

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

Contenido

[Introducción](#)

[Overview](#)

[Utilización de esta guía](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Licencias](#)

[Parte 1: Configuración de ISE para la administración de dispositivos](#)

[Generar solicitud de firma de certificado para autenticación de servidor TACACS+](#)

[Cargar certificado de CA raíz para autenticación de servidor TACACS+](#)

[Enlazar la solicitud de firma de certificado \(CSR\) firmado a ISE](#)

[Habilitar TLS 1.3](#)

[Habilitar Device Administration en ISE](#)

[Habilitar TACACS sobre TLS](#)

[Crear dispositivos de red y grupos de dispositivos de red](#)

[Configurar almacenes de identidad](#)

[Configurar perfiles TACACS+](#)

[IOS XR RW - Perfil del administrador](#)

[IOS XR RO: perfil de operador](#)

[Conjuntos de comandos ConfigureTACACS+](#)

[CISCO IOS XR RW - Conjunto de comandos del administrador](#)

[CISCO IOS XR RO - Conjunto de comandos del operador](#)

[Configurar conjuntos de políticas de administración de dispositivos](#)

[Parte 2 - Configuración de Cisco IOS XR para TACACS+ sobre TLS 1.3](#)

[Configuraciones iniciales](#)

[Configurar Trustpoint](#)

[Configuración de TACACS y AAA con TLS](#)

[Renovación de certificados](#)

[Verificación](#)

[Resolución de problemas](#)

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 a Administración > Sistema > Certificados.



Administration

System

Identity Management

Deployment

Identities

Licensing

Groups

Certificates

External Identity So

Logging

Identity Source Seq

Maintenance

Settings

Upgrade & Rollback

Health Checks

Feed Service

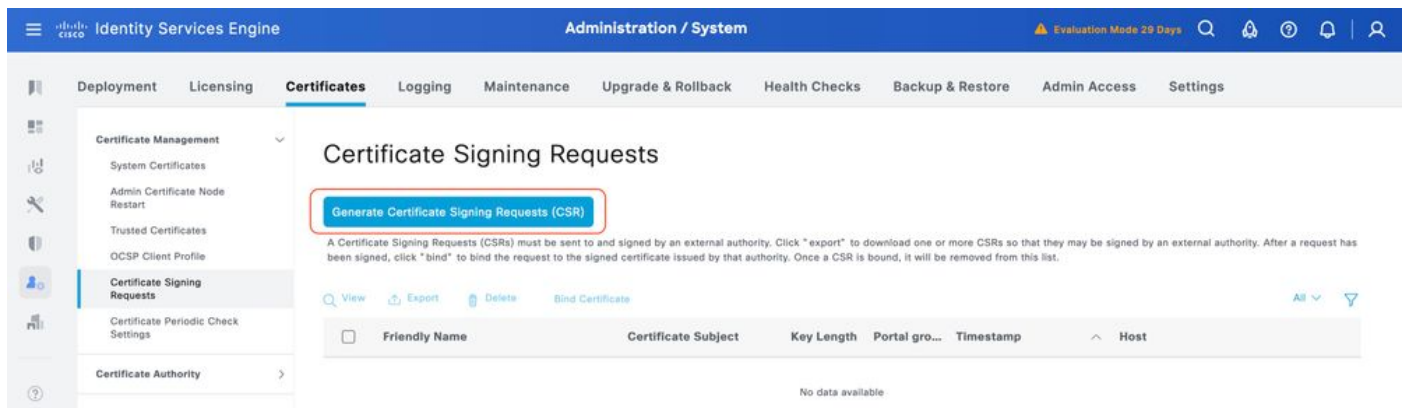
Backup & Restore

Profil

Admin Access

Settings

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



Paso 4. Seleccione TACACS en Usage.

Usage

Certificate(s) will be used for **TACACS** ▼

Allow Wildcard Certificates ☐ ?

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

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☒ ISE1	ISE1#TACACS

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

Subject

Common Name (CN)
\$FQDN\$



Organizational Unit (OU)
CX



Organization (O)
Cisco



City (L)
Raleigh

State (ST)
North Carolina

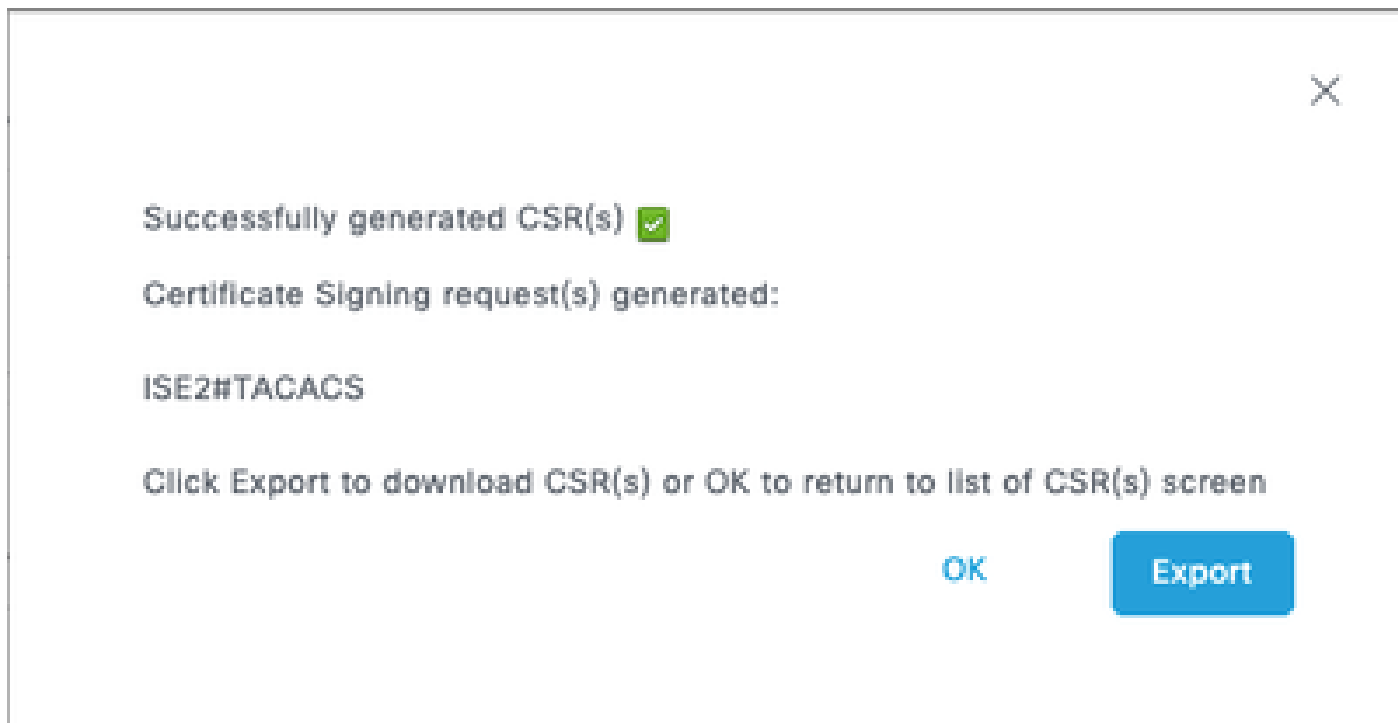
Country (C)
US

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

Subject Alternative Name (SAN)

⋮	DNS Name	✓	ISE1.lab	—	+	
⋮	IP Address	✓	10.225.253.209	—	+	①

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 a Administración > Sistema > Certificados. En Certificados de confianza, haga clic en Importar.

☐	Friendly Name	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Status
☐	Amazon root CA	Infrastructure Cisco Services	06 6C 9F CF ...	Amazon Root CA 1	Amazon Root CA 1	Tue, 26 May 2015	Sun, 17 Jan 2...	En...
☐	Cisco ECC Root CA 2099	Cisco Services	03	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Mon, 7 Sep 2...	En...
☐	Cisco Licensing Root CA	Cisco Services	01	Cisco Licensing R...	Cisco Licensing R...	Thu, 30 May 2013	Sun, 30 May 2...	En...
☐	Cisco Manufacturing CA SHA2	Endpoints Infrastructure	02	Cisco Manufactur...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2...	En...
☐	Cisco Root CA 2048	Endpoints Infrastructure	5F F8 7B 28 2...	Cisco Root CA 20...	Cisco Root CA 20...	Fri, 14 May 2004	Mon, 14 May ...	Dis...
☐	Cisco Root CA 2099	Cisco Services	01 9A 33 58 7...	Cisco Root CA 20...	Cisco Root CA 20...	Tue, 9 Aug 2016	Sun, 9 Aug 20...	En...
☐	Cisco Root CA M1	Cisco Services	2E D2 0E 73 4...	Cisco Root CA M1	Cisco Root CA M1	Tue, 18 Nov 2008	Fri, 18 Nov 20...	En...
☐	Cisco Root CA M2	Infrastructure Endpoints	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2...	En...
☐	Cisco RXC-R2	Cisco Services	01	Cisco RXC-R2	Cisco RXC-R2	Wed, 9 Jul 2014	Sun, 9 Jul 2034	En...

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.

Import a new Certificate into the Certificate Store

* Certificate File ISE SVSLab CA.crt

Friendly Name

Trusted For: ☐

- ☒ Trust for authentication within ISE
 - ☐ Trust for client authentication and Syslog
 - ☐ Trust for certificate based admin authentication
- ☐ Trust for authentication of Cisco Services
- ☐ Trust for Native IPSec certificate based authentication
- ☐ Validate Certificate Extensions

Description

Submit

Cancel

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

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System page. The left sidebar contains navigation links: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (selected), and Work Centers. The main content area is titled "Trusted Certificates" and includes a warning: "For disaster recovery it is recommended to export and backup all your trusted certificates." Below this is a table with columns: Friendly Name, Trusted For, Serial Number, Issued To, Issued By, Valid From, Expiration Date, and Status. One certificate is listed with the Friendly Name "CN=SVS LabCA, OU=SVS, O=Cisco, L=..." and a status of "Valid".

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.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System page, specifically the "Certificate Signing Requests" section. The left sidebar is the same as the previous screenshot. The main content area is titled "Certificate Signing Requests" and includes a button "Generate Certificate Signing Requests (CSR)". Below this is a text block explaining that CSR requests must be sent to and signed by an external authority. At the bottom, there is a table with columns: Friendly Name, Certificate Subject, Key Length, Portal gro..., Timestamp, and Host. A "Bind Certificate" button is highlighted in the top right corner of the table area.

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

Identity Services Engine Administration / System Evaluation Mode 29 Days

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Admin Certificate Node Restart
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests**
- Certificate Periodic Check Settings
- Certificate Authority

Bind CA Signed Certificate

* Certificate File ISE1.lab.crt

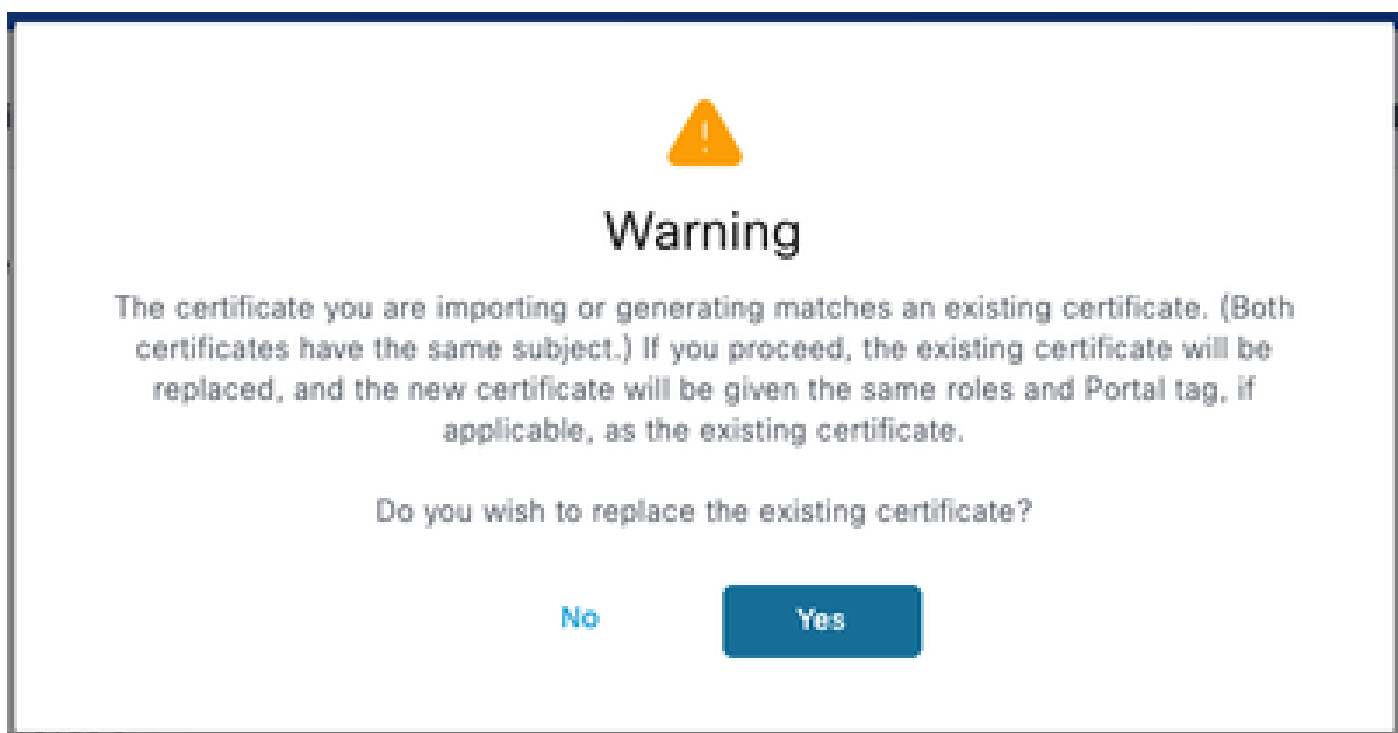
Friendly Name

Validate Certificate Extensions ☐

Usage

☒ TACACS: Use certificate for TACACS Server

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.

Identity Services Engine Administration / System Evaluation Mode 29 Days

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates**
- Admin Certificate Node Restart
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Settings
- Certificate Authority

System Certificates

For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

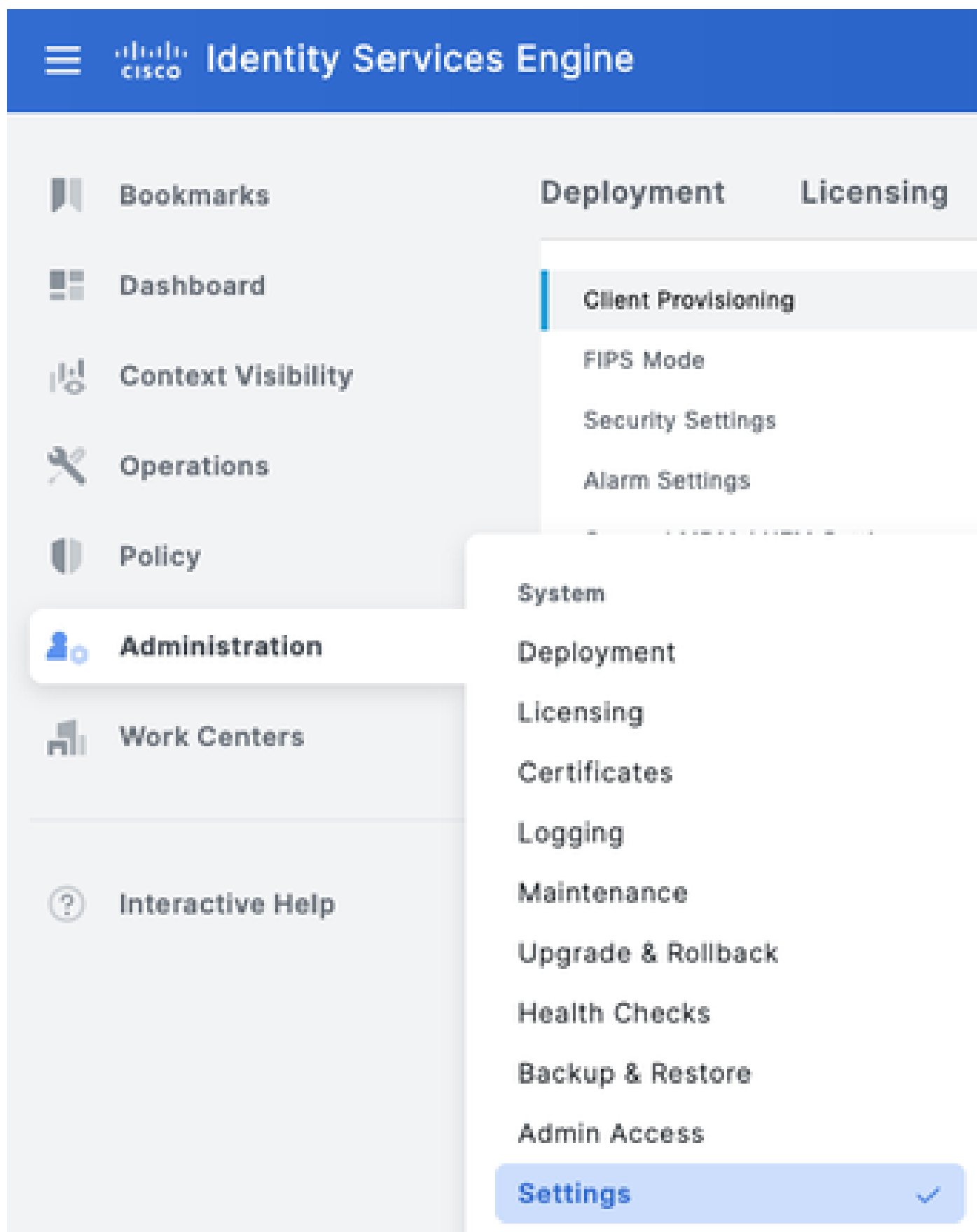
[Edit](#) [+ Generate Self Signed Certificate](#) [+ Import](#) [Export](#) [Delete](#) [View](#)

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
ISE1							
C=US, ST=NC, L=Raleigh, O=Cisco, OU=SVS, CN=I SE1.lab#ISE1.lab#00010	TACACS		ISE1.lab	ISE1.lab	Wed, 10 Sep 2025	Fri, 10 Sep 2027	■ Active

Habilitar TLS 1.3

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

Paso 1. Vaya a Administración > Sistema > Configuración.



The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The left sidebar contains the following menu items: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (selected), Work Centers, and Interactive Help. The main content area shows the 'Deployment' tab, which is expanded to reveal a list of configuration options: Client Provisioning, FIPS Mode, Security Settings, Alarm Settings, System, Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade & Rollback, Health Checks, Backup & Restore, Admin Access, and Settings (highlighted with a blue background and a checkmark).

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.

Client Provisioning

FIPS Mode

Security Settings

Alarm Settings

General MDM / UEM Settings

Posture

Profiling

Protocols

Security Settings

Choose the security settings you want to enable to ensure safe communications across your network.

TLS Versions Settings

TLS 1.2 is enabled by default and can't be deselected. Choose one or a range of consecutive TLS versions.

☐ TLS 1.0

☐ TLS 1.1

☒ TLS 1.2

☒ TLS 1.3

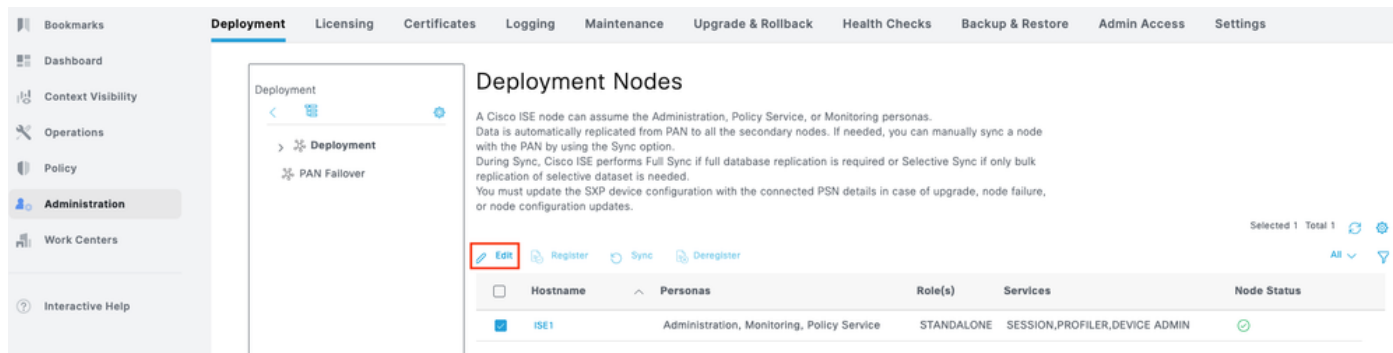


Advertencia: Al cambiar la versión de TLS, el servidor de aplicaciones de Cisco ISE se reinicia en todos los equipos de implementación de Cisco ISE.

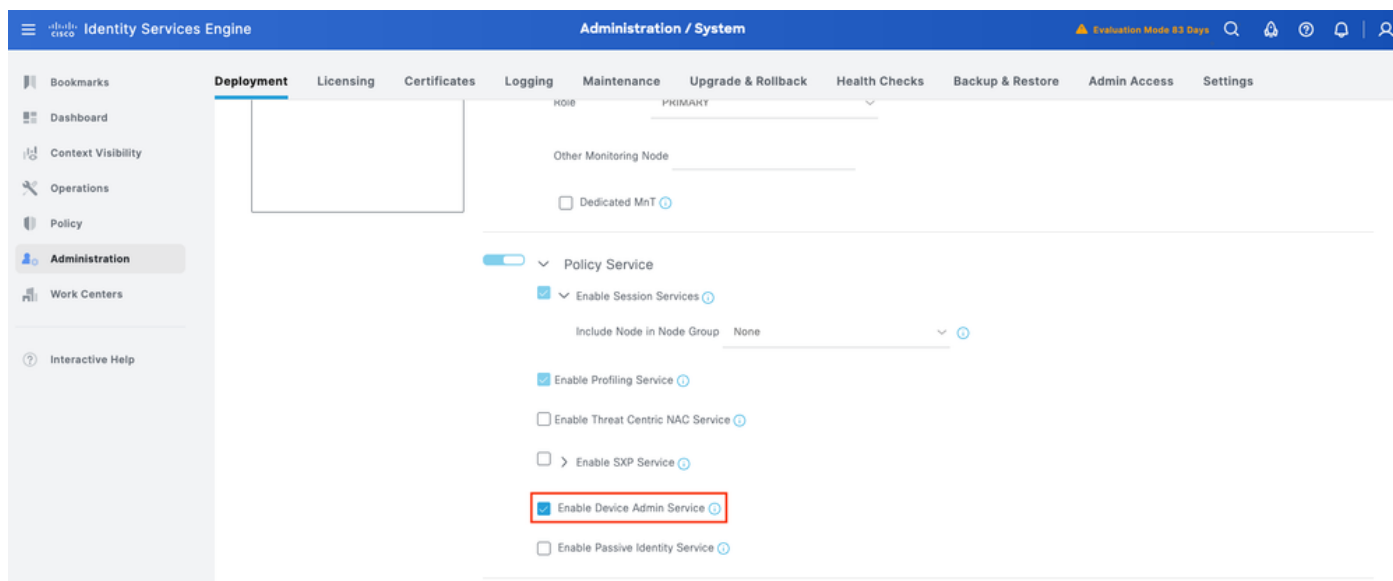
Habilitar Device Administration en ISE

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.



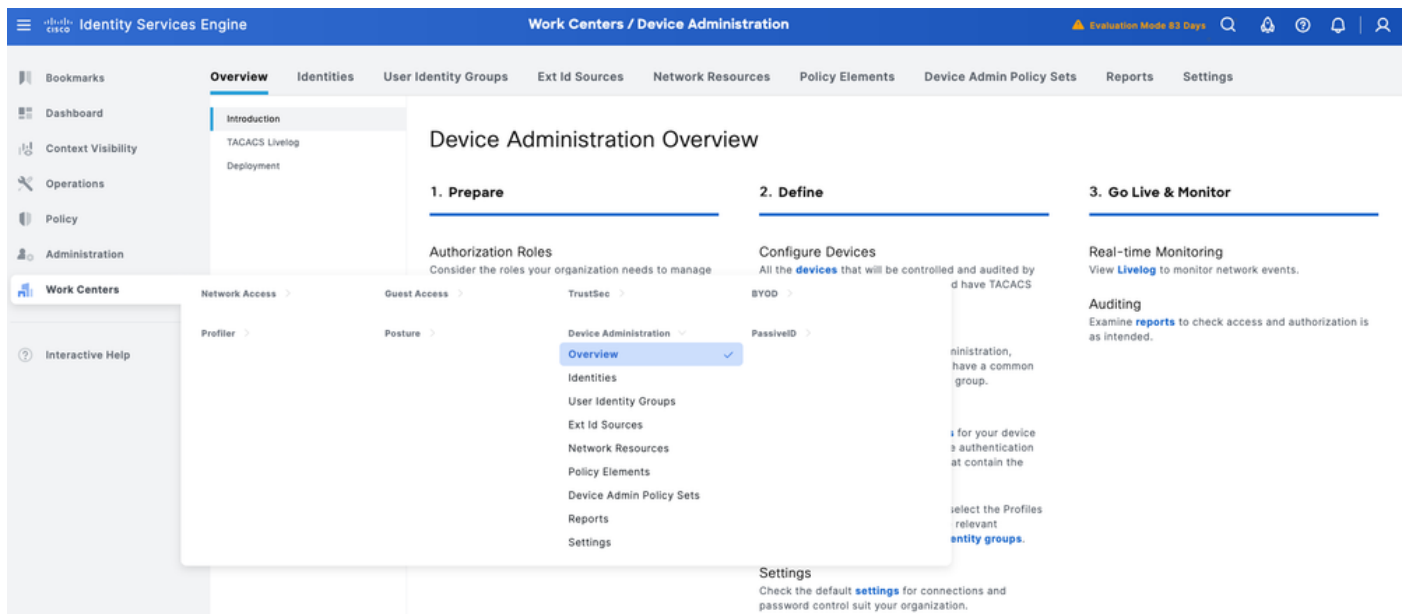
Paso 2. En General Settings, desplácese hacia abajo y seleccione la casilla de verificación junto a Enable Device Admin Service.



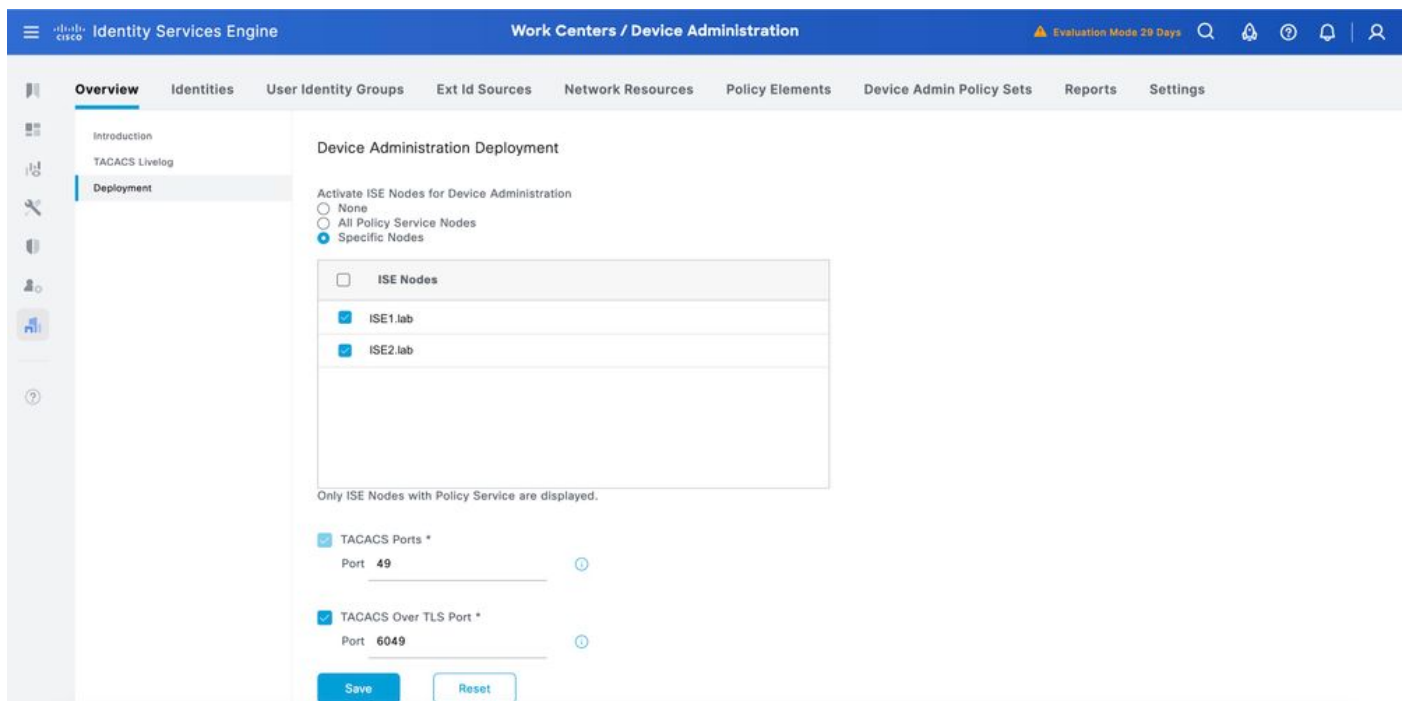
Paso 3. Guarde la configuración. El servicio Device Admin está ahora habilitado en ISE.

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

Evaluation Mode 93 Days

OverviewIdentitiesUsers

Network Devices

Network Device Groups

Default Devices

TACACS External Servers

TACACS Server Sequence

Admin Policy Sets

More

✕

Edit Group

Name*

IOS-XR

Description

Group Hierarchy

Device Type > All Device Types > IOS-XR

Cancel

Save

☐ ADVA

ADVA SyncDirector Network Time Monitoring

No. of Network Device

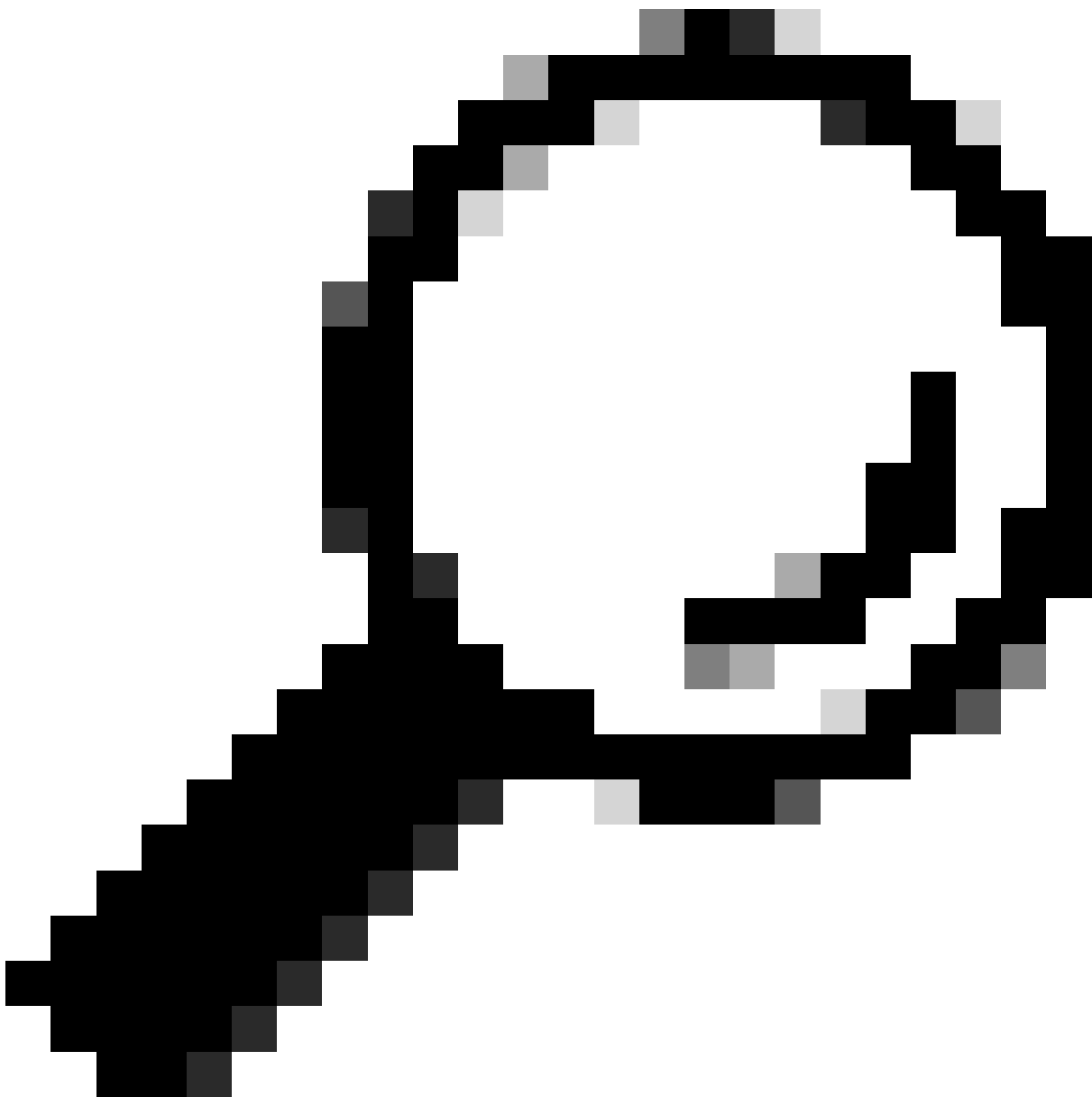
--

702

0

11

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.

Identity Services Engine
Administration / Network Resources
Evaluation Mode 11 Days

Network Devices
Network Device Groups
Network Device Profiles
External RADIUS Servers
RADIUS Server Sequences
External MDM
pxGrid Direct Connectors

Network Devices
Default Device
Device Security Settings

Network Devices List > BRC-8201-1

Network Devices

Name
BRC-8201-1

Description

IP Address
* IP: 10.225.253.167 / 32

IP Address
* IP: /

Device Profile
Cisco

Model Name

Software Version

Network Device Group

Location
All Locations
Set To Default

IPSEC
No
Set To Default

Device Type
IOS-XR
Set To Default

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.

Identity Services Engine
Work Centers / Device Administration
Evaluation Mode 67 Days

Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Help

Overview
Identities
User Identity Groups
Ext Id Sources
Network Resources
Policy Elements
More

Network Devices
Network Device Groups
Default Devices
TACACS External Servers
TACACS Server Sequence

☐ RADIUS Authentication Settings
☐ TACACS Authentication Settings
☒ TACACS over TLS Authentication Settings

This configuration is mandatory for TACACS over TLS, as the selected fields are used to verify the client and matched with the SubjectAltName field in the certificate, including its subtypes.

Subject Alternative Name (SAN)*

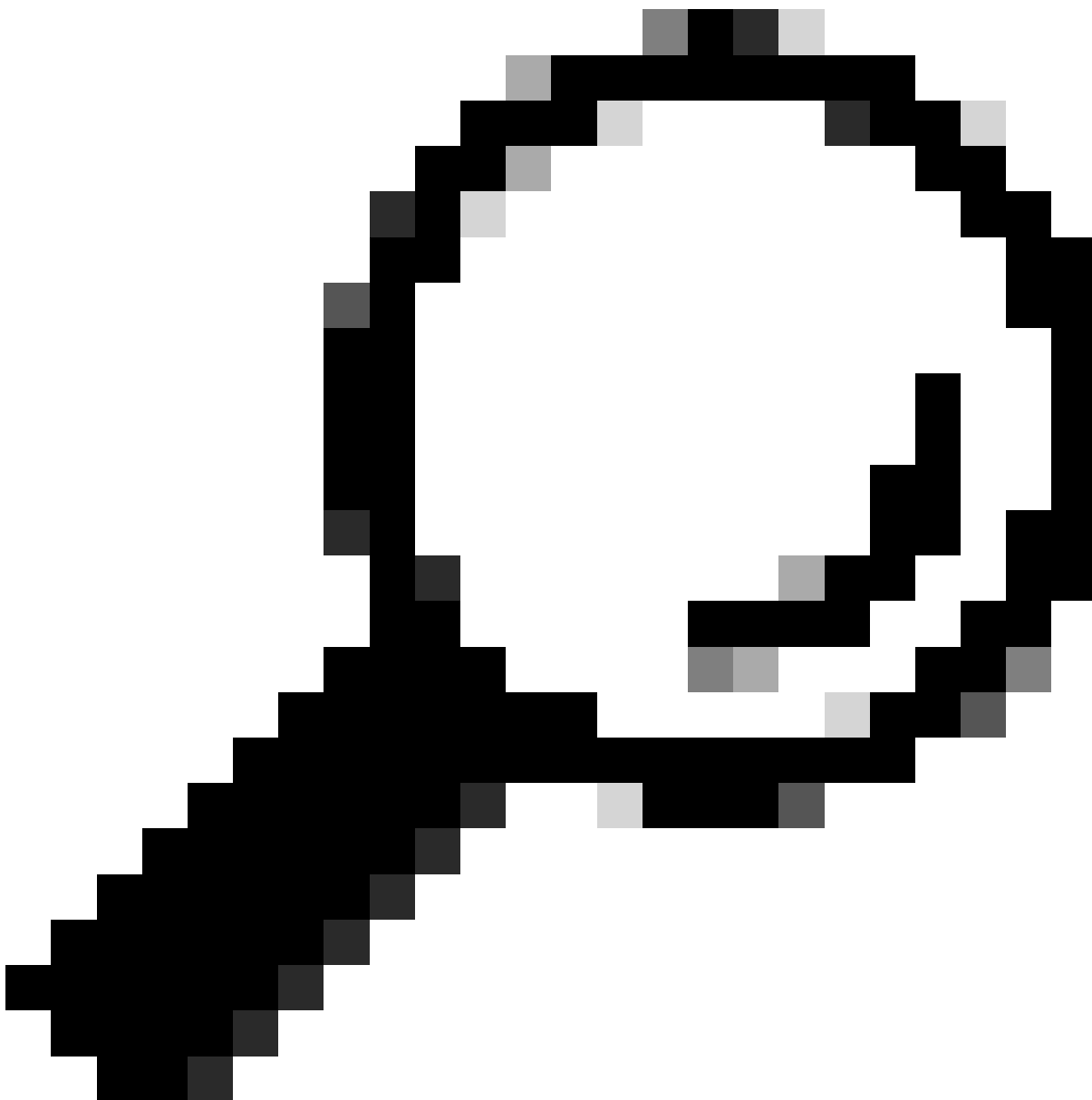
Additional security can be enforced by validating SAN certificate attributes. Cisco ISE supports validating the IP address (IPAddress), DNS Name (dNSName), and Directory Name (directoryName) attributes. The attributes chosen below are evaluated in this order: IP address, DNS Name, Directory Name. When ANY of attributes match, validation is successful, otherwise, validation fails.

☐ IP Address

The IP address(es) listed within the SAN attribute of the certificate is matched with the IP address of the network device. Both IPv4 and IPv6 addresses are supported.

Additional SAN attribute details [Show](#)

Additional SAN Attributes

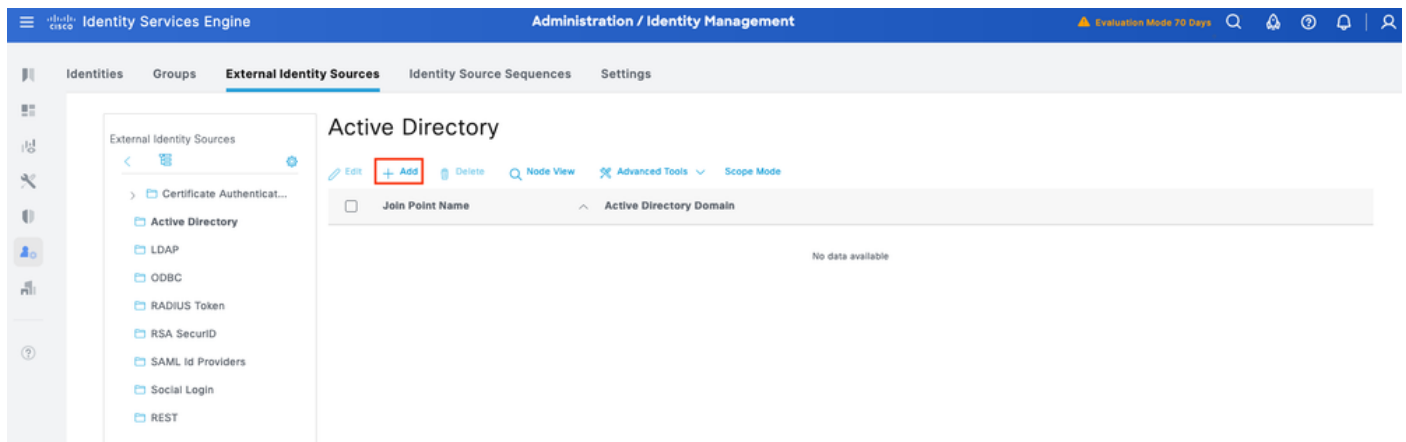


Consejo: Se recomienda habilitar el modo de conexión única para evitar reiniciar la sesión TCP cada vez que se envía un comando al dispositivo.

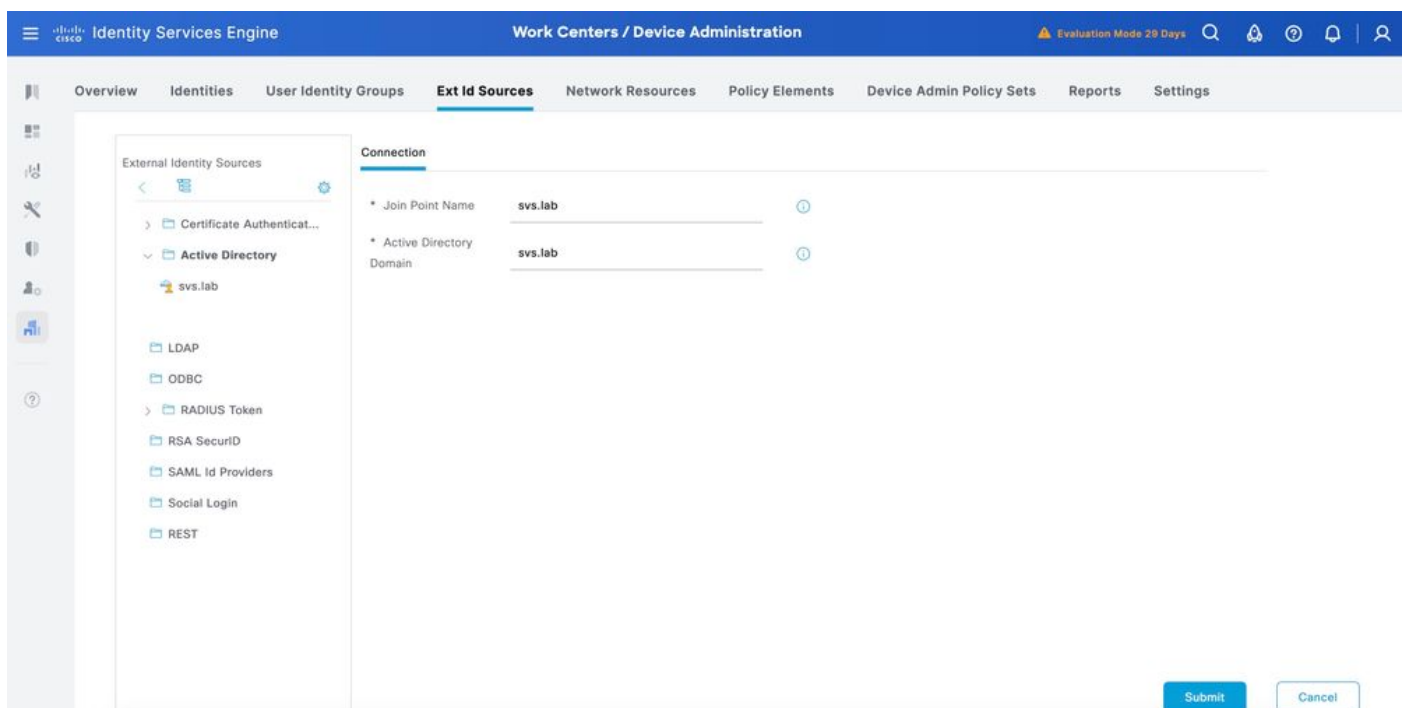
Configurar almacenes de identidad

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.

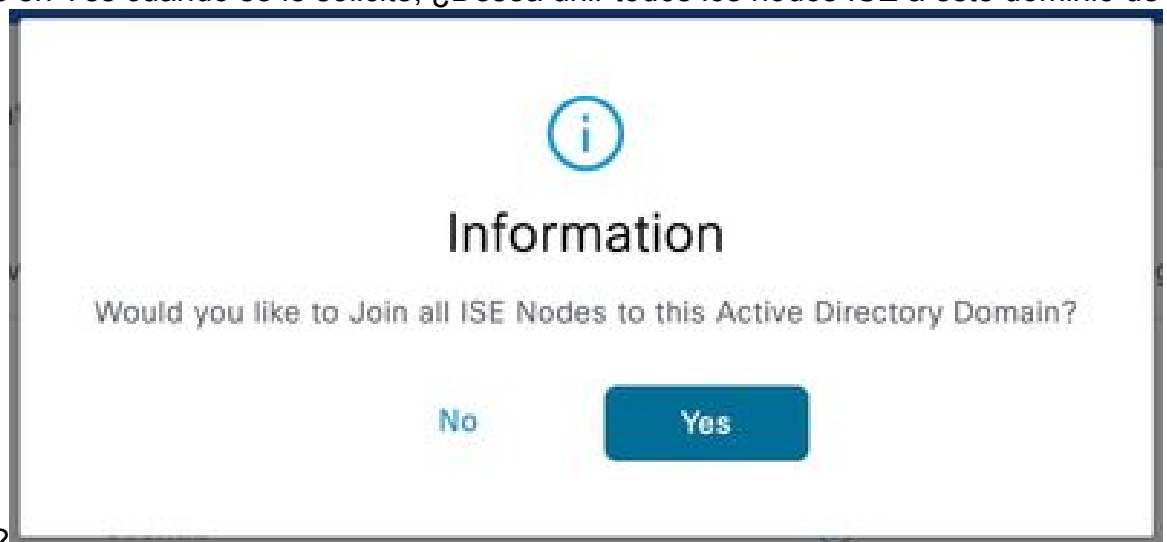
Paso 1. Vaya a **Administración > Gestión de identidad > Almacenes de identidad externos > Active Directory**. Haga clic en **Agregar** para definir un nuevo punto de unión AD.



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.

✕

Join Domain

Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

* AD User Name ⓘ administrator

* Password

☐ Specify Organizational Unit ⓘ

☒ Store Credentials ⓘ

Cancel OK

✕

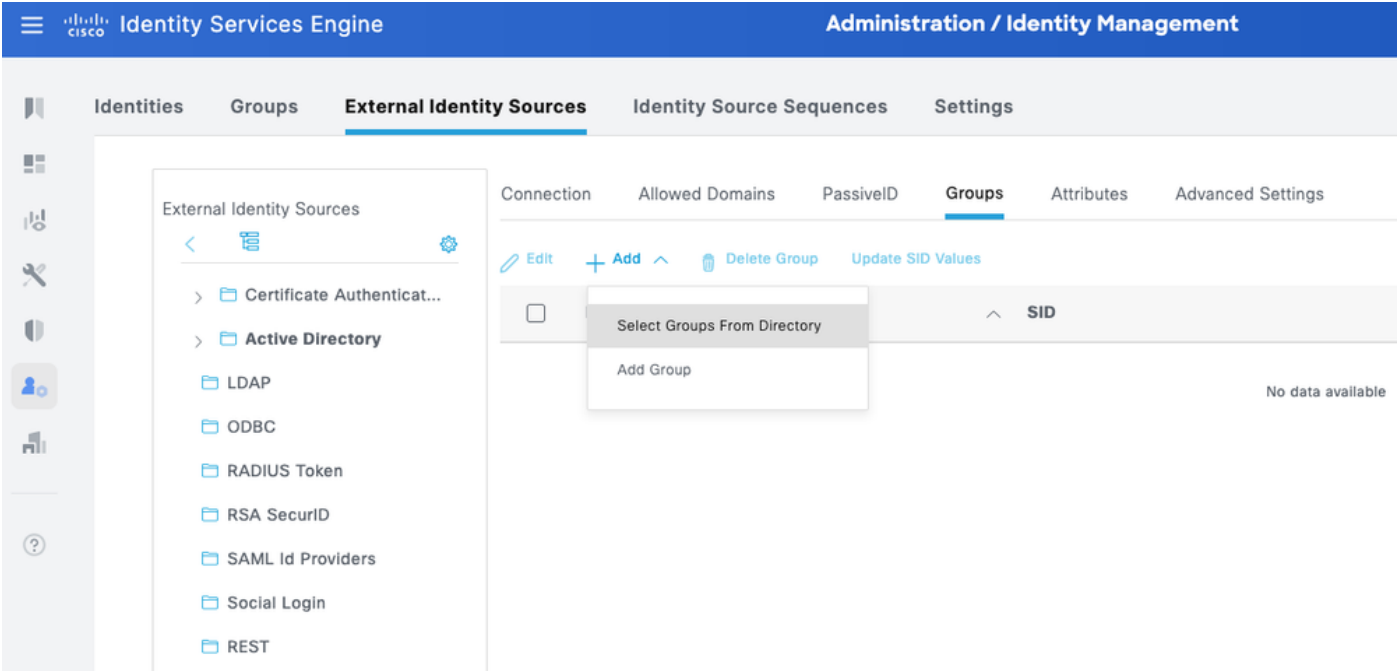
Join Operation Status

Status Summary: Successful

ISE Node	Node Status
ISE1.lab	✔ Completed.

Close

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.



Select Directory Groups

This dialog is used to select groups from the Directory.

Domain

Name Filter

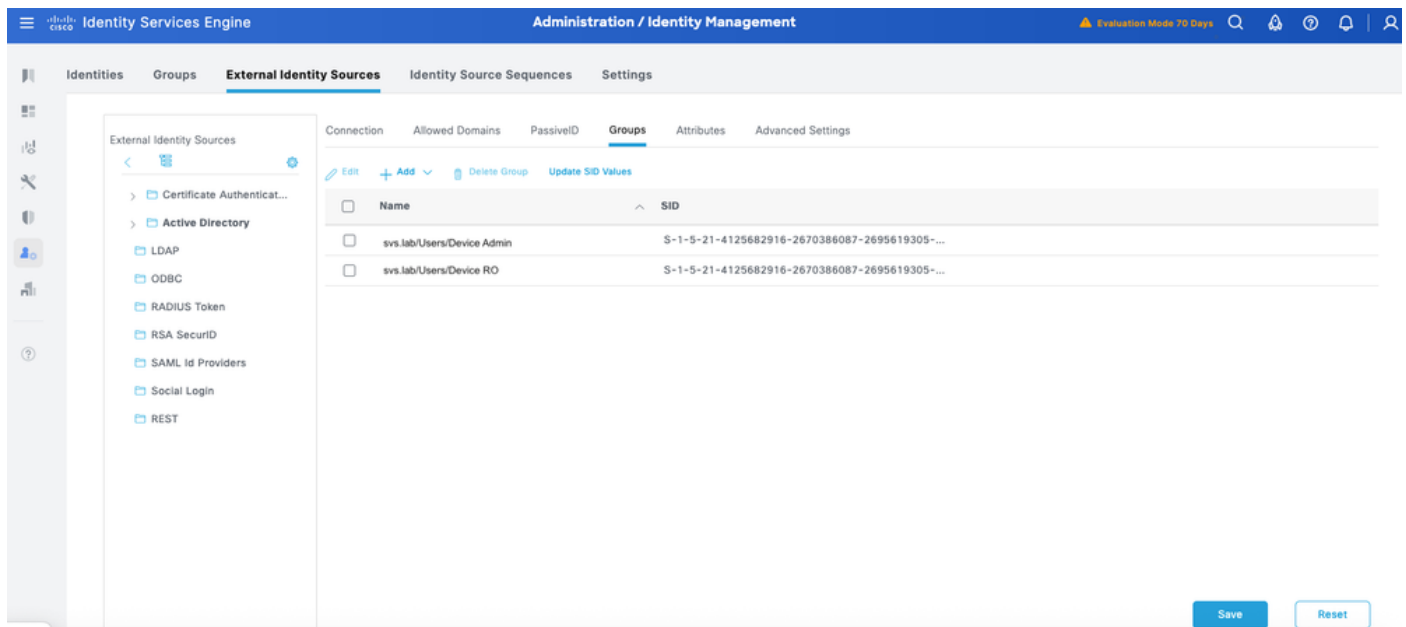
SID * Filter

Type Filter

Retrieve Groups...

2 Groups Retrieved.

☐	Name	Group SID	Group Type
☐	svs.lab/Users/Device Admin	S-1-5-21-4125682916-2670386087-26956193...	GLOBAL
☐	svs.lab/Users/Device RO	S-1-5-21-4125682916-2670386087-26956193...	GLOBAL



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.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes the Cisco logo, 'Identity Services Engine', 'Work Centers / Device Administration', and a status indicator 'Evaluation Mode 63 Days'. The main navigation tabs are Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, **Policy Elements**, Device Admin Policy Sets, Reports, and Settings. The left sidebar shows a tree view with 'TACACS Profiles' selected. The main content area displays the configuration for a TACACS Profile named 'IOSXR_RW'. The 'Name' field is 'IOSXR_RW'. The 'Description' field is empty. Below the 'Task Attribute View' and 'Raw View' tabs, the 'Common Tasks' section shows a 'Common Task Type' of 'Shell'. The configuration includes several fields: 'Default Privilege' (checked, value 15), 'Maximum Privilege' (checked, value 15), 'Access Control List' (unchecked), 'Auto Command' (unchecked), and 'No Escape' (unchecked). Each privilege field has a dropdown menu and a note '(Select 0 to 15)'.

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.

The screenshot shows the Cisco Identity Services Engine (ISE) interface for creating a new TACACS Profile. The top navigation bar is the same as the previous screenshot, but the status indicator now says 'Evaluation Mode 62 Days'. The main navigation tabs are the same, with 'Policy Elements' selected. The left sidebar shows 'TACACS Profiles' selected. The main content area displays the configuration for a new TACACS Profile named 'IOSXR_RO'. The 'Name' field is 'IOSXR_RO'. The 'Description' field is empty. Below the 'Task Attribute View' and 'Raw View' tabs, the 'Common Tasks' section shows a 'Common Task Type' of 'Shell'. The configuration includes several fields: 'Default Privilege' (checked, value 1), 'Maximum Privilege' (checked, value 1), 'Access Control List' (unchecked), 'Auto Command' (unchecked), and 'No Escape' (unchecked). Each privilege field has a dropdown menu and a note '(Select 0 to 15)'.

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.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes the Cisco logo, 'Identity Services Engine', 'Work Centers / Device Administration', and a notification for 'Evaluation Mode 63 Days'. The main navigation menu on the left includes Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements (selected), Device Admin Policy Sets, Reports, and Settings. The 'Policy Elements' section is expanded, showing 'TACACS Command Sets' > 'CISCO_IOSXR_RW'. The 'Command Set' configuration page is displayed, with the 'Name' field set to 'CISCO_IOSXR_RW'. The 'Description' field is empty. Under the 'Commands' section, the checkbox 'Permit any command that is not listed below' is checked. Below this, there are buttons for 'Add', 'Trash', 'Edit', 'Move Up', and 'Move Down'. A table with columns 'Grant', 'Command', and 'Arguments' is shown, but it is empty with the message 'No data found.' at the bottom. At the bottom right, there are 'Cancel' and 'Save' buttons.

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.

The screenshot shows the 'Policy Elements' configuration page in the Cisco ISE 'Work Centers / Device Administration' section. The breadcrumb trail is 'TACACS Command Sets > CISCO_IOSXR_RO'. The page is titled 'Command Set'. The 'Name' field is 'CISCO_IOSXR_RO'. The 'Description' field is empty. Under the 'Commands' section, there is a checkbox for 'Permit any command that is not listed below' which is currently unchecked. Below this, there are buttons for 'Add', 'Trash', 'Edit', 'Move Up', and 'Move Down'. A table lists the commands:

Grant	Command	Arguments
☐	PERMIT	show

At the bottom right, there are 'Cancel' and 'Save' buttons.

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.

The screenshot shows the 'Device Admin Policy Sets' configuration page in the Cisco ISE 'Work Centers / Device Administration' section. The breadcrumb trail is 'Policy Elements > Device Admin Policy Sets'. The page has buttons for 'Reset', 'Reset Policy Set Hit Counts', and 'Save'. Below these is a table of policy sets:

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	IOS-XR devices		DEVICE:Device Type EQUALS All Device Types#IOS-XR	Default Device Admin	73		

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.

Identity Services Engine

Work Centers / Device Administration

Evaluation Mode 62 Days

Overview

Identities

User Identity Groups

Ext Id Sources

Network Resources

Policy Elements

Device Admin Policy Sets

Reports

Settings

Policy Sets→

IOS-XR devices

Reset

Reset Policy Set Hit Counts

Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
Q Search	✓ IOS-XR devices		🖨️ DEVICE-Device Type EQUALS All Device Types#IOS-XR	Default Device Admin	✎ + 77

> Authentication Policy(1)

> Authorization Policy - Local Exceptions

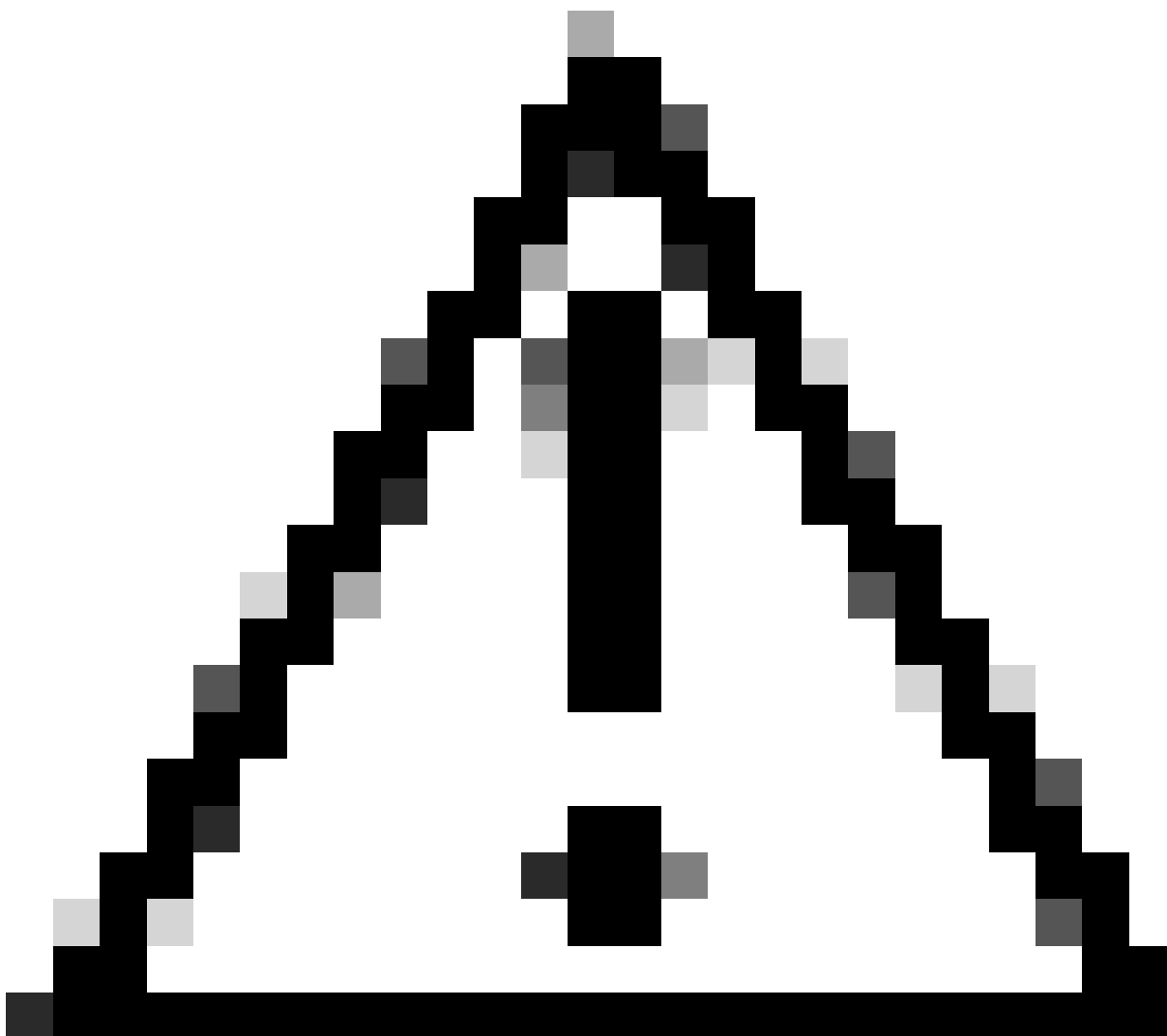
> Authorization Policy - Global Exceptions

∨

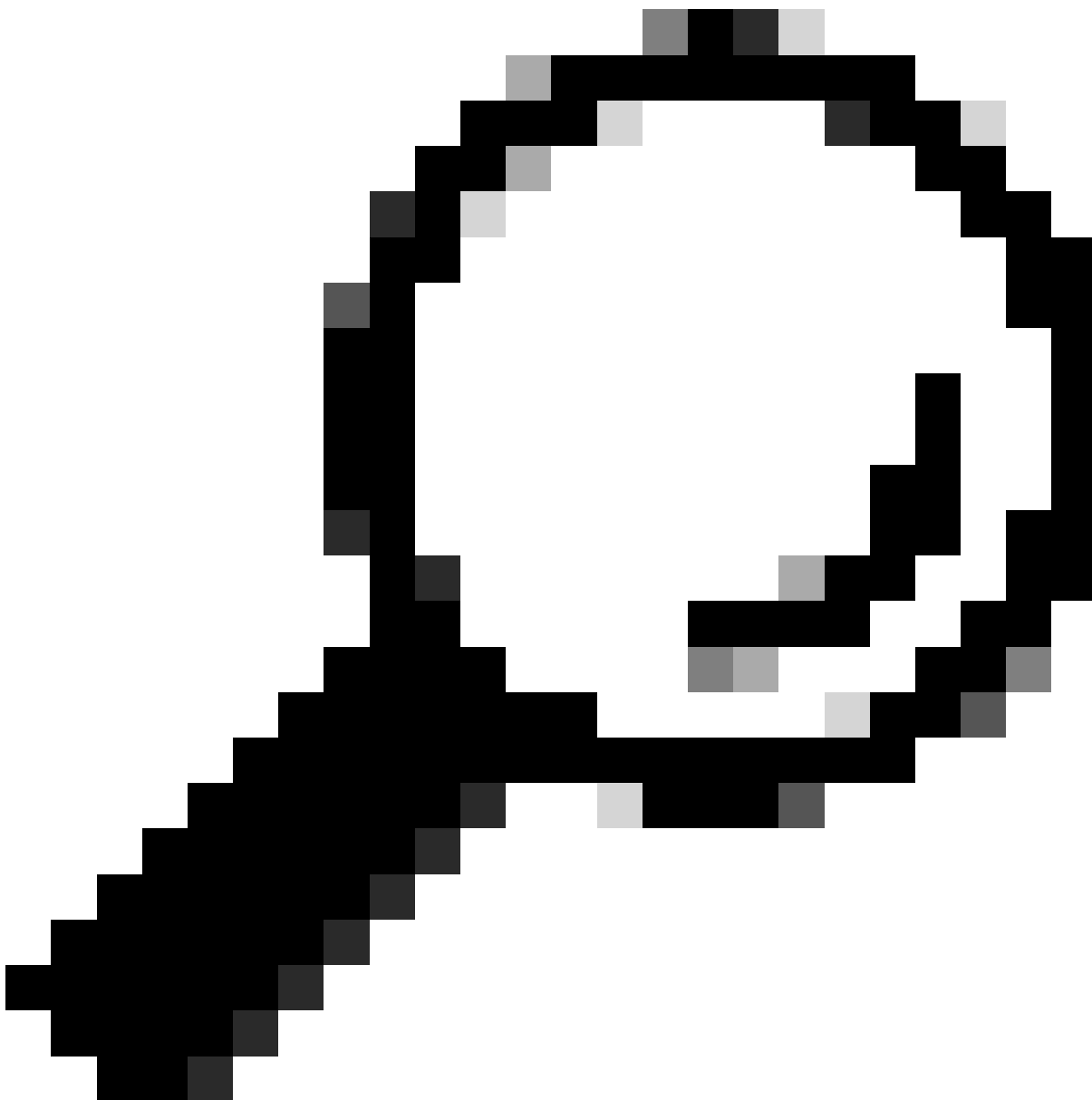
Authorization Policy(3)

+ Status	Rule Name	Conditions	Results		Hits	Actions
			Command Sets	Shell Profiles		
Q Search						
✓	Authorization Rule RO	👤 svs.lab-ExternalGroups EQUALS svs.lab /Users/Device RO	CISCO_IOSXR_RO ✎ +	IOSXR_RO ✎ +	0	⚙️
✓	Authorization Rule RW	👤 svs.lab-ExternalGroups EQUALS svs.lab /Users/Device Admin	CISCO_IOSXR_RW ✎ +	IOSXR_RW ✎ +	77	⚙️
✓	Default		DenyAllCommands ✎ +	Deny All Shell Profile ✎ +	0	⚙️

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 svcs.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
```

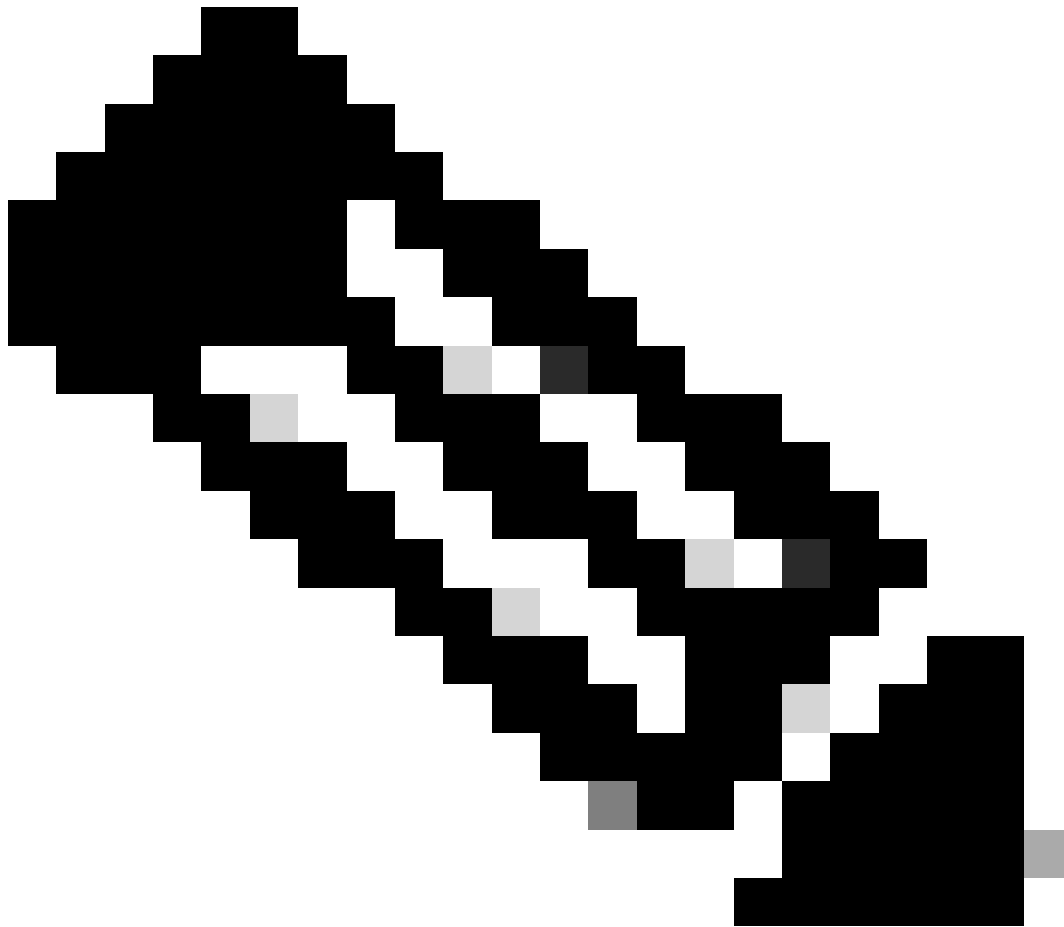
Paso 2. Borre los certificados y los puntos de confianza antiguos o no utilizados. Asegúrese de que no haya certificados y puntos de confianza antiguos. Si ve alguna entrada antigua, elimínela o elimínela.

```
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
```

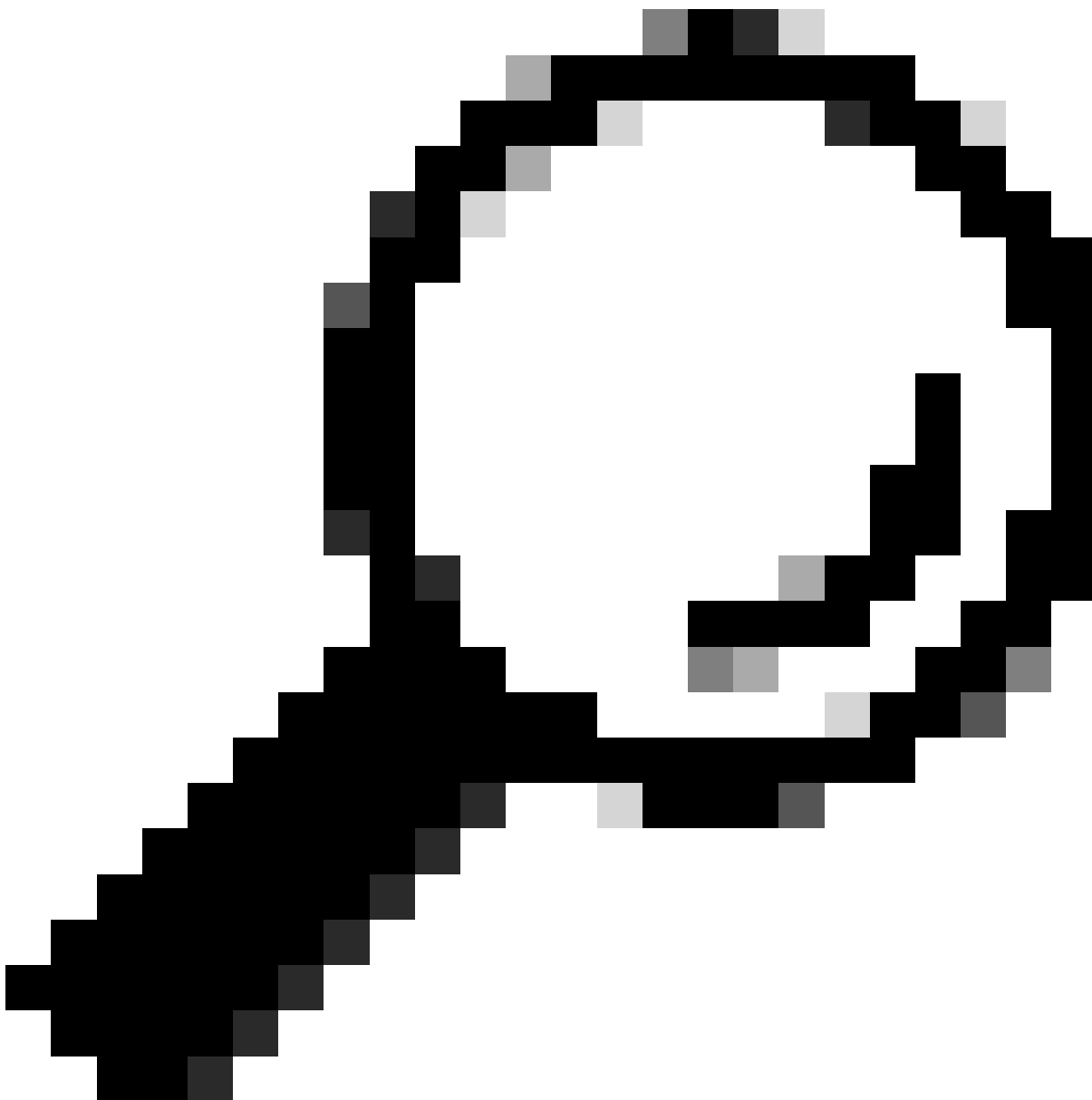
```
RP/0/RP0/CPU0:BRC-8201-1(config)#
```

```
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 sv
```

```
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)#

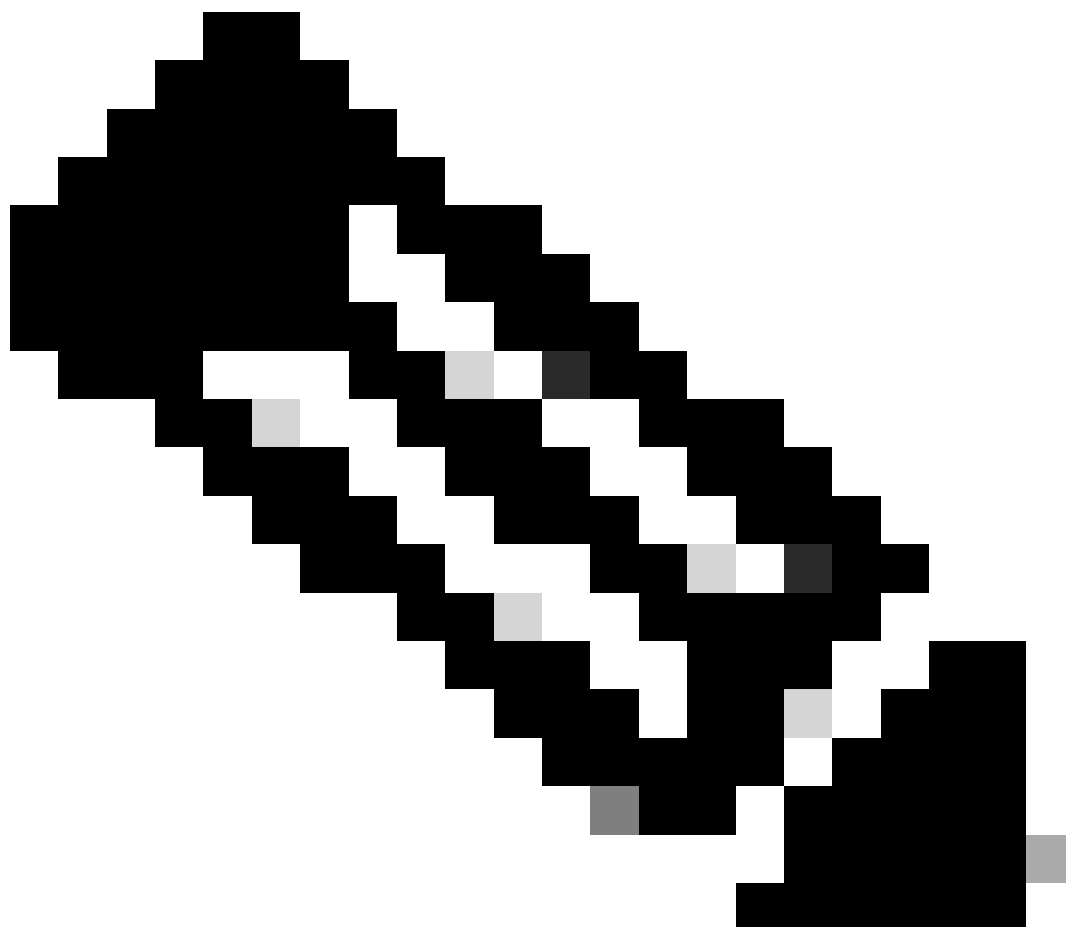
enrollment url terminal

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 svcs

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-----

```
MIIFDCCA3ygAwIBAgIIIM10AsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZmFzAVBgNVBAGTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECjMDU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUGA1UECBM0MjYyZG93ZG93ZG93ZG93ZG93ZG93ZG93ZG93ZG93ZG93ZG93
BgNVBAoTBUNpc2NvMQwwCgYDVQQLLEwNTV1MxEjAQBgNVBAMTCVNWUyBYWJJDQTC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZU0yn2vIn6gKbx3M7vaRq
2YjwZ1zSH6EkEvxnJTty+kksiFD33GyHQepk7vfp4NFU50tQ4HC7t/A0v9grDa3QW
VwvV4MBbJhFM3s0J/ejgDYcMZhIAaPy0Zo5WLboOkXEiKjPLatKXojB8FVrhLF30
jMBSqwa4/Wlniy5S+7s4FFxsCf20COWfBAsnrs0tatIIhmcnx+VLJP7MRm8f0w4m
mutNo7IhbJSrgAFXmj1bBjMmgspObULo/wxMHdTbtPBf11HRHTkNIO3qy04UADL2
WpoGhgT/FaxxBo2UBcnYVaP+jjREONYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7B0e8oDNKU6gX1ojKyLP/gC7j8AeP03ir+KZui8
b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
gJ+kQXe7QtT/u6m1MrtjE3gAEVpl334rTixy9hpKZIKB86t2ZA3JX8CLsbCa13sA
z1XC0NX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTA01xh60I4QnK+MNQKpTjt/E4
ydH10rrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVL1783nTc9wYptQEPi5sw
83g9EMgKV0ARIiVUa/q1AgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAyb4
QgEBBAQDAgAHMBkGCWCSAGG+EIBDQMFgptTV1MgTGFiIENBMAOGCSqGSIb3DQEB
CwUAA4ICAQAITA308oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oK0dGayi
iSEkSSX9qyflFINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXR67X+v
0+ja6zTQqj06lqJhmrSkyFbYf/ZTpe4d10zJsZjNsN0r8bF9n0A/7qNZLp3Z3cpU
PU0KdbiSvRqnPw3e8TfITVmAzcx8COI2SrYFMSUazo1VBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIE0f5ay1PKURO/8aj/B7a1uJapXkmnj5qPeGhN0pB
Q9r14reov4so2EspkXS7CrH9yGfpiYtprokz1UvZBZ8v1oI7YZmjFmem+5rT6Gnk
eU/1X7nV61SYG5W5K+I8uaKuyBHOMn7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggz1P0dsS/i6Lo7ypYX0eB9HgVDCkzQsLXQuHGj/2WsgPgDRcjkvnyURk4Jx+Ib
xDrmo7e0XPPSW4172a6K18CR3U2Cr4wsuvndPEq/qd2NRSBWffFOXE/AJHQG7STT
HaXLU9r2Ko603oecu8ysGTWl1It/9T1/F0b0xZRugWcpJrVoTgDGUA==
```

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

quit

Serial Number : AB:CD:87:FD:41:12:C3:FE:FD:87:D5

Subject:

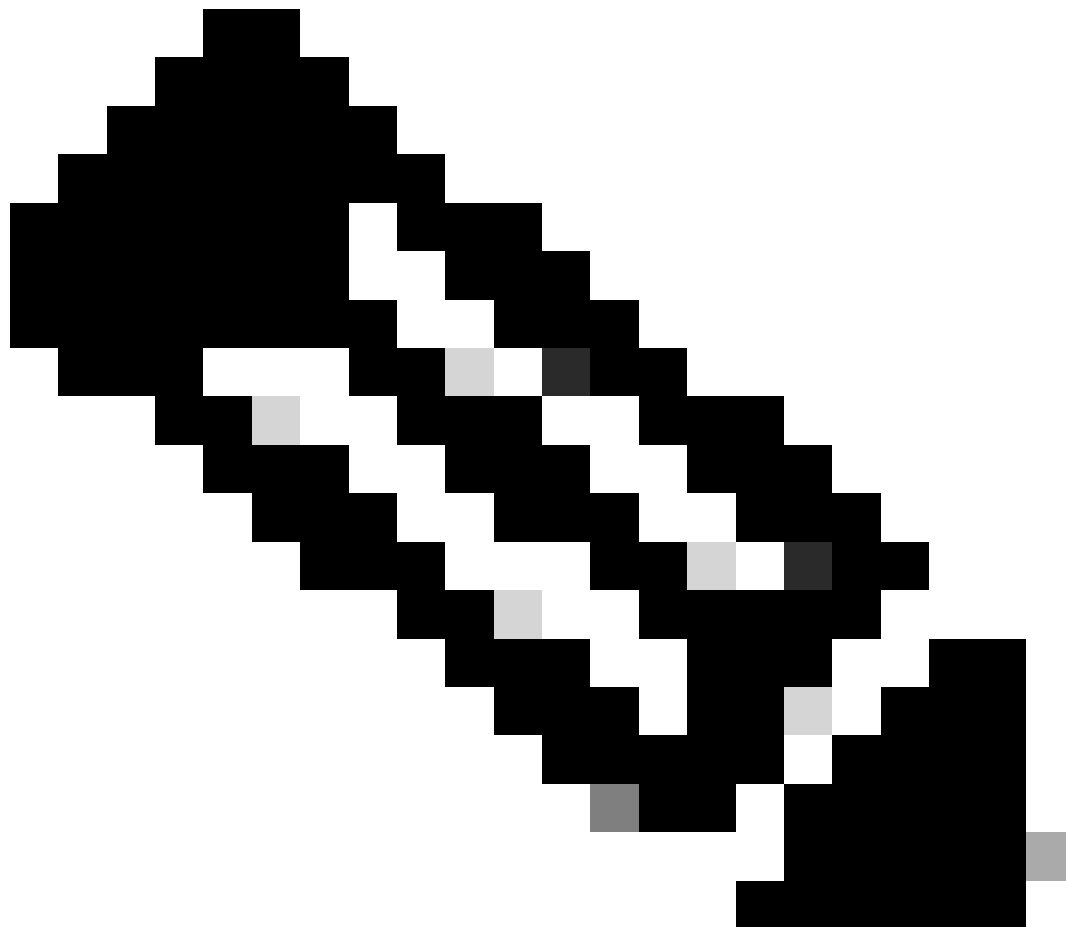
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US

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 svcs

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-----

MIIDQTCCAikCAQAwcjELMAkGA1UEBhMCVVMxCzAJBgNVBAGMAk5DMQwwCgYDVQQQH
DANSVFAXDjAMBGNVBAoMBUNpc2NmMQwwCgYDVQQQLDANTVlMxZzAVBgNVBAMMDjEw
LjIyNS4yNTMuMTY3MREwDwYDVQQFEwg0MDkwODQzYjCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBALwx9w4DnTtr1oDH9iOZxPvEDARwN0t4WrPEjaQc1ZUA
6ax6Cqx/0JlQiUf2+eQv+4rKZqAZ1xDhiaIMGqETn00LKpwmtx10IqXL7UYMHwF
9vRII52zomkWA8a63Wx66UkExaXoeXaf5HkLoqDu68X83U7LPvMe1sMwvmq7Rmy2
DAu30HB/JfYlQCHmTVFz3M5fBt86xx4t1nxTFU/4lRwMC73UdL5YdKJLjMpBT2tN
E3piZ+kL4p1c9U4RIBkU8/G4drzFbGvHCIkKwI0cb1X2HgtbVQdCXTAwJDmr209
zd2ZCa5enTbOKHbNXuHjpy0k8MewKOV2muwxVcQbej8CAwEAAACBiTAYBgqhkiG
9w0BCQcxCMJQzFzY28uMTIzMG0GCSqGSIb3DQEJJDJFgMF4wDgYDVROPAQH/BAQD
AgWgMCAGA1UdJQEB/wQWMBQGCSqGSIb3DQEJJDJFgMF4wDgYDVROPAQH/BAQD
MB8GA1UdEQQYMBaCDjEwLjIyNS4yNTMuMTY3hwQK4f2nMA0GCSqGSIb3DQEBBQUA
A4IBAQBbX0eWF5ZUz701GFjuQHBBdgYb+3lhF0xbYm9psIWfv1uwjKkOL297tGHv
Iux7nMyrDVkSJ81i5BSTdd9FE6AbSFswj1YpO+IxxUM971Ejwg2rj+jABDR7I8SU
06Y06mS9x2ZJYqImeq8xwIr19Hi+7tyaLe6apfTI1jdgVxB+Xyz0FJMckI05US3j
T/3aw/115RcXerdrh36oMUHEepUjIx/15u9s1c7e1mxACoQE6f90A+fdg2zYt0ME
Z6VAw64cY+YF6iLbYv7c4l1z05Zj2NJBuKpeqijkFAKY/1rIXTHypzH/p2ma4zuS
46a+kLXsVHZ716ZMB3WrUzB2ZN00

```
-----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 svcs 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
BhMCVVMxZjZAVBgNVBAGTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWx1aWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECXMdU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNTA5MTQ1NzAwWWhcNMjUwNTA5MTQ1NzAwWjByMQswCQYDVQQGEwJV
UzELMAkGA1UECAwCTkxMDDAKBgNVBACMA1JUUEDEOMAwGA1UECgwFQ21zY28xDDAK
BgNVBAsMA1NWUzEXMBUGA1UEAwwOMTAUMjI1LjI1My4xNjcxETAPBgNVBAUTCDQw
OTA4NDNiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvDH3DgOd02uW
gMf2I5nE+8QMBHA3S3has8SNpByV1QDprHoLGr/QmVCJR/b55C/7ispmoBnXE0GJ
qIwaoR0c7QsqnCa3HXQipcvrtRgwcFAX29EgjnboiARyDxrdbHrpSQTfpeh5dp/k
eQuio07rxfdzTss+8x7WwzC+artGbLYMC7fQcH819iVAIeZNUXPcz18G3zrHHI3W
fFMVT/iVFYwLvdR0v1h0okuMykFPa00TemJn6QvinVz1ThEgGRTz8bh2vMVsa8cI
iRaTajRxvVfYeC1tVB0JdMDAK0avY73N3Zkjr16dNs4ods1e4eOnLSTwx7Ao5Xaa
7DFVxBt6PwIDAQABo4GAMH4wHgYJYIZIAyb4QgENBBEWD3hjYSBjZXJ0aWZpY2F0
ZTA0BgNVHQ8BAf8EBAMCBaAwIAyDVR01AQH/BBYwFAYIKwYBBQUHAWEGCCsGAQUF
BwMCMAMkGA1UdEwQCMAAwHwYDVR0RBBGwFoIOMTAUMjI1LjI1My4xNjEhBARh/acw
DQYJKoZIhvcNAQELBQADggIBAARpS5bEck+oj012106WxedDQ8Vdu0bBtrn0H+Nt
94EA1co7HEe4USf1FiASAX7rNveLpY3ICmLh+tQZYTzRQ93tb9mMTZg7exqN89ZU
V1XoB2U0Tri5K10/+izEGgyNq42/ytAP8Y007HR/2jf7gfhovwvR5QN0EHv4o61
Zma5Xio1sBbkA7JB2mpzzZg4ZjsyV81RGXxxgyt1mwNmb7EiAc81odRcgyp7FNh3
F/k9cMMMr51M4Ysvo1tx1k9AeLjb2syv5/fG6Qu0ZdWwTaaQh0Y2h/cVDiV97wg
0D1mEfDsv6QrxQSujZr22RzVykKH1tuiV2B74pthUuGRBtFHS5XFy7uTTbfGX8M6
ZJw8rX1SADr8tDp1rf1ZIrPmv3ZPP7woTB22yWzyd0use+5Ia1b0w70twN4t/Iiw
8CJu6HfnDXLDPZ0jsC8stefrS1opwGccp3j6aZKPFz+I/Purb44a9WxEwa2TA7H
+r1oynBcGMet0HxVLnptlsC7Q4mN/MDXeGyW+OTNCirNEG/gqcu+dn9EnNKkE2WV
oF5370w+uNHok8Bdt8mqadUT40oUSqY8ArV0Bom05tzbemreVPmQAZ/IahZ7TqKo
3dGNontAFTTESM1iujQ81iRKsikdHysnwcCM2ni1CKZrhVq5IB8NK6jKRJZ0eQAX
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 svcs 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 svcs

Wed May 14 14:55:58.173 UTC

Trustpoint : svcs-new
=====

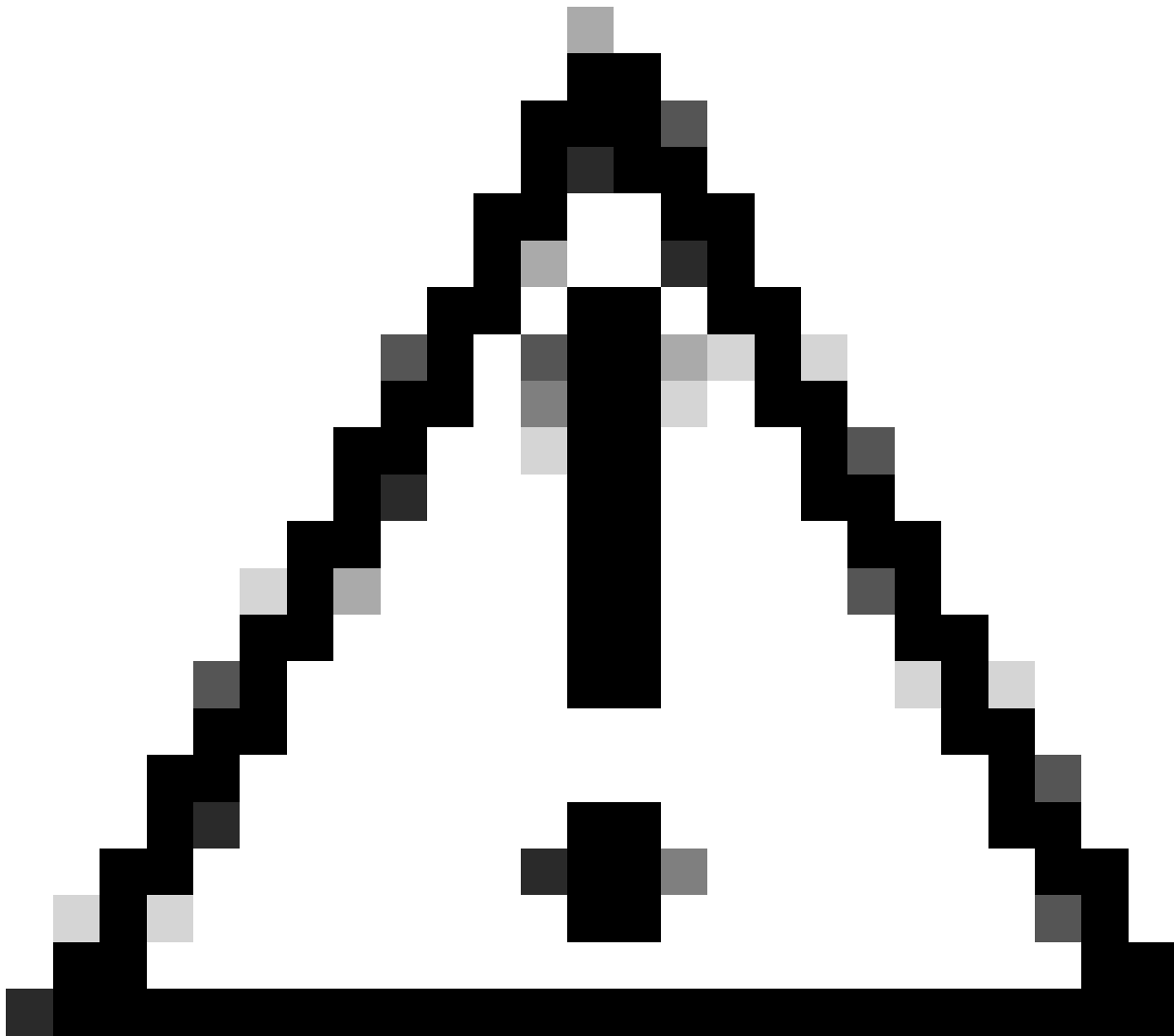
CA certificate
Serial Number : 20:01:20:1F:B6:9D:C3:FE:43:78:FF:64
Subject:
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
Issued By :
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
Validity Start : 17:05:00 UTC Mon Apr 28 2025
Validity End : 17:05:00 UTC Sat Apr 28 2035
SHA1 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: svcs

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
```

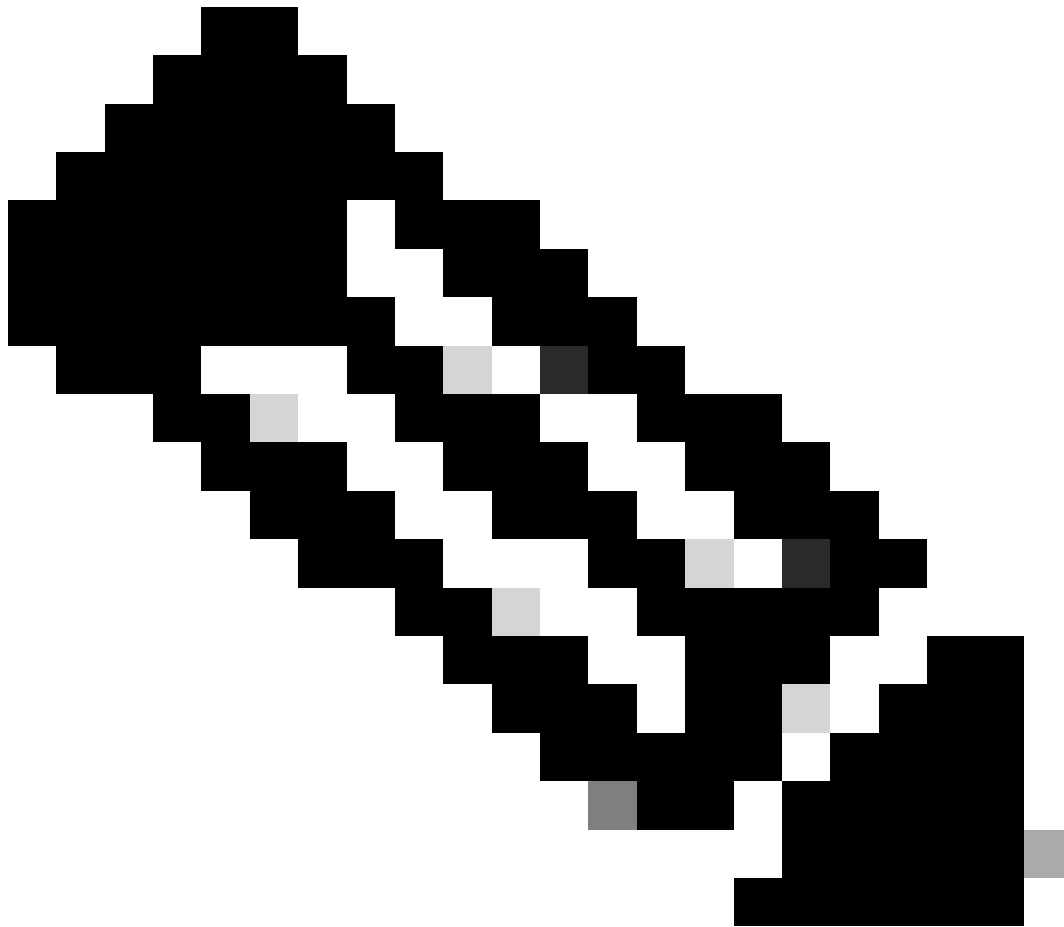
Paso 2. Configure el grupo AAA.

```
aaa group server tacacs+ tac_tls_sc
vrf mgmt
server-private 10.225.253.209 port 6049
timeout 10
tls
  trustpoint sv
!
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 svcs-new
Thu Aug 14 15:13:37.465 UTC
```

```
Trustpoint : svcs-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=m9uB1QsZDYy6wxomiFWB5Gv0AZM>

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+6I9Bd4Qg1Qa8g1xoH8GY>

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 updated
```

```
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=m9uB1QsZDYy6wxomiFWB5Gv0AZM>

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+6I9Bd4Qg1Qa8g1xoH8GY>

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).