

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

Contenido

[Introducción](#)

[Overview](#)

[Utilización de esta guía](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Licencias](#)

[Parte 1: Configure 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 XE RW - Perfil del administrador](#)

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

[Conjuntos de comandos Configure TACACS+](#)

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

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

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

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

[Método de configuración 1: par de claves generado por el dispositivo](#)

[Configuración del servidor TACACS+](#)

[Configuración de Trustpoint](#)

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

[Método de configuración 2: par de claves generado por CA](#)

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

[Verificación](#)

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 in Usage.

Usage

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

Allow Wildcard Certificates ☐ 

Paso 5. Seleccione los PSNs que tendrán 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.



Successfully generated CSR(s)

Certificate Signing request(s) generated:

ISE2#TACACS

Click Export to download CSR(s) or OK to return to list of CSR(s) screen

OK

Export

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.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System page. The 'Certificates' tab is selected in the top navigation bar. On the left, the 'Certificate Management' sidebar is expanded, showing 'Trusted Certificates' as the active section. The main content area displays the 'Trusted Certificates' table, which lists various certificates and their details. The table has columns for Friendly Name, Trusted For, Serial Number, Issued To, Issued By, Valid From, Expiration Date, and Status. The 'Import' button is highlighted with a red box.

☐	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...	Ent
☐	Cisco ECC Root CA 2099	Cisco Services	03	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Mon, 7 Sep 2...	Ent
☐	Cisco Licensing Root CA	Cisco Services	01	Cisco Licensing R...	Cisco Licensing R...	Thu, 30 May 2013	Sun, 30 May 2...	Ent
☐	Cisco Manufacturing CA SHA2	Endpoints Infrastructure	02	Cisco Manufactur...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2...	Ent
☐	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...	Ent
☐	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...	Ent
☐	Cisco Root CA M2	Infrastructure Endpoints	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2...	Ent
☐	Cisco RXC-R2	Cisco Services	01	Cisco RXC-R2	Cisco RXC-R2	Wed, 9 Jul 2014	Sun, 9 Jul 2034	Ent

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 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

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

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

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System page. The left sidebar contains navigation links: Deployment, Licensing, Certificates (selected), Logging, Maintenance, Upgrade & Rollback, Health Checks, Backup & Restore, Admin Access, and Settings. The main content area is titled "Certificate Signing Requests" and includes a button "Generate Certificate Signing Requests (CSR)". Below this is a table with columns: Friendly Name, Certificate Subject, Key Length, Portal gro..., Timestamp, and Host. A "Bind Certificate" button is highlighted in the table.

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 Examinar...

Friendly Name

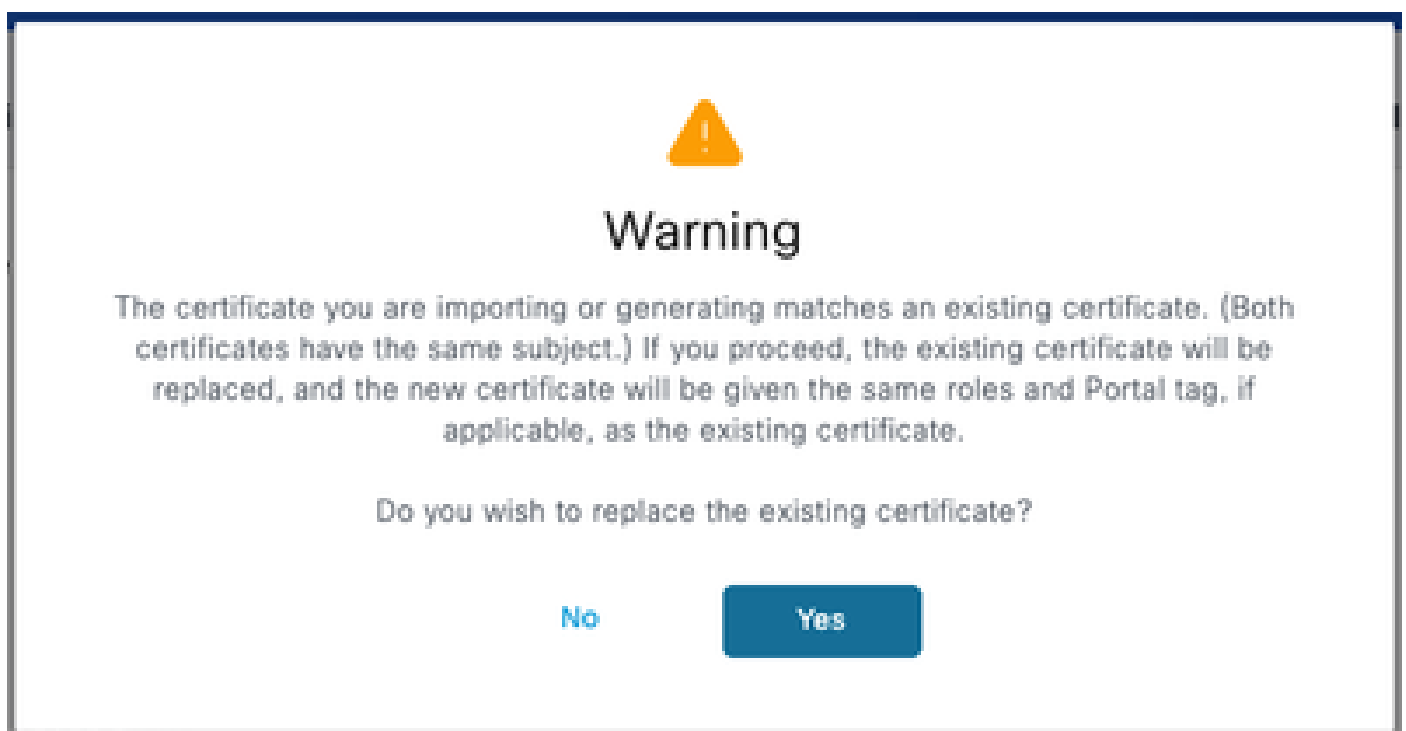
Validate Certificate Extensions ☐

Usage

☒ TACACS: Use certificate for TACACS Server

Submit Cancel

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.

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.

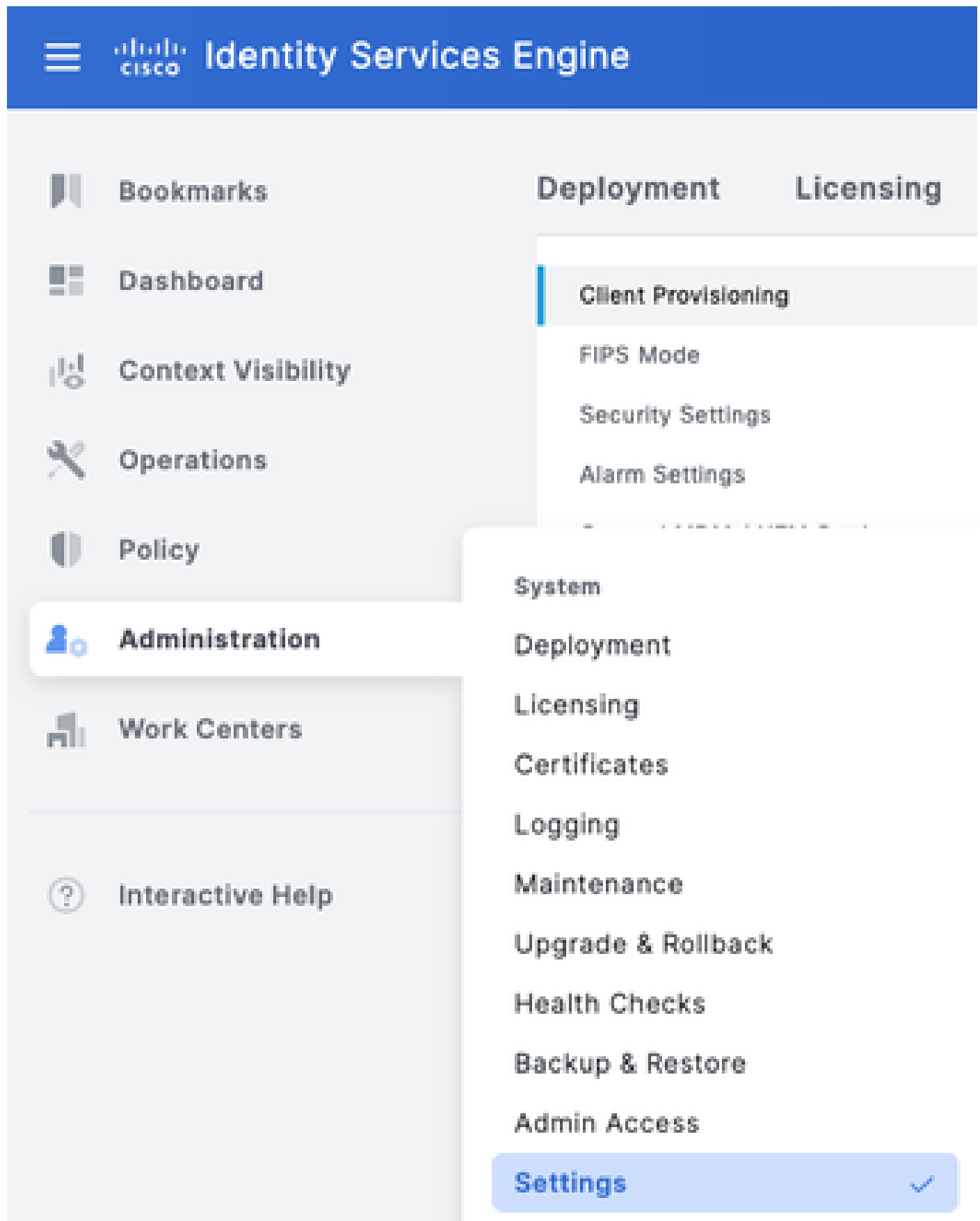
Edit + Generate Self Signed Certificate + Import Export Delete View

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 activarse 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 (highlighted), Work Centers, and Interactive Help. The main content area shows the 'Deployment' and 'Licensing' tabs. Under the 'Deployment' tab, the 'Client Provisioning' option is selected, showing a list of settings: FIPS Mode, Security Settings, Alarm Settings, and a partially visible 'System' option. The 'Settings' option at the bottom of the list is highlighted with a blue background and a checkmark.

Deployment	Licensing
Client Provisioning	
FIPS Mode	
Security Settings	
Alarm Settings	
System	
Deployment	
Licensing	
Certificates	
Logging	
Maintenance	
Upgrade & Rollback	
Health Checks	
Backup & Restore	
Admin Access	
Settings	

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.

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

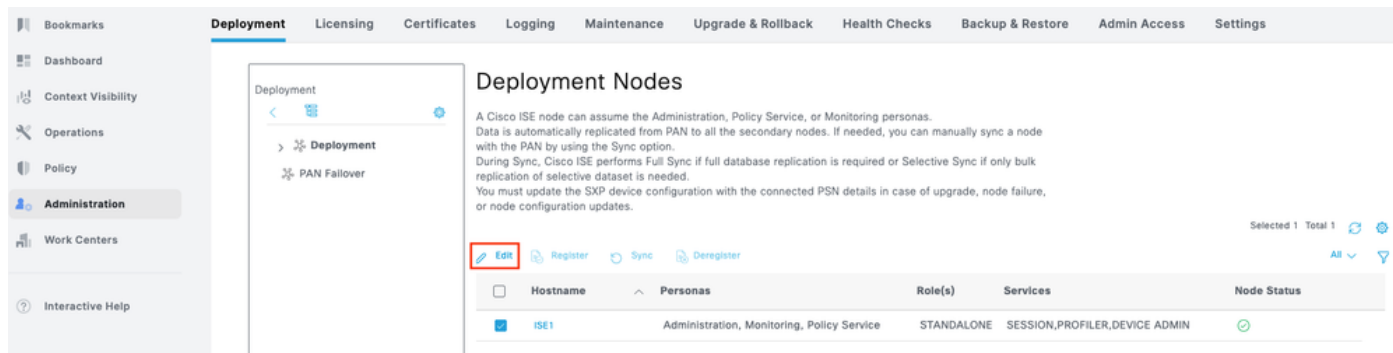


Advertencia: Al cambiar la versión de TLS, el servidor de aplicaciones de Cisco ISE se reinicia en todos los equipos de implementación de Cisco ISE.

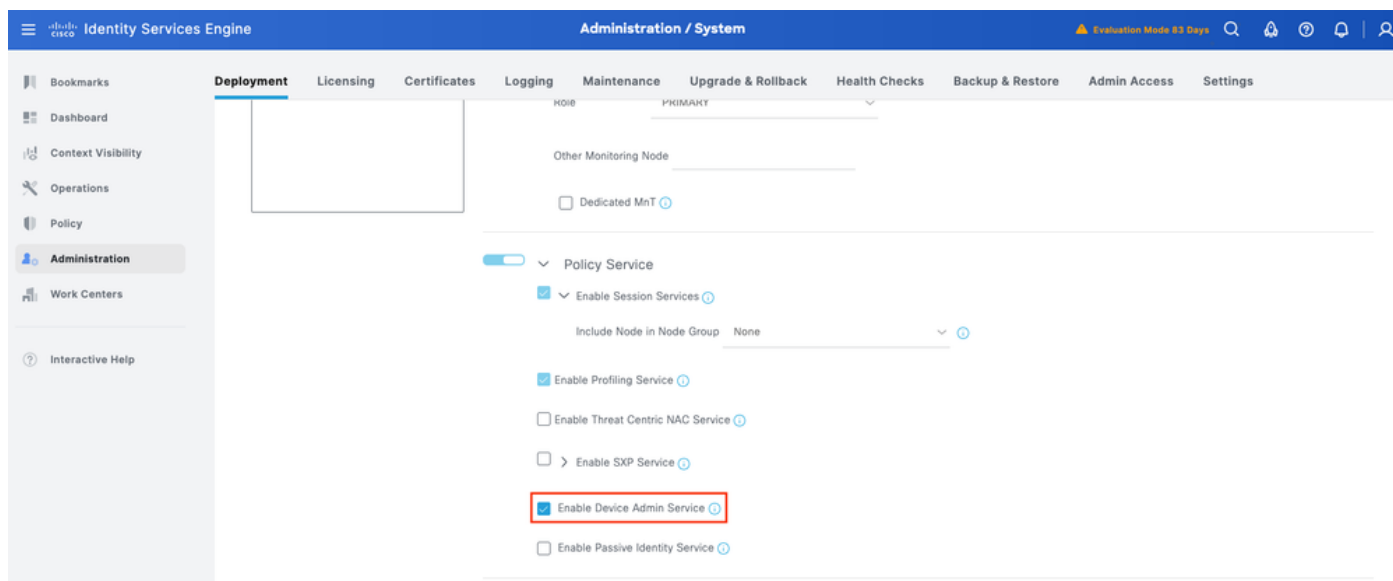
Habilitar Device Administration en ISE

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



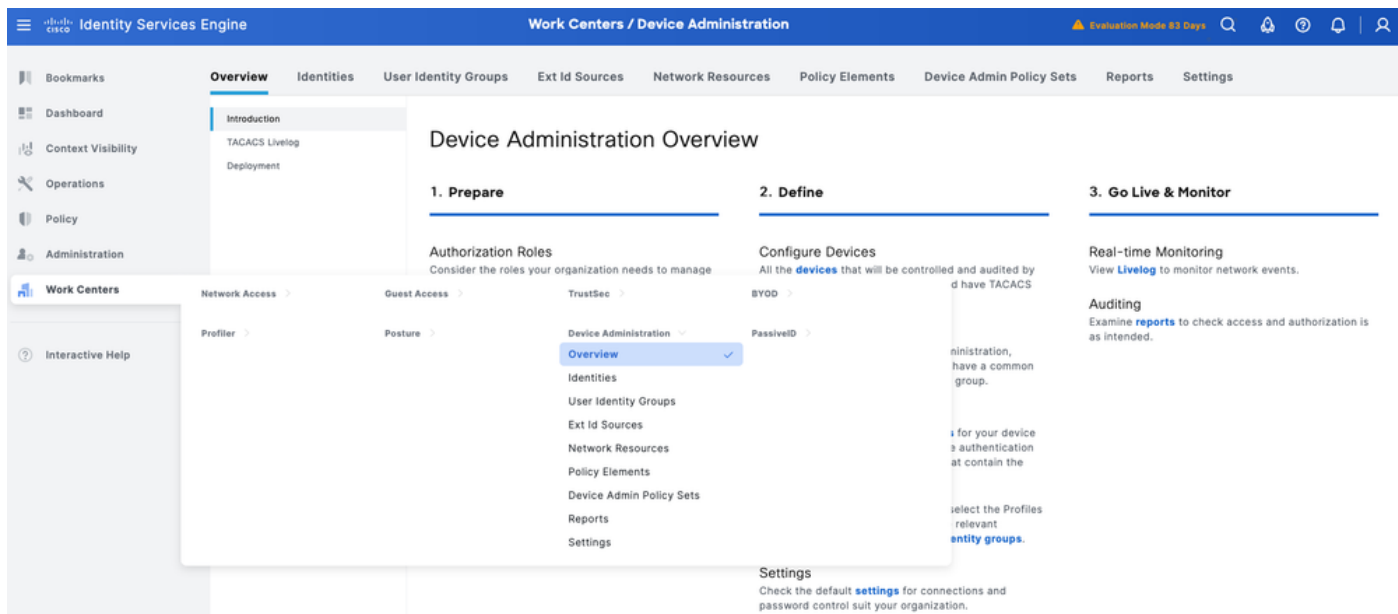
Paso 2. En General Settings, desplácese hacia abajo y seleccione la casilla de verificación junto a Enable Device Admin Service.



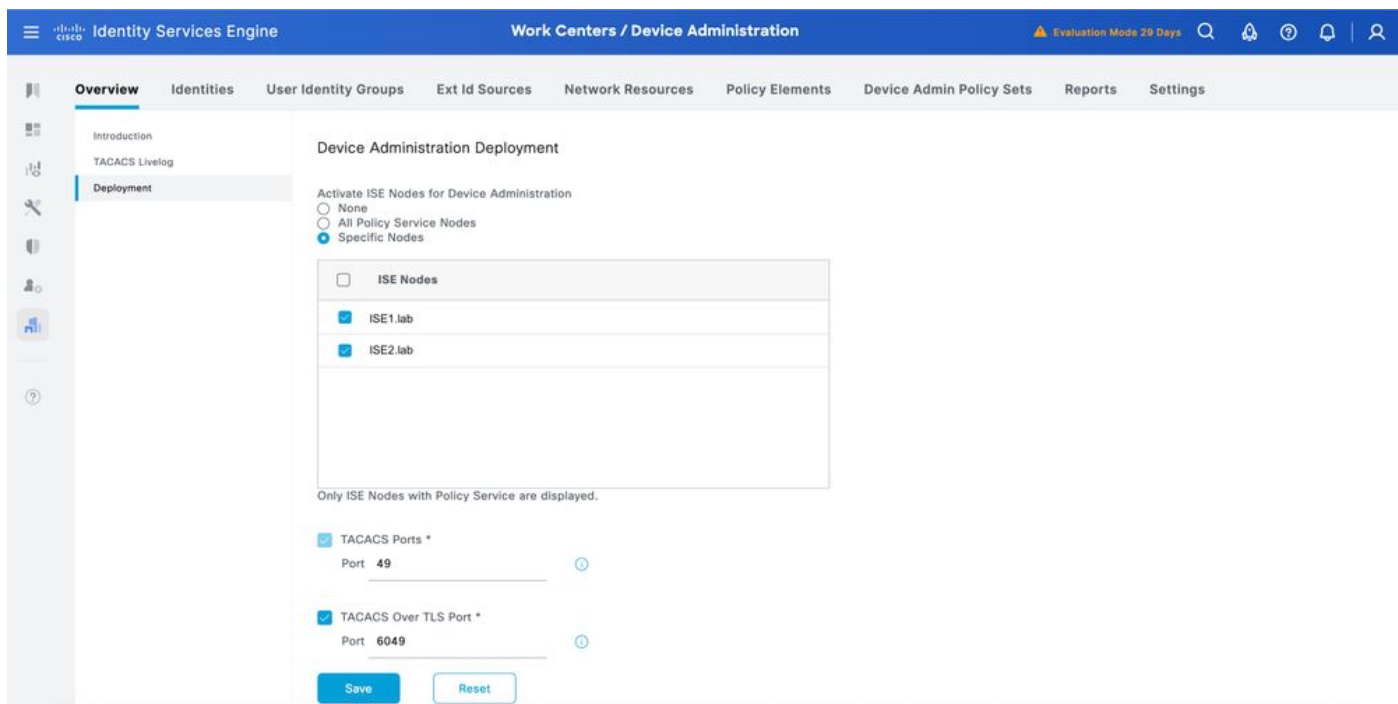
Paso 3. Guarde la configuración. El servicio Device Admin está ahora habilitado en ISE.

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 XE.

Add Group

Name*

IOSXE



Description

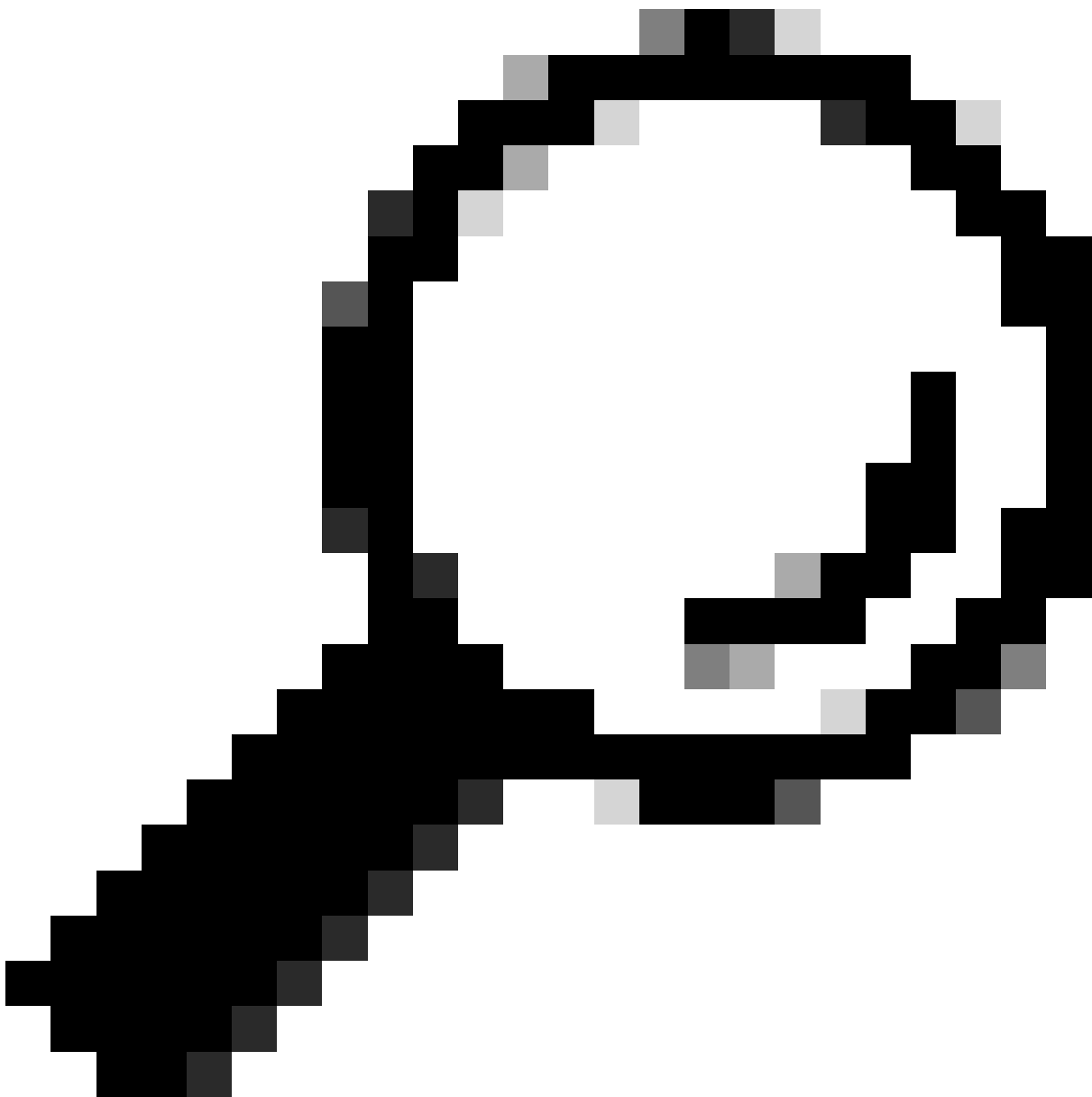
Parent Group*

Select Group or Add as root group



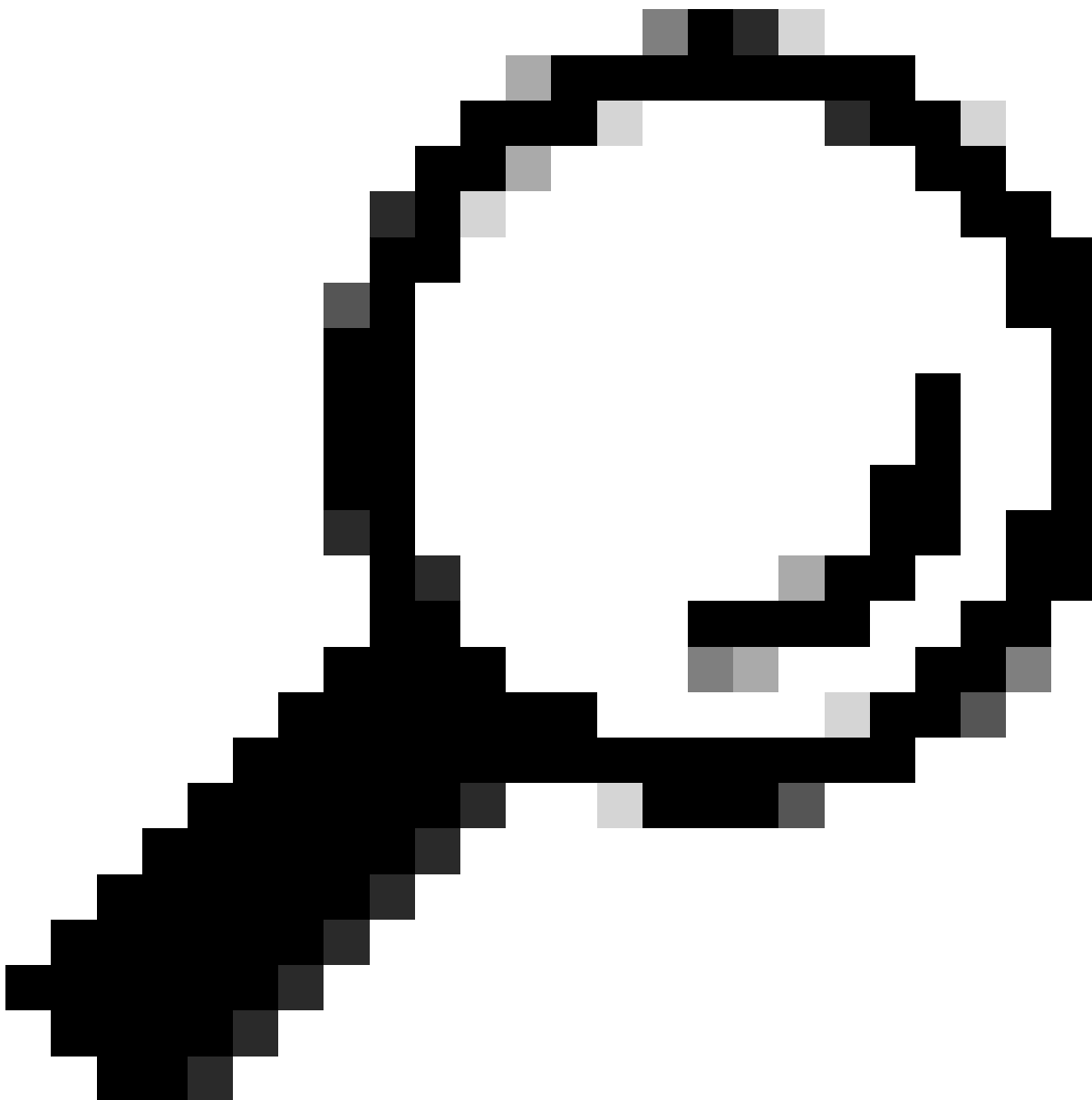
Cancel

Save



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.

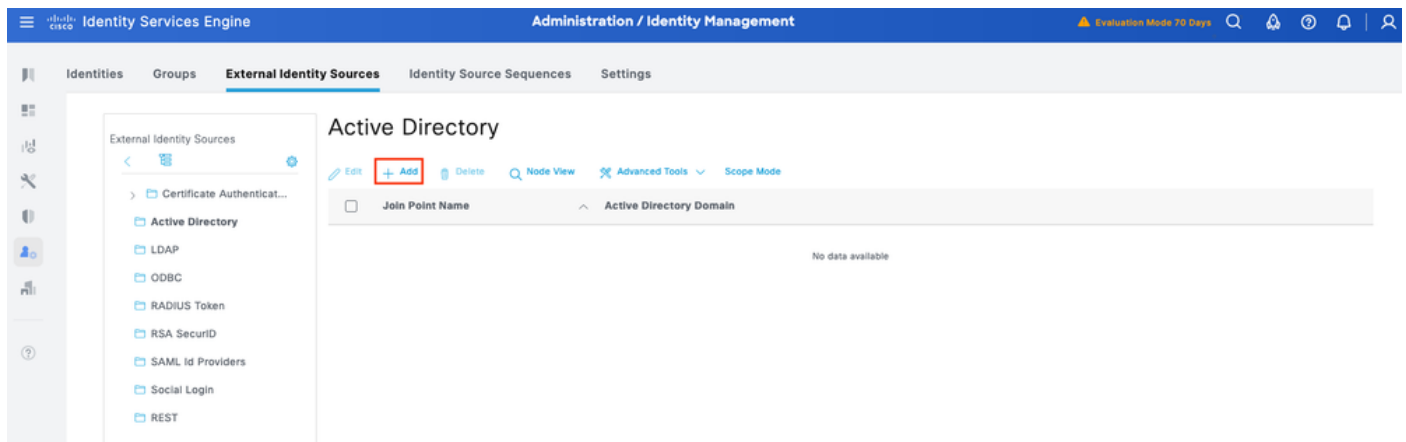


Consejo: Se recomienda habilitar el modo de conexión única para evitar reiniciar la sesión TCP cada vez que se envía un comando al dispositivo.

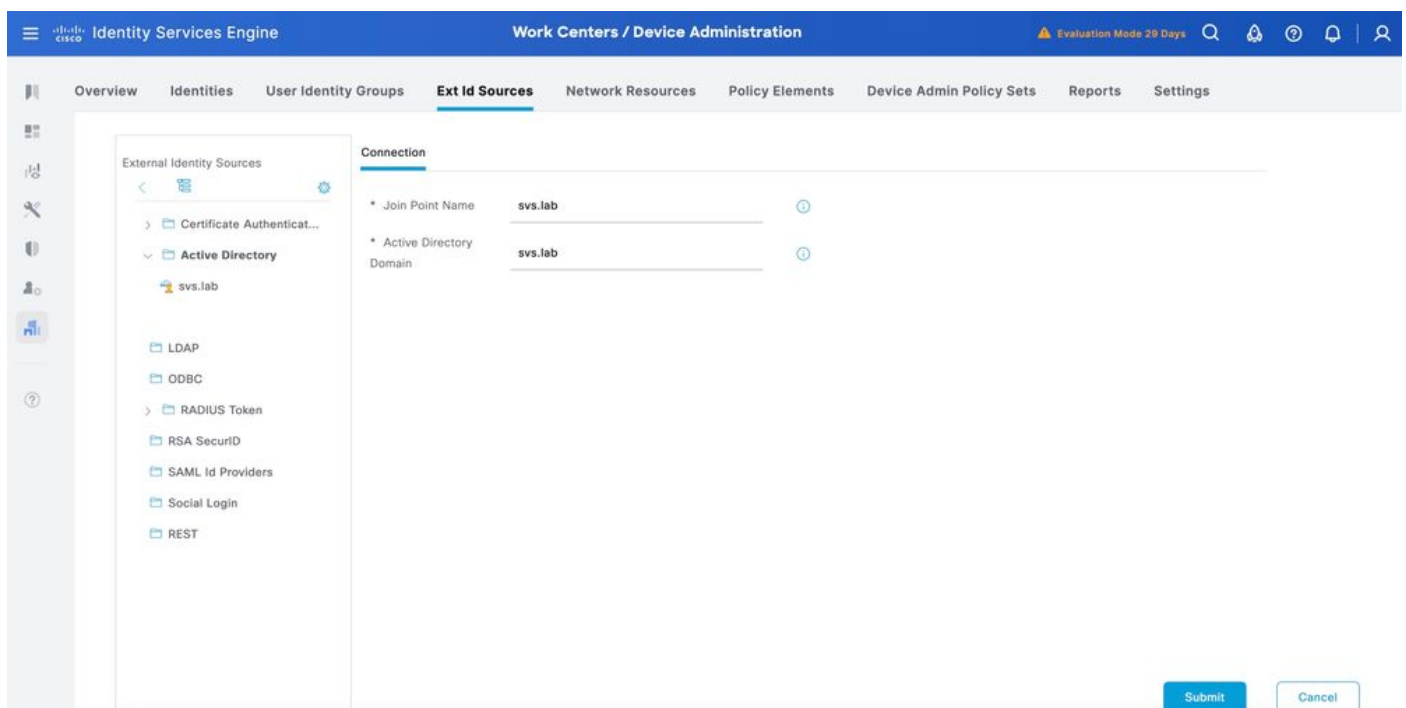
Configurar almacenes de identidad

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.

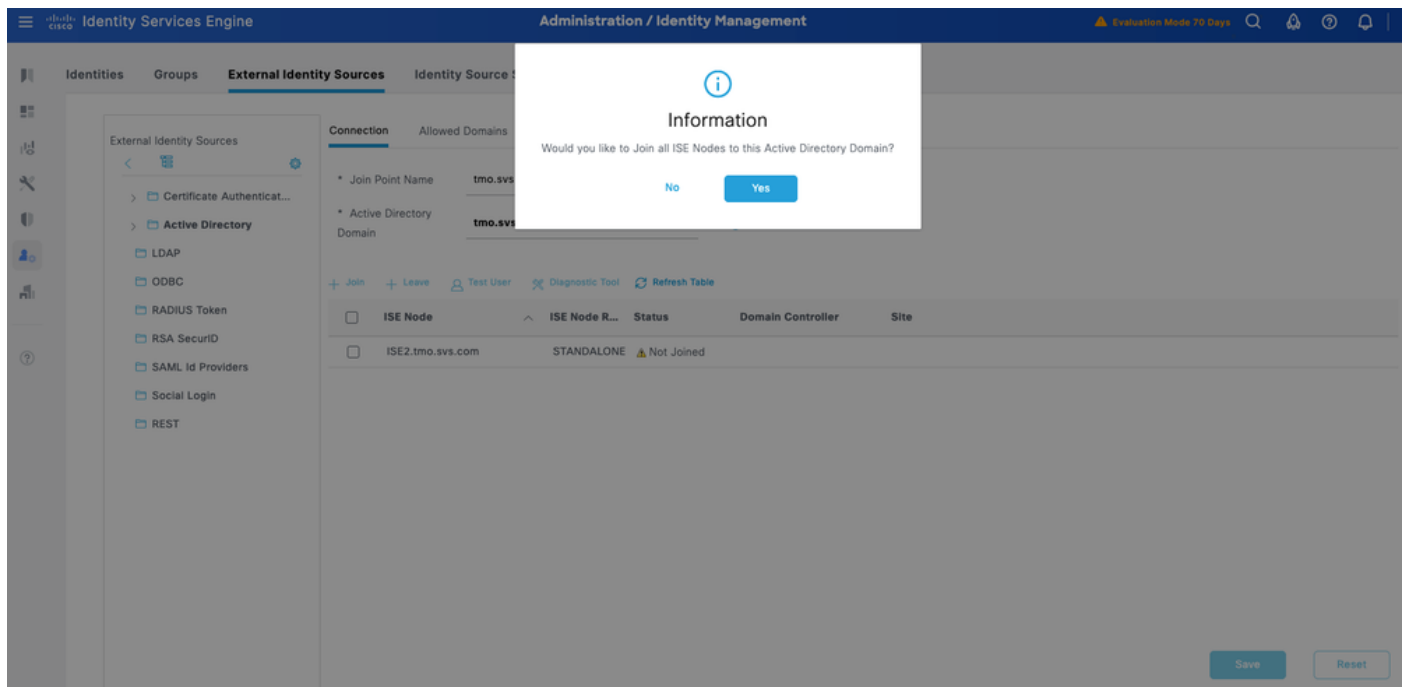
Paso 1. Navegue hasta Administración > Administración de identidad > Almacenes de identidad externos > Active Directory. Haga clic en Agregar para definir un nuevo punto de unión AD.



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.

×

Join Domain

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

* AD User Name ⓘ

administrator

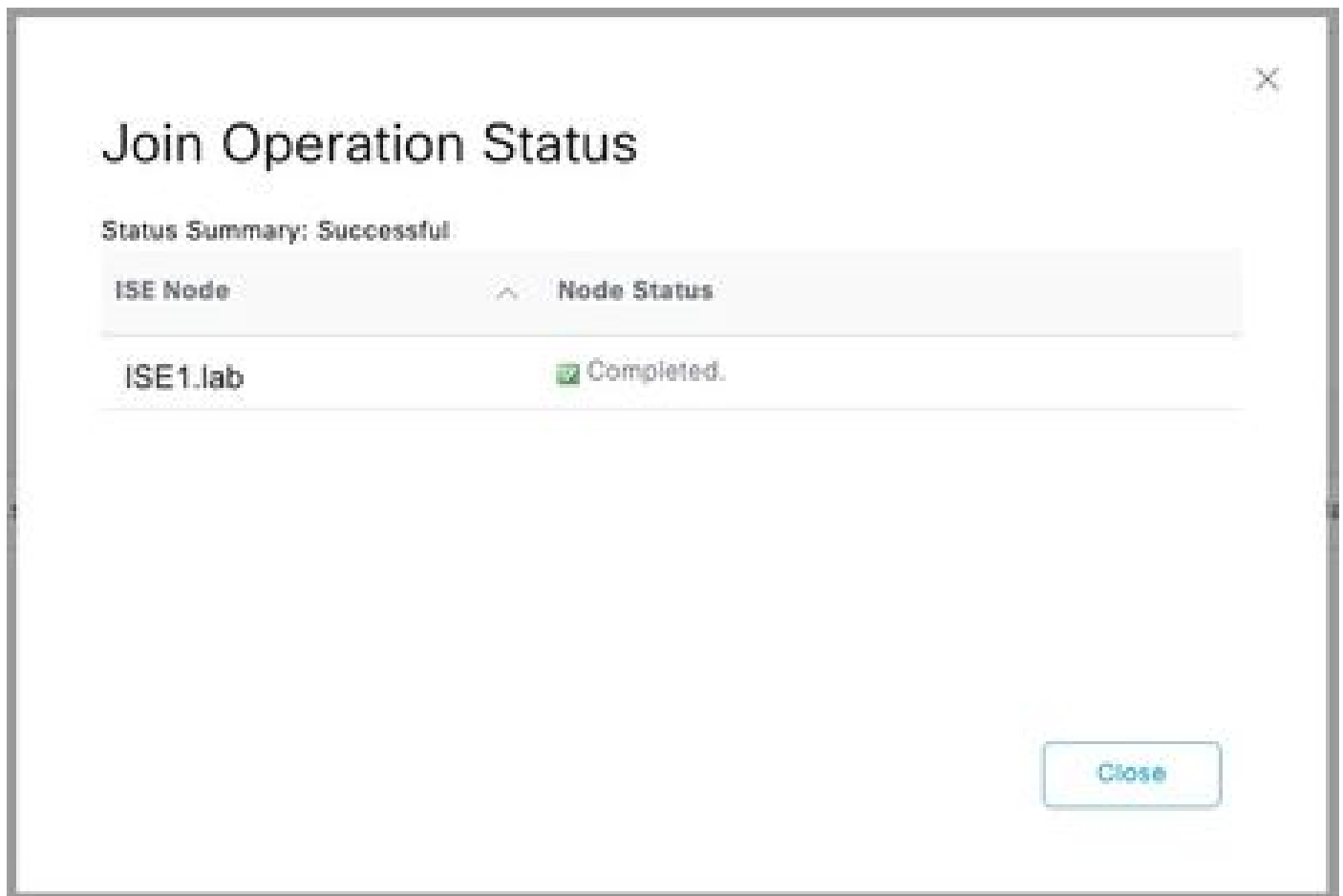
* Password ⓘ

☐ Specify Organizational Unit ⓘ

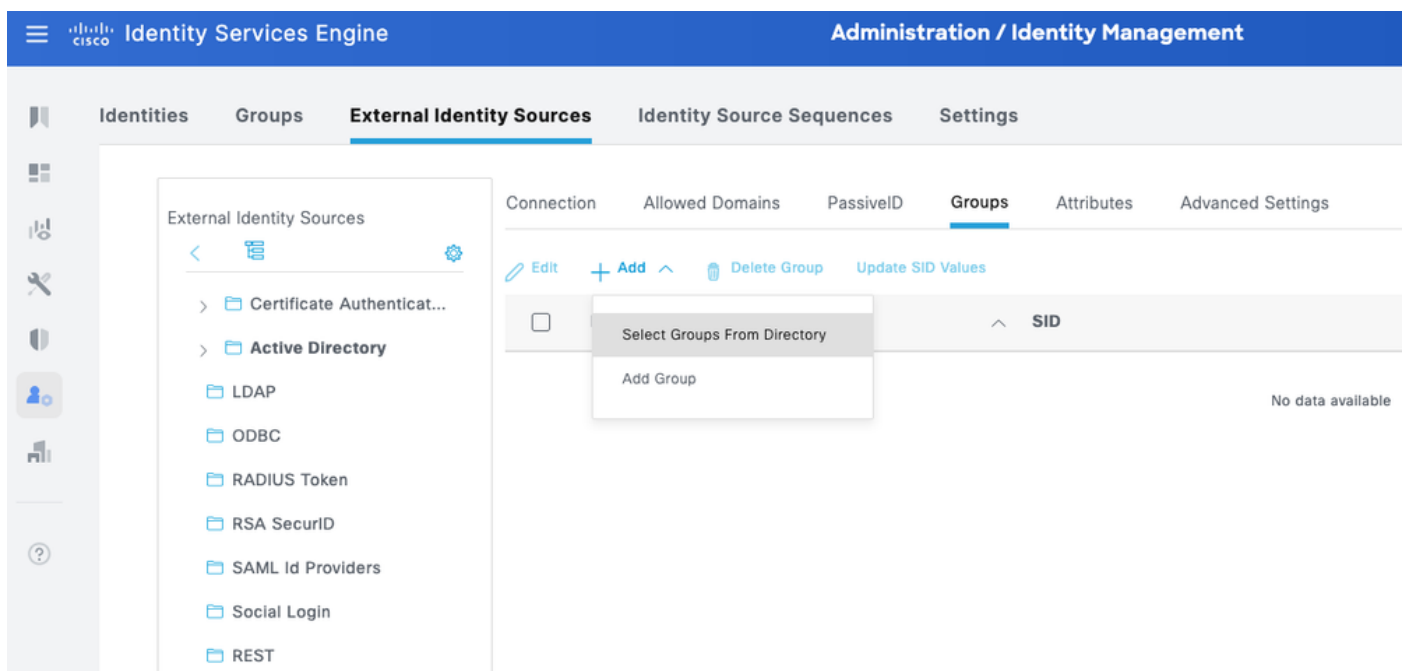
☒ Store Credentials ⓘ

Cancel

OK



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



Select Directory Groups

This dialog is used to select groups from the Directory.

Domain

Name Filter

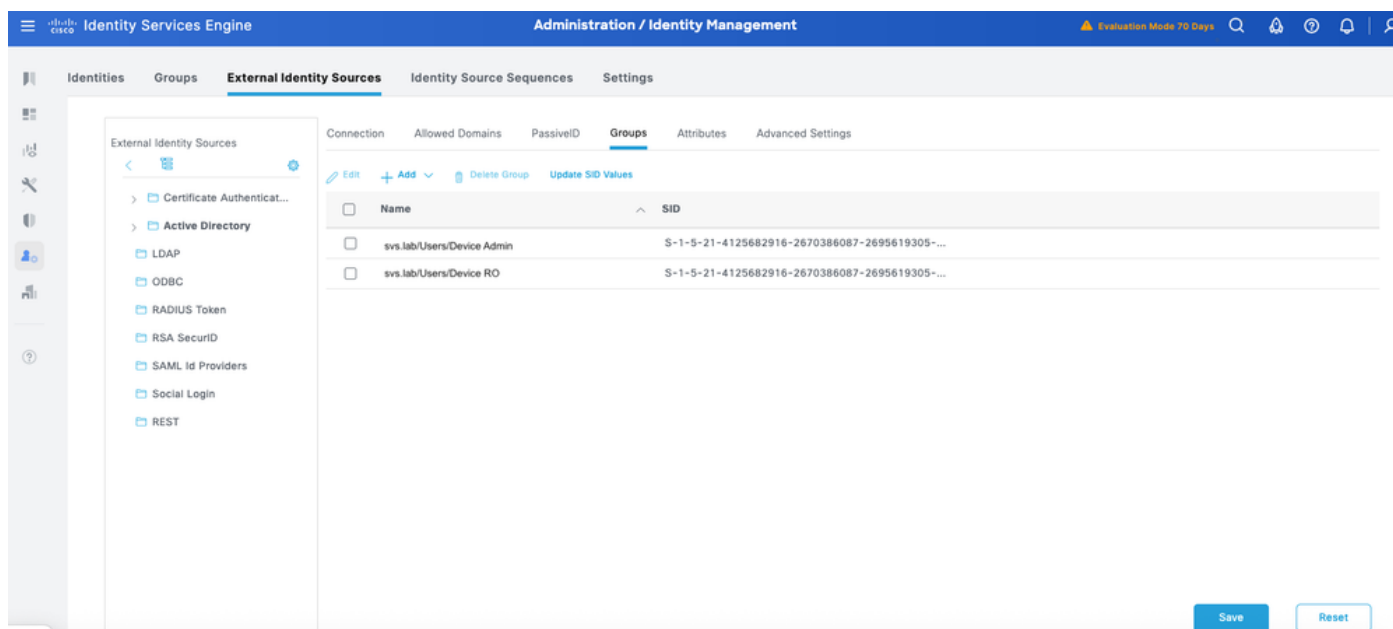
SID Filter

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+

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.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes the Cisco logo, 'Identity Services Engine', and 'Work Centers / Device Administration'. The left sidebar contains a menu with 'Overview', 'Identities', 'User Identity Groups', 'Ext Id Sources', 'Network Resources', 'Policy Elements' (selected), 'Device Admin Policy Sets', and 'More'. The main content area is titled 'TACACS Profiles > IOSXE_RW TACACS Profile'. It shows the 'Name' as 'IOSXE_RW' and a 'Description' field. Below this, there are tabs for 'Task Attribute View' (selected) and 'Raw View'. Under 'Task Attribute View', there is a 'Common Tasks' section with a 'Common Task Type' dropdown set to 'Shell'. Two attributes are listed: 'Default Privilege' and 'Maximum Privilege', both set to '15' with a dropdown arrow and a note '(Select 0 to 15)'.

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.

Identity Services Engine Work Centers / Device Administration

Overview Identities User Identity Groups Ext Id Sources Network Resources **Policy Elements** Device Admin Policy Sets More

Conditions

Network Conditions

Results

Allowed Protocols

TACACS Command Sets

TACACS Profiles

Name
IOSXE_RO

Description

Task Attribute View Raw View

Common Tasks

Common Task Type Shell

☒ Default Privilege 1 (Select 0 to 15)

☒ Maximum Privilege 1 (Select 0 to 15)

☐ Access Control List

☐ Auto Command

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.

Identity Services Engine | **Work Centers / Device Administration**

Overview | Identities | User Identity Groups | Ext Id Sources | Network Resources | **Policy Elements** | Device Admin Policy Sets | More

TACACS Command Sets > CISCO_IOSXE_RW
Command Set

Name: CISCO_IOSXE_RW

Description:

Commands

Permit any command that is not listed below ☒

Add | Trash | Edit | Move Up | Move Down

Grant	Command	Arguments
-------	---------	-----------

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.

Identity Services Engine | **Work Centers / Device Administration**

Overview | Identities | User Identity Groups | Ext Id Sources | Network Resources | **Policy Elements** | Device Admin Policy Sets | More

TACACS Command Sets > CISCO_IOSXE_RO
Command Set

Name: CISCO_IOSXE_RO

Description:

Commands

Permit any command that is not listed below ☐

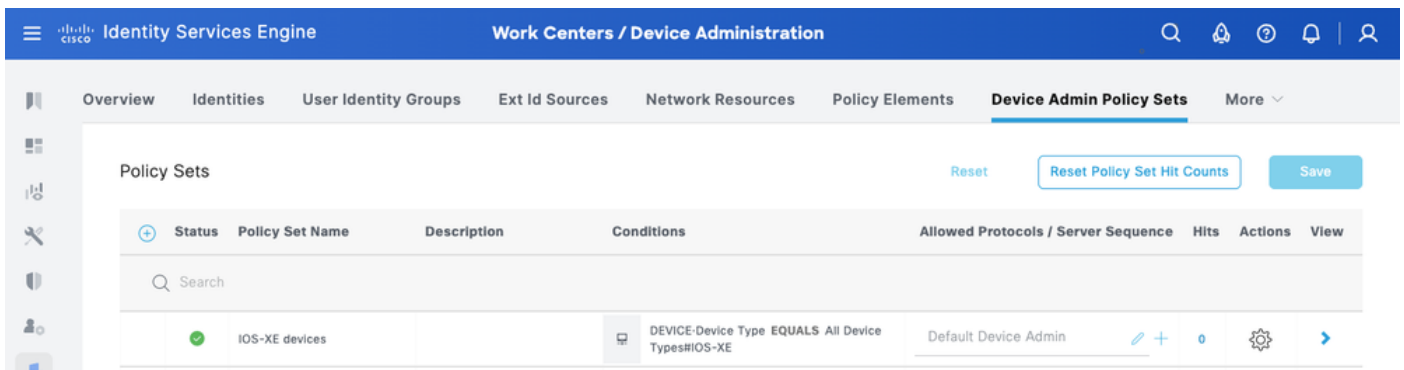
Add | Trash | Edit | Move Up | Move Down

Grant	Command	Arguments
☐	PERMIT	show

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.

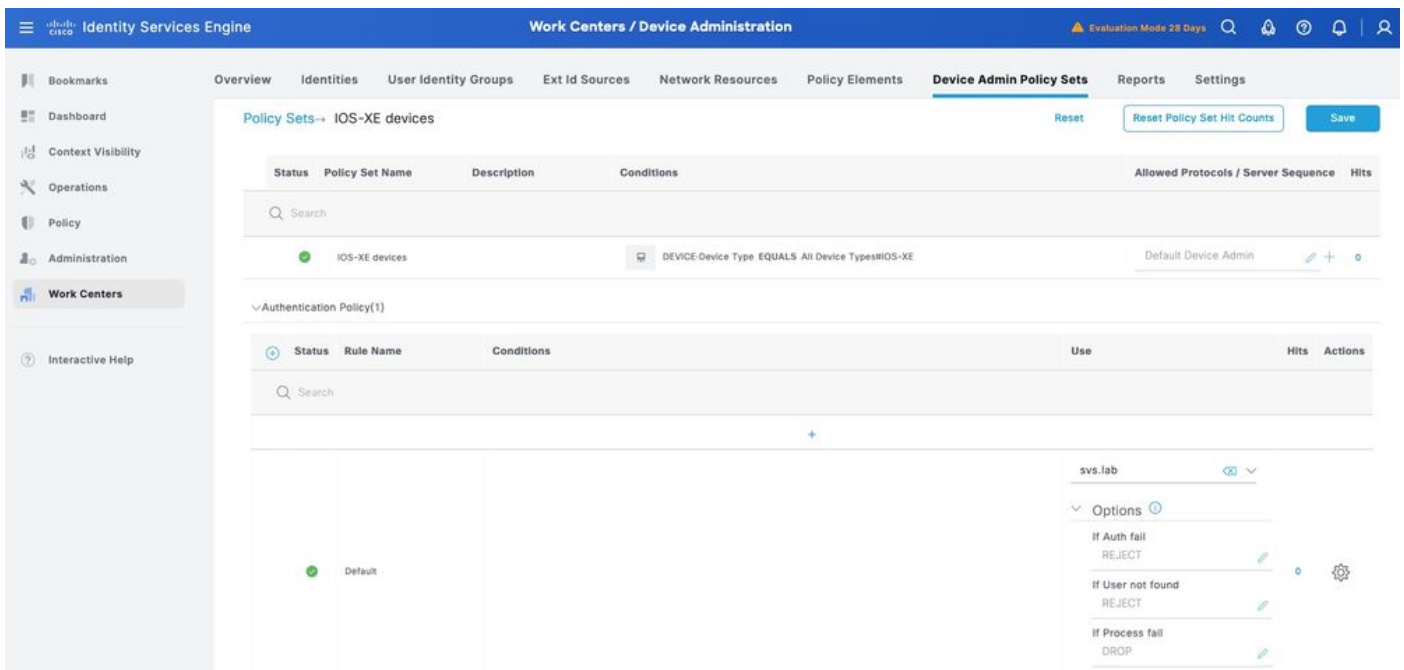


The screenshot shows the 'Device Admin Policy Sets' configuration page in the Cisco ISE interface. The page has a blue header with the Cisco logo and 'Identity Services Engine' text. Below the header is a navigation bar with tabs: Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements, and Device Admin Policy Sets (selected). The main content area shows a table of Policy Sets. The table has columns: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, Hits, Actions, and View. There is one policy set named 'IOS-XE devices' with a status of 'On'. The condition is 'DEVICE:Device Type EQUALS All Device Types#IOS-XE' and the allowed protocols are 'Default Device Admin'. There are buttons for 'Reset', 'Reset Policy Set Hit Counts', and 'Save'.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
On	IOS-XE devices		DEVICE:Device Type EQUALS All Device Types#IOS-XE	Default Device Admin	0		

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.



The screenshot shows the 'Authentication Policy' configuration page in the Cisco ISE interface. The page has a blue header with the Cisco logo and 'Identity Services Engine' text. Below the header is a navigation bar with tabs: Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements, Device Admin Policy Sets (selected), Reports, and Settings. The main content area shows a table of Authentication Policies. The table has columns: Status, Rule Name, Conditions, Use, Hits, and Actions. There is one policy set named 'Default' with a status of 'On'. The condition is 'DEVICE:Device Type EQUALS All Device Types#IOS-XE'. The 'Options' section shows 'If Auth fail' set to 'REJECT', 'If User not found' set to 'REJECT', and 'If Process fail' set to 'DROP'.

Status	Rule Name	Conditions	Use	Hits	Actions
On	Default	DEVICE:Device Type EQUALS All Device Types#IOS-XE		0	

Options:

- If Auth fail: REJECT
- If User not found: REJECT
- If Process fail: DROP

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.

Identity Services Engine Work Centers / Device Administration

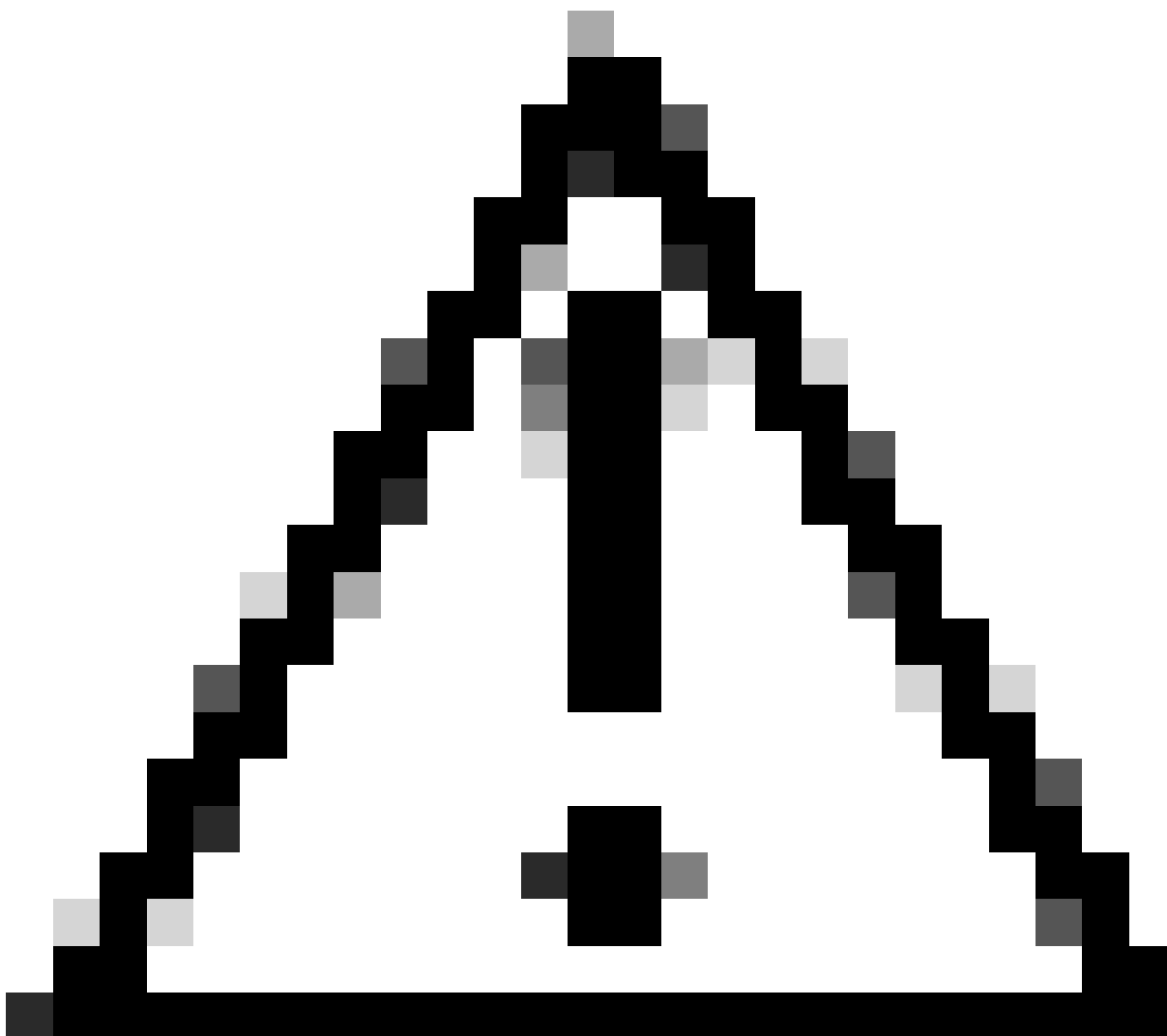
Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements **Device Admin Policy Sets** More

Policy Sets → IOS-XE devices [Reset](#) [Reset Policy Set Hit Counts](#) [Save](#)

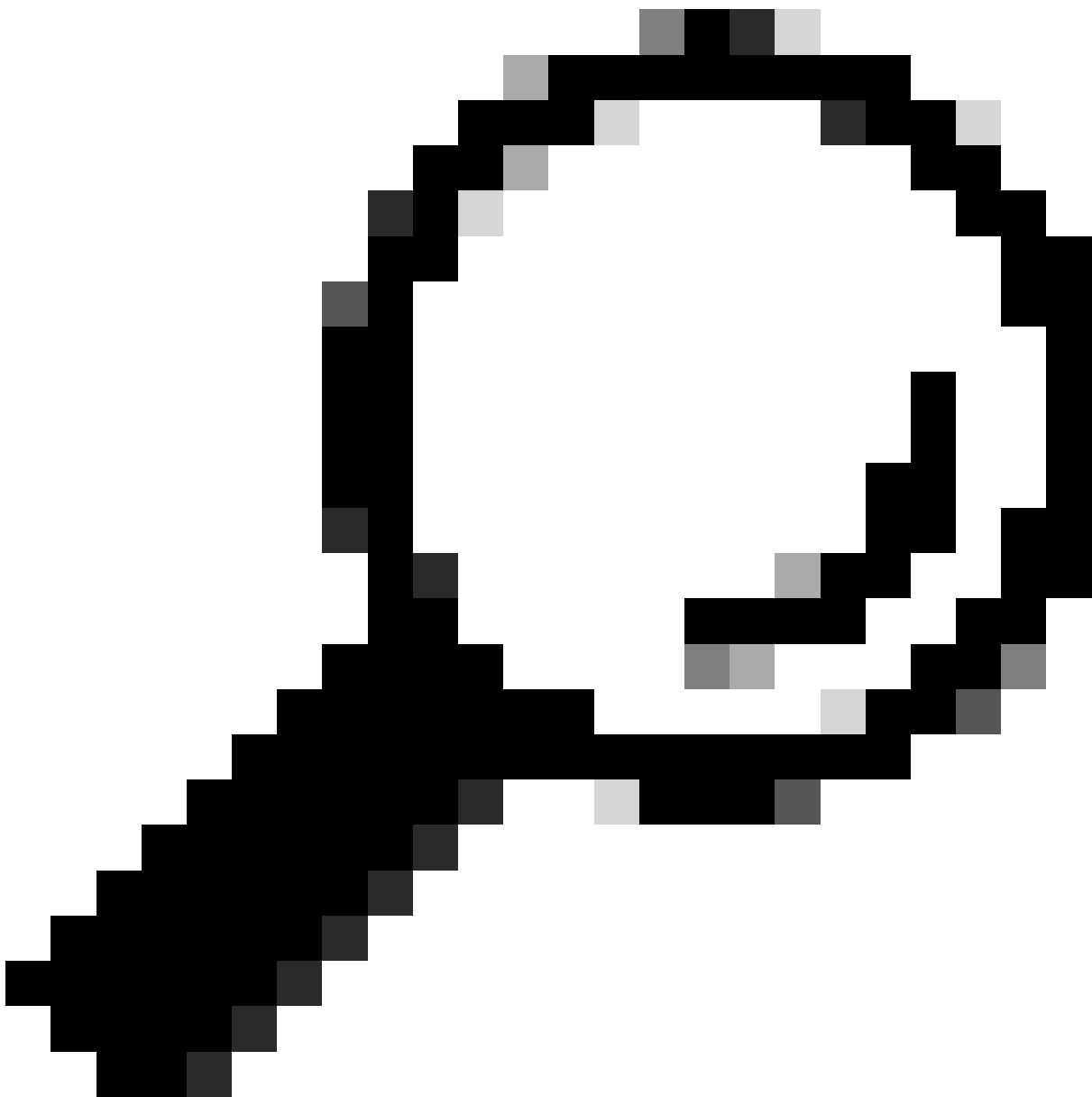
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	IOS-XE devices		DEVICE:Device Type EQUALS All Device Types#IOS-XE	Default Device Admin	0
> Authentication Policy(1)					
> Authorization Policy - Local Exceptions					
> Authorization Policy - Global Exceptions					
✓ Authorization Policy(3)					

				Results			
+	Status	Rule Name	Conditions	Command Sets	Shell Profiles	Hits	Actions
✓		Authorization Rule RO	svs.lab-ExternalGroups EQUALS svs.lab/Users/Device RO	CISCO_IOSXE_RO	IOSXE_RO	0	⚙
✓		Authorization Rule RW	svs.lab-ExternalGroups EQUALS svs.lab/Users/Device Admin	CISCO_IOSXE_RW	IOSXE_RW	0	⚙
✓		Default		DenyAllCommands	Deny All Shell Profile	0	⚙

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

```
ip domain name sv.s.lab
```

```
crypto key generate ec keysiz 256 label sv-256ec-key
```

Configuración de Trustpoint

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

```
crypto pki trustpoint sv_cat9k
  enrollment terminal pem
  subject-name C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=cat9k.sv.s.lab
  serial-number none
  ip-address none
  revocation-check none
  eckeypair sv-256ec-key
```

Paso 2. Autentique Trustpoint instalando el certificado de CA.

```
<#root>
```

```
cat9k(config)#
```

```
crypto pki authenticate sv_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
BhMCVVMxZzFzAVBgNVBAGTDk5vbnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECXMdU1ZTMRIwEAYDVQQDEw1TVlMgTGFi
Q0EwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUGA1UECBM0MjYyYzZlSH6EkEvxnJTy+kksFD33GyHqepk7vfp4NFU50tQ4HC7t/A0v9grDa3QW
VwV4MBBjHFM3s0J/ejgDYCMZhIAaPy0Zo5WLboOkXEiKjPLatKXojB8FVrhLF30
jMBSQwa4/Wlniy5S+7s4FFxsCf20COWfBAsnrs0tatIIhmcnx+VLJP7MRm8f0w4m
mutNo7IhbJSrgAFXmjlbBjMmgsp0bULo/wxMHdTbtPBf11HRHTkNI03qy04UADL2
WpoGhgT/FaxxBo2UBcnYVaP+jjREONYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7B0e8oDNKU6gX1ojKyLP/gC7j8AeP03ir+KZui8
```

```
b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
gJ+kQXe7QtT/u6m1MrtjE3gAEVpL334rTixy9hpKZIkB86t2ZA3JX8CLsbCa13sA
z1XCoONX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTA01xh60I4QnK+MNQKpTjt/E4
ydHl0rrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVL1783nTc9wYptQEPi5sw
83g9EMgKV0ARIiVUa/q1AgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAyb4
QgEBBAAQDAgAHMBkGCWCGSAGG+EIBDQQMFGpTVlMgTGFIEENBMAOGCSqGSIB3DQEB
CwUAA4ICAQAIT308oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oK0dGayi
iSEkSSX9qyflFINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXRX67X+v
0+ja6zTQqj06lqJhmrSkyFbYf/ZTpe4d10zJsZjNsN0r8bF9n0A/7qNZLp3Z3cpU
PU0KdbiSvRqnPw3e8TfITVmAzcx8COI2SrYFMSUazo1VBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIEOf5ay1PKURO/8aj/B7a1uJapXkmnj5qPeGhN0pB
Q9r14reov4so2EspkXS7CrH9yGfpIyTprokz1UvZBZ8v1oI7YZmjFmem+5rT6Gnk
eU/1X7nV61SYG5W5K+I8uaKuyBHOMn7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggz1P0dsS/i6Lo7ypYX0eB9HgVDCkzQsLXQuHGj/2WsgPgDRcjkvnyURk4Jx+Ib
xDrmo7e0XPpSW4l72a6K18CR3U2Cr4wsuvndPEq/qd2NRSBWffFOXE/AJHQG7STT
HaXLU9r2Ko603oecu8ysGTWl1It/9T1/F0b0xZRugWcpJrVoTgDGUA==
```

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

Certificate has the following attributes:

Fingerprint MD5: D9C404B2 EC08A260 EC3539E7 F54ED17D

Fingerprint SHA1: 0EB181E9 5A3ED780 3BC5A805 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 svcs_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-----

```
MIIBfDCCASMAQAwgYQxGjAYBgNVBAMTEWdhD1rLnRtby5zdnMuY29tMQwwCgYD
VQQLewNTVlMxDjAMBgNVBAoTBUNpc2NvMQwwCgYDVQQHEwNSVFAXCzAJBgNVBAGT
Ak5DMQswCQYDVQQGEwJVUzEgMB4GCsqGSIB3DQEJAhyRY2F0OWsudG1vLnN2cy5j
b20wWTATBgqhkJOPQIBggqhkJOPQMBBwNCAATpYE7atscrt14ddevCh3UgxjYi
4N4oBGWrpJBctKy4so8V5i6RXDt7kHgPzp14Qnf20bcXVODE1wtTAHHBrIXqoDww
```

```
OgYJKoZIhvcNAQkOMSOwKzAcBgNVHREEFTATghFjYXQ5ay50bW8uc3ZzLmNvbTAL
BgNVHQ8EBAMCB4AwCgYIKoZIzj0EAwQDRwAwRAIgZqP2QTWm3ZZrmIphJ7+jSTER
40kTx2DiVs1c1Xf+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 svcs_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
BhMCVVMxZzAVBgNVBAGTDk5vcmRoIENhcm9saW5hMRwwDgYDVQQHEwdSYWx1aWdo
MQ4wDAYDVQQKEwVDAxNjBzEMMAoGA1UECXMUDU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNTE0MTUxMjAwWhcNMjUwNTE0MTUxMjAwWjCBhDEaMBGGA1UEAxMR
Y2F0OWsudG1vLnN2cy5jb20xDDAKBgNVBAsTA1NWUzE0MAwGA1UEChMFQ21zY28x
DDAKBgNVBAcTA1JUUEDEMAkGA1UECBMCTkMxCzAJBgNVBAYTA1VTMSAwHgYJKoZI
hvcNAQkCFhFjYXQ5ay50bW8uc3ZzLmNvbTBZMBMGByqGSM49AgEGCCqGSM49AwEH
A0IAB01gTtq2xyu2Xh1168KHdSDGniLg3igEZaukkFy0rLiYjXmLpFc03uQeA/O
nXhCd/bRtxdU4MTXC1MAccGsheqjTTBLMB4GCWCGSAGG+EIBDQRRFg94Y2EgY2Vy
dG1maWNhdGUwHAYDVR0RBBUwE4IRY2F0OWsudG1vLnN2cy5jb20wCwYDVR0PBAQD
AgeAMAOGCSqGSIb3DQEBGwUAA4ICAQB0bgKVykeyVC9Usvuu0AUsGaZHGwy2H9Yd
m5vIauI6PJczkCzIoAIghHPGQhIgpEcRqtGyXPZ2r8TCJP11WXNN/G73sFyWAHzY
RtmIM5KIojiDHLtiFpayxv9juDu0ZRx+wYR2PIQ5eLv1bafg7K8E82sq0Cf0tcPr
Oc0NU8UCxq0bd0gu4XsdBN1+wcWFqeQSDLP7nxvh00m/LXwCWUhwgVio0AuU2Fe
k5NthtvdXNAhRAImQdTyq6u/yB7vwTwJHcRiJc5USsyZCsTBb6RvL+HsXqBgXGc5
1xCSoltY0dUxFipJyK2MOZBY2zq2cNSc8Xbso5/OEQmnHtpWPvij4rSPUHQSY+4m
Qq2Sn3iqf4mGh/A08T4iXfWdWfNezh7ZxMsCSCK/ZR1ELZ2hj60fzwX1H27Uf8XU
ecr0Wx+WzRn7LVRCaGQzFkukfi8S4DLLNtxNHFSLBVX5yHXCLEL+CQ7n8Z/pxcB
VVRpitwN3Zb09poZyWiRLTnBsb42xNaWiL9bjQznA0iTDfmfFFourBsaAioz7ouY
2r1Mh+OpE83Uu+41OTMawDgGiEv7iaiJ6xWc95EC+Adm0x3FvBXmtIM9qr7WwHW6
3C2hVYHJH254e1V5+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 sv_s_tacacs
  address ipv4 10.225.253.209
  single-connection
  tls port 6049
  tls idle-timeout 60
  tls connection-timeout 60
  tls trustpoint cli_s_cat9k
  tls ip tacacs source-interface GigabitEthernet0/0
  tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ sv_s_tls
  server name sv_s_tacacs
  ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request
```

Paso 2. Configure los métodos AAA.

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

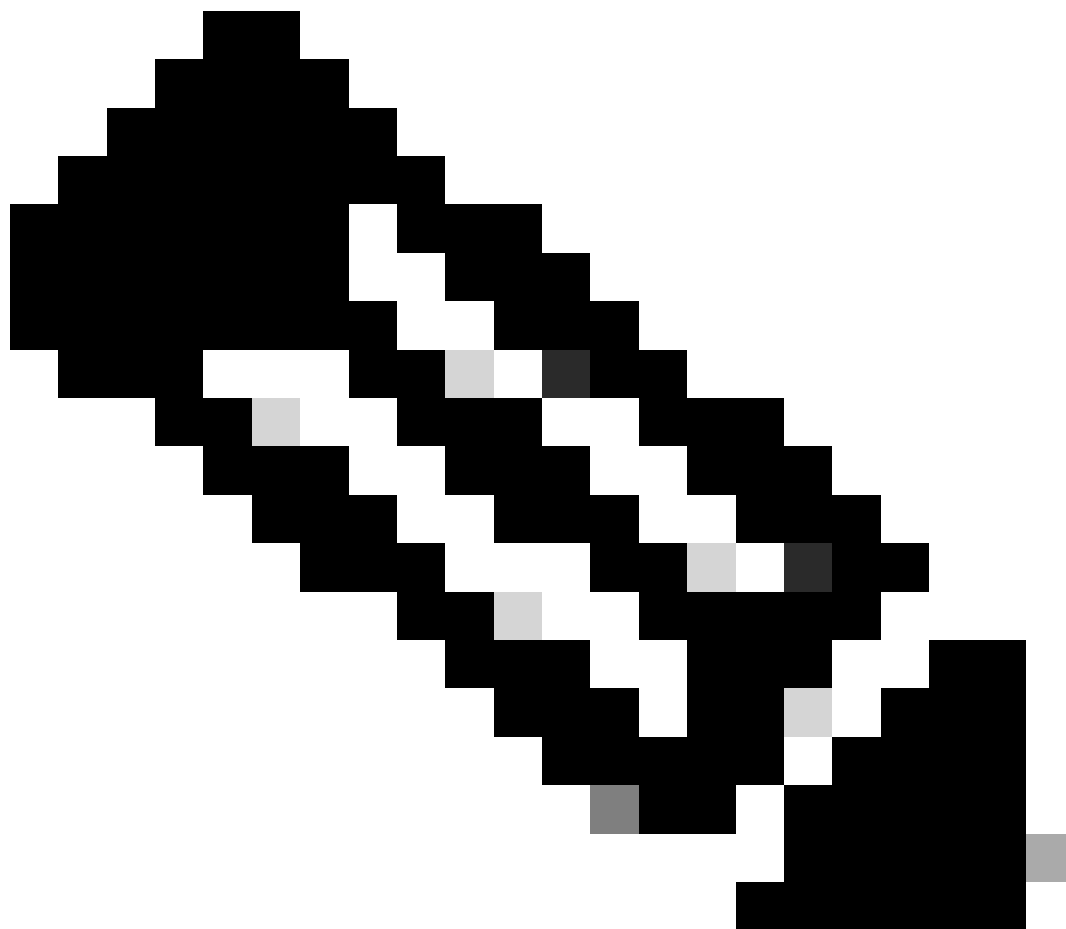
Método de configuración 2: par de claves generado por CA

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.

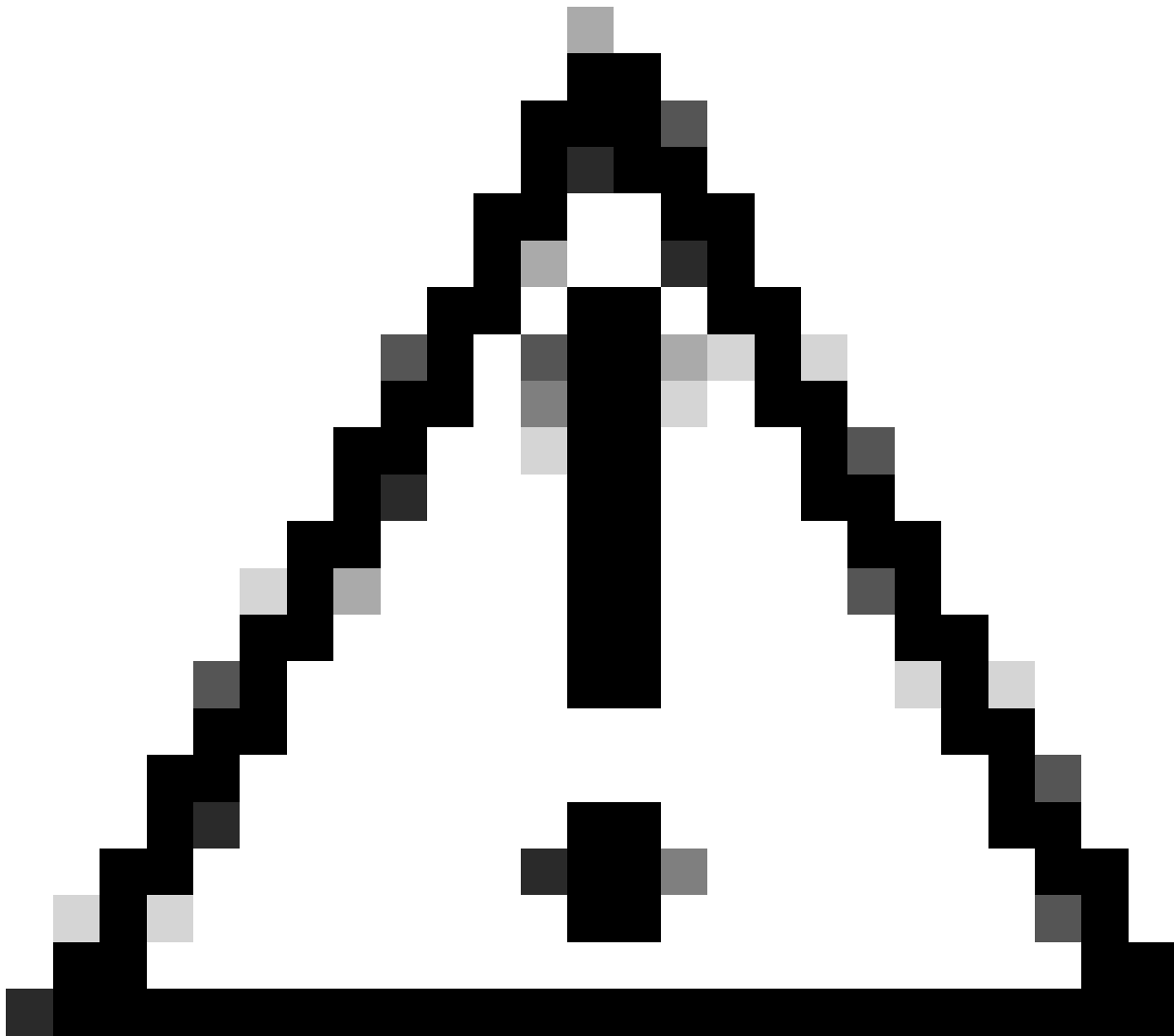
Paso 1. Crear punto de confianza de cliente.

```
cat9k(config)#crypto pki trustpoint sv_s_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 svc_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 svc_cat9k_25jun17

Certificate

Status: Available

Certificate Serial Number (hex): 5860BF33A2033365

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: svc_cat9k_25jun17

CA Certificate

Status: Available

Certificate Serial Number (hex): 20CD7402C4DA37F5

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: svc_cat9k_25jun17 svc_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 svb_tacacs
  address ipv4 10.225.253.209
  single-connection
  tls port 6049
  tls idle-timeout 60
  tls connection-timeout 60
  tls trustpoint client svb_cat9k
  tls ip tacacs source-interface GigabitEthernet0/0
  tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ svb_tls
  server name svb_tacacs
  ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request
```

Paso 2. Configure los métodos AAA.

```
aaa authentication login default group svb_tls local enable
aaa authentication login console local enable
aaa authentication enable default group svb_tls enable
aaa authorization config-commands
aaa authorization exec default group svb_tls local if-authenticated
aaa authorization commands 1 default group svb_tls local if-authenticated
aaa authorization commands 15 default group svb_tls
aaa accounting exec default start-stop group svb_tls
aaa accounting commands 1 default start-stop group svb_tls
aaa accounting commands 15 default start-stop group svb_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).