

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

Contenido

[Introducción](#)

[Overview](#)

[Utilización de esta guía](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Licencias](#)

[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](#)

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

[Configurar almacenes de identidad](#)

[Configurar perfiles de shell TACACS+](#)

[Administrador de NX-OS](#)

[Soporte técnico de NX-OS](#)

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

[Configuración de Cisco NX-OS para TACACS+ sobre TLS](#)

[Configuración del servidor TACACS+](#)

[Configuración de Trustpoint](#)

[Configuración de TACACS+ TLS](#)

[Configuración AAA](#)

[Prueba y solución de problemas de acceso de usuario para NX-OS](#)

[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 NX-OS 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 NX-OS.

- Parte 1: Configuración de ISE para la administración de dispositivos
- Parte 2: Configuración de Cisco NX-OS para TACACS+ sobre TLS

Prerequisites

Requirements

Prerrequisitos 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 estas versiones de software y hardware:

- Dispositivo virtual ISE VMware, versión 3.4, parche 2.
- Switch Nexus 9000 modelo C9364D-GX2A, Cisco NX-OS versión 10.5(3t).

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.

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. Navegue hasta Administración > Sistema > Certificados.



Summary

Endpoints

Guests

Vulnerability

Administration

System

Deployment

Licensing

Certificates

Logging

Maintenance

Upgrade & Rollback

Health Checks

Backup & Restore

Admin Access

Settings

Identity Management

Identities

Groups

External Identity Sources

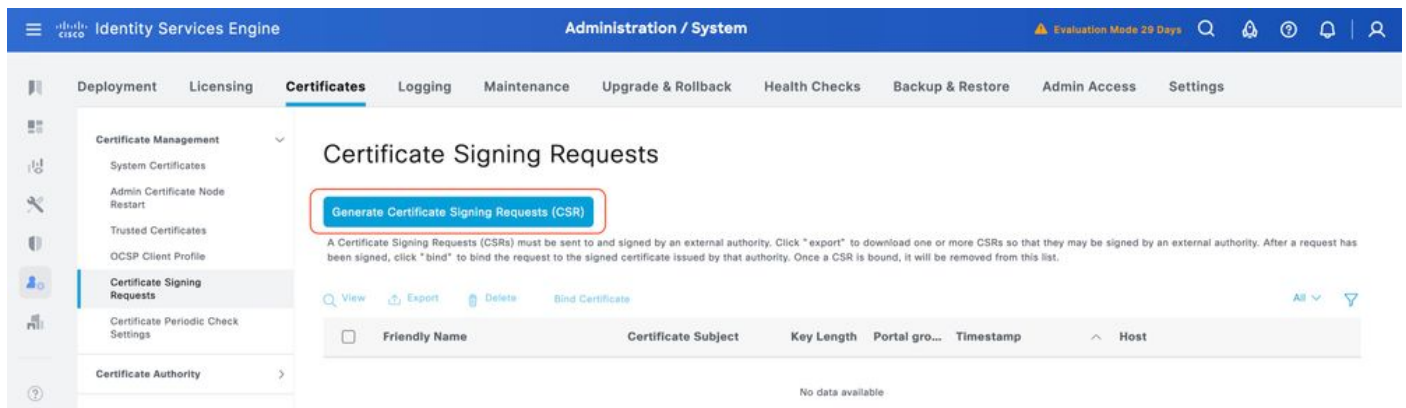
Identity Source Sequences

Settings

Feed Service

Profiler

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



Paso 4. Seleccione TACACS en Uso.

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 adecuada.

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 bajo Nombre alternativo del sujeto (SAN).

Subject Alternative Name (SAN)

⋮	DNS Name	✓	ISE1.lab	−	+	
⋮	IP Address	✓	10.225.253.209	−	+	ⓘ

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



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

Cargar certificado de CA raíz para autenticación de servidor TACACS+

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

Trusted Certificates For disaster recovery it is recommended to export and backup all your trusted certificates.

Buttons: Edit, **Import**, Export, Delete, View, show internal CA certificates

☐	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 la opción Confianza para la autenticación dentro de ISE esté habilitada.

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 Certificados Protegidos.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System page. The left sidebar contains the navigation menu with 'Certificates' selected. The main content area displays the 'Trusted Certificates' page. A table lists the trusted certificates, with the first row highlighted in red. The table has columns: Friendly Name, Trusted For, Serial Number, Issued To, Issued By, Valid From, Expiration Date, and Status.

Friendly Name	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Status
CN=SVS LabCA, OU=SVS, O=Cisco, L=...	Infrastructure Cisco Services Endpoints AdminAuth	20 CD 74 02 ...	SVS LabCA	SVS LabCA	Mon, 28 Apr 2025	Sat, 28 Apr 2...	Enz
Default self-signed server certificate	Endpoints Infrastructure	02 36 30 F4 6...	ISE2.tmo.svs.com	ISE2.tmo.svs.com	Fri, 11 Jul 2025	Sun, 11 Jul 2...	Enz
DigiCert Global Root CA	Cisco Services	08 3B E0 56 9...	DigiCert Global R...	DigiCert Global R...	Fri, 10 Nov 2006	Mon, 10 Nov ...	Enz
DigiCert Global Root G2 CA	Cisco Services	03 3A F1 E6 ...	DigiCert Global R...	DigiCert Global R...	Thu, 1 Aug 2013	Fri, 15 Jan 20...	Enz
DigiCert root CA	Endpoints Infrastructure	02 AC 5C 26 ...	DigiCert High Ass...	DigiCert High Ass...	Fri, 10 Nov 2006	Mon, 10 Nov ...	Enz
DigiCert SHA2 High Assurance Server ...	Endpoints Infrastructure	04 E1 E7 A4 ...	DigiCert SHA2 Hi...	DigiCert High Ass...	Tue, 22 Oct 2013	Sun, 22 Oct 2...	Enz

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. Navegue hasta 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 the navigation menu with 'Certificates' selected. The main content area displays the 'Certificate Signing Requests' page. A button 'Generate Certificate Signing Requests (CSR)' is visible. Below it, a text block explains 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 red.

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

Identity Services EngineAdministration / SystemEvaluation Mode 29 Days

DeploymentLicensingCertificatesLoggingMaintenanceUpgrade & RollbackHealth ChecksBackup & RestoreAdmin AccessSettings

Certificate ManagementSystem CertificatesAdmin Certificate Node RestartTrusted CertificatesOCSP Client ProfileCertificate Signing RequestsCertificate Periodic Check SettingsCertificate Authority

Bind CA Signed Certificate* Certificate FileExaminar...ISE1.lab.crtFriendly NameValidate Certificate ExtensionsUsage☒ TACACS: Use certificate for TACACS ServerSubmitCancel

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

Warning

The certificate you are importing or generating matches an existing certificate. (Both certificates have the same subject.) If you proceed, the existing certificate will be replaced, and the new certificate will be given the same roles and Portal tag, if applicable, as the existing certificate.

Do you wish to replace the existing certificate?

NoYes

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

Identity Services EngineAdministration / SystemEvaluation Mode 29 Days

DeploymentLicensingCertificatesLoggingMaintenanceUpgrade & RollbackHealth ChecksBackup & RestoreAdmin AccessSettings

Certificate ManagementSystem CertificatesAdmin Certificate Node RestartTrusted CertificatesOCSP Client ProfileCertificate Signing RequestsCertificate Periodic Check SettingsCertificate Authority

System Certificates

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

EditGenerate Self Signed CertificateImportExportDeleteView

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=ISE1.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. Navegue hasta Administración > Sistema > Configuración.



Identity Services Engine



Bookmarks



Dashboard



Context Visibility



Operations



Policy



Administration



Work Centers



Interactive Help

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 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

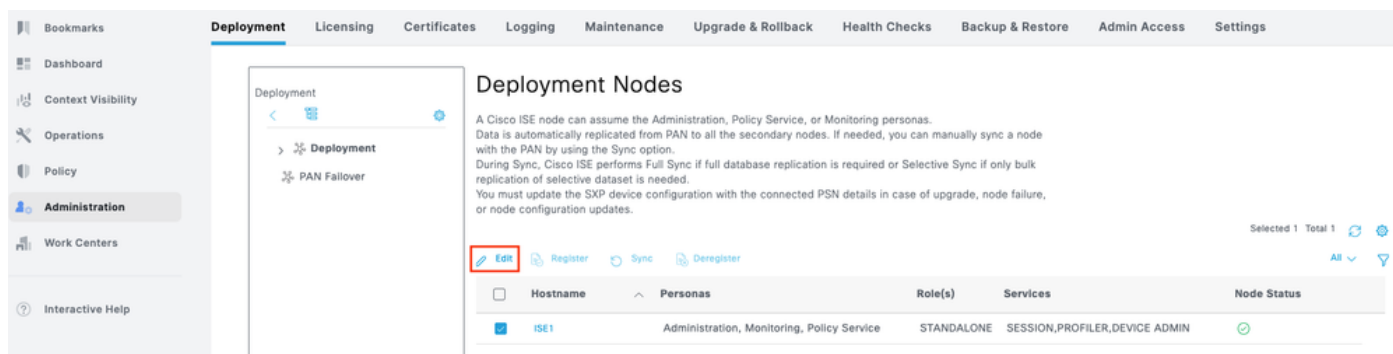
☒ TLS 1.3



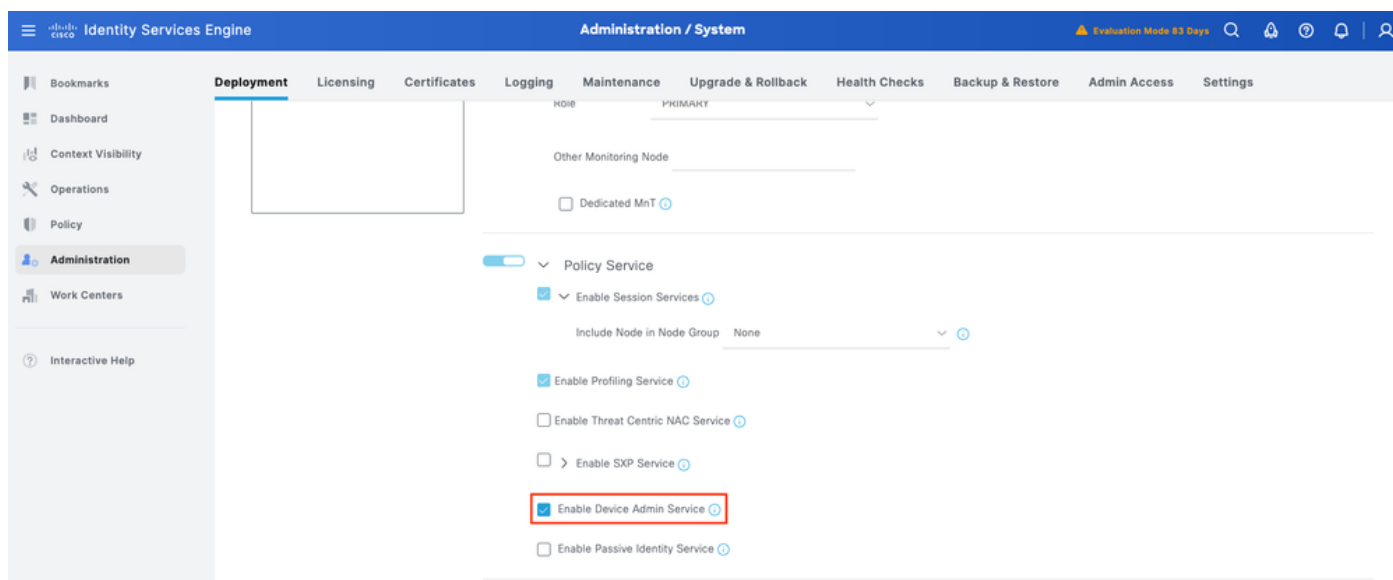
Advertencia: Al cambiar la versión de TLS, el servidor de aplicaciones de Cisco ISE se reinicia en todos los equipos de implementación de Cisco ISE.

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. Seleccione la casilla de verificación junto al nodo ISE y haga clic en Editar.



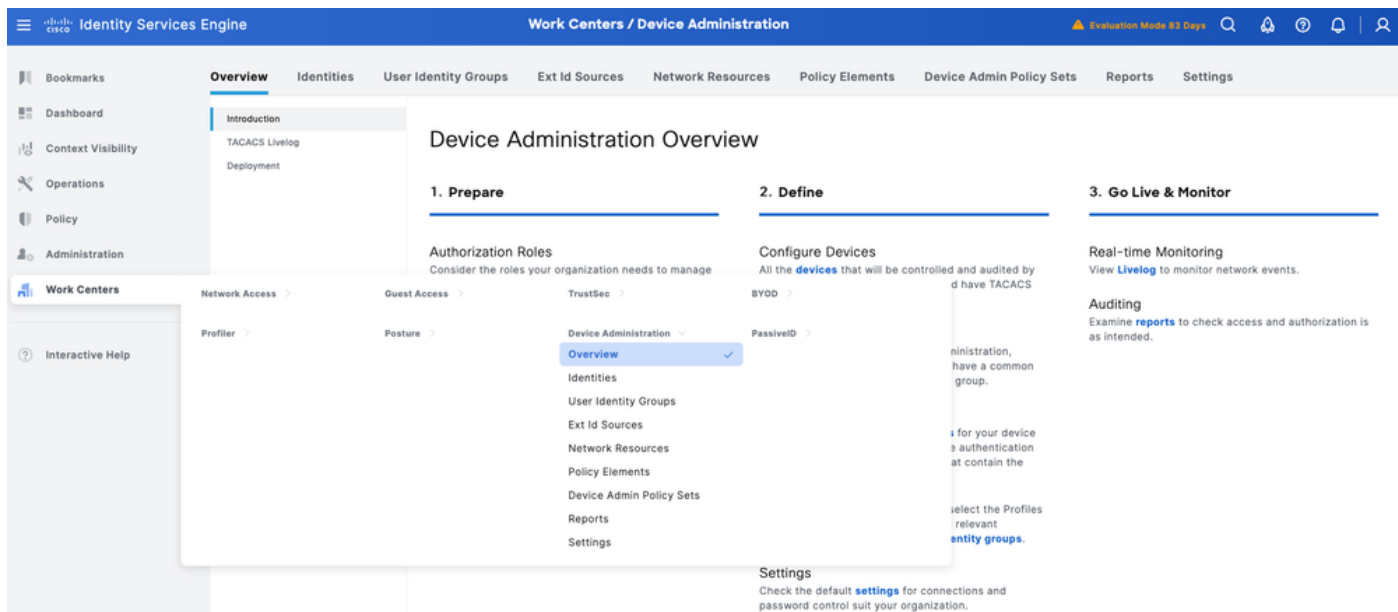
Paso 2. En General Settings, desplácese hacia abajo y seleccione la casilla de verificación junto a Enable Device Admin Service.



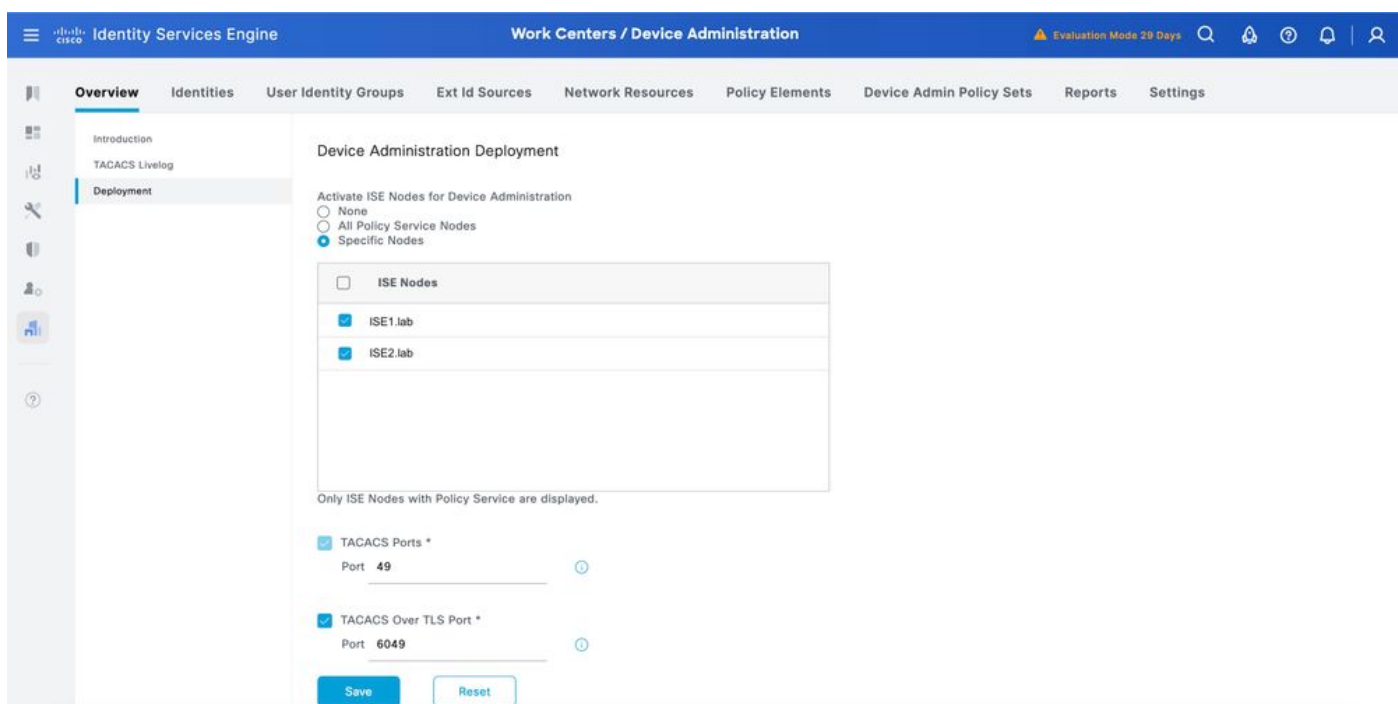
Paso 3. Guarde la configuración. El servicio Device Admin está ahora habilitado en ISE.

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.

Dispositivo 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. Vaya a Centros de trabajo > Administración de dispositivos > Recurso de red. Haga clic en Network Device Groups.

Identity Services Engine Work Centers / Device Administration

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

Network Devices

Network Device Groups

Default Devices

TACACS External Servers

TACACS Server Sequence

All Groups Choose group

Add Duplicate Edit Trash Show group members Import Export Flat Table Expand All Collapse All

Name	Description	No. of Network Devices
> All Device Types	All Device Types	--
> All Locations	All Locations	--
Atlanta		0
Los Angeles		0
New York		0
> Is IPSEC Device	Is this a RADIUS over IPSEC Device	--

Todos los tipos de dispositivos y todas las ubicaciones son jerarquías predeterminadas proporcionadas por ISE. Agregue sus propias jerarquías y defina 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 NS-OX como dispositivo de red. Vaya a Centros de trabajo > Administración de dispositivos > Recursos de red. Haga clic en Add para agregar un nuevo POD2IPN2 del dispositivo de red.

Identity Services Engine Administration / Network Resources

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences External MDM More

Network Devices List > POD2IPN2

Network Devices

Name POD2IPN2

Description

IP Address * IP : 10.225.253.177 / 32

Device Profile Cisco

Model Name C9364D-GX2A

Software Version 10.5(3t)

Network Device Group

Location Atlanta Set To Default

IPSEC No Set To Default

Device Type NXOS Set To Default

Paso 3. Ingrese la dirección IP del Dispositivo y asegúrese de asignar la Ubicación y el Tipo de Dispositivo para el Dispositivo. Finalmente, habilite los ajustes de autenticación de TACACS+ sobre TLS.

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

Network Devices

Network Device Groups

Network Device Profiles

External RADIUS Servers

RADIUS Server Sequences

External MDM

More

Network Devices

Default Device

Device Security Settings

☐ 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

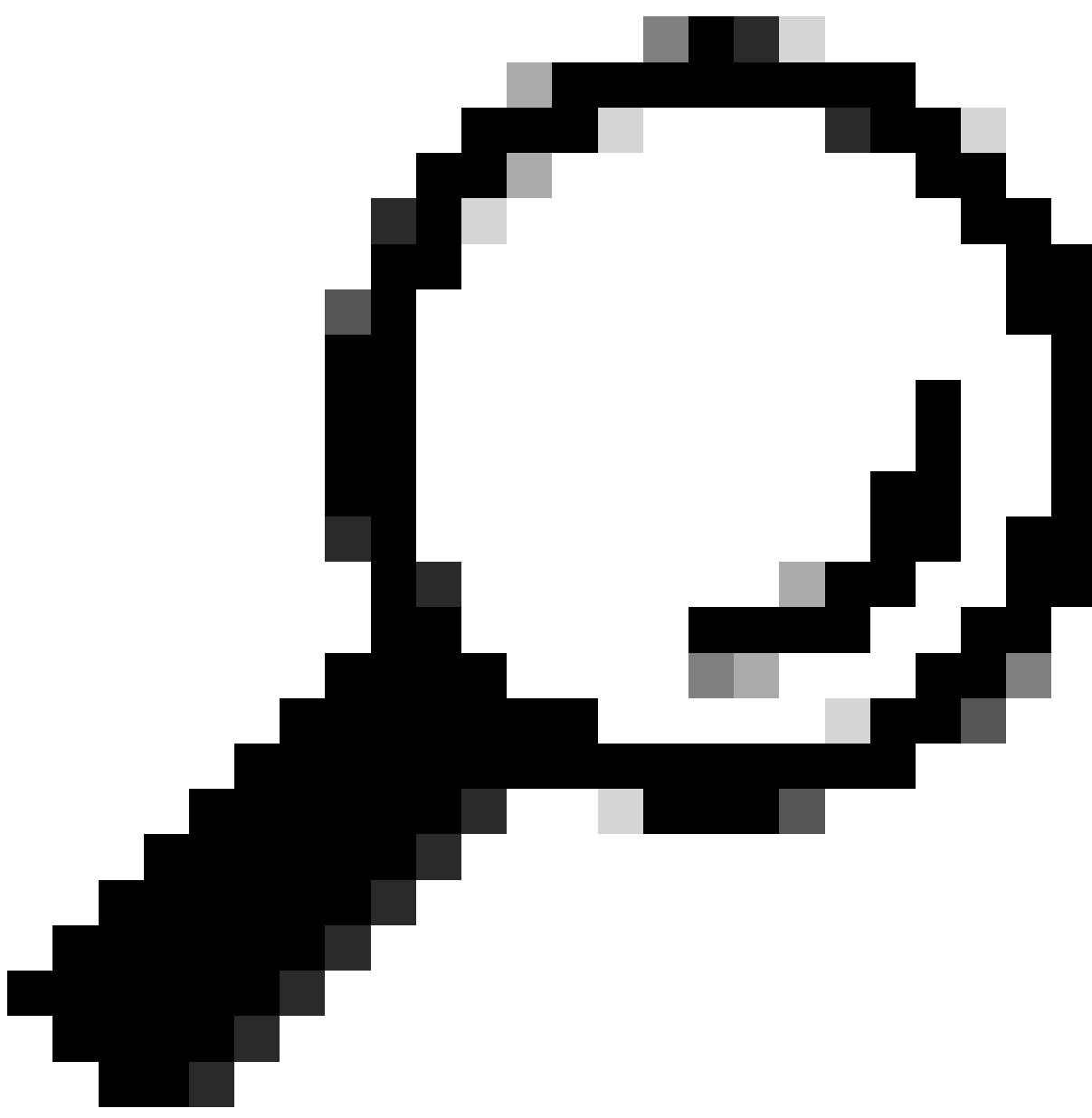
The IP address(es) listed within the SAN attribute of the certificate is matched with the IP address of the network device. Both IPv4 and IPv6 addresses are supported.

Additional SAN attribute details [Show](#)

Additional SAN Attributes

☒ Enable Single Connect Mode

Allow a network device to use one TCP connection for all TACACS+ requests, reducing overhead from repeatedly establishing and closing connections, especially for high-traffic devices.

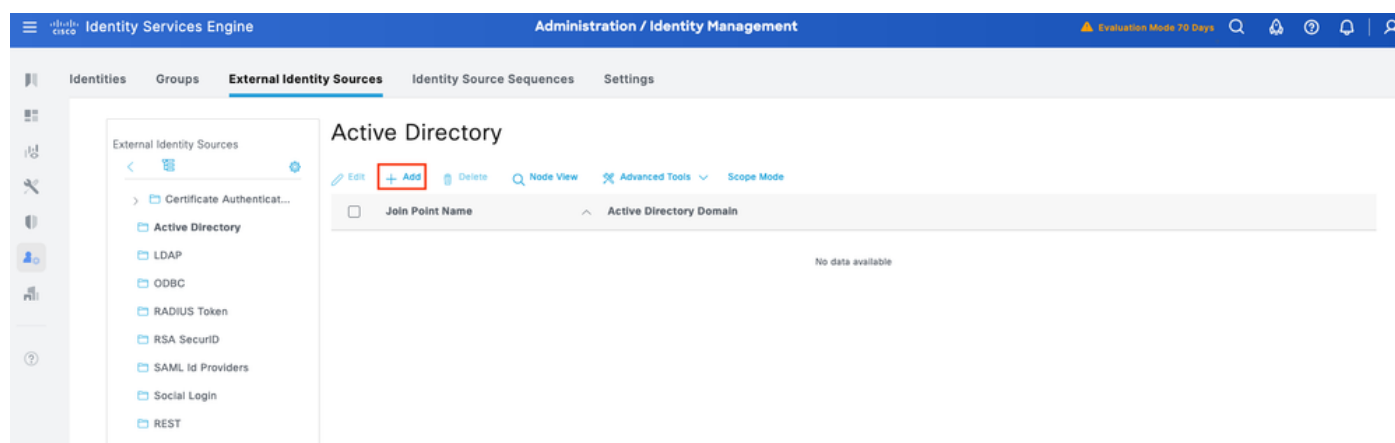


Consejo: Se recomienda habilitar el modo de conexión única para evitar reiniciar la sesión TCP cada vez que se envía un comando al dispositivo.

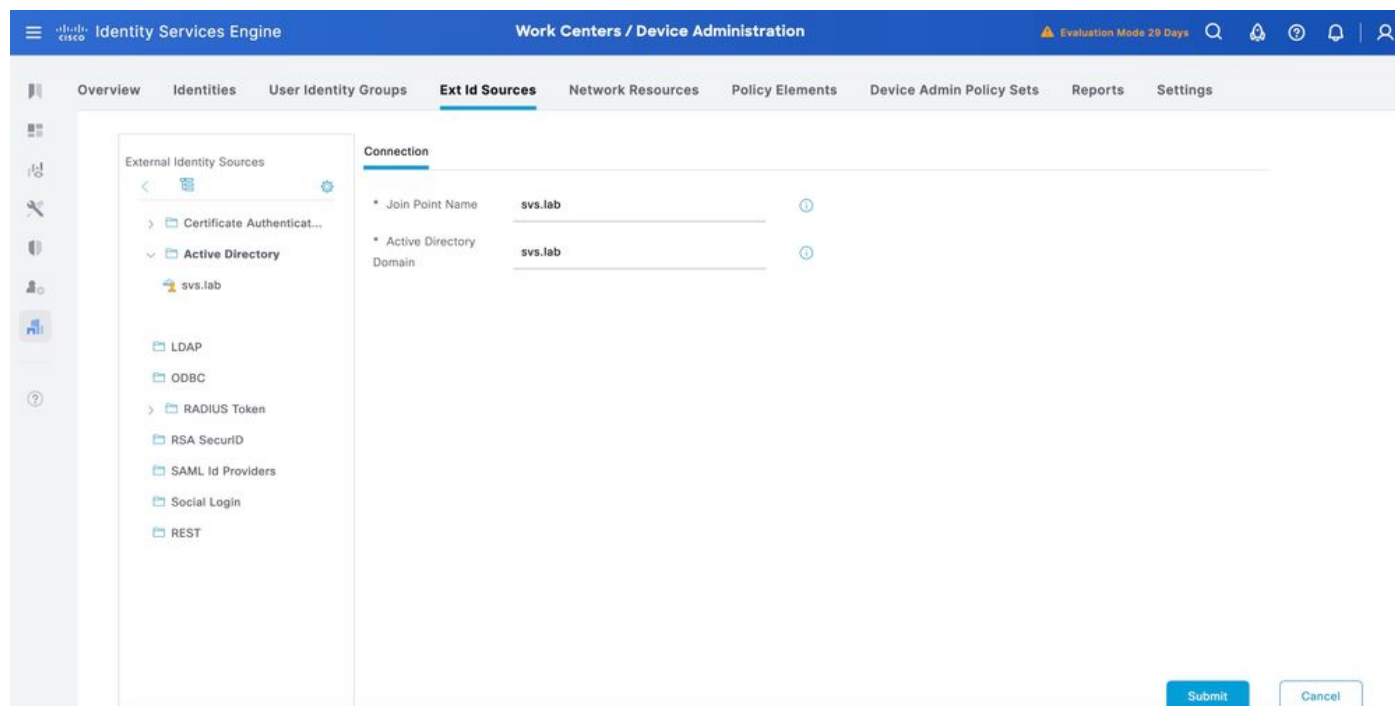
Configurar almacenes de identidad

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 Sí cuando se le pregunte "¿Desea unir todos los nodos ISE a este dominio de Active Directory?"



Information

Would you like to Join all ISE Nodes to this Active Directory Domain?

No

Yes

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

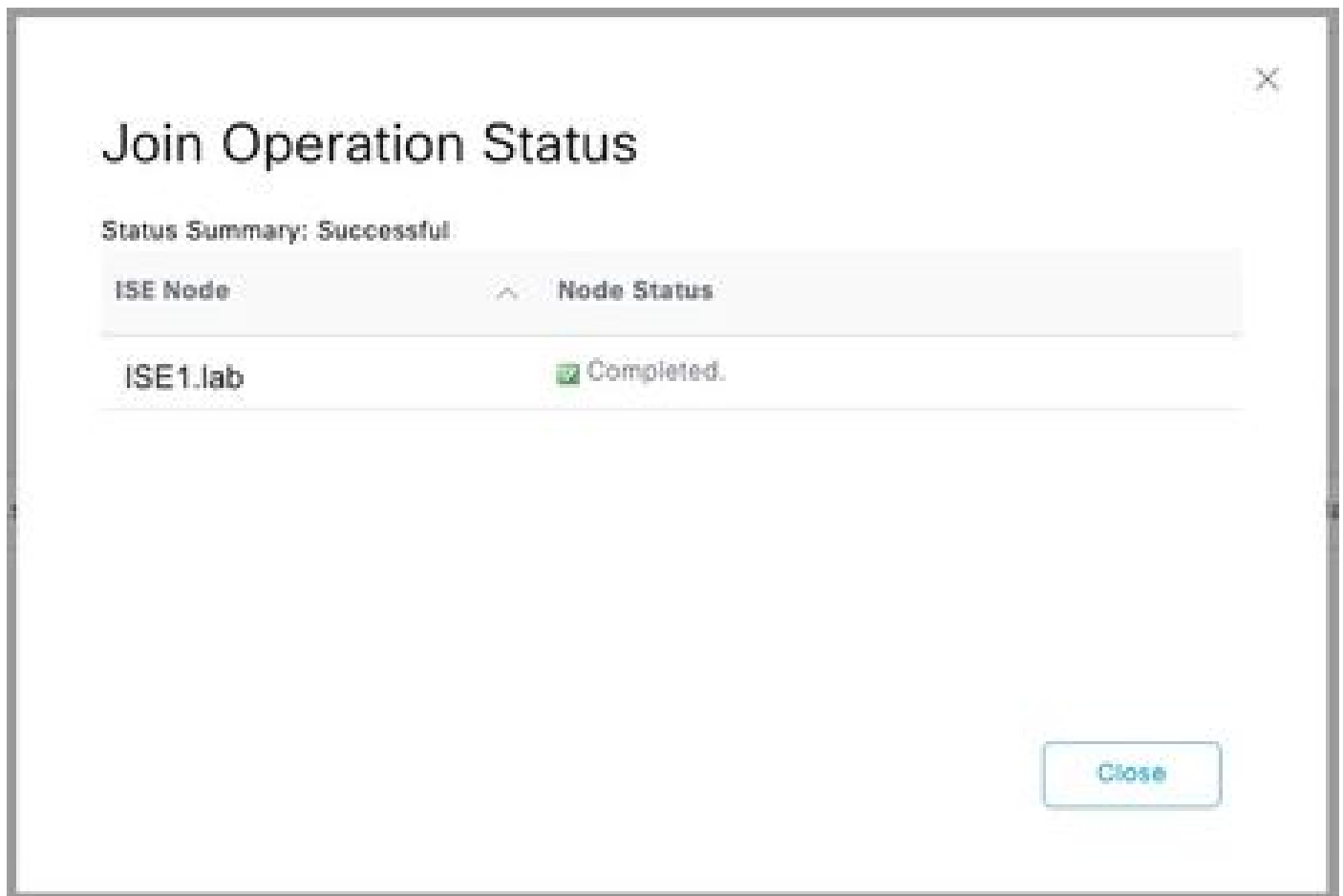
* Password

☐ Specify Organizational Unit ⓘ

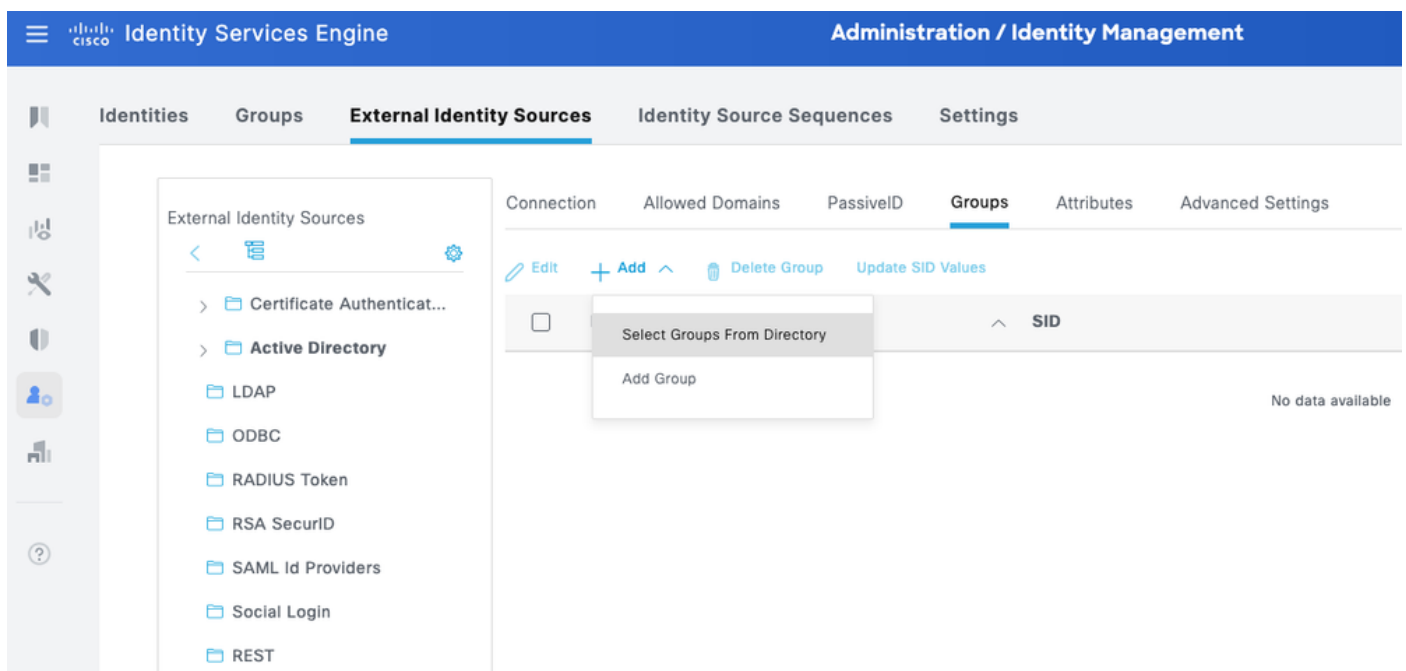
☒ Store Credentials ⓘ

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. En este ejemplo se muestran los grupos utilizados en la directiva de autorización de esta guía.



Select Directory Groups

This dialog is used to select groups from the Directory.

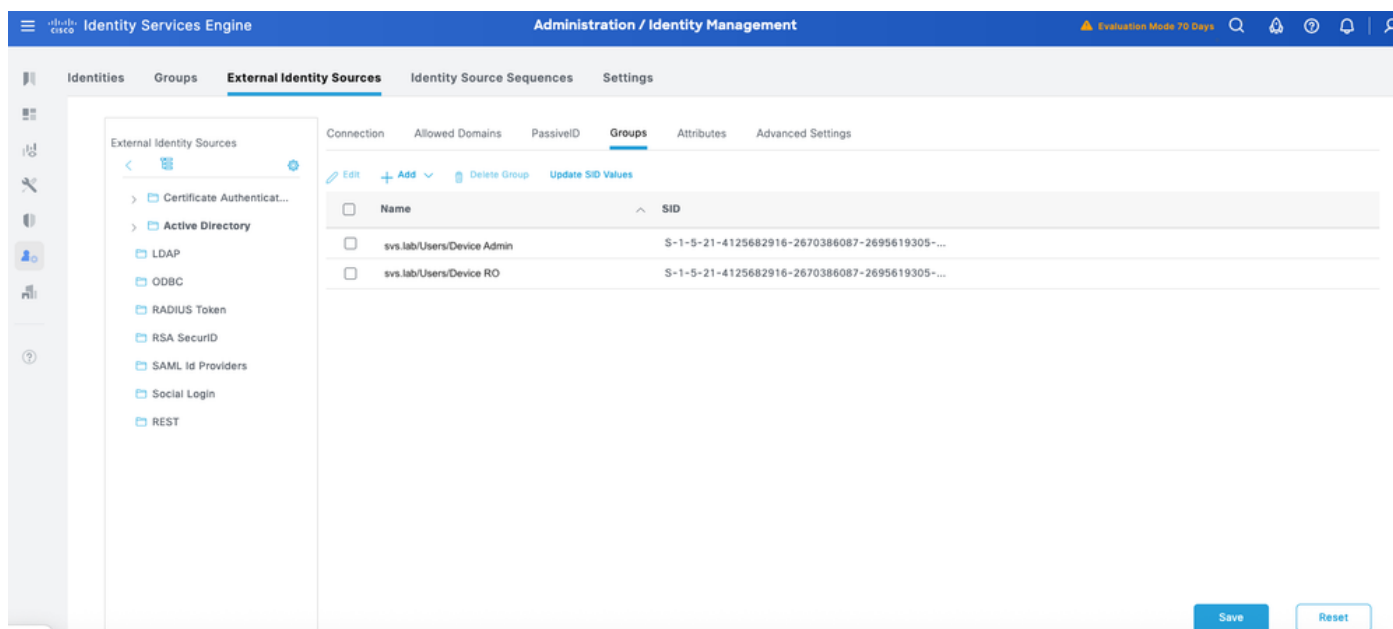
Domain

Name SID

Filter Type Filter

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 de shell TACACS+

A diferencia de los dispositivos Cisco IOS, que utilizan niveles de privilegio para la autorización, los dispositivos Cisco NX-OS implementan el control de acceso basado en roles (RBAC). En ISE, puede asignar perfiles TACACS+ a funciones de usuario en dispositivos Cisco NX-OS mediante tareas comunes del tipo Nexus.

Las funciones predefinidas en los dispositivos NX-OS difieren entre las plataformas NX-OS. Dos comunes son:

- network-admin: el rol de administrador de red predefinido tiene acceso de lectura y escritura completo a todos los comandos del switch; disponible en el contexto de dispositivo virtual (VDC) predeterminado sólo si los dispositivos (por ejemplo, Nexus 7000) tienen varios VDC. Utilice el comando NX-OS CLI `show cli syntax roles network-admin` para ver la lista de

comandos completa disponible para este rol.

- operador de red: el rol de administrador de red predeterminado tiene acceso de lectura completo a todos los comandos del switch; disponible en el VDC predeterminado solo si los dispositivos (por ejemplo, Nexus 7000) tienen varios VDC. Utilice el comando NX-OS CLI show cli authentication roles network-operator para ver la lista de comandos completa disponible para este rol.

A continuación, se definen dos perfiles TACACS: NXOS Admin y NXOS HelpDesk.

Administrador de NX-OS

Paso 1. Agregue otro perfil y denomínelo NX-OS Admin.

Paso 2. Seleccione Obligatorio en la lista desplegable Definir atributos como. Seleccione la opción Administrador de Función de red en Tareas comunes.

The screenshot displays the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes the Cisco logo, 'Identity Services Engine', and 'Work Centers / Device Administration'. A secondary navigation bar contains tabs: Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements (selected), Device Admin Policy Sets, Reports, and Settings. On the left, a sidebar menu lists various configuration areas, with 'TACACS Profiles' selected. The main content area shows the configuration for a TACACS profile named 'NXOS Admin'. It includes fields for 'Name' (NXOS Admin) and 'Description'. Below these, there are tabs for 'Task Attribute View' (selected) and 'Raw View'. Under 'Task Attribute View', there is a section for 'Common Tasks' with a dropdown for 'Common Task Type' set to 'Nexus'. Below this, there are two sections: 'Set attributes as' (set to 'Mandatory') and 'Network role' (with radio buttons for 'None', 'Operator (Read Only)', and 'Administrator (Read Write)', where 'Administrator (Read Write)' is selected). A 'VDC role' section also has radio buttons for 'None', 'Operator (Read Only)', and 'Administrator (Read Write)', with 'None' selected.

Paso 3. Haga clic en Enviar para guardar el perfil.

Soporte técnico de NX-OS

Paso 1. Desde la interfaz de usuario de ISE, navegue hasta Centros de trabajo > Administración de dispositivos > Elementos de política > Resultados > Perfiles TACACS. Agregue un nuevo perfil TACACS y denomínelo NXOS HelpDesk. Vaya al menú desplegable Tipo de tarea común y seleccione Nexus.

Puede ver los cambios de plantilla específicos de la función de usuario. Puede seleccionar las opciones correspondientes a la función de usuario que desea configurar.

Paso 2. Seleccione Obligatorio en la lista desplegable Definir atributos como. Seleccione la opción Operador de Función de red en Tareas comunes.

The screenshot shows the 'Policy Elements' configuration page in the Cisco ISE Work Centers / Device Administration section. The left sidebar contains navigation links: Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements (selected), Device Admin Policy Sets, Reports, and Settings. The main content area is titled 'TACACS Profile' and includes a breadcrumb 'TACACS Profiles > NXOS HelpDesk'. The 'Name' field is set to 'NXOS HelpDesk'. Below it is a 'Description' text area. Further down, there are tabs for 'Task Attribute View' and 'Raw View'. Under 'Common Tasks', the 'Common Task Type' is set to 'Nexus'. Below this, there are two sections: 'Set attributes as' (set to 'Optional') and 'Network role' (with options: None, Operator (Read Only) - selected, and Administrator (Read Write)). The 'VDC role' section also has options: None - selected, Operator (Read Only), and Administrator (Read Write).

Paso 3. Haga clic en Save para guardar el perfil.

Configurar conjuntos de directivas 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. Por ejemplo, los dispositivos Cisco IOS utilizan niveles de privilegio o conjuntos de comandos, mientras que los dispositivos Cisco NX-OS utilizan atributos personalizados.

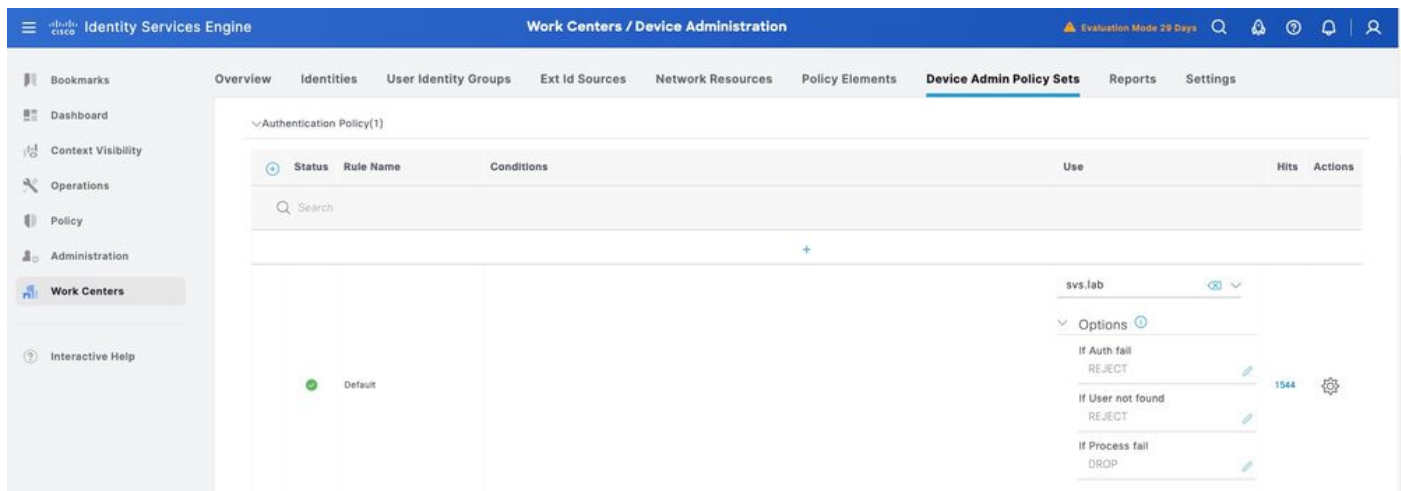
Paso 1. Vaya a Centros de trabajo > Administración de dispositivos > Conjuntos de políticas de administración de dispositivos. Agregue un nuevo conjunto de políticas para dispositivos NX-OS. En condition, especifique DEVICE:Device Type EQUALS All Device Types#NXOS. En Protocolos permitidos, seleccione Default Device Admin.

The screenshot shows the 'Device Admin Policy Sets' configuration page in the Cisco ISE Work Centers / Device Administration section. The left sidebar is the same as the previous screenshot. The main content area is titled 'Policy Sets' and includes a 'Reset' button, a 'Reset Policy Set Hit Counts' button, and a 'Save' button. Below this is a table with columns: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, Hits, Actions, and View. The table contains one entry: 'NX-OS Devices' with a status of 'On' and a condition of 'DEVICE:Device Type EQUALS All Device Types#NXOS'. The 'Allowed Protocols / Server Sequence' column shows 'Default Device Admin' with a dropdown arrow and a plus sign.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
On	NX-OS Devices		DEVICE:Device Type EQUALS All Device Types#NXOS	Default Device Admin			

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

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



Paso 4. Defina la Política de Autorización.

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

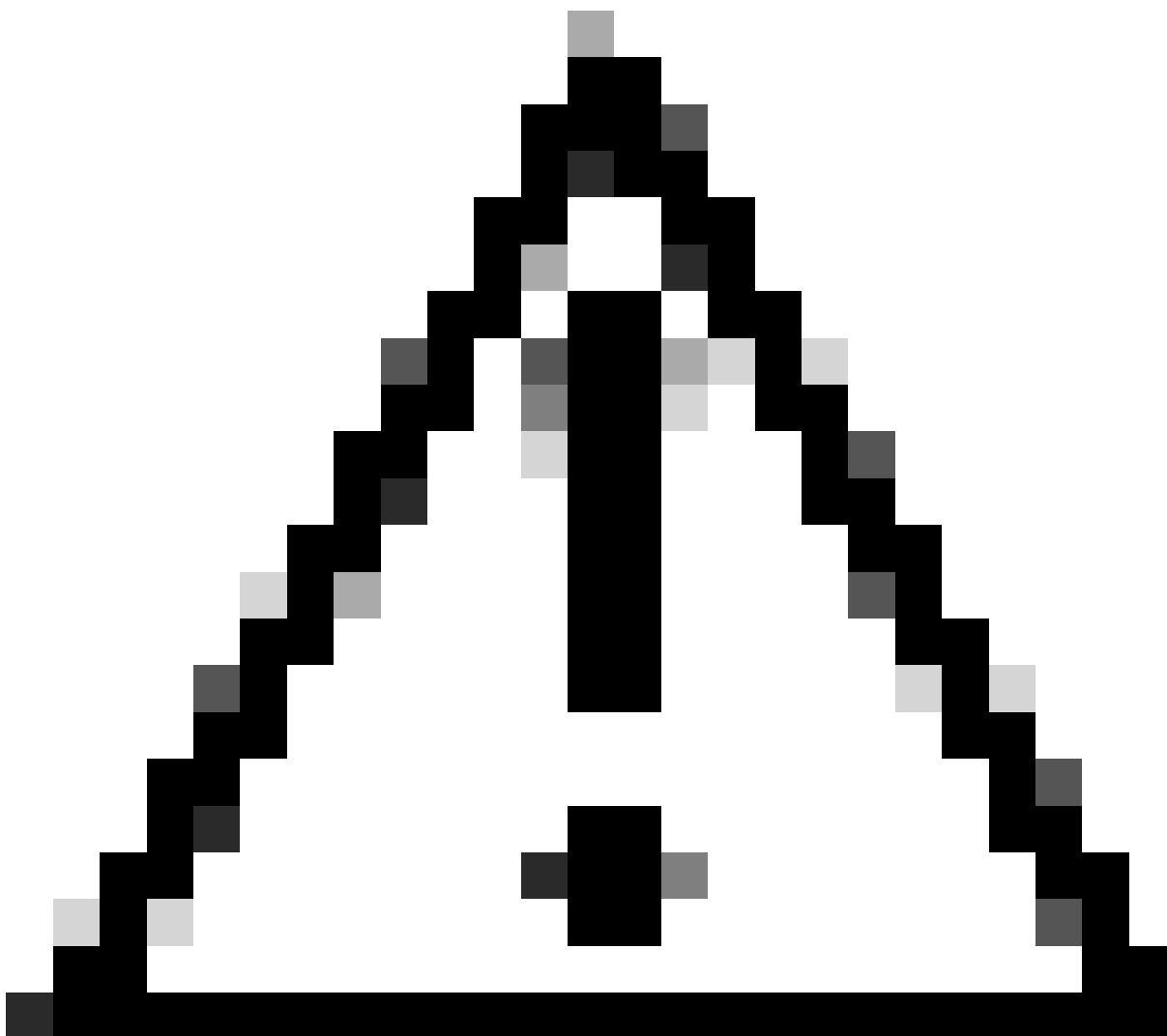
Por ejemplo:

- A los usuarios del grupo de AD Device Admin se les asigna el perfil TACACS de administrador de NXOS.
- A los usuarios del grupo AD Device RO se les asigna el perfil TACACS de NXOS HelpDesk.

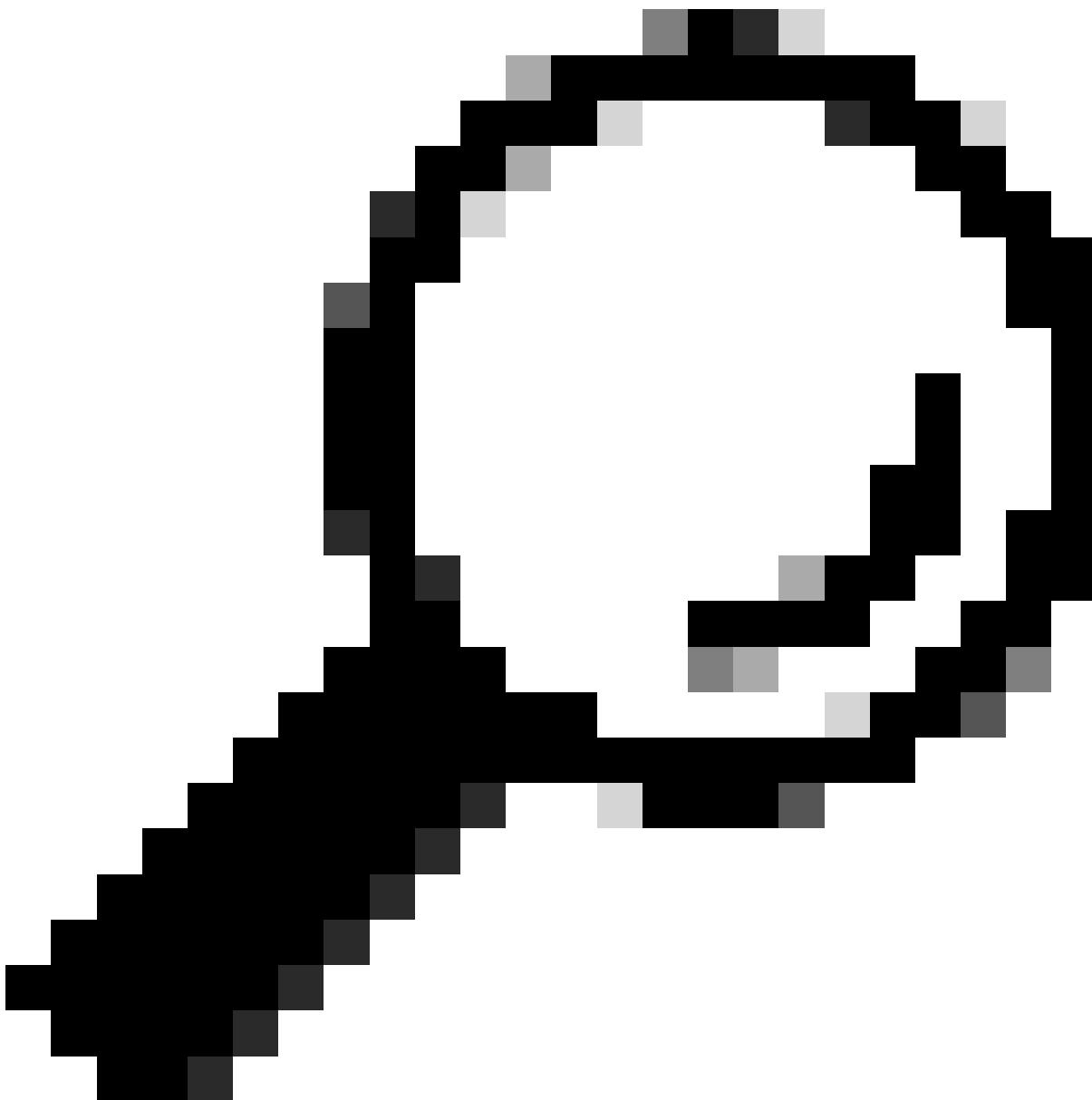
Authorization Policy(3)

Status	Rule Name	Conditions	Results			Hits	Actions
			Command Sets	Shell Profiles			
Search							
✓	Authorization Rule RO	 svs.lab-ExternalGroups EQUALS svs.lab/Users/Device RO	Select from list	+	NXOS HelpDe	 + 0	
✓	Authorization Rule RW	 svs.lab-ExternalGroups EQUALS svs.lab/Users/Device Admin	Select from list	+	NXOS Admin	 + 2	
✓	Default		DenyAllCommands	+	Deny All Shell Profile	 + 0	

Configuración de Cisco NX-OS para TACACS+ sobre TLS



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.

Configuración del servidor TACACS+

Paso 1. Configuración inicial.

```
POD2IPN2# sho run tacacs
```

```
feature tacacs+
```

```
tacacs-server host 10.225.253.209 key 7 "F1whg.123"
```

```
aaa group server tacacs+ tacacs2
server 10.225.253.209
use-vrf management
```

Configuración de Trustpoint

Paso 1. Cree una etiqueta de clave, en su caso, utilice el par de claves ecc.

```
<#root>

POD2IPN2(config)#

crypto key generate ecc label ec521-label exportable modulus 521
```

Paso 2. Asocie esto a un punto de confianza.

```
<#root>

POD2IPN2(config)#

crypto ca trustpoint ec521-tp

POD2IPN2(config-trustpoint)#

ecckeypair ec521-label
```

Paso 3. Instale la clave pública de la CA.

```
<#root>

POD2IPN2(config)#

crypto ca authenticate ec521-tp

input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----BEGIN CERTIFICATE-----
MIIFlDCCA3ygAwIBAgIIIM10AsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZzAVBgNVBAGTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECjMDU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUa1UECBM0Tm9ydGggQ2Fyb2xpbmExEDAOBgNVBACTB1JhbGVpZ2gxDjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTV1MxEjAQBgNVBAMTCVNWUyBMWJJDQTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZU0yn2vIn6gKbx3M7vaRq
2YjwZlZSH6EkEvxnJT+y+kksiFD33GyHQepk7vfp4NFU50tQ4HC7t/A0v9grDa3QW
VwvV4MBbJhFM3s0J/ejgDYcMZhIAaPy0Zo5WLboOkXEiKjPLatkXojB8FVrhLF3O
jMBSqwa4/Wlniy5S+7s4FFxsCf20COWfBAsnrs0tatIIhmcnx+VLJP7MRm8f0w4m
mutNo7IhbJSrgAFXmj1bBjMmgspObULO/wxMHdTbtPBf11HRHTkNIo3qy04UADL2
WpoGhgT/FaxxBo2UBCnYVaP+jjREONYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
```

```
+qh23SL43uW5A3iSw/BuU1E9p7B0e8oDNKU6gXl0jKyLP/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/ZTpe4d10zJsZjNsN0r8bF9nOA/7qNZLp3Z3cpU
PU0KdbiSvRqnPw3e8TFITVmAzcX8COI2SrYFMSUazo1VBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIEOf5ay1PKURO/8aj/B7a1uJapXkmnj5qPeGhN0pB
Q9r14reov4so2EspkXS7CrH9yGfpIyTprokz1UvZBZ8v1oI7YZmjFmem+5rT6Gnk
eU/1X7nV61SYG5W5K+I8uaKuyBHOMn7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggz1POdsS/i6Lo7ypYX0eB9HgVDckzQsLXQuHGj/2WsgPgDRcjkvnyURk4Jx+Ib
xDrmo7e0XPpSW4172a6K18CR3U2Cr4wsuvndPEq/qd2NRSBWffFOX/AJHQG7STT
HaXLU9r2Ko603oecu8ysGTWl1It/9T1/F0b0xZRugWcpJrVoTgDGuA==
-----END CERTIFICATE-----
```

END OF INPUT

Fingerprint(s): SHA1

Fingerprint=0E:B1:81:E9:5A:3E:D7:80:3B:C5:A8:05:9A:85:4A:95:C8:3A:C7:37

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

POD2IPN2(config)#

POD2IPN2(config)#

show crypto ca certificates ec521-tp

Trustpoint: ec521-tp

CA certificate 0:

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

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

serial=20CD7402C4DA37F5

notBefore=Apr 28 17:05:00 2025 GMT

notAfter=Apr 28 17:05:00 2035 GMT

SHA1 Fingerprint=0E:B1:81:E9:5A:3E:D7:80:3B:C5:A8:05:9A:85:4A:95:C8:3A:C7:37

purposes: sslserver sslclient

POD2IPN2(config)#

Paso 4. Generar solicitud de certificado de identidad del switch.

<#root>

POD2IPN2(config)#

crypto ca enroll ec521-tp

Create the certificate request ..

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:Cisco.123

The subject name in the certificate will be the name of the switch.

Include the switch serial number in the subject name? [yes/no]:

yes

The serial number in the certificate will be: FD026490P4T

Include an IP address in the subject name [yes/no]:

yes

ip address:10.225.253.177

Include the Alternate Subject Name ? [yes/no]:

no

The certificate request will be displayed...

-----BEGIN CERTIFICATE REQUEST-----

```
MIIBtjCCARcCAQAwKTERMA8GA1UEAwIUE9EMk1QTjIxFDASBgNVBAUTC0ZETzI2
NDkwUDRUMIGbMBAGByqGSM49AgEGBSuBBAAjA4GGAAQBGYT0iw7OvqIKQ/a22Lkg
Na9IhqWQvetjxKq485gqTSBEo6Lzpk0hPAGE4jBveNHxYeIA7PfNWvJ7xTBWjDNX
/IYBm6E7Hd7q420mCe8Mef+bqJBdJ9wzpyEjhI2lIIoXt4814nBx0bkIWWyR5cZN
IiXTLk8P4IMZvPq8jRnELRxd8RGgSTAYBgkqhkiG9w0BCQcxCwwJQzFzY28uMTIz
MCOGCSqGSIb3DQEJDDjEgMB4wHAYDVR0RAQH/BBIwEIIIUE9EMk1QTjKHBArh/bEw
CgYIKoZIZj0EAWIDgYwAMIGIAkIAtzQ/knrW2ovCvoHAuq1v2cr0n3NenS/441u1
+3H1y52vn4Rm4CGU3wkzXU3qG03YjhNjCXjhp3+uN2afFf1Wf3ECQgC4bumHVsfj
b5rwPIC5tvXS/A8upqIzqc0yt30hpaDD0TWzzvZY7qFf1C015p6pvUpHiqqoZNg5
9xhNdM1CQSyk0g==
```

-----END CERTIFICATE REQUEST-----

Paso 5. Importe el certificado de identidad del switch firmado por CA.

<#root>

POD2IPN2(config)#

crypto ca import ec521-tp certificate

input (cut & paste) certificate in PEM format:

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

```
MIIDzTCCAbWgAwIBAgIIC6zS76XYDm8wDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZmFzAVBgNVBAGTDk5vcnRoIENhcm9saW5hMRwwDgYDVQQHEwdSYWx1aWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECXMdU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNTA3MTkxMDAwWhcNMjUwNTA3MTkxMDAwWjApMREwDwYDVQQDDAhQ
TOQySVBOMjEUMBIGA1UEBRMLRkRPMjY0OTBQNFQwgZswEAYHKoZIzj0CAQYFK4EE
ACMDgYYABAEZhpSLDs6+ogpD9rbYuSA1r0iGpZC962PEqrjzmCpNIESjovOmQ6E8
AYTiMG940fFh4gDs981a8nvFMFAmM1f8hgGboTsd3urjY6YJ7wx5/5uokF0n3DOn
ISOEjaUgihe3jzXiCHE5uQhZbJH1xk0iJdMuTw/ggxm8+ryNGCQtHF3xEaNAMD4w
HgYJYIZIAyb4QgENBBEWD3hjYSBjZXJ0aWZpY2F0ZTAzBgNVHREBAf8EEjAQgghQ
TOQySVBOMocECuH9sTANBgkqhkiG9w0BAQsFAAOCAGANWGb6zm9TDPaM1yhPMx7
8uai/pF7VQC8NSCdOKqr4w4+695ZjJuzqFL3msodOQK0EdgxpQ4+pEa5msRtK0i8
mms2X/Px3/EShxoHrZ01PUXNTyZidXpGd/yTrdQA15JzpW4pEudrbCJMZEYtqoP
wD+40E8vKoYEgyWlDrpRZ0ZG1usZczUUhLZ8orkjXMhWC26Q5aqiCKkyg10Nt6nb
1iToeYy2Q0cTesSZCKvRBv6Ewj5JuSLeMURyB4GHY+LT+A9UNmEUM2n+OSVEL329
3hS0qd/YVaEuxjjlg7jNiZb+UsW7IRx3Q8Rouo++ISACpH/PJ61Ln1VxhXombiS6
INoaOGvQONr1+lFT8ADIdZ/Ukd5Ubhc9bh/sYzf4MwtK1wV016Hv7vGpSMYonD6
a271im+tJPyKneezQ60yKz1GqsL/Ta6J0dip/fEYp8UmRq9InDh23gDjqrojl7k
1R/bZpc+baMYXd/2pohHMSN0sKN3zNrJT1nuk5KCqFx//4P7mAoyZYiTIDp1pkYS
```

```
VK65fJKD+pYxIhSP9wN8rnwtzSCWb0Z78sg006Y6wIXyTP0UB3FWhD+GxtTkmEce
ZnAQbgxpgrg5lhpAEVabpC/zRU4UzTuBmv/WoY12zwXCr5WLXEOWtIe8CwFjSnch
1fKuuebdZkbwz72r70yyX/U=
-----END CERTIFICATE-----
POD2IPN2(config)#
```

Verifique que el certificado de identidad del switch esté inscrito.

```
<#root>
```

```
POD2IPN2(config)#
```

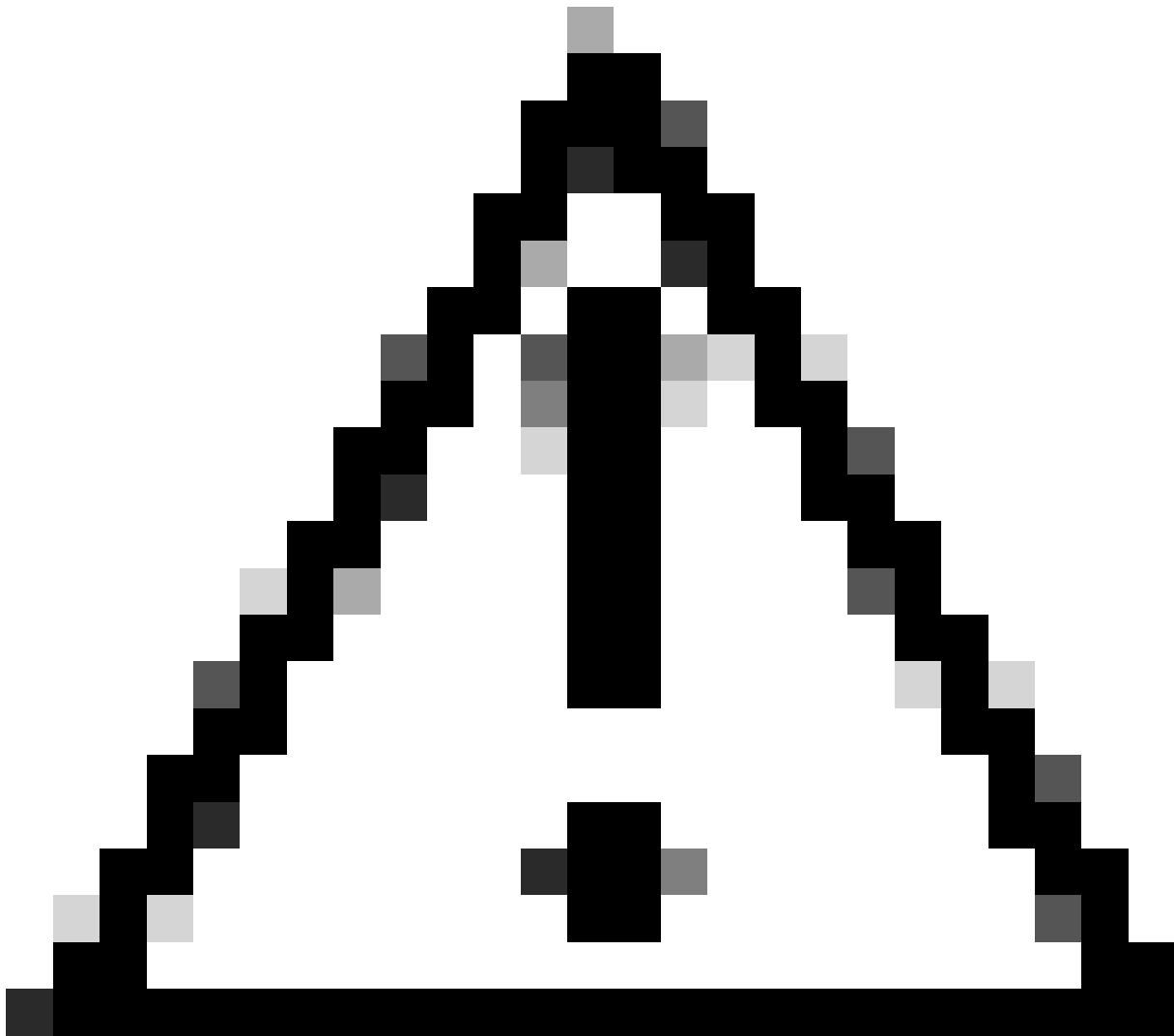
```
show crypto ca certificates ec521-tp
```

```
Trustpoint: ec521-tp
certificate:
subject=CN = POD2IPN2, serialNumber = FD026490P4T
issuer=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
serial=0BACD2EFA5D80E6F
notBefore=May  7 19:10:00 2025 GMT
notAfter=May  7 19:10:00 2026 GMT
SHA1 Fingerprint=CA:B2:BF:3F:ED:2F:06:0B:C1:E4:DC:21:9F:9D:54:61:98:32:C5:13
purposes: sslserver sslclient
```

```
CA certificate 0:
subject=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
issuer=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
serial=20CD7402C4DA37F5
notBefore=Apr 28 17:05:00 2025 GMT
notAfter=Apr 28 17:05:00 2035 GMT
SHA1 Fingerprint=0E:B1:81:E9:5A:3E:D7:80:3B:C5:A8:05:9A:85:4A:95:C8:3A:C7:37
purposes: sslserver sslclient
```

```
POD2IPN2(config)#
```

Configuración de TACACS+ TLS



Precaución: Realice estos cambios de configuración a través de la consola con credenciales locales.

Paso 1. Configure global tacacs tls.

```
<#root>
```

```
POD2IPN2(config)#
```

```
tacacs-server secure tls
```

Paso 2. Cambie el puerto ISE por el puerto TLS con el que está configurado el servidor ISE.

```
<#root>
```

```
POD2IPN2(config)#
```

```
tacacs-server host 10.225.253.209 port 6049 timeout 60 single-connection
```

Paso 3. Asocie el servidor ISE configurado en el switch al punto de confianza para la conexión TLS.

```
<#root>
```

```
POD2IPN2(config)#
```

```
tacacs-server host 10.225.253.209 tls client-trustpoint ec521-tp
```

Paso 4. Crear grupo de servidores tacacs.

```
<#root>
```

```
POD2IPN2(config)#
```

```
aaa group server tacacs+ tacacs2
```

```
POD2IPN2(config-tacacs+)#
```

```
server 10.225.253.209
```

```
POD2IPN2(config-tacacs+)#
```

```
use-vrf management
```

Paso 5. Verifique la configuración.

```
<#root>
```

```
POD2IPN2#
```

```
sho run tacacs
```

```
feature tacacs+
```

```
tacacs-server secure tls
```

```
tacacs-server host 10.225.253.209 port 6049 timeout 60 single-connection
```

```
tacacs-server host 10.225.253.209 tls client-trustpoint ec521-tp
```

```
aaa group server tacacs+ tacacs2
```

```
server 10.225.253.209
```

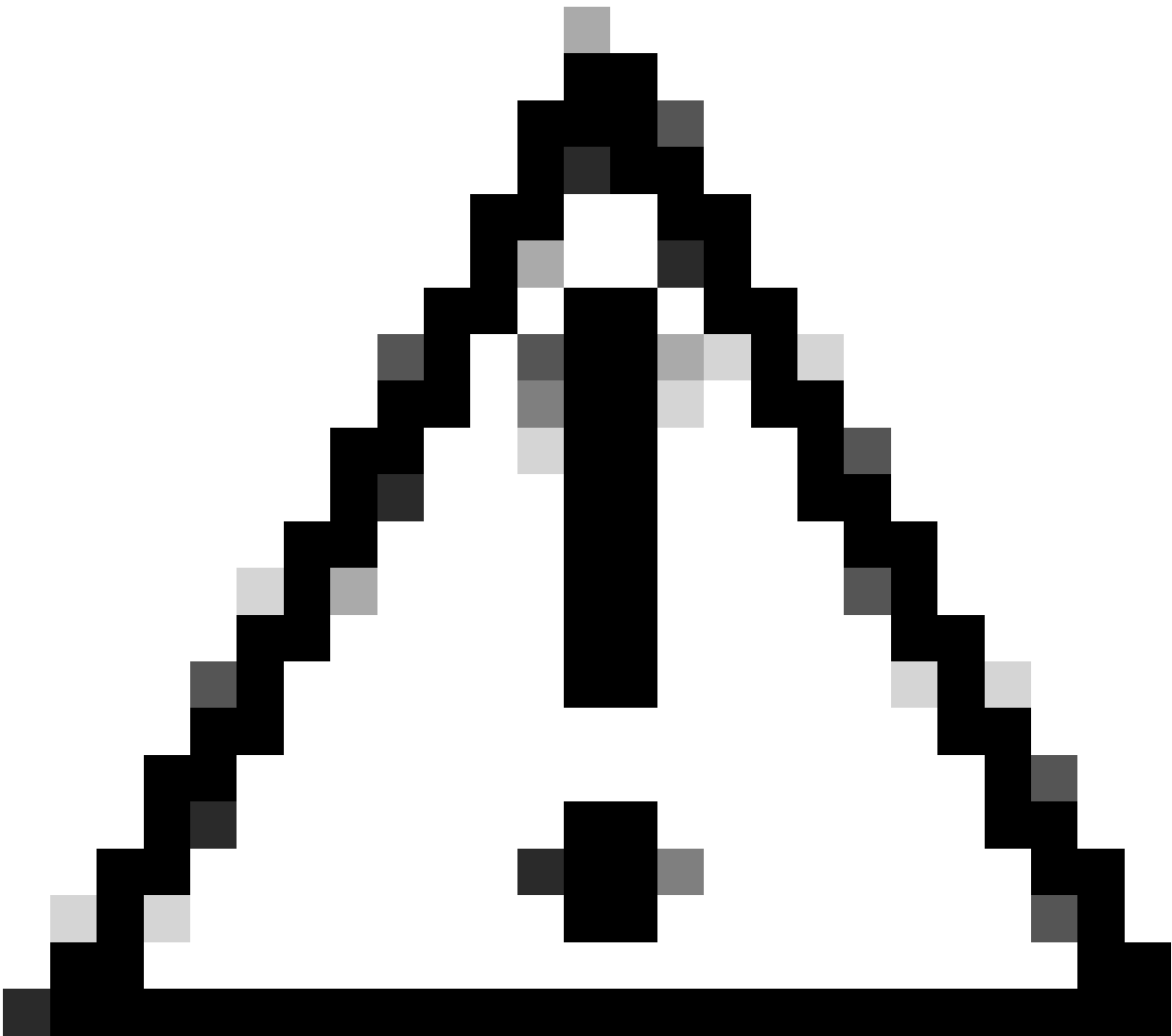
```
use-vrf management
```

Paso 6. Pruebe el usuario remoto antes de configurar la autenticación AAA.

```
<#root>
POD2IPN2#
test aaa group tacacs2
```

```
user has been authenticated
POD2IPN2#
```

Configuración AAA



Precaución: Asegúrese de que la autenticación de usuario remoto sea correcta antes de continuar con las configuraciones AAA.

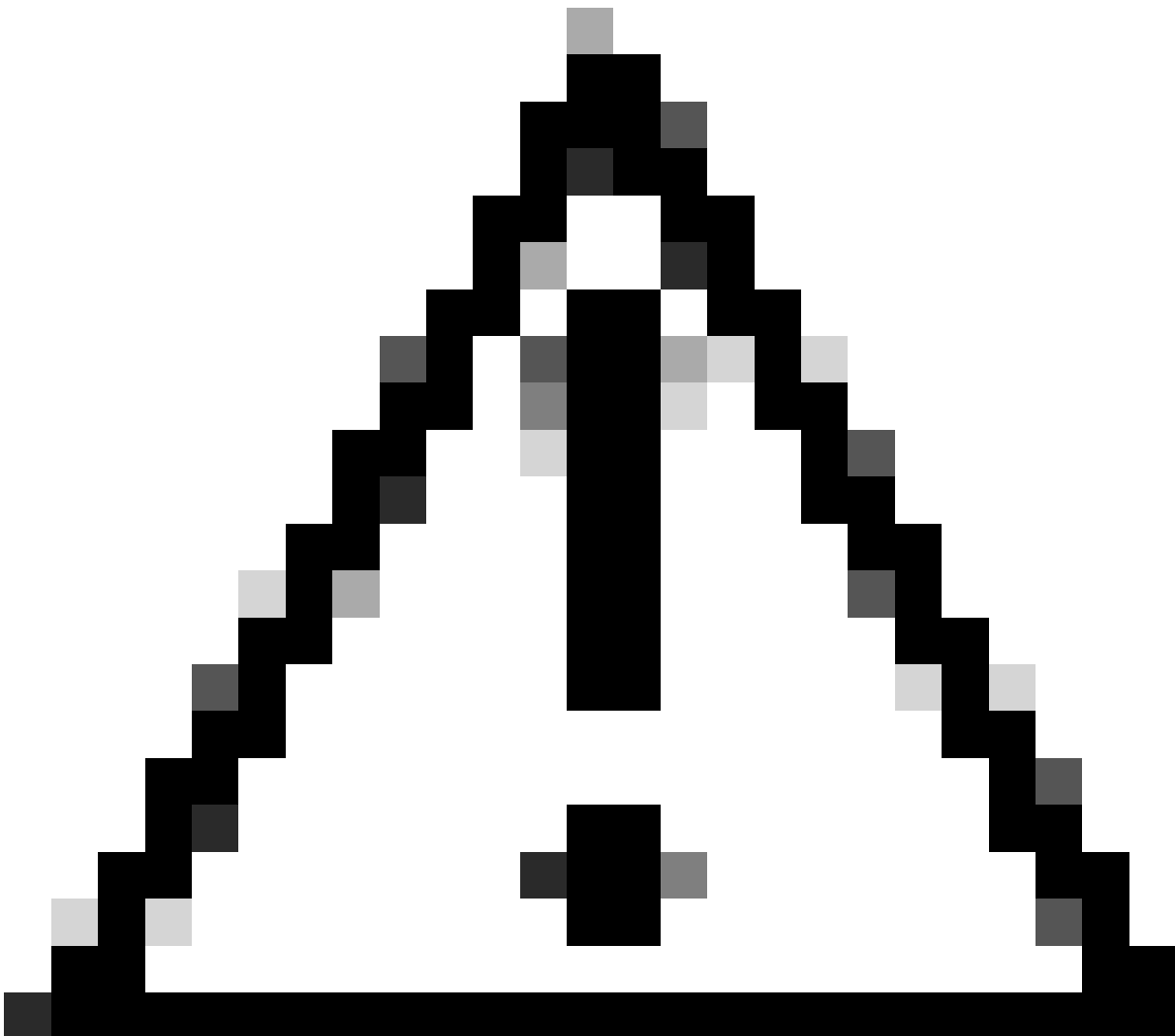
Paso 1. Configure la autenticación remota AAA.

```
<#root>
```

```
POD2IPN2(config)#
```

```
aaa authentication login default group tacacs2
```

Paso 2. Configure la autorización remota AAA después de probar el comando.



Precaución: Asegúrese de que ve authorization-status como "AAA_AUTHOR_STATUS_PASS_ADD.

```
<#root>
```

```
POD2IPN2#
```

```
test aaa authorization command-type config-commands default user
```

```
command "feature bgp"
```

```
sending authorization request for: user: pamemart, author-type:3, cmd "feature bgp"  
user pamemart, author type 3, command: feature bgp, authorization-status:0x1(AAA_AUTHOR_STATUS_PASS_ADD)
```

Paso 3. Configure el comando AAA y la autorización config-command.

```
<#root>
```

```
POD2IPN2(config)#
```

```
aaa authorization config-commands default group tacacs2 local
```

```
POD2IPN2(config)#
```

```
aaa authorization commands default group tacacs2 local
```

Prueba y solución de problemas de acceso de usuario para NX-OS

Verificación

La configuración de Device Administration para Cisco NX-OS ha finalizado. Debe validar la configuración.

Paso 1. SSH e inicie sesión en los dispositivos NX-OS con distintas funciones.

Paso 2. Una vez en la interfaz de línea de comandos (CLI) del dispositivo, compruebe que el usuario tiene acceso a los comandos adecuados. Por ejemplo, un usuario de Helpdesk debe poder hacer ping a una dirección IP normal (por ejemplo, 10.225.253.129) pero se le debe denegar mostrar la configuración en ejecución.

```
POD2IPN1# ping 10.225.253.129 vrf management  
PING 10.225.253.129 (10.225.253.129): 56 data bytes  
64 bytes from 10.225.253.129: icmp_seq=0 ttl=254 time=0.817 ms  
64 bytes from 10.225.253.129: icmp_seq=1 ttl=254 time=0.638 ms
```

```
64 bytes from 10.225.253.129: icmp_seq=2 ttl=254 time=0.642 ms
64 bytes from 10.225.253.129: icmp_seq=3 ttl=254 time=0.651 ms
64 bytes from 10.225.253.129: icmp_seq=4 ttl=254 time=0.712 ms
```

```
--- 10.225.253.129 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.638/0.692/0.817 ms
POD2IPN1#
POD2IPN1# show running-config
% Permission denied for the role
```

Resolución de problemas

Validación de la configuración de NX-OS.

```
POD2IPN2# show crypto ca certificates
POD2IPN2# show crypto ca trustpoints
POD2IPN2# show tacacs-server statistics <server ip>
```

Para mostrar las conexiones de usuario y los roles, utilice estos comandos.

```
show users
show user-account [<user-name>]
A sample output is shown below:
POD2IPN1# show users
NAME LINE TIME IDLE PID COMMENT
Admin-ro pts/5 May 15 23:49 . 16526 (10.189.1.151) session=ssh *
POD2IPN1# show user-account Admin-ro
user:Admin-ro
roles:network-operator
account created through REMOTE authentication
Credentials such as ssh server key will be cached temporarily only for this user account
Local login not possible...
```

Estas son depuraciones útiles en la resolución de problemas de TACACS+:

```
debug TACACS+ aaa-request
2016 Jan 11 03:03:08.652514 TACACS[6288]: process_aaa_tplus_request:Checking for state of mgmt0 port w
2016 Jan 11 03:03:08.652543 TACACS[6288]: process_aaa_tplus_request: Group demoTG found. corresponding
2016 Jan 11 03:03:08.652552 TACACS[6288]: process_aaa_tplus_request: checking for mgmt0 vrf:management
2016 Jan 11 03:03:08.652559 TACACS[6288]: process_aaa_tplus_request:port_check will be done
2016 Jan 11 03:03:08.652568 TACACS[6288]: state machine count 0
2016 Jan 11 03:03:08.652677 TACACS[6288]: is_intf_up_with_valid_ip(1258):Proper IOD is found.
2016 Jan 11 03:03:08.652699 TACACS[6288]: is_intf_up_with_valid_ip(1261):Port is up.
2016 Jan 11 03:03:08.653919 TACACS[6288]: debug_av_list(797):Printing list
2016 Jan 11 03:03:08.653930 TACACS[6288]: 35 : 4 : ping
2016 Jan 11 03:03:08.653938 TACACS[6288]: 36 : 12 : 10.1.100.255
2016 Jan 11 03:03:08.653945 TACACS[6288]: 36 : 4 : <cr>
```

```

2016 Jan 11 03:03:08.653952 TACACS[6288]: debug_av_list(807):Done printing list, exiting function
2016 Jan 11 03:03:08.654004 TACACS[6288]: tplus_encrypt(659):key is configured for this aaa sessin.
2016 Jan 11 03:03:08.655054 TACACS[6288]: num_inet_addrs: 1 first s_addr: -1268514550 10.100.1.10 s6_a
2016 Jan 11 03:03:08.655065 TACACS[6288]: non_blocking_connect(259):interface ip_type: IPV4
2016 Jan 11 03:03:08.656023 TACACS[6288]: non_blocking_connect(369): Proceeding with bind
2016 Jan 11 03:03:08.656216 TACACS[6288]: non_blocking_connect(388): setsockopt success error:22
2016 Jan 11 03:03:08.656694 TACACS[6288]: non_blocking_connect(489): connect() is in-progress for serv
2016 Jan 11 03:03:08.679815 TACACS[6288]: tplus_decode_authen_response: copying hostname into context

```

Habilite la depuración SSL.

```
touch '/bootflash/.enable_ssl_debugs'
```

Mostrar contenido del archivo de depuración.

```
cat /tmp/ssl_wrapper.log.*
```

Desde la GUI de ISE, navegue hasta Operations > TACACS LiveLog. Todas las solicitudes de autenticación y autorización de TACACS se capturan aquí, y el botón de detalles proporciona información detallada sobre por qué una transacción en particular pasó/falló.

Identity Services Engine

Operations / TACACS

Evaluation Mode 80 Days

Live Logs

Refresh

Every 10 sec...

Show

Latest 20 reco...

Within

Last 3 hours

Export To

Filter

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Devic...	Network Dr
			Identity		Authentication Policy	Authorization Policy	Ise Node	Network Device Ni	Network Dev
May 15, 2025 07:39:57.081 PM			Admin-ro	Authorization		Test NXOS >> Authorization Rule RO	ISE1	POD2IPN1	10.225.253.1
May 15, 2025 07:39:57.061 PM			Admin-ro	Authentication	Test NXOS >> Default		ISE1	POD2IPN1	10.225.253.1
May 15, 2025 07:39:54.462 PM			panemart	Authorization		Test NXOS >> Authorization Rule RW	ISE1	POD2IPN1	10.225.253.1
May 15, 2025 07:39:54.443 PM			panemart	Authentication	Test NXOS >> Default		ISE1	POD2IPN1	10.225.253.1

Para informes históricos: Vaya a Centros de trabajo > Administración de dispositivos > Informes > Administración de dispositivos para obtener los informes de autenticación, autorización y contabilidad.

Overview

Identities

User Identity Groups

Ext Id Sources

Network Resources

Policy Elements

Device Admin Policy Sets

Reports

Settings

Export Summary

My Reports

Reports

Device Administration Reports

Authentication Summary

TACACS Accounting

TACACS Authentication

TACACS Authorization

TACACS Command Accounting

Top N Authentication by Failure Reason

Top N Authentication by Network Device

Top N Authentication by User

Scheduled Reports

TACACS Authentication

From 2025-05-15 00:00:00.0 To 2025-05-15 20:00:45.0

Reports exported in last 7 days 0

Add to My Reports

Export To

Schedule

Filter

Refresh

Logged Time	Status	Details	Identity	Authentication Policy	ISE Node	Network Device Name	Network Device IP	Failure
Today			Identity	Authentication Policy	ISE Node	Network Device Name	Network Device IP	Failure
2025-05-15 19:39:57.061			Admin-ro	Test NXOS >> Default	ISE1	POD2IPN1	10.225.253.176	
2025-05-15 19:39:54.443			pamemart	Test NXOS >> Default	ISE1	POD2IPN1	10.225.253.176	
2025-05-15 19:39:43.001			pamemart	Test NXOS >> Default	ISE1	POD2IPN1	10.225.253.176	
2025-05-15 19:35:39.809			pamemart	Test NXOS >> Default	ISE1	POD2IPN1	10.225.253.176	
2025-05-15 18:49:11.209			pamemart	Test NXOS >> Default	ISE1	POD2IPN1	10.225.253.176	
2025-05-15 18:49:10.303			Admin-ro	Test NXOS >> Default	ISE1	POD2IPN1	10.225.253.176	

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).