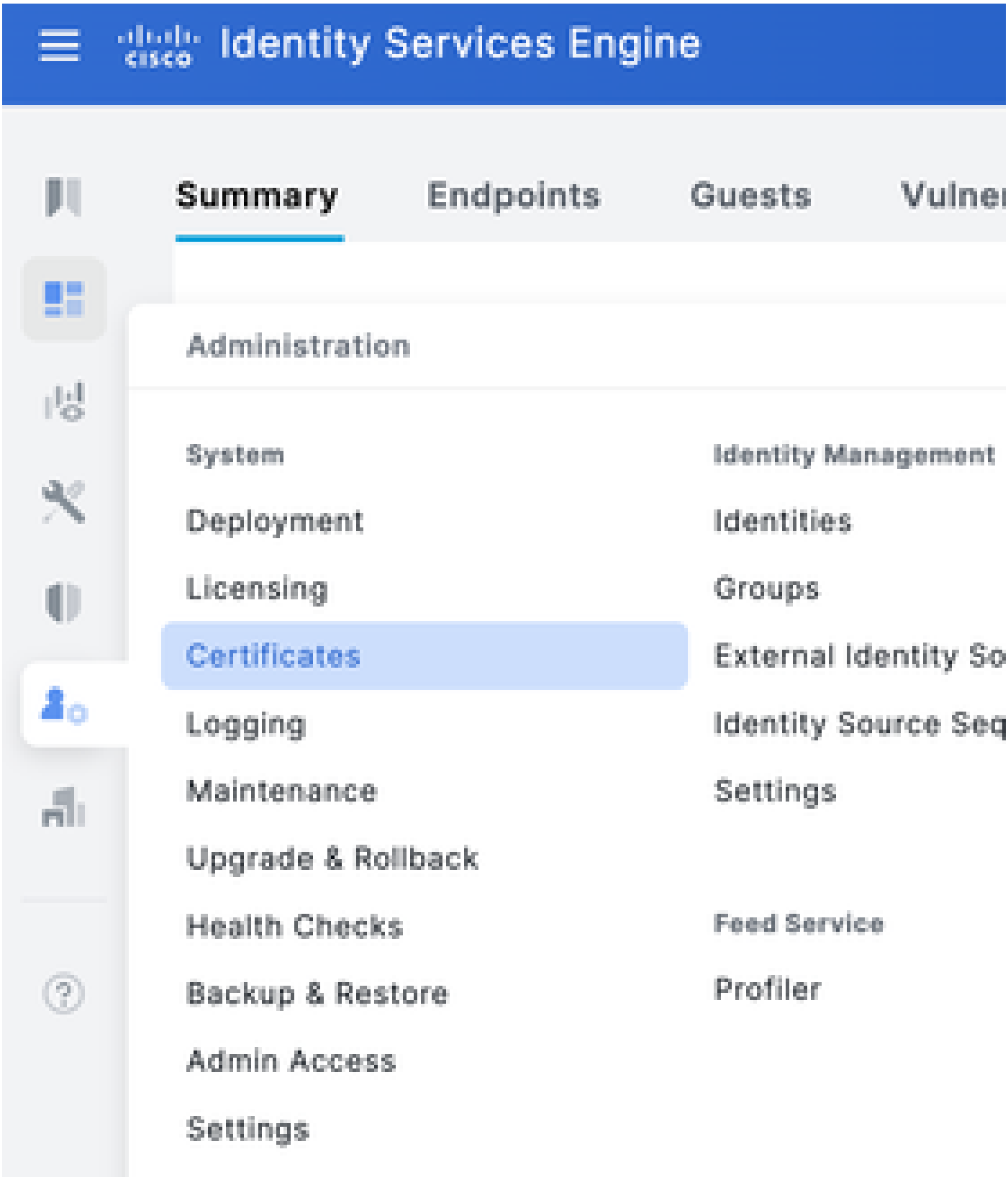
Parte 1: Configuración de ISE para la administración de dispositivos

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).

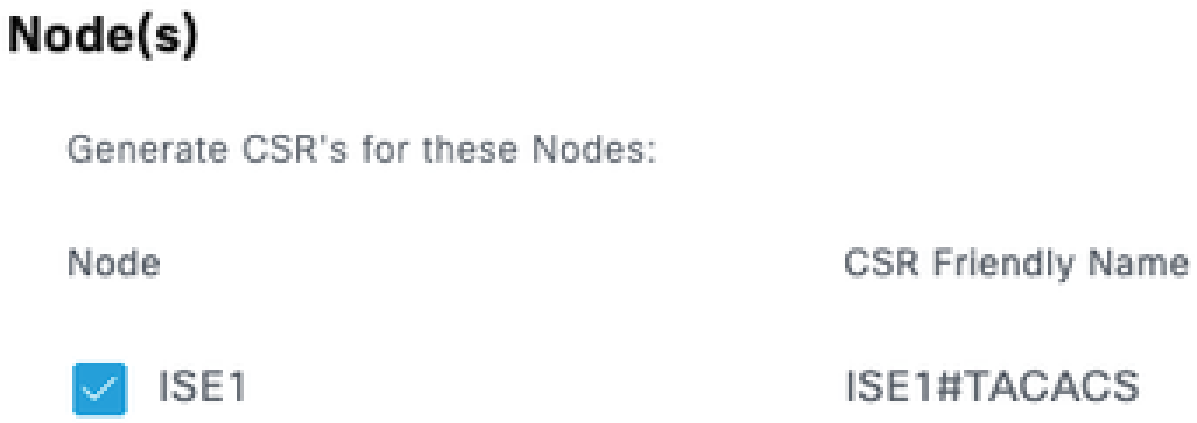
Paso 2.Vaya a Administración > Sistema > Certificados.



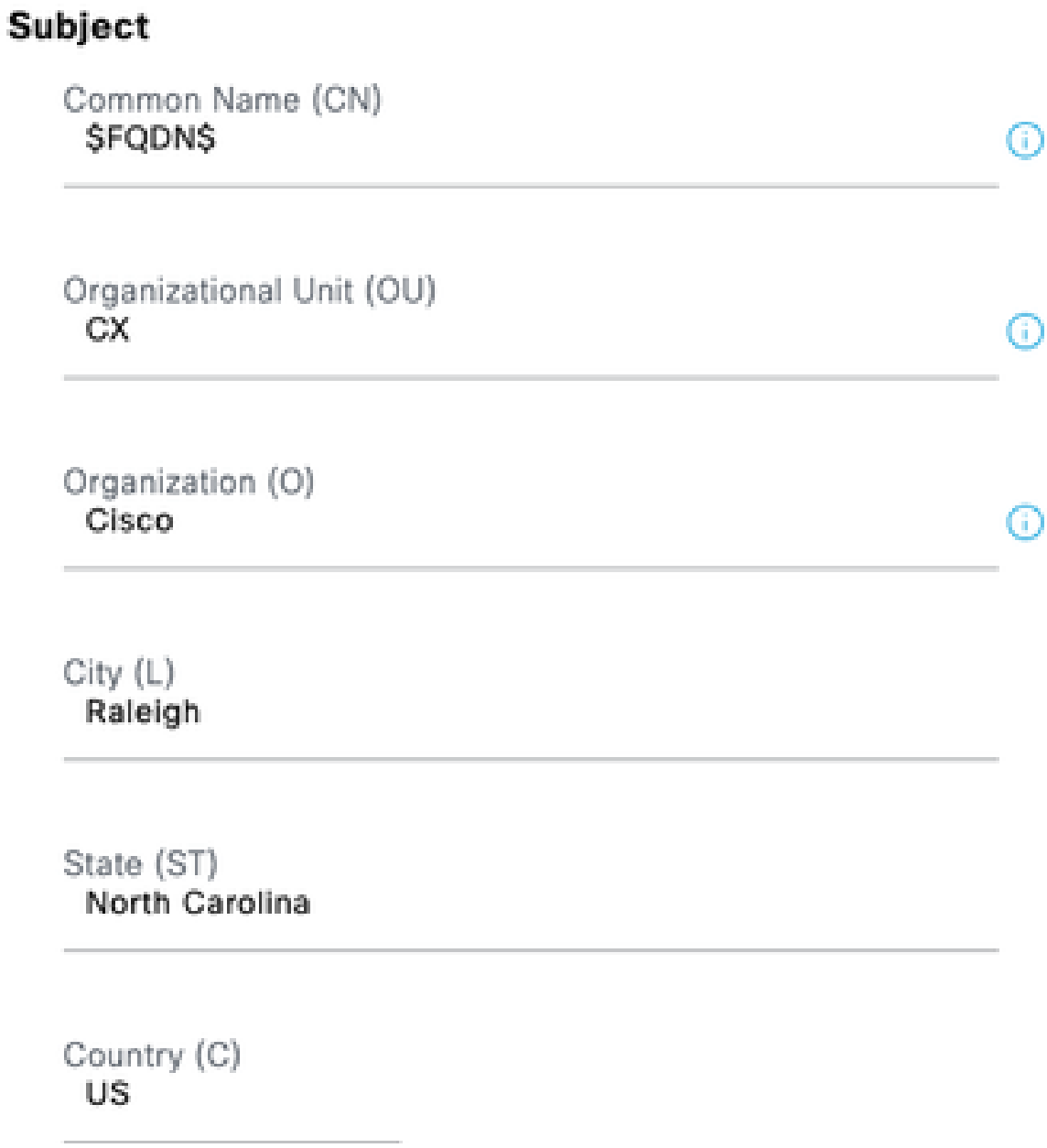
Paso 3. En Solicitudes de firma de certificado, haga clic en Generar solicitud de firma de certificado.

Paso 4.Seleccione TACACS inUsage.

Paso 5.Seleccione los PSNs que tendrán TACACS+ habilitado.

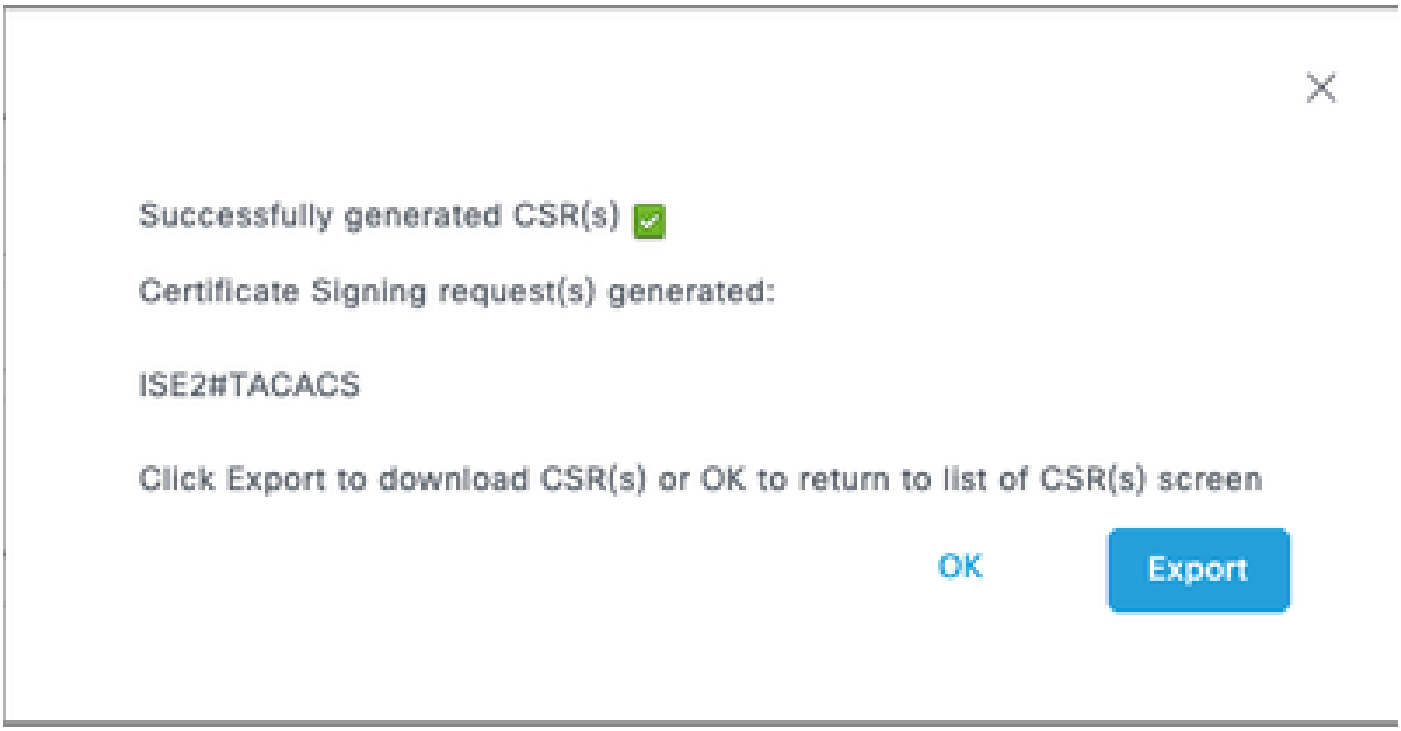


Paso 6. Rellene los campos Asunto con la información correspondiente.



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

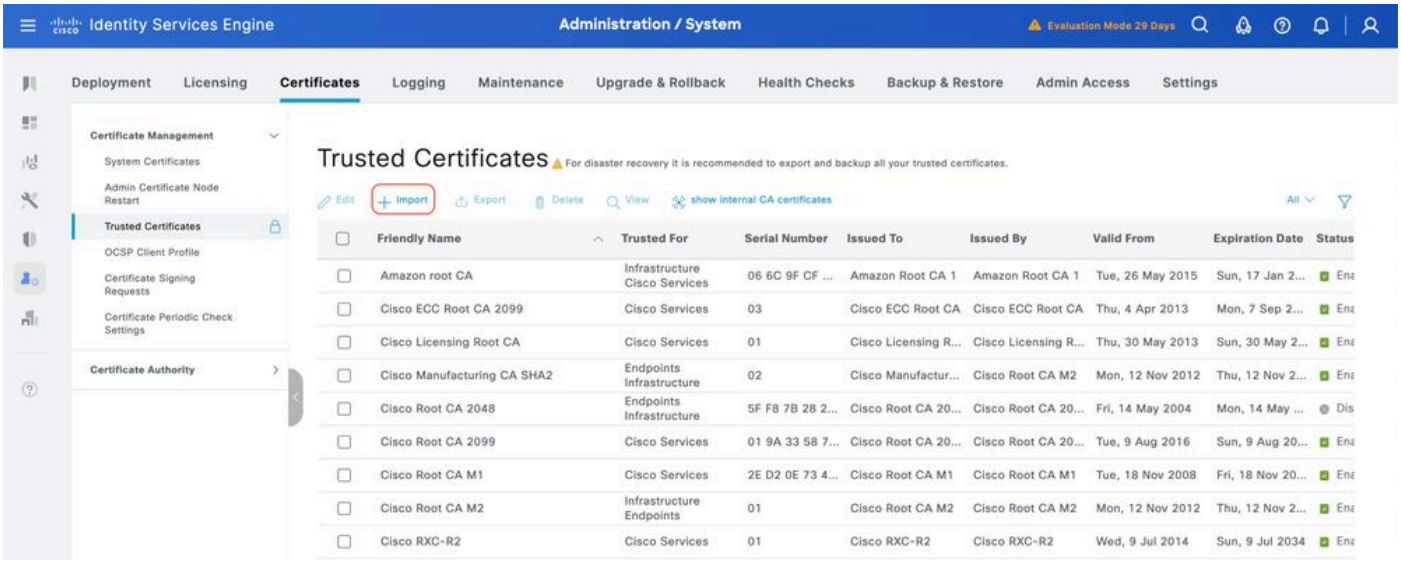
Paso 8.Haga clic en Generar y luego en Exportar.



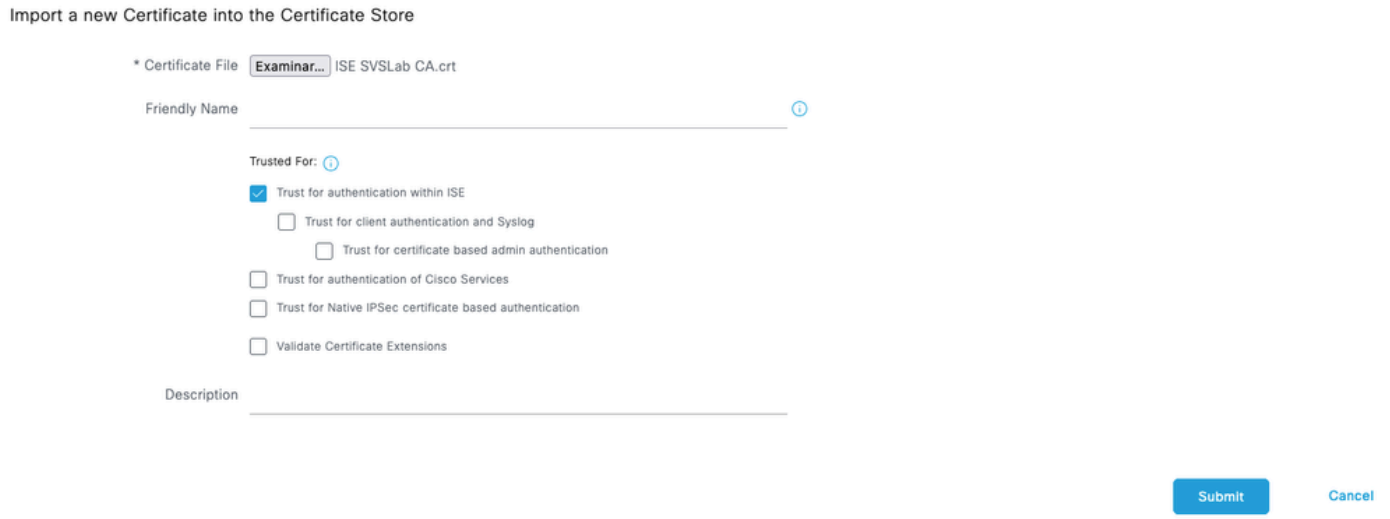
Ahora, puede hacer que la autoridad de certificación (CA) firme el certificado (CRT).

Cargar certificado de CA raíz para autenticación de servidor TACACS+

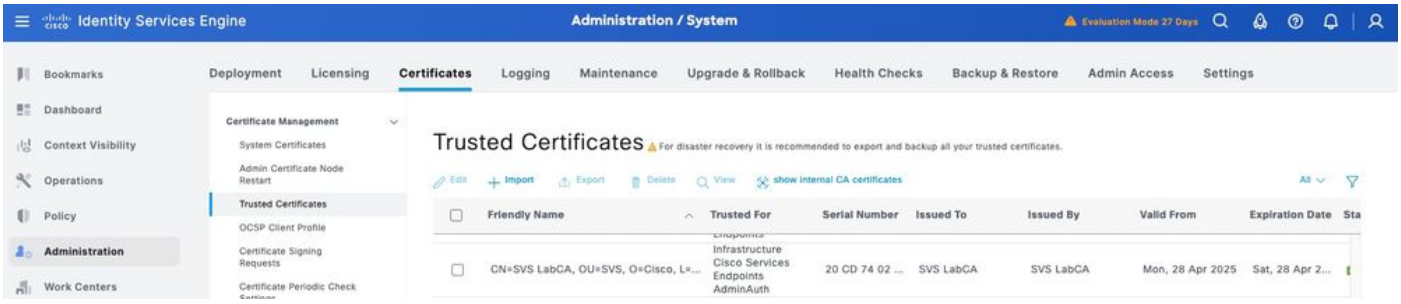
Paso 1. Navegue hasta Administración > Sistema > Certificados. En Certificados de confianza, haga clic en Importar.



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



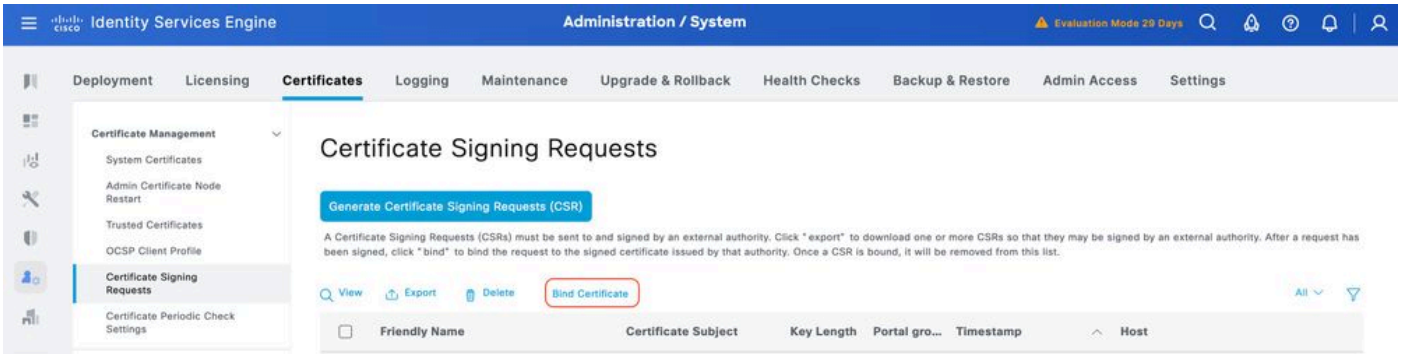
Paso 3. Haga clic en Enviar. El certificado debe aparecer ahora en Certificados Protegidos.



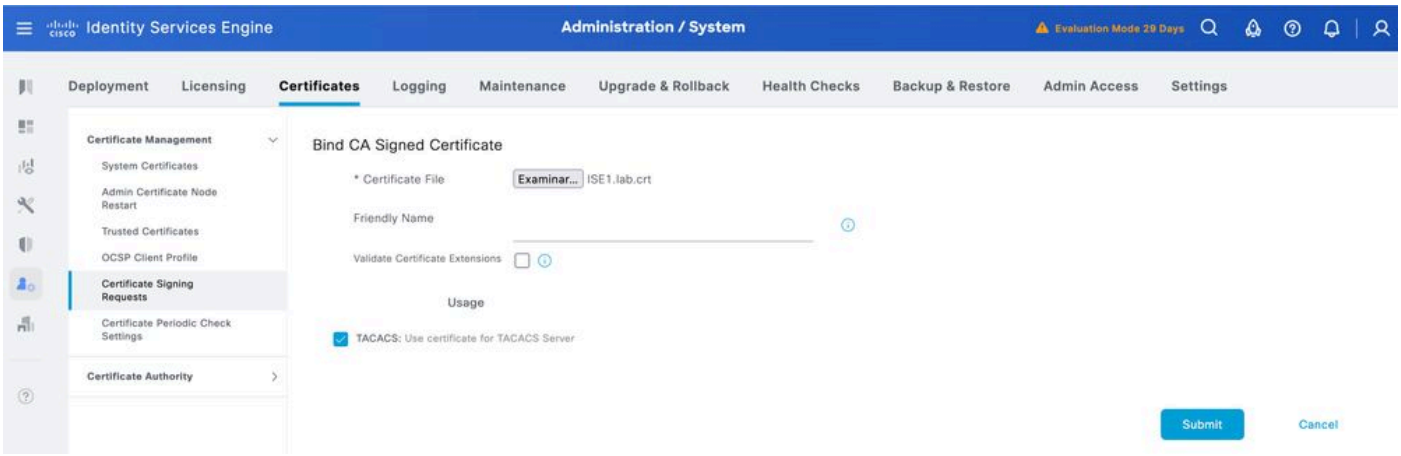
Enlazar la solicitud de firma de certificado (CSR) firmado a ISE

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 TACACS CSR generado en el paso anterior y haga clic en Enlazar certificado.

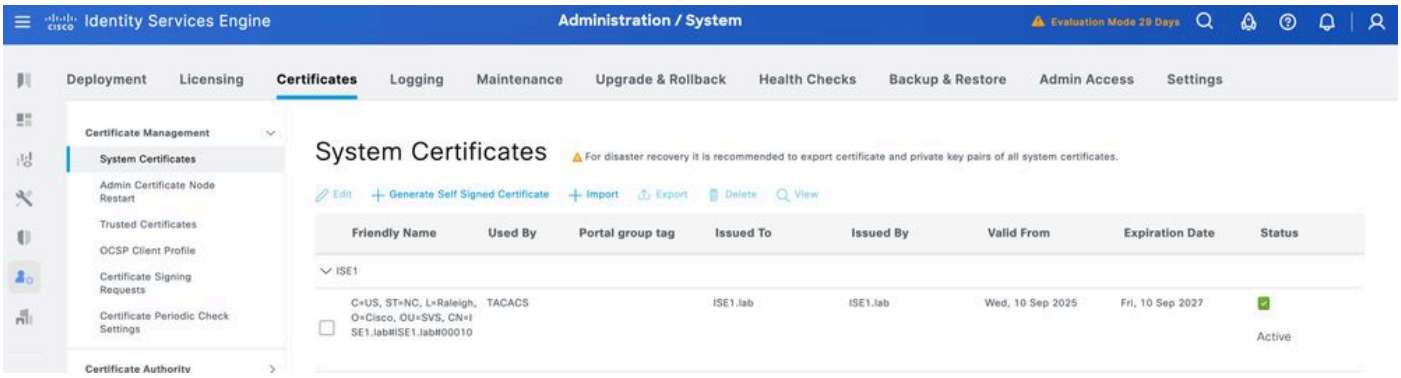


Paso 2.Seleccione el certificado firmado y asegúrese de que la casilla de verificación TACACS bajo Uso permanezca seleccionada.



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

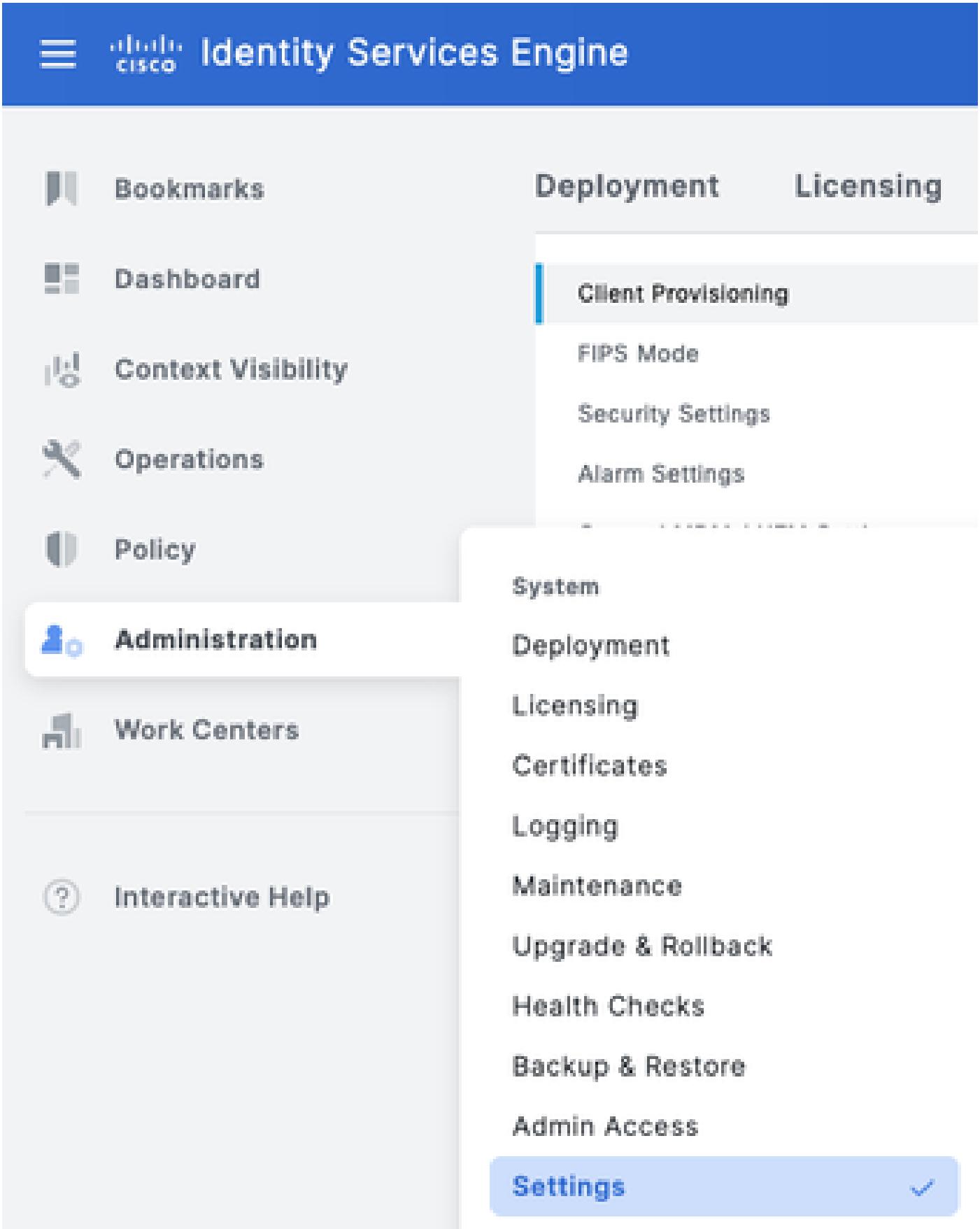
El certificado debe estar instalado correctamente. Puede verificarlo en Certificados del sistema.



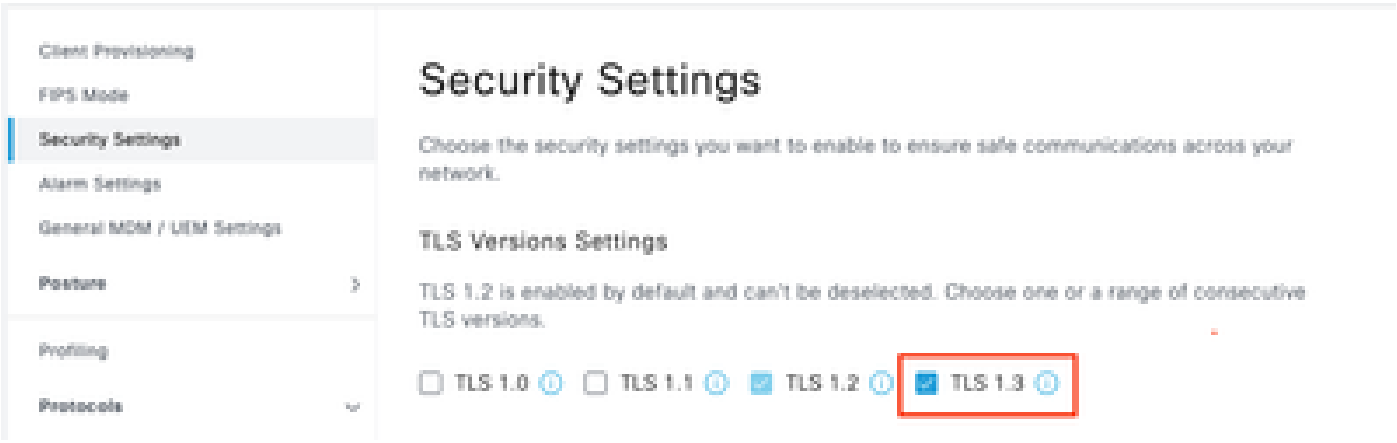
Habilitar TLS 1.3

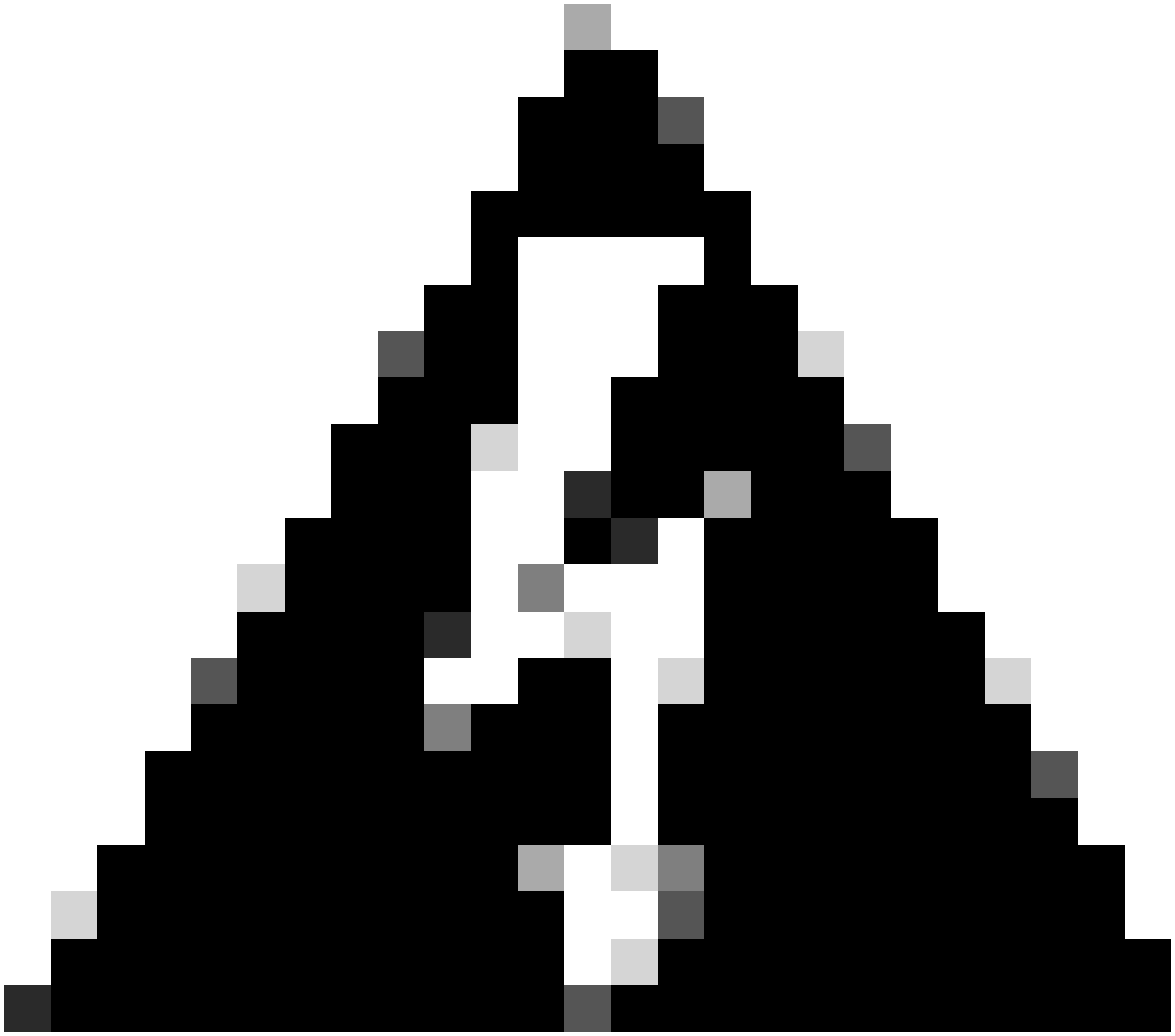
TLS 1.3 no está habilitado de forma predeterminada en ISE 3.4.x. Debe activarse manualmente.

Paso 1.Vaya a Administración > Sistema > Configuración.



Paso 2.Haga clic en Security Settings, seleccione la casilla de verificación junto a TLS1.3 en TLS Version Settings, luego haga clic en Save.



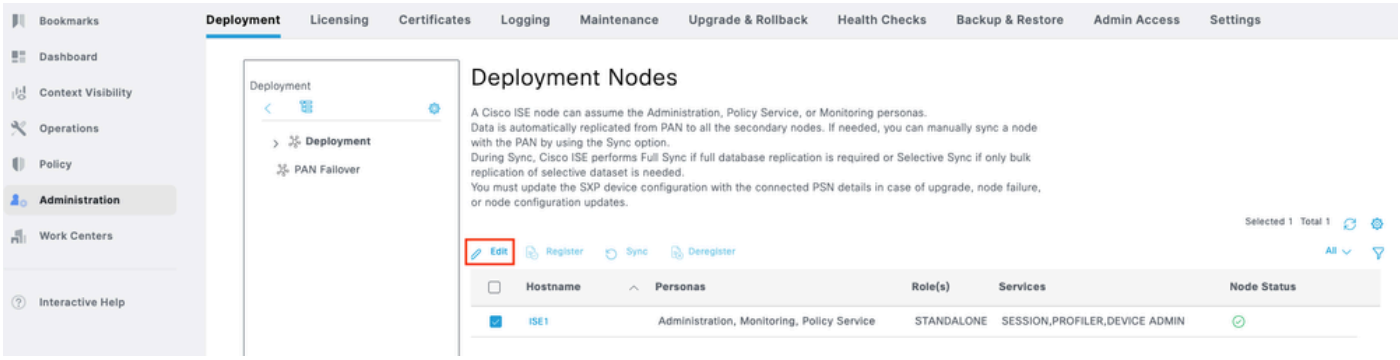


Advertencia: Al cambiar la versión de TLS, el servidor de aplicaciones de Cisco ISE se reinicia en todos los equipos de implementación de Cisco ISE.

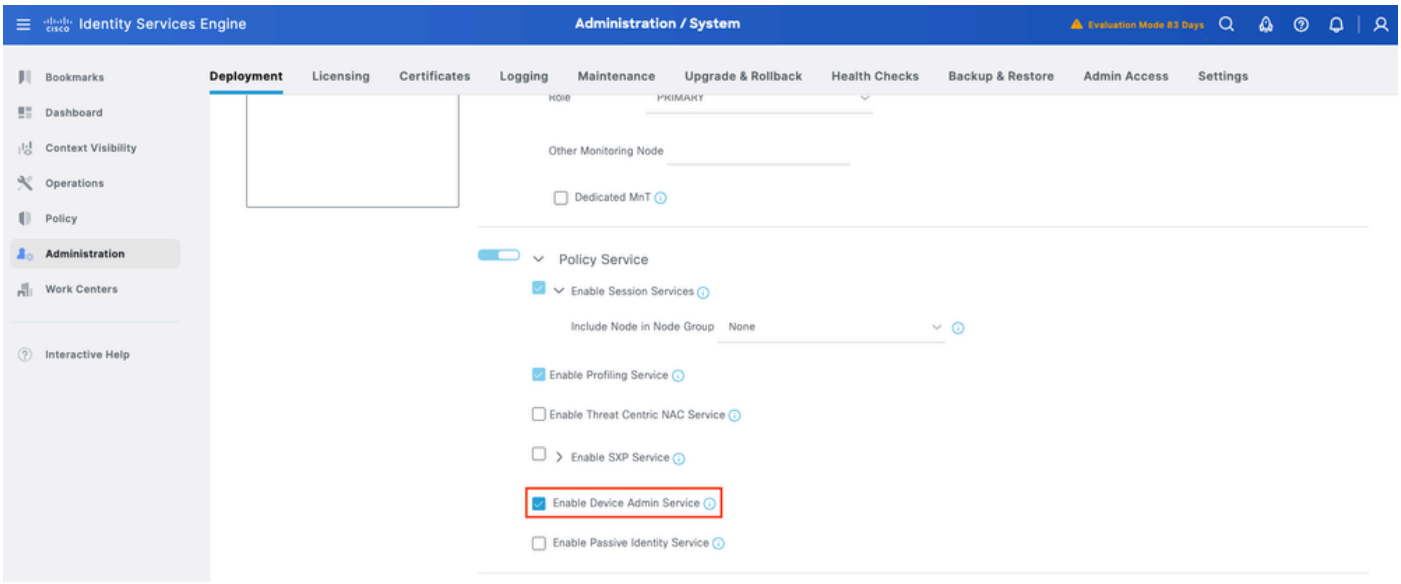
Habilitar Device Administration en ISE

El servicio Device Administration (TACACS+) no está habilitado de forma predeterminada en un nodo ISE. Habilite 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.



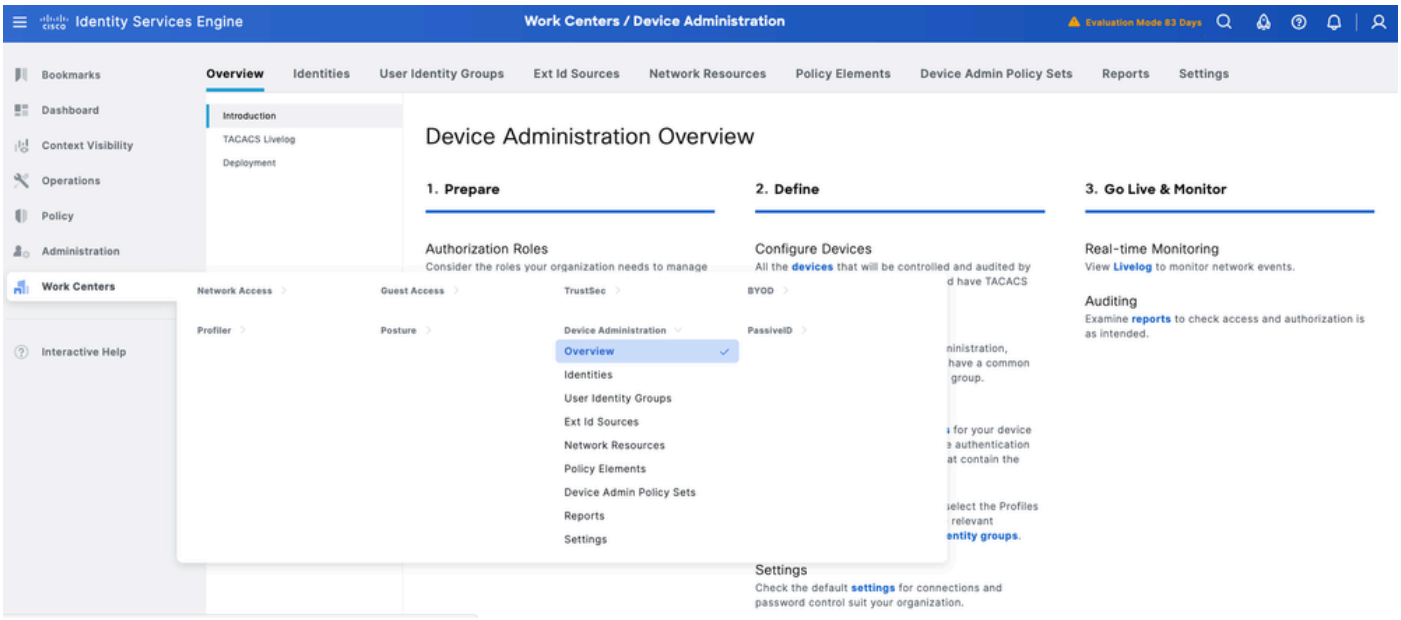
Paso 2.En GeneralSettings, desplácese hacia abajo y seleccione la casilla de verificación junto a Enable Device Admin Service.



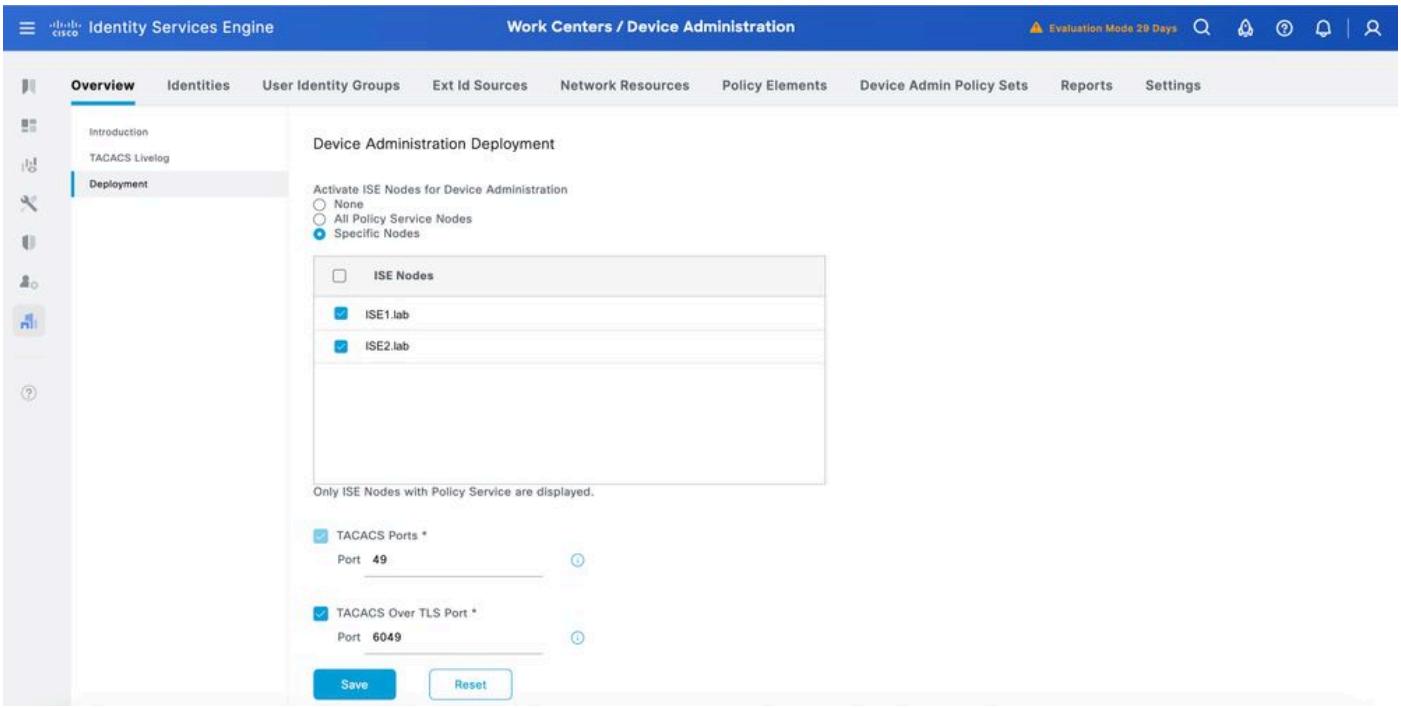
Paso 3. Guarde la configuración. El servicio Device Admin está ahora habilitado en ISE.

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.

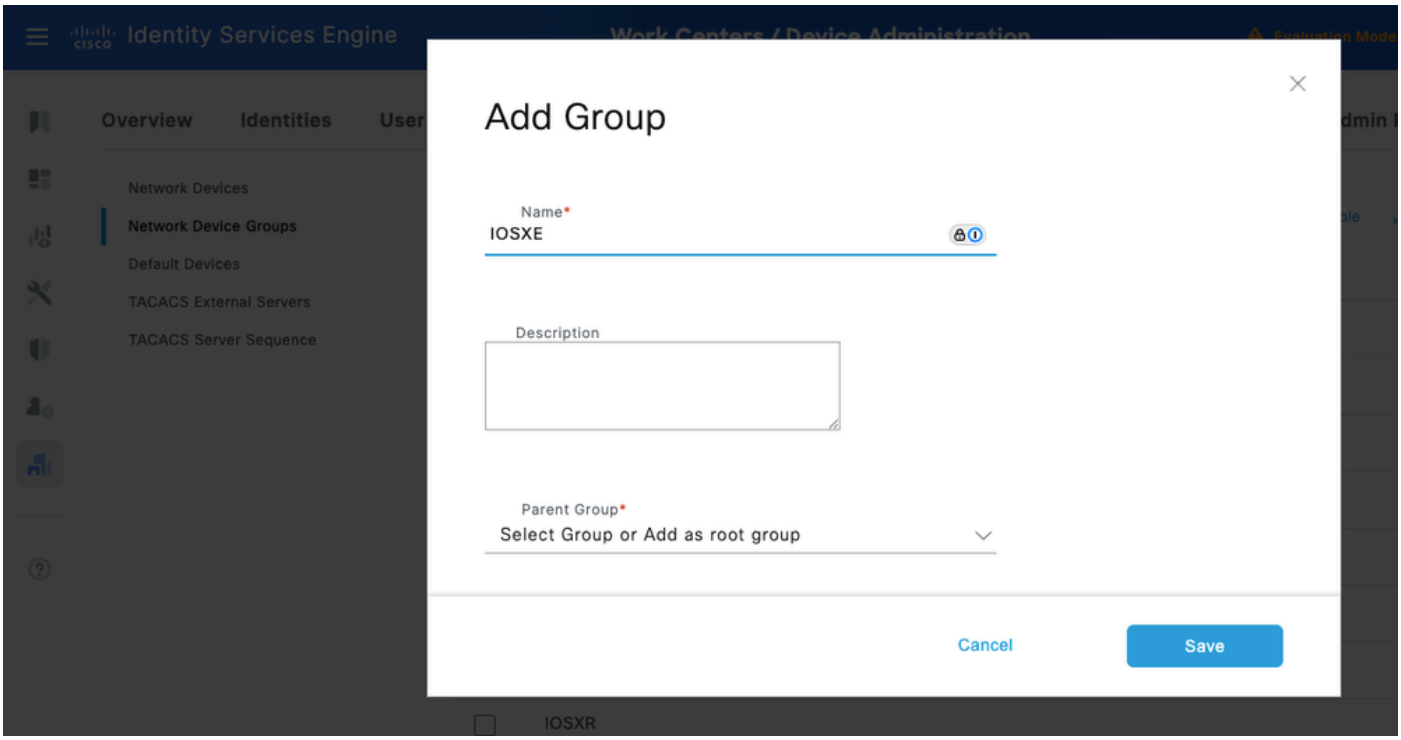


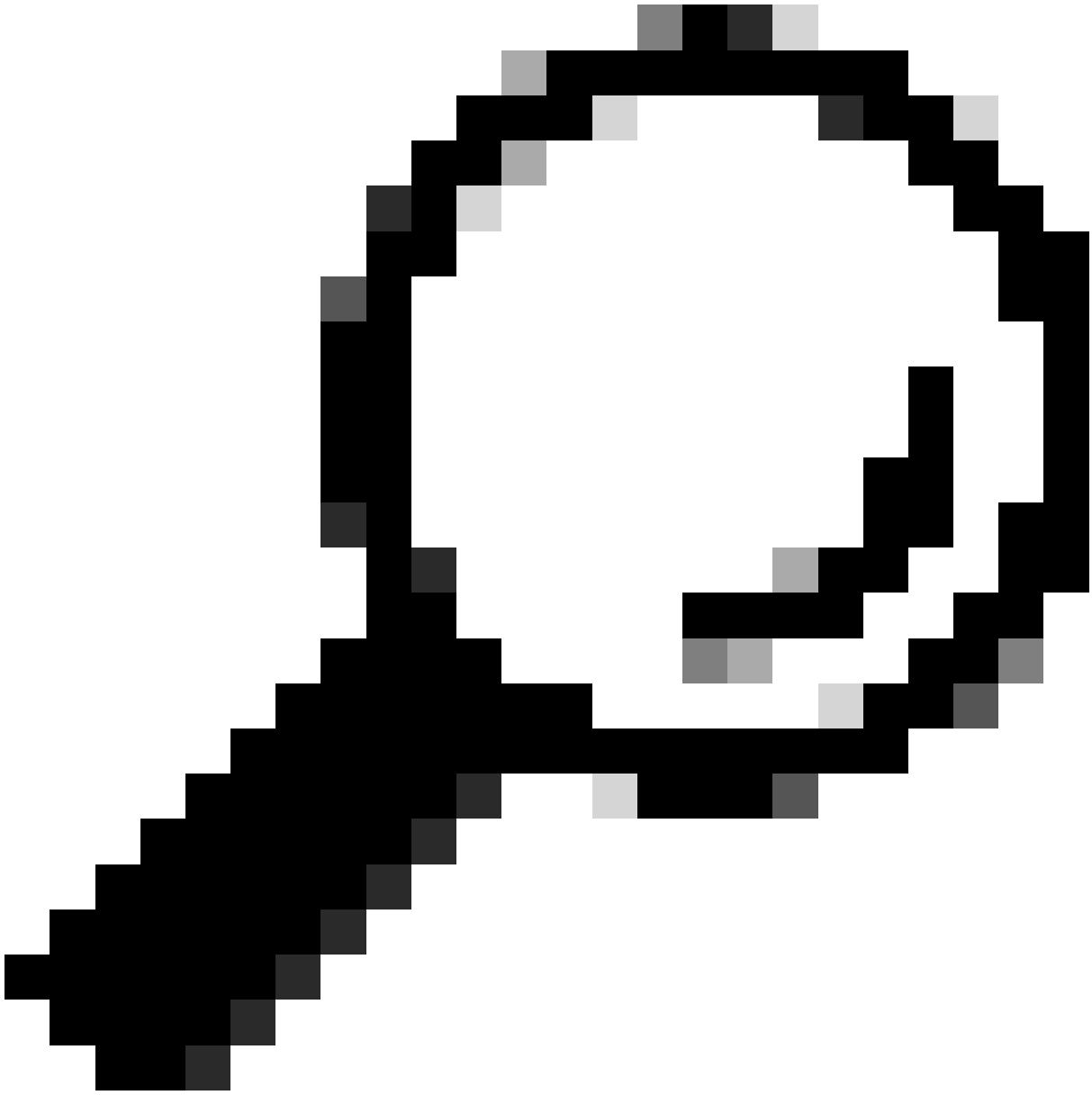
Paso 3.Mantenga el puerto predeterminado 6049 o especifique un puerto TCP diferente para TACACS sobre TLS, luego haga clic en Guardar.

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 XE.

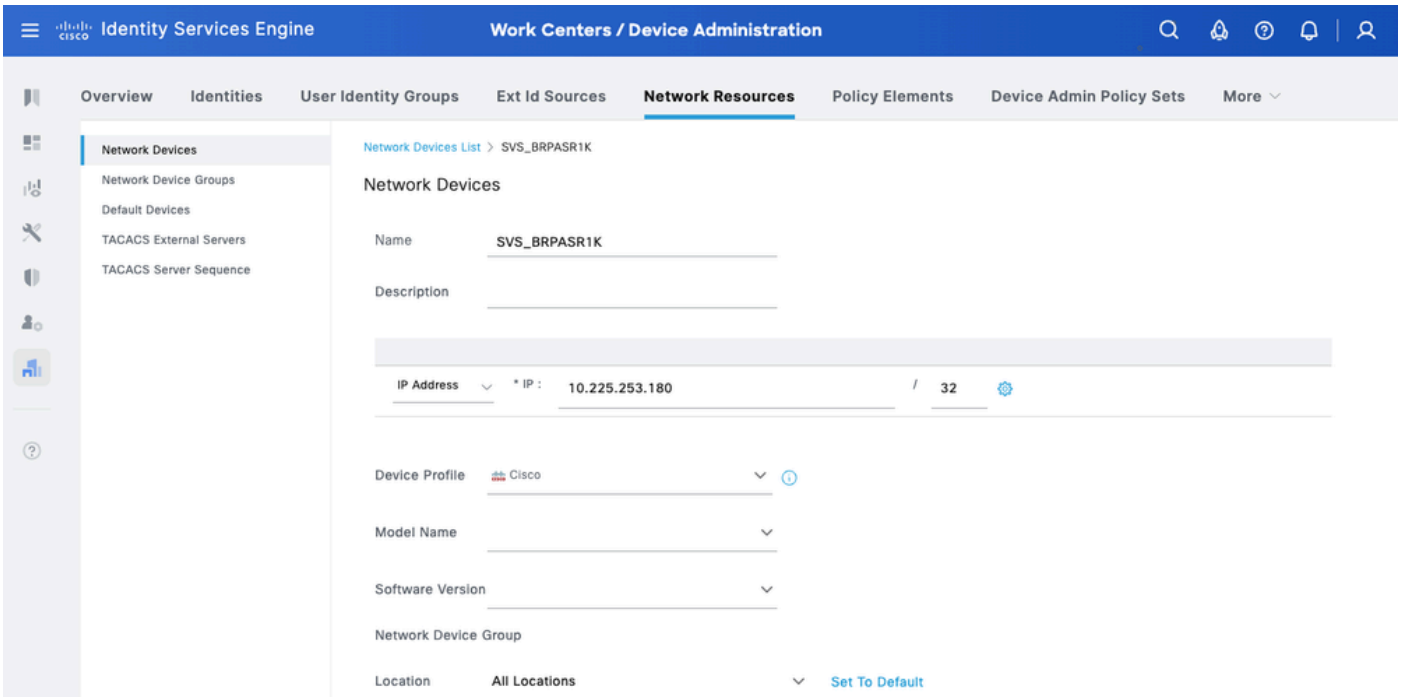

Identity Services Engine
Overview
Identities
Network Devices
Network Device Groups
Default Devices
TACACS External Servers
TACACS Server Sequence
Add Group
Name*
IOSXE
Description
Parent Group*
Select Group or Add as root group
Cancel
Save
IOSXR



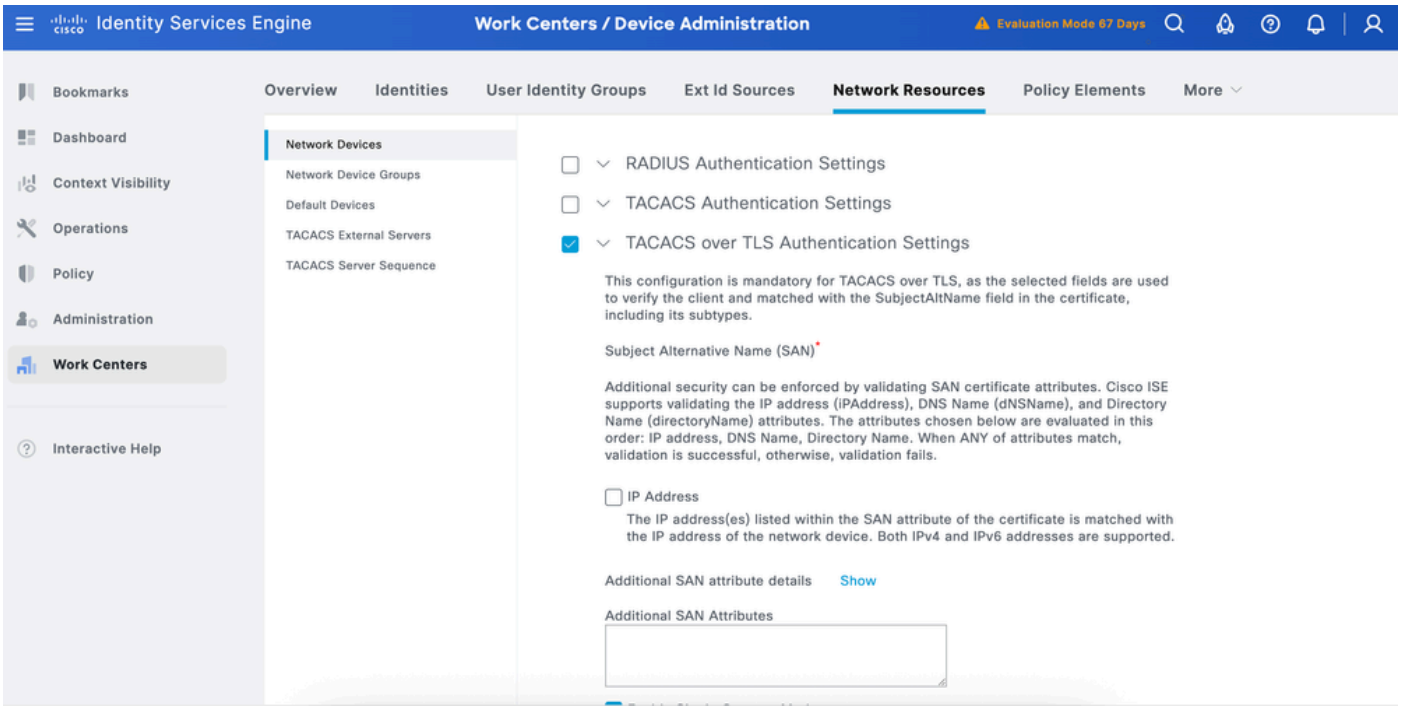
Consejo: Todos los tipos de dispositivos y todas las ubicaciones son jerarquías predeterminadas proporcionadas por ISE. Puede agregar sus propias jerarquías y definir los diversos componentes al identificar un dispositivo de red que se puede utilizar más adelante en la Condición de directiva

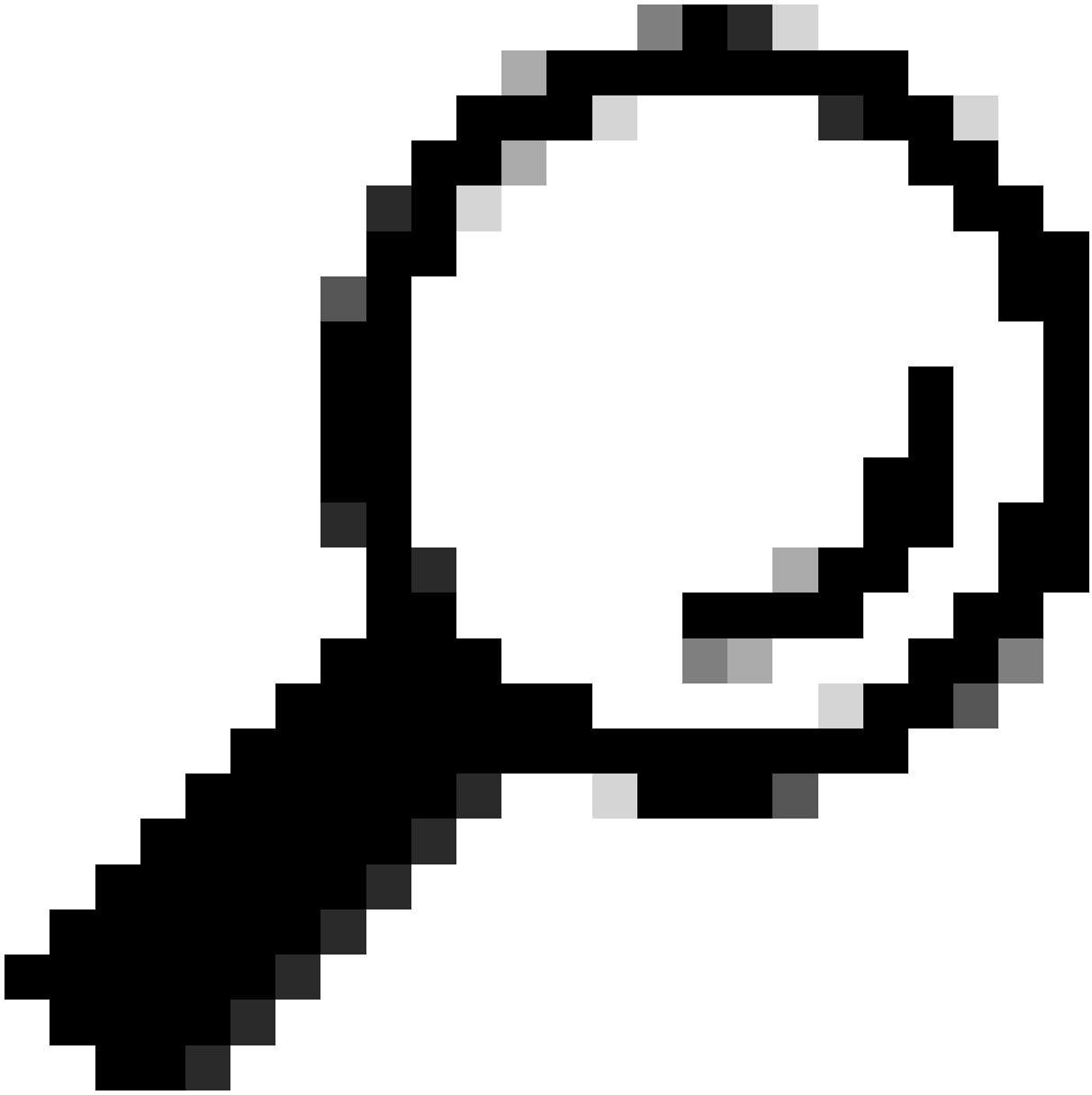
---

Paso 2.Ahora, agregue un dispositivo Cisco IOS XE 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. Para esta prueba, sería SVS_BRPASR1K.



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



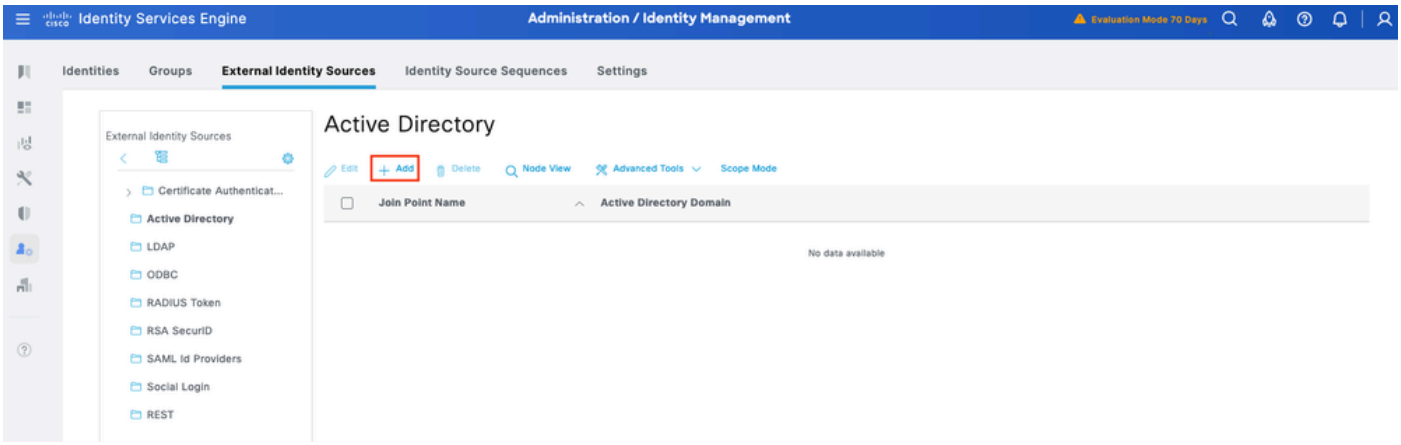


Consejo: Se recomienda habilitar el modo de conexión única para evitar reiniciar la sesión TCP cada vez que se envía un comando al dispositivo.

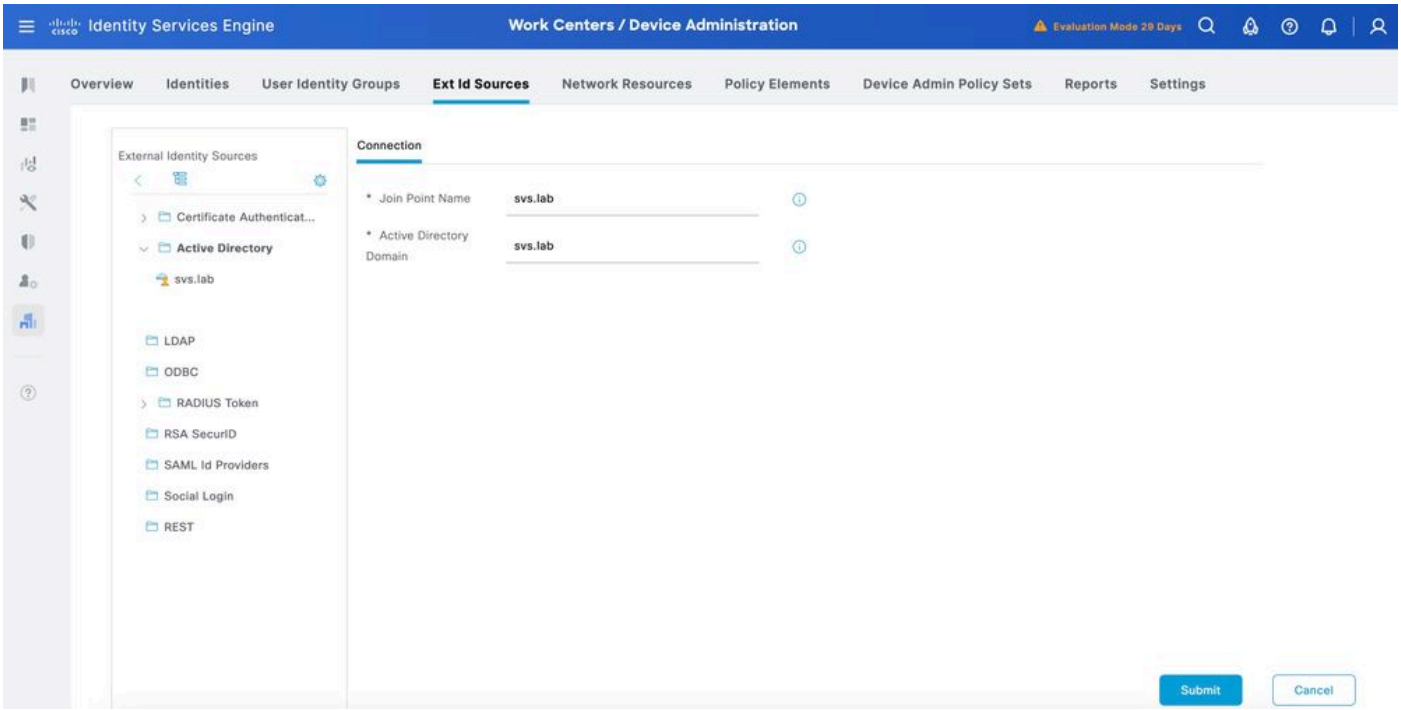
Configurar almacenes de identidad

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.

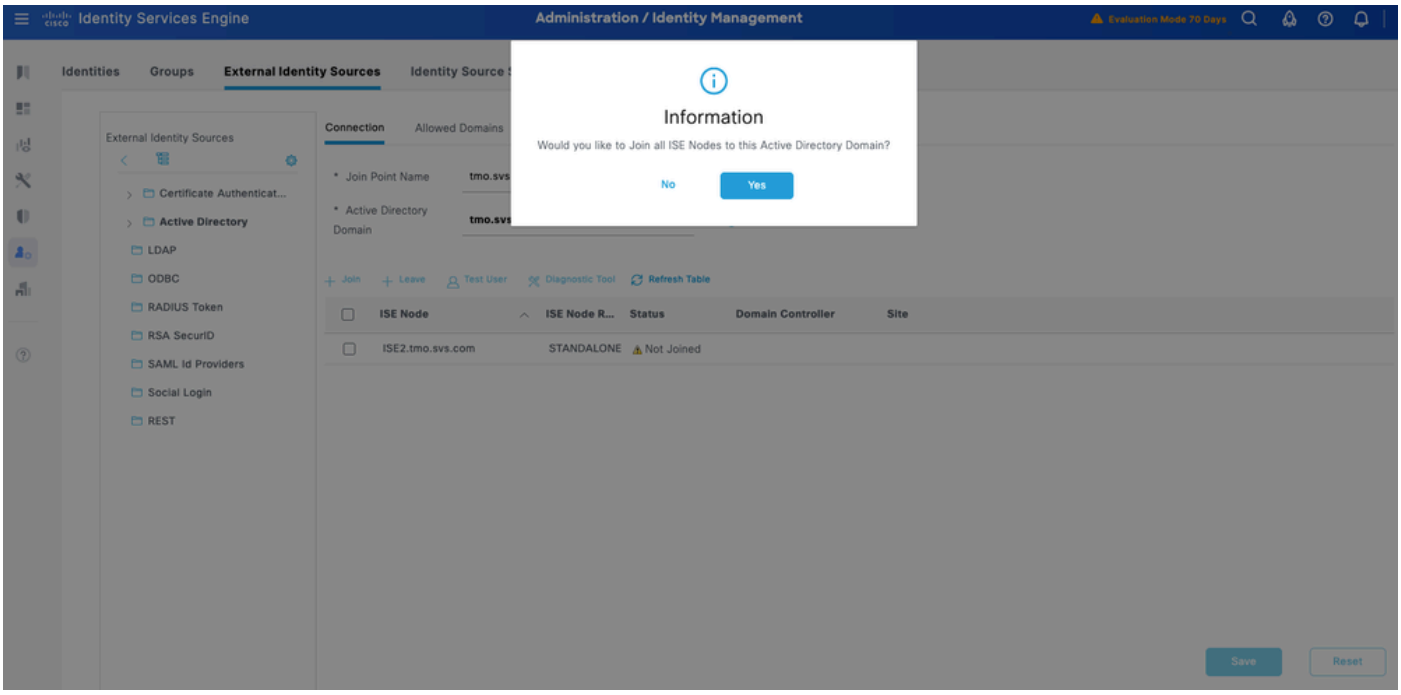
Paso 1. Navegue hasta Administración > Administración de identidad > Almacenes de identidad externos > Active Directory. Haga clic en Agregar para definir un nuevo punto de unión AD.



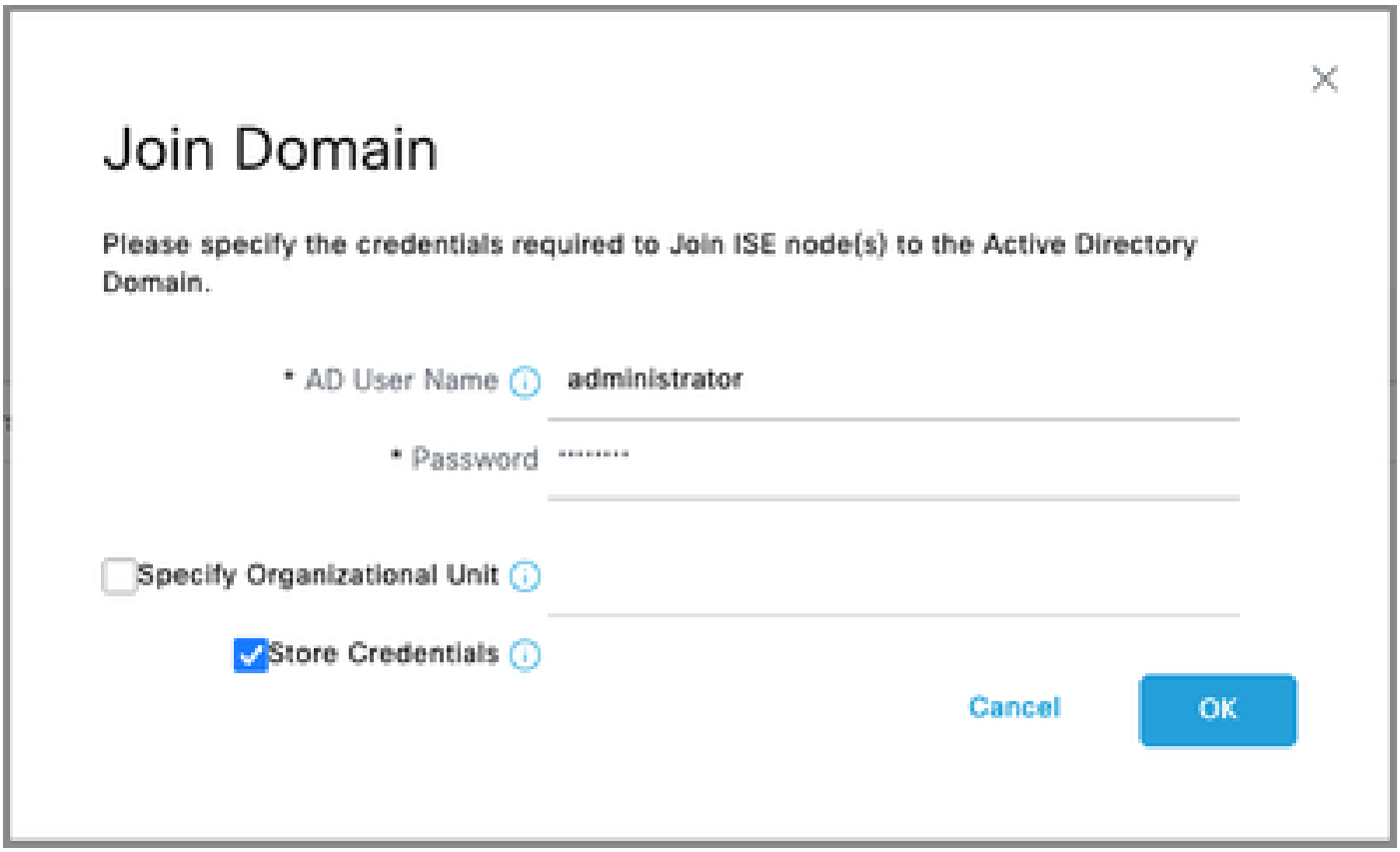
Paso 2. Especifique el nombre del punto de unión y el nombre de dominio AD y haga clic en Enviar.

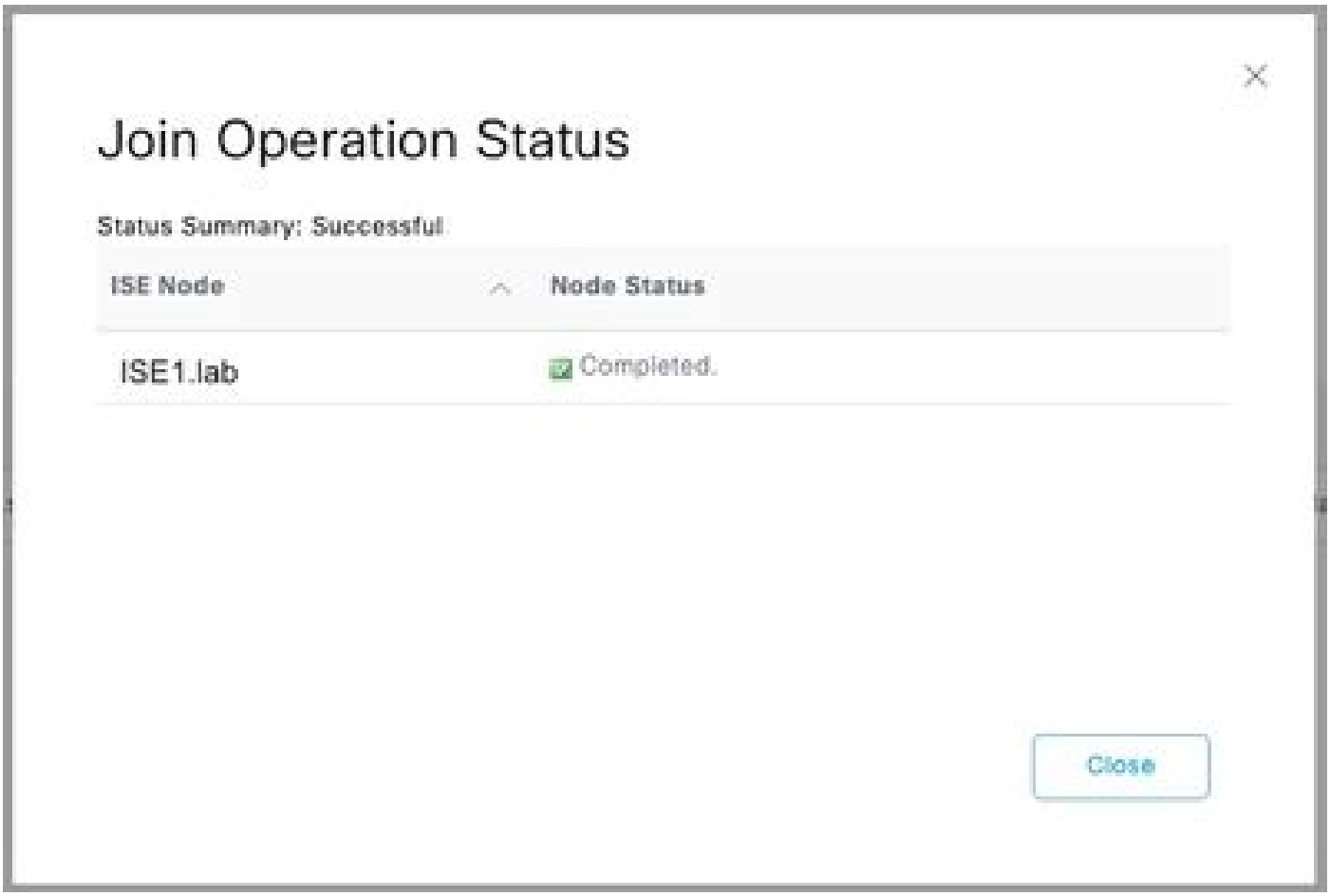


Paso 3. Haga clic en Yes cuando se le pregunte ¿Desea unir todos los nodos ISE a este dominio de Active Directory?

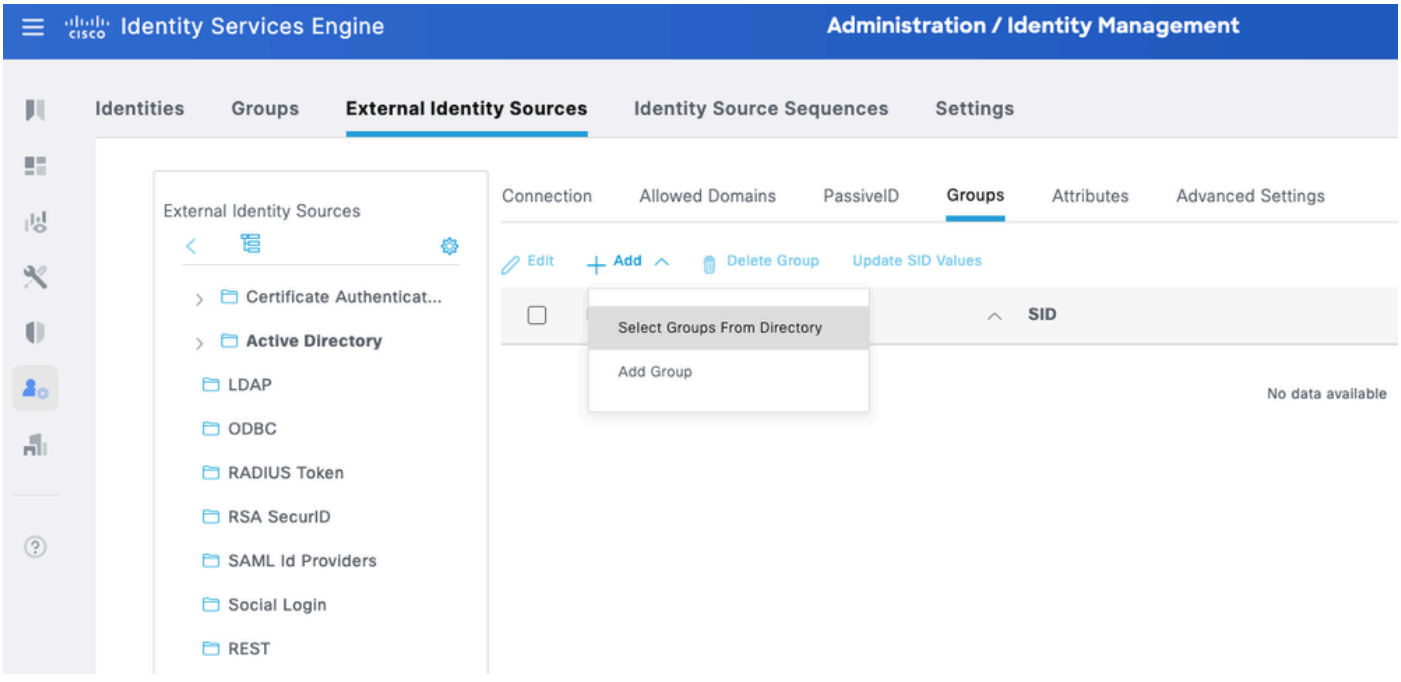


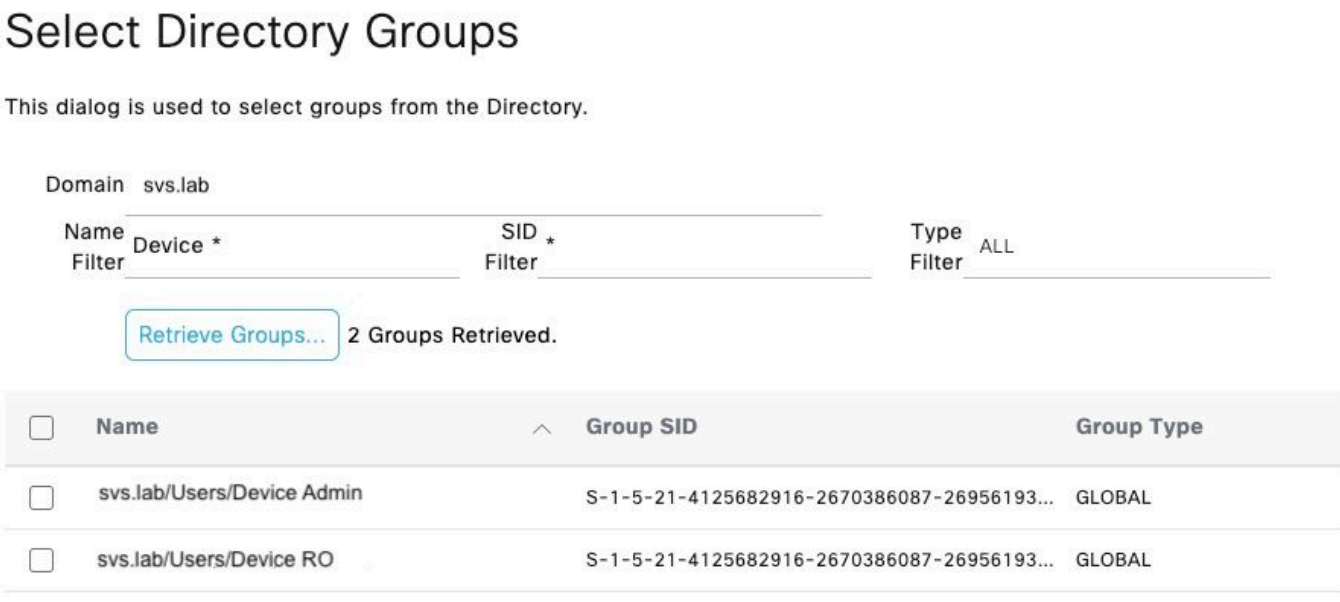
Paso 4. Introduzca las credenciales con privilegios de unión a AD y Unir ISE a AD. Compruebe el estado para verificar que funciona.

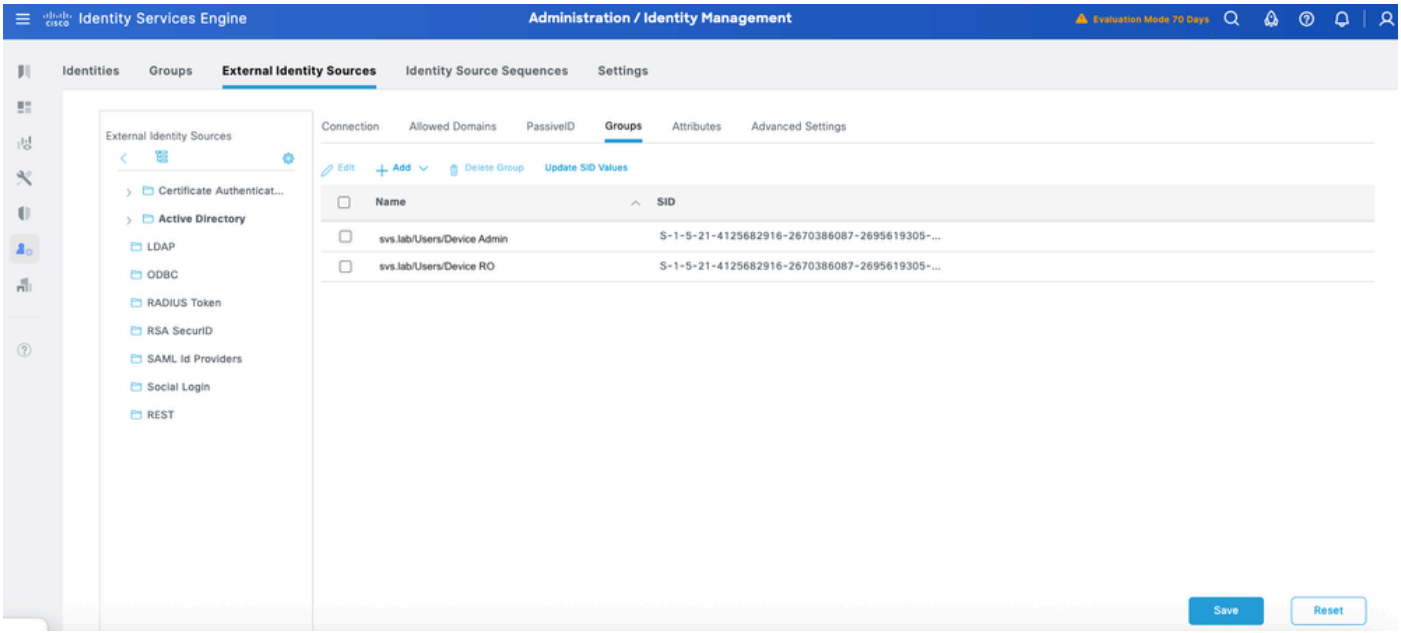




Paso 5. Navegue hasta la pestaña Groups y haga clic en Add para obtener todos los grupos necesarios según los cuales los usuarios están autorizados para el acceso del dispositivo. Este ejemplo muestra los grupos utilizados en la directiva de autorización de esta guía







Configurar perfiles TACACS+

Va a asignar los perfiles TACACS+ a las dos funciones de usuario principales en los dispositivos Cisco IOS XE:

- 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.

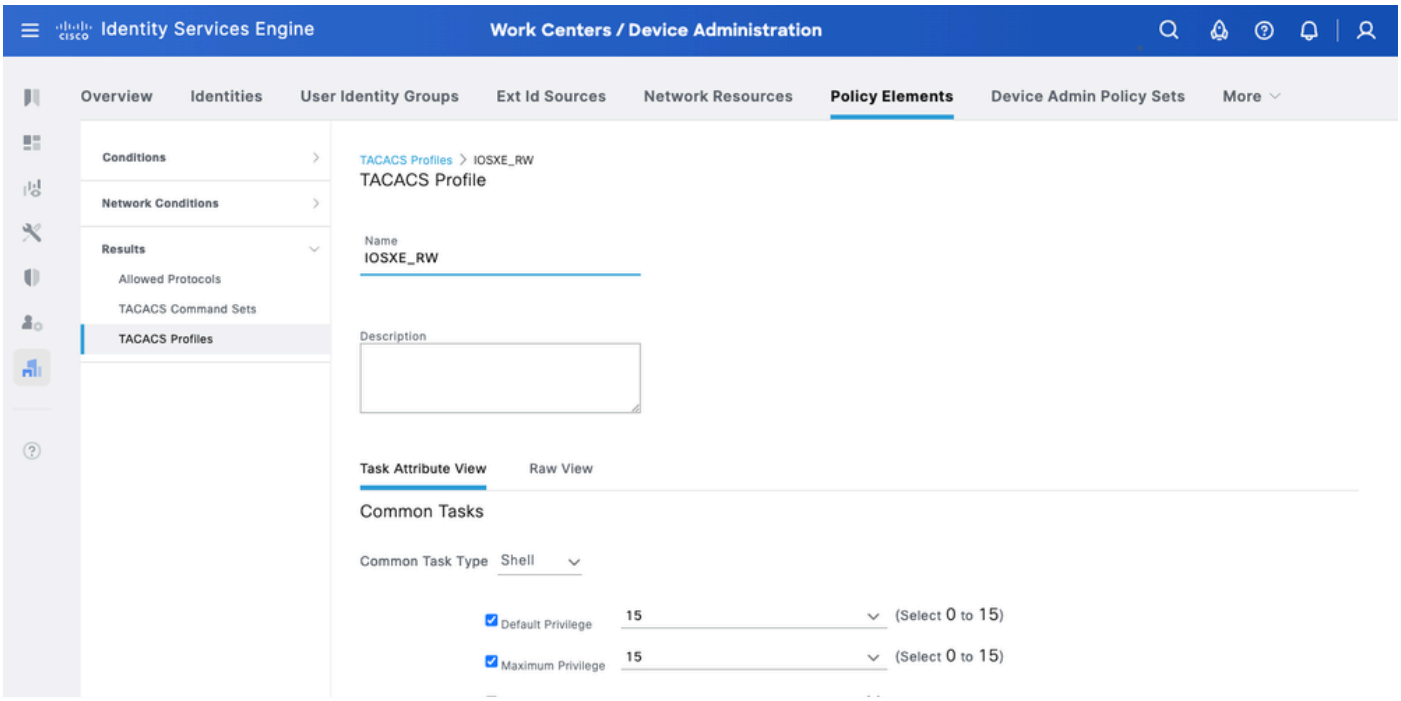
Estos se definen como dos perfiles TACACS+: IOS XE_RW e IOSXR_RO.

IOS XE_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 IOS XE_RW.

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

Paso 3.Confirme la configuración y guarde.

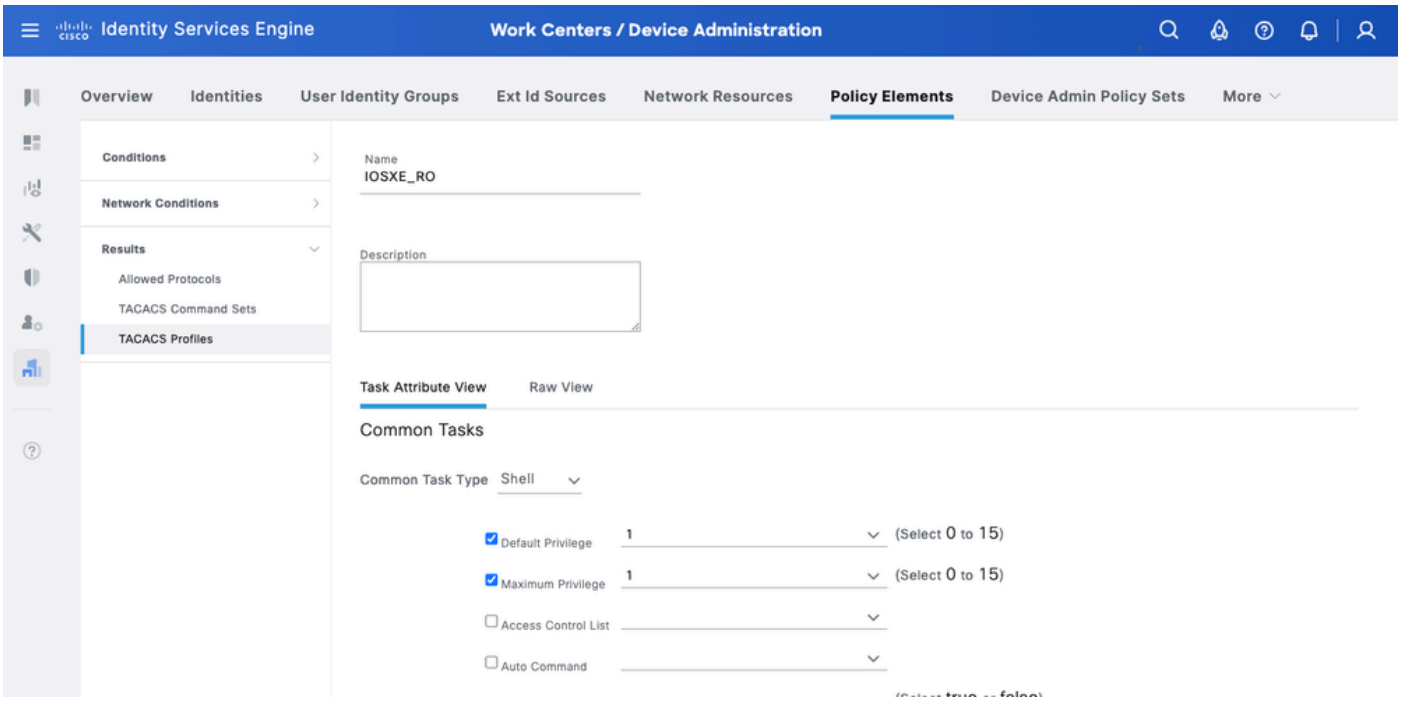


IOS XE_RO: perfil de operador

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

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

Paso 3.Confirme la configuración y guarde.



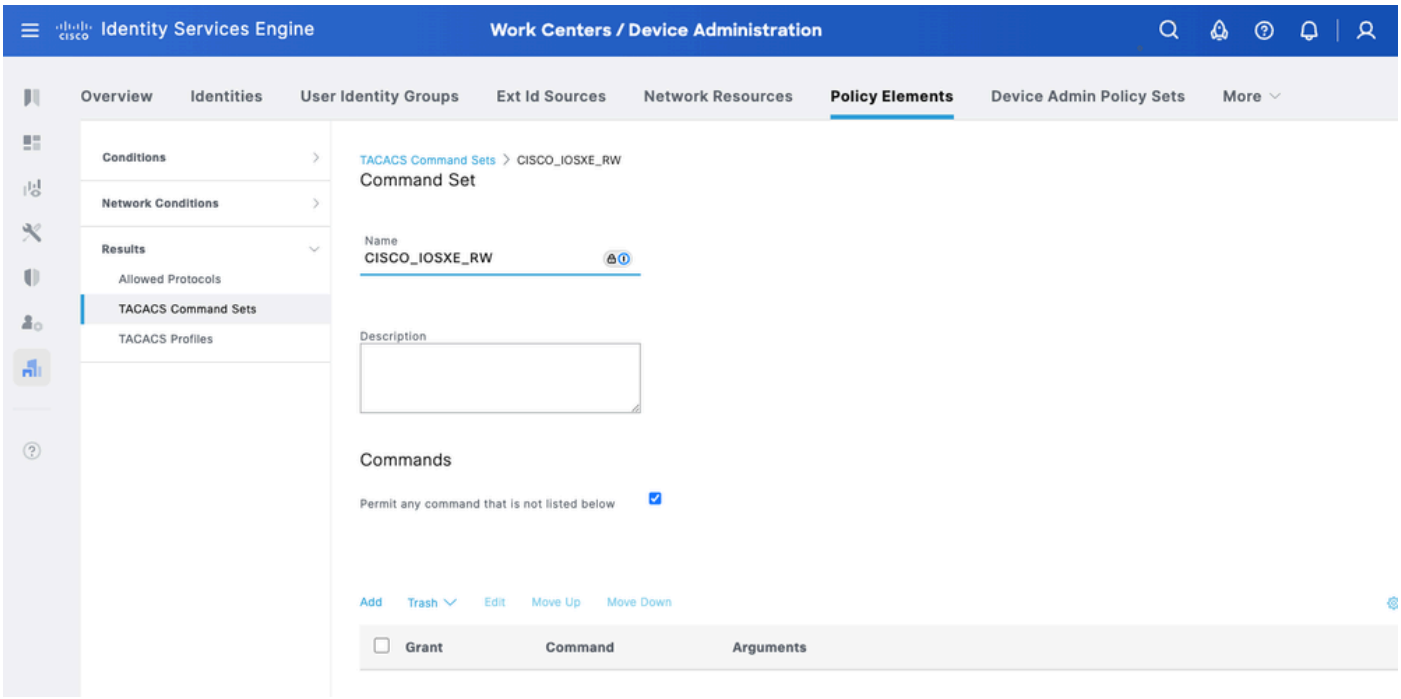
Conjuntos de comandos ConfigureTACACS+

estos se definen como dos conjuntos de comandos TACACS+: CISCO_IOS XE_RW y CISCO_IOS XE_RO.

CISCO_IOS XE_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 Conjunto de Comandos TACACS y denomínelo CISCO_IOS XE_RW.

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



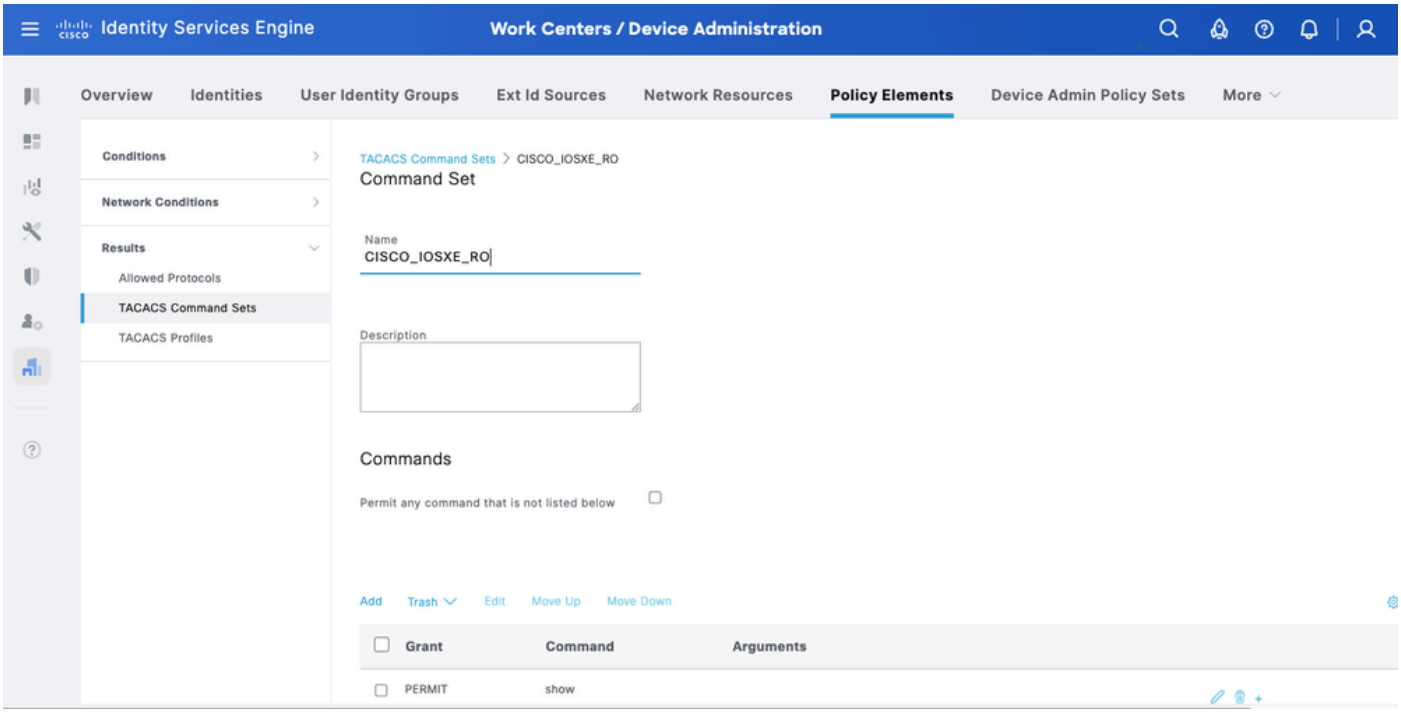
CISCO_IOS XE_RO - Conjunto de comandos del operador

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 denomínelo CISCO_IOS XE_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.

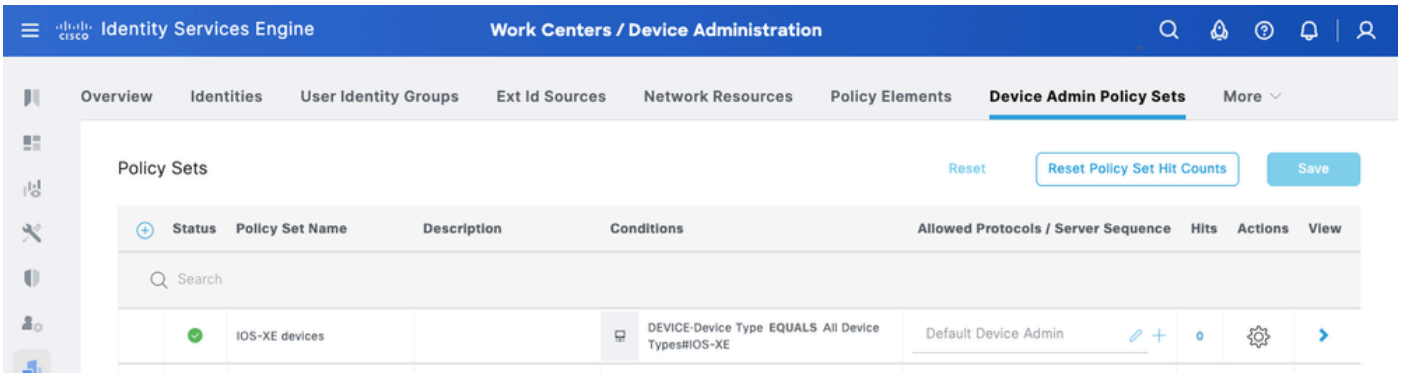
Paso 4. Confirme los datos y haga clic en Guardar.



Configurar conjuntos de políticas de administración de dispositivos

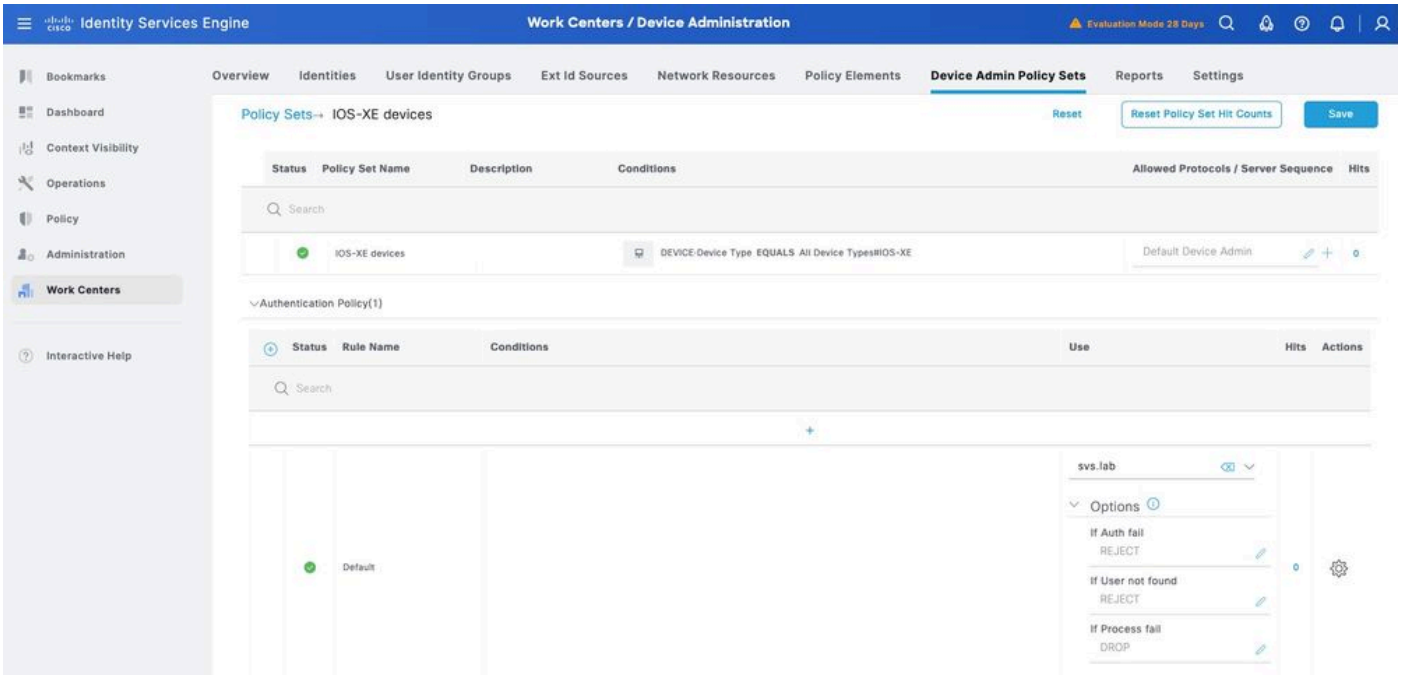
Los conjuntos de directivas están habilitados de forma predeterminada para la administración de dispositivos. Los conjuntos de políticas pueden dividir las políticas según los tipos de dispositivos para facilitar la aplicación de perfiles TACACS.

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 XE. En la condición especifique DEVICE:Device Type EQUALS All Device Types#IOS XE. 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.Crear la política de autenticación. Para la autenticación, se utiliza AD como almacén de ID. Deje las opciones predeterminadas en If Auth fail, If User not found y If Process fail.



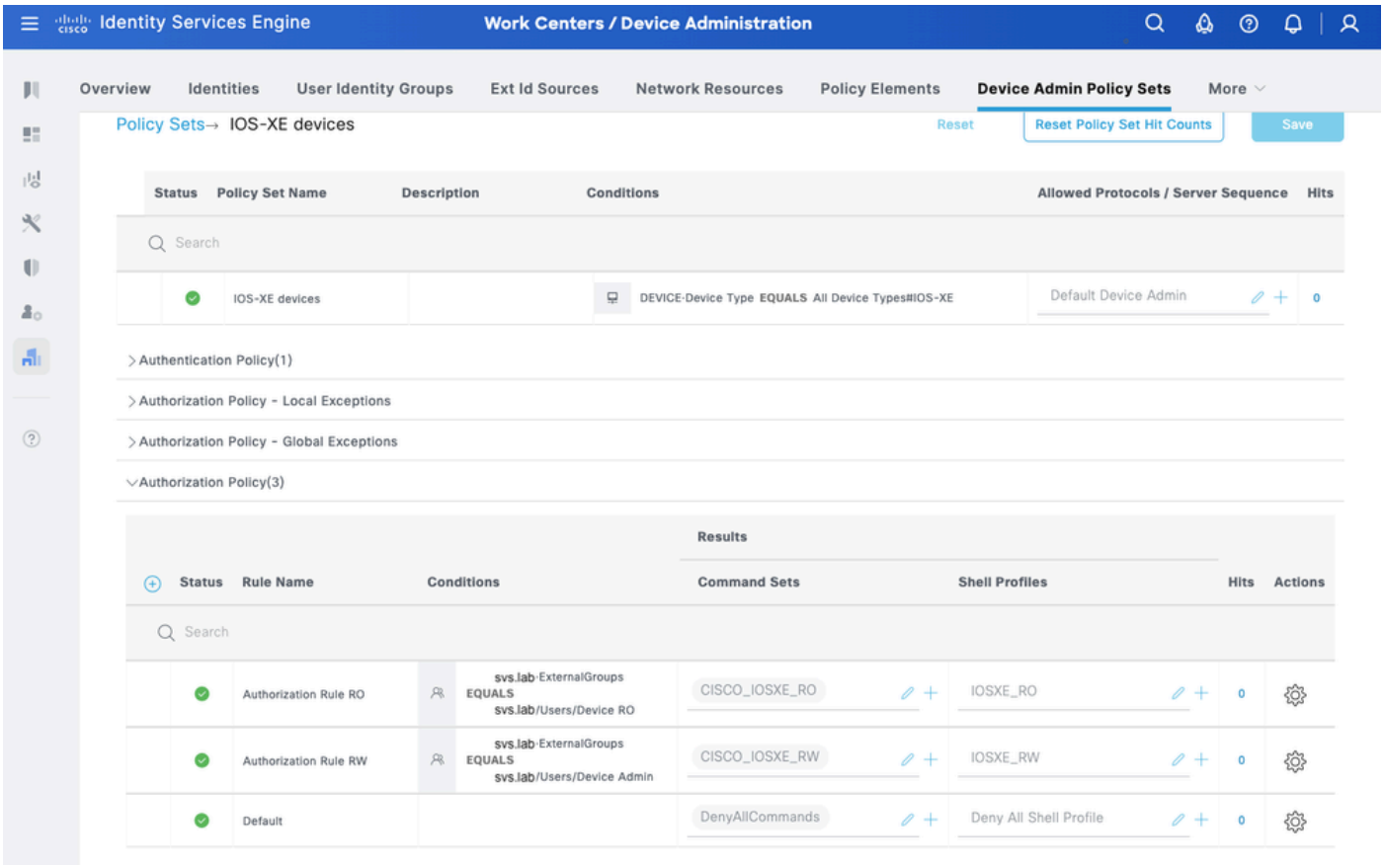
Paso 4. Defina la Política de Autorización.

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

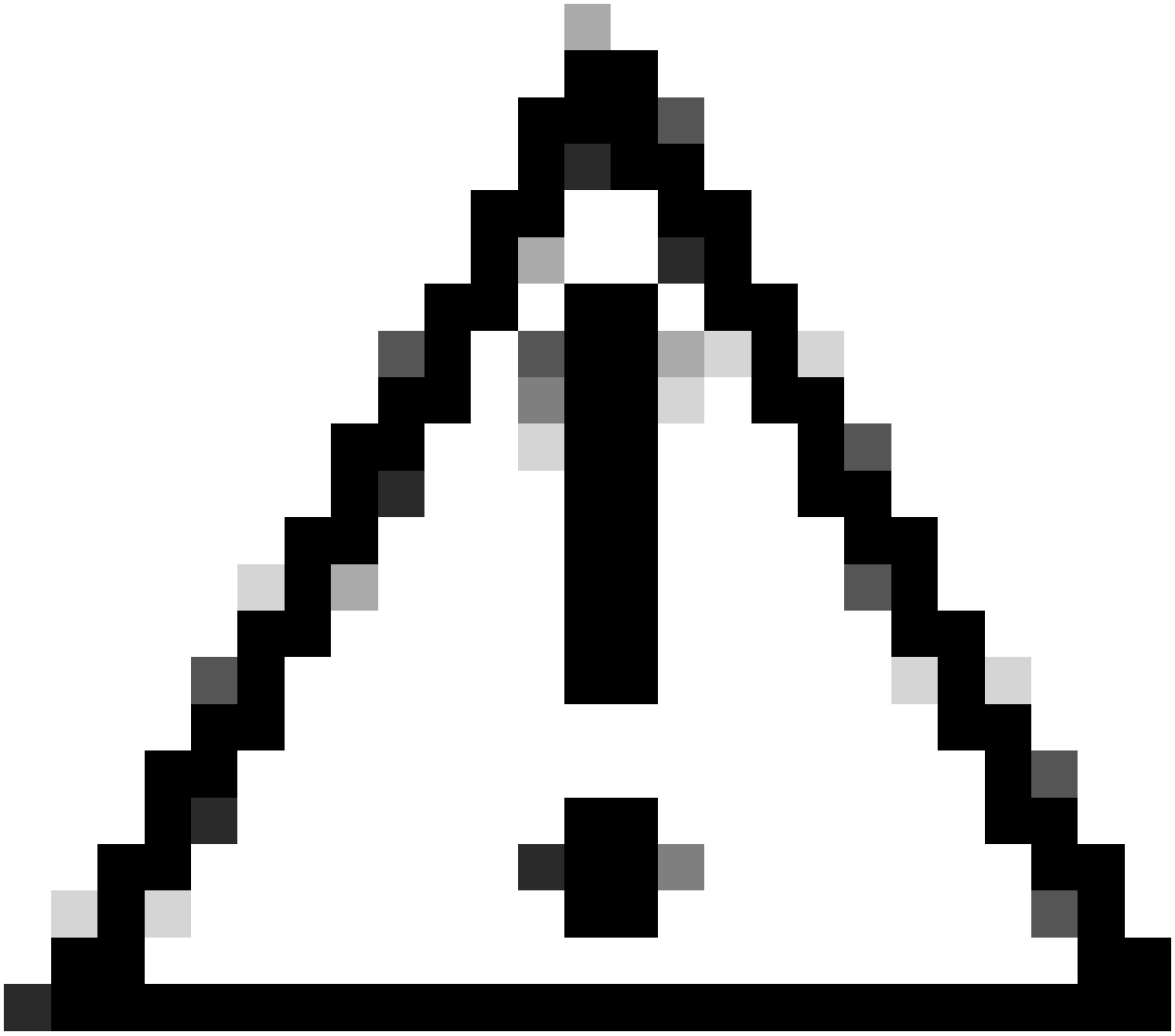
Por ejemplo:

· 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.

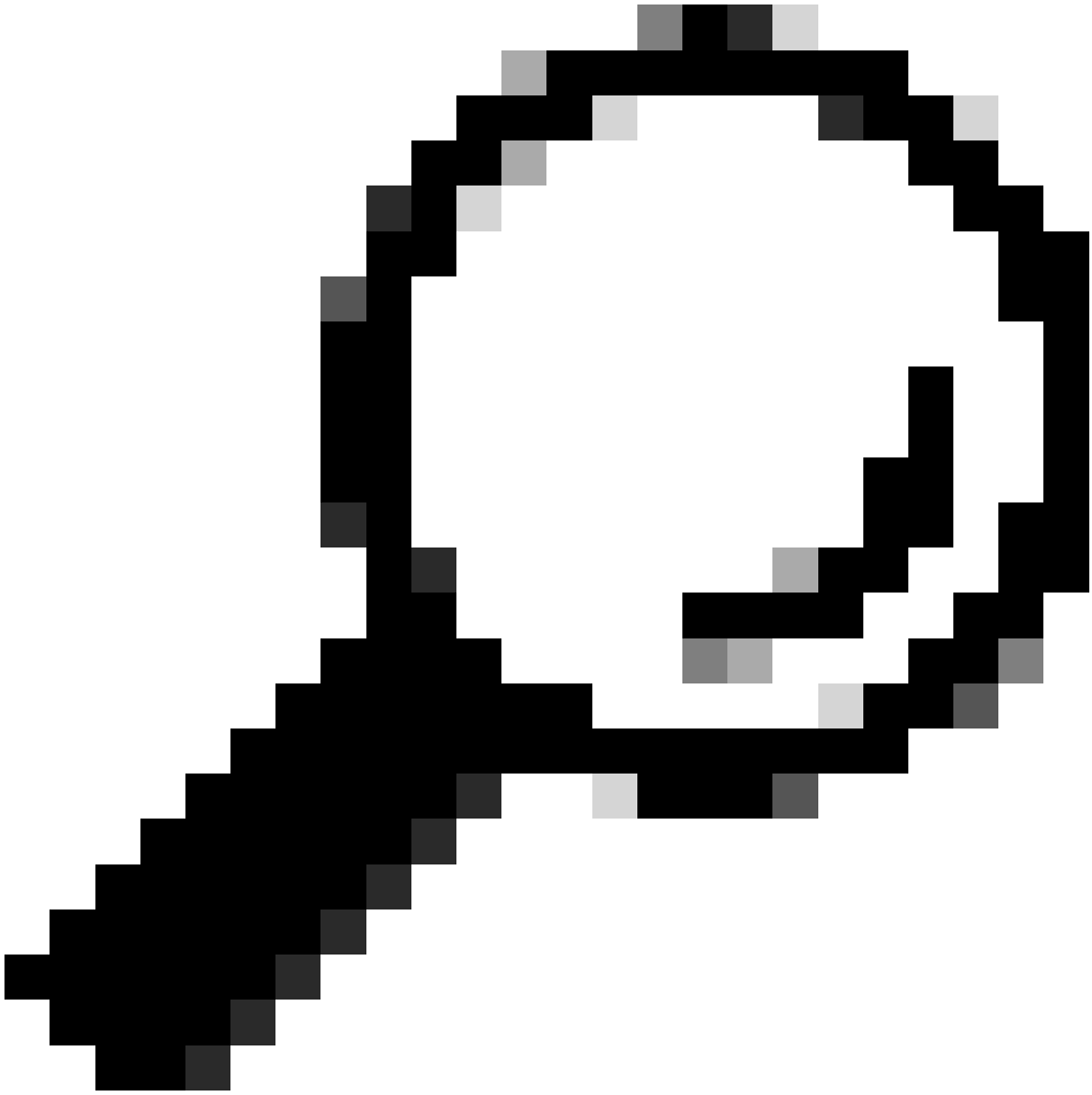
· A los usuarios del grupo AD Device Admin se les asigna el conjunto de comandos CISCO_IOSXR_RW y el perfil de shell IOSXR_RW.



Parte 2 - Configuración de Cisco IOS XE 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.

Método de configuración 1: par de claves generado por el dispositivo

Configuración del servidor TACACS+

Paso 1Configure el nombre de dominio y genere un par de claves utilizado para el punto de confianza del router.

```
ip domain name svs.lab

crypto key generate ec keysize 256 label svs-256ec-key
```

Configuración de Trustpoint

Paso 1 Crear punto de confianza del router y asociar el par de claves.

```
crypto pki trustpoint svs_cat9k
  enrollment terminal pem
  subject-name C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=cat9k.svs.lab
  serial-number none
  ip-address none
  revocation-check none
  eckeypair svs-256ec-key
```

Paso 2. Autentique Trustpoint instalando el certificado de CA.

```
<#root>

cat9k(config)#

crypto pki authenticate svs_cat9k


Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----

MIIFlDCCA3ygAwIBAgIIIM10AsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
QOEwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUGA1UECBMOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBAcTB1JhbGVpZ2gxDjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTVlMxEjAQBgNVBAMTCVNWUyBMYWJDQTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZUOyn2vIn6gKbx3M7vaRq
2YjwZlzSH6EkEvxnJTy+kksiFD33GyHQepk7vfp4NFU5OtQ4HC7t/AOv9grDa3QW
VwvV4MBbJhFM3s0J/ejgDYcMZhIAaPyOZo5WLboOkXEiKjPLatkXojB8FVrhLF3O
jMBSqwa4/Wlniy5S+7s4FFxsCf2OCOWfBAsnrs0tatIIhmcnx+VLJP7MRm8fOw4m
mutNo7IhbJSrgAFXmjlbBjMmgspObULo/wxMHdTbtPBf11HRHTkNIo3qyO4UADL2
WpoGhgT/FaxxBo2UBcnYVaP+jjRE0NYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7BOe8oDNKU6gXlojKyLP/gC7j8AeP03ir+KZui8
```

```
b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
gJ+kQXe7QtT/u6m1MrtjE3gAEVpL334rTIxy9hpKZIkB86t2ZA3JX8CLsbCa13sA
z1XCoONX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTAO1xh6OI4QnK+MNQKpTjt/E4
ydHlOrrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVLl783nTc9wYptQEPi5sw
83g9EMgKVOARIiVUa/qlAgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAYb4
QgEBBAQDAgAHMBkGCWCGSAGG+EIBDQQMFgpTVlMgTGFiIENBMAOGCSqGSIb3DQEB
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
xDrmo7eOXPpSW4l72a6Kl8CR3U2Cr4wsuvndPEq/qd2NRSBWffFOXE/AJHQG7STT
HaXLU9r2Ko6O3oecu8ysGTwLlIt/9T1/FOb0xZRugWcpJrVoTgDGuA==

-----END CERTIFICATE-----

Certificate has the following attributes:
   Fingerprint MD5: D9C4O4B2 EC08A26O EC3539E7 F54ED17D
   Fingerprint SHA1: OEB181E9 5A3ED78O 3BC5A8O5 9A854A95 C83AC737

% Do you accept this certificate? [yes/no]:

yes


Trustpoint CA certificate accepted.
% Certificate successfully imported

cat9k(config)#
```

Paso 3. Generar solicitud de firma de certificado (CSR).

<#root>

```
cat9k(config)#

crypto pki enroll svs_cat9k


% Start certificate enrollment ..

% The subject name in the certificate will include: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=cat9k.svs.lab
% The subject name in the certificate will include: cat9k.svs.lab
Display Certificate Request to terminal? [yes/no]:

yes


Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
MIIBfDCCASMCAQAwgYQxGjAYBgNVBAMTEWNhdDlrLnRtby5zdnMuY29tMQwwCgYD
VQQLEwNTVlMxDjAMBgNVBAoTBUNpc2NvMQwwCgYDVQQHEwNSVFAxCzAJBgNVBAgT
Ak5DMQswCQYDVQQGEwJVUzEgMB4GCSqGSIb3DQEJAhYRY2FOOWsudG1vLnN2cy5j
b2OwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATpYE7atscrtl4ddevCh3UgxjYi
4N4oBGWrpJBctKy4so8V5i6RXDt7kHgPzp14Qnf2ObcXVODE1wtTAHHBrIXqoDww
```

```
OgYJKoZIhvcNAQkOMSOwKzAcBgNVHREEFTATghFjYXQ5ay5ObW8uc3ZzLmNvbTAL
BgNVHQ8EBAMCB4AwCgYIKoZIzj0EAwQDRwAwRAIgZqP2QTwM3ZZrmIphJ7+jSTER
4OkTx2DiVs1c1Xf+vR4CIBcSb18DIYz84DmgMHUaf778/cmpe9cWakvdaxMWseBH
-----END CERTIFICATE REQUEST-----

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]:
```

no

```
cat9k(config)#
```

Paso 4. Importe el certificado firmado por la CA.

<#root>

```
cat9k(config)#
```

crypto pki import svs_cat9k certificate

```
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIID8zCCAdugAwIBAgIIKfdYWg5WpskwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
QOEwHhcNMjUwNTE0MTUxMjAwWhcNMjYwNTE0MTUxMjAwWjCBhDEaMBgGA1UEAxMR
Y2F0OWsudG1vLnN2cy5jb20xDDAKBgNVBAsTA1NWUzEOMAwGA1UEChMFQ2lzY28x
DDAKBgNVBAcTA1JUUDELMAkGA1UECBMCTkMxCzAJBgNVBAYTAlVTMSAwHgYJKoZI
hvcNAQkCFhFjYXQ5ay5ObW8uc3ZzLmNvbTBZMBMGByqGSM49AgEGCCqGSM49AwEH
A0IABOlgTtq2xyu2Xh1168KHdSDGNiLg3igEZaukkFyOrLiyjxXmLpFcO3uQeA/O
nXhCd/bRtxdU4MTXC1MAccGsheqjTTBLMB4GCWCGSAGG+EIBDQQRFg94Y2EgY2Vy
dGlmaWNhdGUwHAYDVR0RBBUwE4IRY2FOOWsudG1vLnN2cy5jb2OwCwYDVR0PBAQD
AgeAMA0GCSqGSIb3DQEBCwUAA4ICAQBObgKVykeyVC9UsvuuOAUsGaZHGwy2H9Yd
m5vIaui6PJczkCzIoAIghHPGQhIgpEcRqtGyXPZ2r8TCJP11WXNN/G73sFyWAhzY
RtmIM5KIojiDHLtifPayxv9juDuOZRx+wYR2PIQ5eLv1bafg7K8E82sqOCfOtcPr
OcONU8UCxqObdOgu4XsdBN1+wcWFqeQSDLmP7nxvhOOm/LXwCWUHwgVioOAuU2Fe
k5NthtvdxNAhRAImQdTyq6u/yB7vwTwJHcRiJc5USsyzCsTBb6RvL+HsXqBgXGc5
lxCSoLtYOdUxFIpJyK2MOZBY2zq2cNSc8Xbso5/OEQmnHtpWPvij4rSPUhQSY+4m
Qq2Sn3iqf4mGh/AO8T4iXfWDWfNezh7ZxMsCSCK/ZRlELZ2hj6OfzwX1H27Uf8XU
ecrOWx+WzRn7LVRCaGQzFkukfi8S4DLLNtxnNHfsLBVX5yHXCLEL+CQ7n8Z/pxcB
VVrPitwN3ZbO9poZyWiRLTnBsb42xNaWiL9bjQznAOiTDfmfFFourBsaAioz7ouY
2r1Mh+OpE83Uu+4lOTMawDgGiEv7iaiJ6xWc95EC+AdmOx3FvBXMtIM9qr7WwHW6
3C2hVYHJH254elV5+H8iiz7rovEPm8ZDsnvYpJn4Km3iDvBNqp/vvAHOFcyXrvG6
3i/1b9erGQ==
-----END CERTIFICATE-----

% Router Certificate successfully imported

cat9k(config)#
```

TACACS y AAA con configuración de TLS

Paso 1. Crear servidor TACACS y grupos AAA, asociar el punto de confianza del cliente (router).

```
tacacs server svs_tacacs
 address ipv4 10.225.253.209
 single-connection
 tls port 6049
 tls idle-timeout 60
 tls connection-timeout 60
 tls trustpoint client svs_cat9k
 tls ip tacacs source-interface GigabitEthernet0/0
 tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ svs_tls
 server name svs_tacacs
 ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request
```

Paso 2. Configure los métodos AAA.

```
aaa authentication login default group svs_tls local enable
aaa authentication login console local enable
aaa authentication enable default group svs_tls enable
aaa authorization config-commands
aaa authorization exec default group svs_tls local if-authenticated
aaa authorization commands 1 default group svs_tls local if-authenticated
aaa authorization commands 15 default group svs_tls
aaa accounting exec default start-stop group svs_tls
aaa accounting commands 1 default start-stop group svs_tls
aaa accounting commands 15 default start-stop group svs_tls
aaa session-id common
```

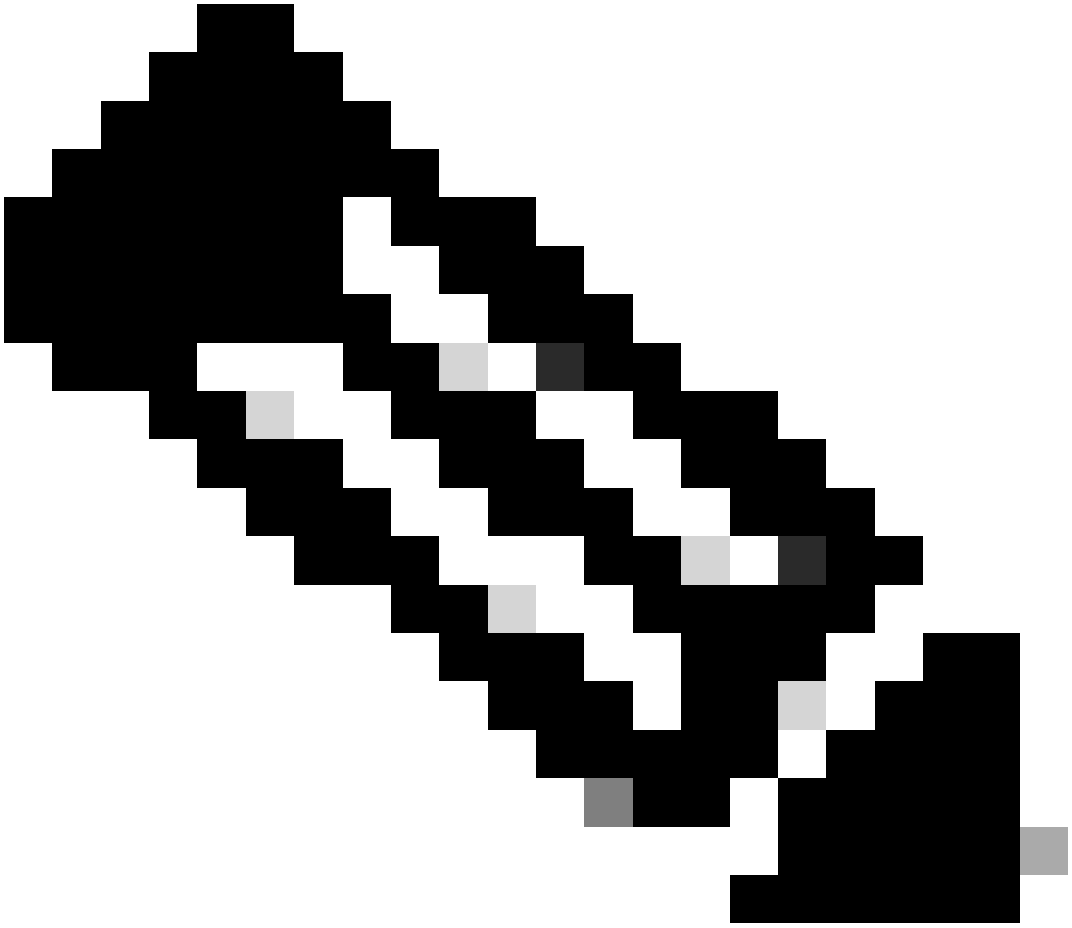
Método de configuración 2: par de claves generado por CA

Si va a importar las claves, así como los certificados de dispositivo y CA directamente en un formato PKCS#12 en lugar del método CSR, puede utilizar este método.

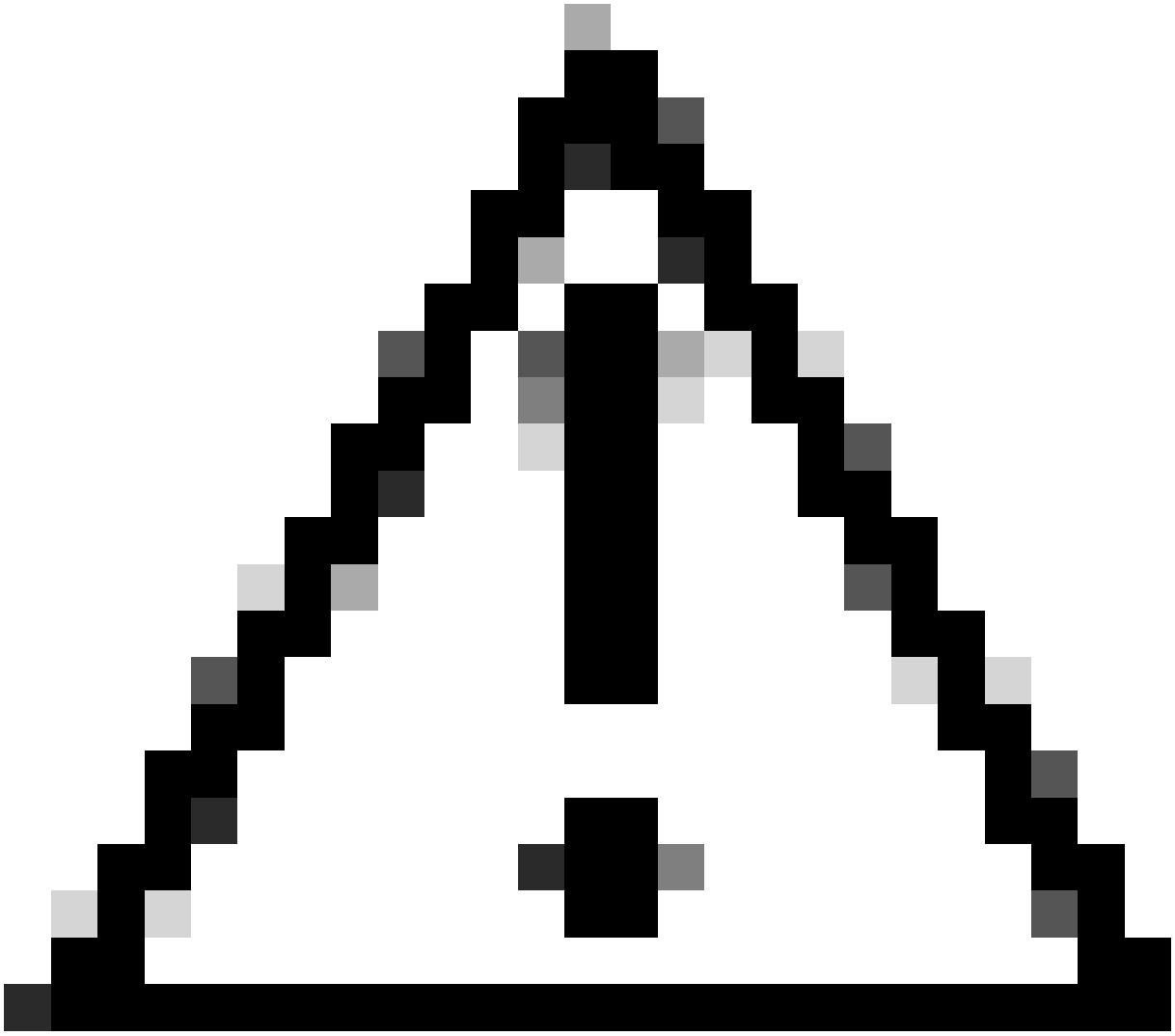
Paso 1. Crear punto de confianza de cliente.

```
cat9k(config)#crypto pki trustpoint svs_cat9k_25jun17
cat9k(ca-trustpoint)#revocation-check none
```

Paso 2. Copie el archivo PKCS#12 en bootflash.



Nota: Asegúrese de que el archivo PKCS#12 contenga la cadena de certificados completa y la clave privada como archivo cifrado.



Precaución: Las claves en el PKCS#12 importado deben ser de RSA (por ejemplo: RSA 2048), no ECC.

<#root>

cat9k#

copy sftp bootflash: vrf Mgmt-vrf

```
Address or name of remote host [10.225.253.247]?
Source username [svs-user]?
Source filename [cat9k.svs.lab.pfx]? /home/svs-user/upload/cat9k-25jun17.pfx
Destination filename [cat9k-25jun17.pfx]?
Password:
!
2960 bytes copied in 3.022 secs (979 bytes/sec)
```

Paso 3. Importe el archivo PKCS#12 mediante el comando import.

<#root>

```
cat9k#

crypto pki import svs_cat9k_25jun17 pkcs12 bootflash:cat9k-25jun17.pfx

 password C1sco.123
% Importing pkcs12...Reading file from bootflash:cat9k-25jun17.pfx
CRYPTO_PKI: Imported PKCS12 file successfully.
cat9k#

cat9k#

show crypto pki certificates svs_cat9k_25jun17


Certificate
  Status: Available
  Certificate Serial Number (hex): 586OBF33A2O33365
  Certificate Usage: General Purpose
  Issuer:
    cn=SVS LabCA
    ou=SVS
    o=Cisco
    l=Raleigh
    st=North Carolina
    c=US
  Subject:
    Name: cat9k.svs.lab
    e=pkalkur@cisco.com
    cn=cat9k.svs.lab
    ou=svs
    o=cisco
    l=rtp
    st=nc
    c=us
  Validity Date:
    start date: 17:56:00 UTC Jun 17 2025
    end   date: 17:56:00 UTC Jun 17 2026
  Associated Trustpoints: svs_cat9k_25jun17

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 2OCD74O2C4DA37F5
  Certificate Usage: General Purpose
  Issuer:
    cn=SVS LabCA
    ou=SVS
    o=Cisco
    l=Raleigh
    st=North Carolina
    c=US
  Subject:
    cn=SVS LabCA
    ou=SVS
    o=Cisco
    l=Raleigh
    st=North Carolina
    c=US
  Validity Date:
    start date: 17:05:00 UTC Apr 28 2025
    end   date: 17:05:00 UTC Apr 28 2035
  Associated Trustpoints: svs_cat9k_25jun17 svs_cat9k
```

```
  Storage: nvram:SVSLabCA#37F5CA.cer
```

TACACS y AAA con configuración de TLS

Paso 1. Crear servidor TACACS y grupos AAA, asociar el punto de confianza del cliente (router).

```
tacacs server svs_tacacs
 address ipv4 10.225.253.209
 single-connection
 tls port 6049
 tls idle-timeout 60
 tls connection-timeout 60
 tls trustpoint client svs_cat9k
 tls ip tacacs source-interface GigabitEthernet0/0
 tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ svs_tls
 server name svs_tacacs
 ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request
```

Paso 2. Configure los métodos AAA.

```
aaa authentication login default group svs_tls local enable
aaa authentication login console local enable
aaa authentication enable default group svs_tls enable
aaa authorization config-commands
aaa authorization exec default group svs_tls local if-authenticated
aaa authorization commands 1 default group svs_tls local if-authenticated
aaa authorization commands 15 default group svs_tls
aaa accounting exec default start-stop group svs_tls
aaa accounting commands 1 default start-stop group svs_tls
aaa accounting commands 15 default start-stop group svs_tls
aaa session-id common
```

Verificación

Verifique la Configuración.

```
show tacacs
show crypto pki certificates <>
show crypto pki trustpoints <>
```

Depuración para AAA y TACACS+.

```
debug aaa authentication
debug aaa authorization
debug aaa accounting
debug aaa subsys
debug aaa protocol local
debug tacacs authentication
debug tacacs authorization
debug tacacs accounting
debug tacacs events
debug tacacs packet
debug tacacs
debug tacacs secure

! Below debugs will be needed only if there is any issue with SSL Handshake
debug ip tcp transactions
debug ip tcp packet
debug crypto pki transactions
debug crypto pki API
debug crypto pki messages
debug crypto pki server
debug ssl openssl errors
debug ssl openssl msg
debug ssl openssl states
clear logging
```

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).