

# Configurazione di TACACS+ over TLS 1.3 su un dispositivo IOS XE con ISE

## Sommario

---

[Introduzione](#)

[Panoramica](#)

[Utilizzo della Guida](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Licenze](#)

[Parte 1 - Configurare ISE per l'amministrazione dei dispositivi](#)

[Genera richiesta di firma del certificato per autenticazione server TACACS+](#)

[Carica certificato CA radice per autenticazione server TACACS+](#)

[Associare la richiesta di firma del certificato \(CSR\) firmata a ISE](#)

[Abilita TLS 1.3](#)

[Abilita amministrazione dispositivi su ISE](#)

[Abilita TACACS su TLS](#)

[Creazione di gruppi di dispositivi di rete e di dispositivi di rete](#)

[Configura archivi identità](#)

[Configura profili TACACS+](#)

[IOS XE RW - Profilo dell'amministratore](#)

[IOS XE RO - Profilo operatore](#)

[Set di comandi Configure TACACS+](#)

[CISCO IOS XE RW - Set comandi amministratore](#)

[CISCO IOS XE RO - Set di comandi dell'operatore](#)

[Set di criteri di amministrazione del dispositivo](#)

[Parte 2 - Configurazione di Cisco IOS XE per TACACS+ su TLS 1.3](#)

[Metodo di configurazione 1 - Coppia di chiavi generata dal dispositivo](#)

[Configurazione server TACACS+](#)

[Configurazione del punto di trust](#)

[TACACS e AAA con configurazione TLS](#)

[Metodo di configurazione 2 - Coppia di chiavi generata dalla CA](#)

[TACACS e AAA con configurazione TLS](#)

[Verifica](#)

---

## Introduzione

Questo documento descrive un esempio per TACACS+ over TLS con Cisco Identity Services Engine (ISE) come server e un dispositivo Cisco IOS® XE come client.

# Panoramica

Il protocollo [RFC8907] TACACS+ (Terminal Access Controller System Plus) consente l'amministrazione centralizzata dei dispositivi per router, server di accesso alla rete e altri dispositivi di rete tramite uno o più server TACACS+. Fornisce servizi di autenticazione, autorizzazione e accounting (AAA), specificamente progettati per casi di utilizzo in cui è richiesta l'amministrazione di dispositivi.

TACACS+ over TLS 1.3 [RFC846] migliora il protocollo introducendo un livello di trasporto sicuro, per la protezione dei dati altamente sensibili. Questa integrazione garantisce riservatezza, integrità e autenticazione per la connessione e il traffico di rete tra i client e i server TACACS+.

## Utilizzo della Guida

Questa guida divide le attività in due parti per consentire ad ISE di gestire l'accesso amministrativo per i dispositivi di rete basati su Cisco IOS XE.

- Parte 1 - Configurazione di ISE per l'amministrazione dei dispositivi
- Parte 2 - Configurazione di Cisco IOS XE per TACACS+ over TLS

## Prerequisiti

### Requisiti

Requisiti per configurare TACACS+ over TLS:

- Un'Autorità di certificazione (CA) per firmare il certificato utilizzato da TACACS+ su TLS per firmare i certificati dell'ISE e dei dispositivi di rete.
- Il certificato radice dell'Autorità di certificazione (CA).
- I dispositivi di rete e ISE hanno una raggiungibilità DNS e possono risolvere i nomi host.

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ISE VMware virtual appliance, release 3.4 patch 2
- Software Cisco IOS XE, versione 17.15+

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

### Licenze

Una licenza di Device Administration consente di utilizzare i servizi TACACS+ su un nodo di Policy Service. In un'implementazione standalone ad alta disponibilità (HA), una licenza di Device Administration consente di utilizzare i servizi TACACS+ su un singolo nodo Policy Service nella coppia HA.

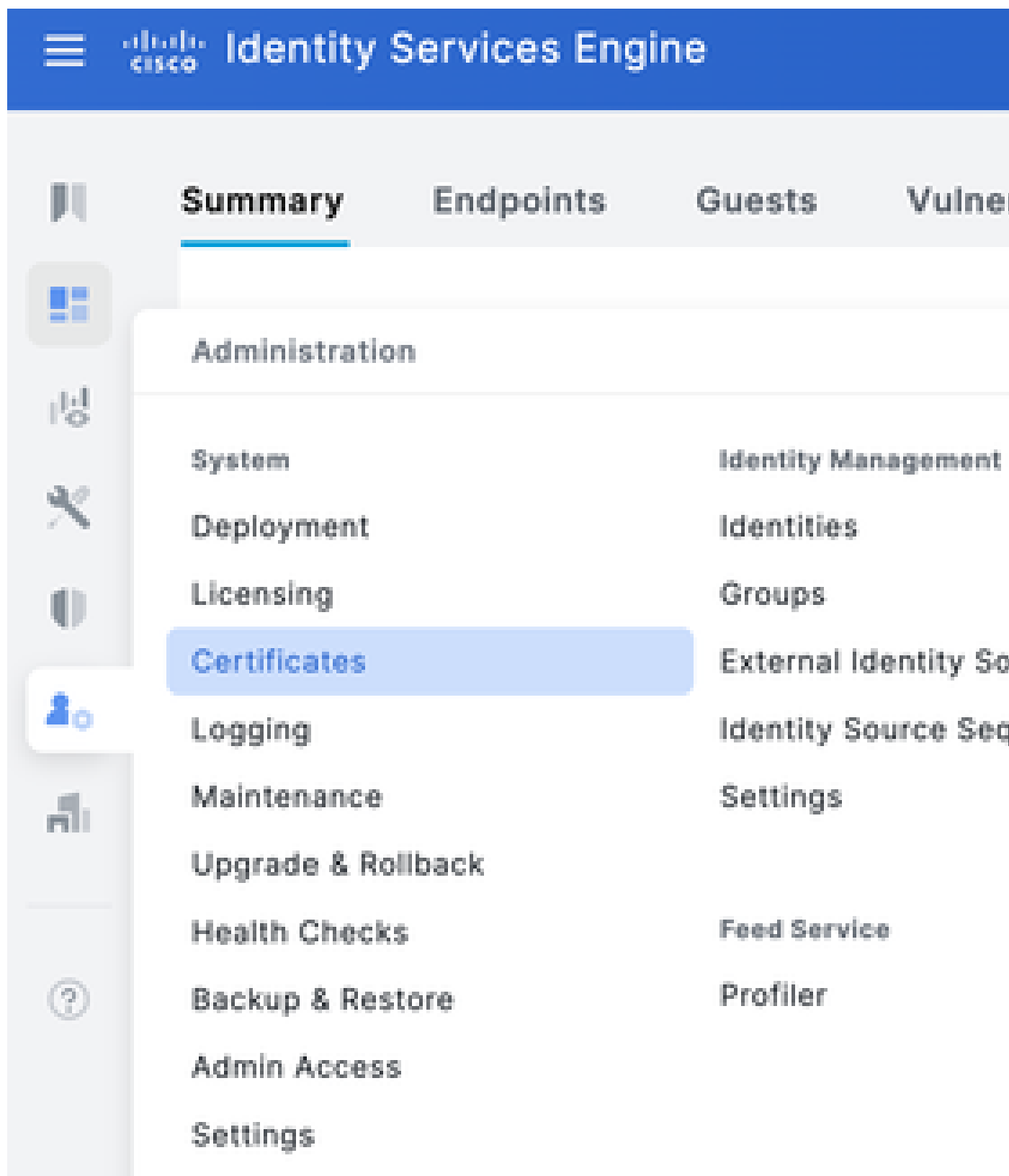
## Parte 1 - Configurare ISE per l'amministrazione dei dispositivi

Genera richiesta di firma del certificato per autenticazione server TACACS+

Passaggio 1. Accedere al portale Web di amministrazione di ISE utilizzando uno dei browser supportati.

Per impostazione predefinita, ISE utilizza un certificato autofirmato per tutti i servizi. Il primo passaggio consiste nella generazione di una richiesta di firma del certificato (CSR) per la firma da parte dell'Autorità di certificazione (CA).

Passare alla fase 2. Passare ad Amministrazione > Sistema > Certificati.



Passaggio 3. In Richieste di firma del certificato fare clic su Genera richiesta di firma del certificato.



Passaggio 4. Selezionare TACACS in Usage.

## Usage

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

---

Allow Wildcard Certificates ☐ 

Passaggio 5. Selezionare i nomi PSN per cui sarà abilitato TACACS+.

## Node(s)

Generate CSR's for these Nodes:

| Node                                     | CSR Friendly Name |
|------------------------------------------|-------------------|
| <input checked="" type="checkbox"/> ISE1 | ISE1#TACACS       |

Passaggio 6. Inserire le informazioni appropriate nei campi Oggetto.

## Subject

Common Name (CN)  
**\$FQDN\$**



Organizational Unit (OU)  
**CX**



Organization (O)  
**Cisco**



City (L)  
**Raleigh**

State (ST)  
**North Carolina**

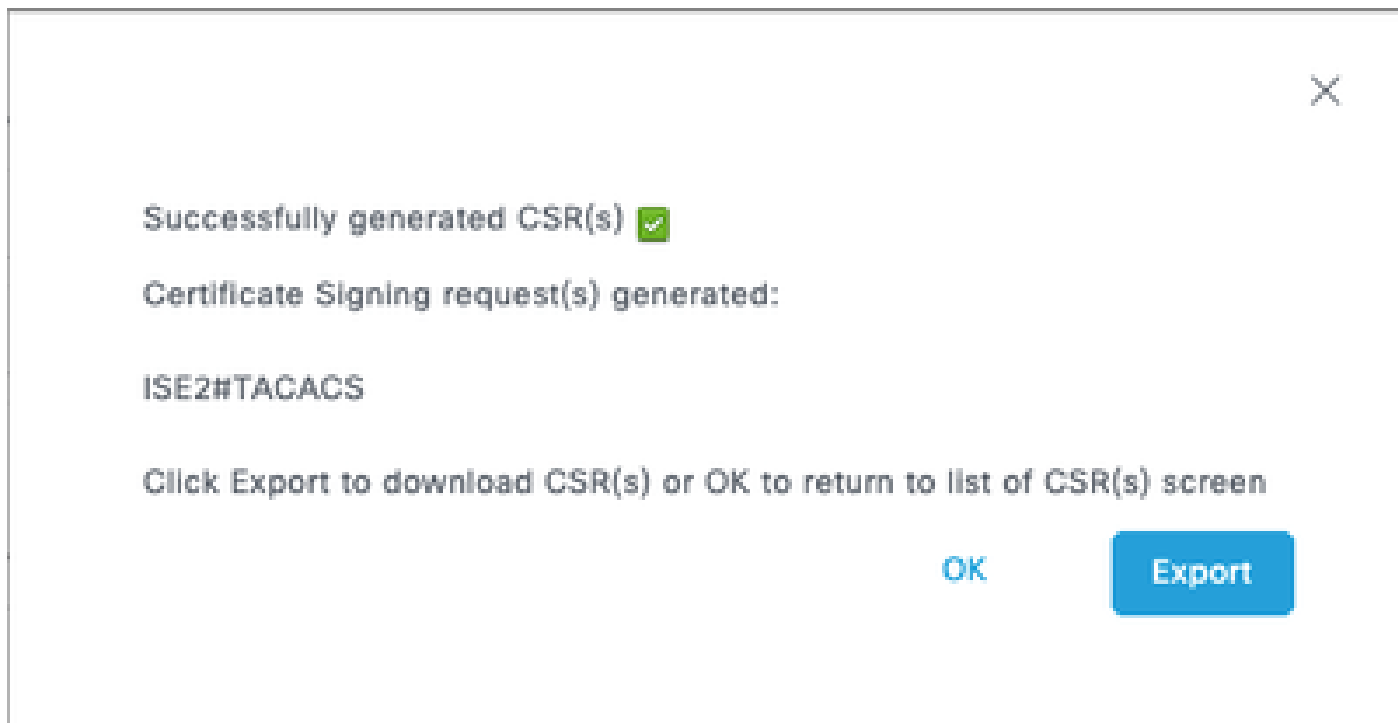
Country (C)  
**US**

Passaggio 7. Aggiungere il nome DNS e l'indirizzo IP in Nome alternativo soggetto (SAN).

### Subject Alternative Name (SAN)

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

Passaggio 8. Fare clic su Genera, quindi su Esporta.



A questo punto, è possibile far firmare il certificato (CRT) all'autorità di certificazione (CA).

Carica certificato CA radice per autenticazione server TACACS+

Passaggio 1. Passare ad Amministrazione > Sistema > Certificati. In Certificati attendibili fare clic su Importa.

| <input type="checkbox"/> | Friendly Name               | Trusted For                      | Serial Number    | Issued To            | Issued By            | Valid From       | Expiration Date   | Status |
|--------------------------|-----------------------------|----------------------------------|------------------|----------------------|----------------------|------------------|-------------------|--------|
| <input type="checkbox"/> | Amazon root CA              | Infrastructure<br>Cisco Services | 06 6C 9F CF ...  | Amazon Root CA 1     | Amazon Root CA 1     | Tue, 26 May 2015 | Sun, 17 Jan 2...  | Ent    |
| <input type="checkbox"/> | 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    |
| <input type="checkbox"/> | Cisco Licensing Root CA     | Cisco Services                   | 01               | Cisco Licensing R... | Cisco Licensing R... | Thu, 30 May 2013 | Sun, 30 May 2...  | Ent    |
| <input type="checkbox"/> | Cisco Manufacturing CA SHA2 | Endpoints<br>Infrastructure      | 02               | Cisco Manufactur...  | Cisco Root CA M2     | Mon, 12 Nov 2012 | Thu, 12 Nov 2...  | Ent    |
| <input type="checkbox"/> | Cisco Root CA 2048          | Endpoints<br>Infrastructure      | 5F F8 7B 28 2... | Cisco Root CA 20...  | Cisco Root CA 20...  | Fri, 14 May 2004 | Mon, 14 May ...   | Dis    |
| <input type="checkbox"/> | 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    |
| <input type="checkbox"/> | 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    |
| <input type="checkbox"/> | Cisco Root CA M2            | Infrastructure<br>Endpoints      | 01               | Cisco Root CA M2     | Cisco Root CA M2     | Mon, 12 Nov 2012 | Thu, 12 Nov 2...  | Ent    |
| <input type="checkbox"/> | Cisco RXC-R2                | Cisco Services                   | 01               | Cisco RXC-R2         | Cisco RXC-R2         | Wed, 9 Jul 2014  | Sun, 9 Jul 2034   | Ent    |

Passaggio 2. Selezionare il certificato rilasciato dall'Autorità di certificazione (CA) che ha firmato la richiesta di firma del certificato TACACS (CSR). Assicurarsi che ilFiducia nell'autenticazione ad ISE è attivata.

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

Passaggio 3. Fare clic su Invia. Il certificato deve essere visualizzato in Certificati attendibili.

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 the Trusted For field set to "Infrastructure Cisco Services Endpoints AdminAuth".

Associare la richiesta di firma del certificato (CSR) firmata a ISE

Una volta firmata la richiesta di firma del certificato (CSR), è possibile installare il certificato firmato in ISE.

Passaggio 1. Passare a Amministrazione > Sistema > Certificati. In Richieste di firma del certificato, selezionare il CSR TACACS generato nel passaggio precedente e fare clic su Associa certificato.

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 "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 red.

Passaggio 2. Selezionare il certificato firmato e assicurarsi che la casella di controllo TACACS in Uso rimanga selezionata.

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

Friendly Name

Validate Certificate Extensions ☐

Usage

☒ TACACS: Use certificate for TACACS Server

Passaggio 3. Fare clic su Submit (Invia). Se viene visualizzato un avviso relativo alla sostituzione del certificato esistente, fare clic su Sì per continuare.



## 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?

A questo punto è necessario installare correttamente il certificato. È possibile verificare questa condizione in Certificati di 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 |

Abilita TLS 1.3

TLS 1.3 non è abilitato per impostazione predefinita in ISE 3.4.x. Deve essere attivata manualmente.

Passaggio 1. Passare a Amministrazione > Sistema > Impostazioni.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration web interface. The top navigation bar is blue with the Cisco logo and the text "Identity Services Engine". Below this, the main navigation menu is visible on the left, and the right-hand side shows the "Deployment" and "Licensing" tabs. The "Administration" menu item is highlighted, and its sub-menu is expanded, showing various system management options. The "Settings" option at the bottom of this sub-menu is highlighted with a blue background and a checkmark icon.

**Navigation Menu (Left):**

- Bookmarks
- Dashboard
- Context Visibility
- Operations
- Policy
- Administration**
- Work Centers
- Interactive Help

**Deployment and Licensing Tabs (Right):**

- Client Provisioning
- FIPS Mode
- Security Settings
- Alarm Settings

**Administration Sub-menu (Right):**

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

Passaggio 2. Fare clic su Impostazioni protezione, selezionare la casella di controllo accanto a TLS1.3 in Impostazioni versione TLS, quindi fare clic su Salva.

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

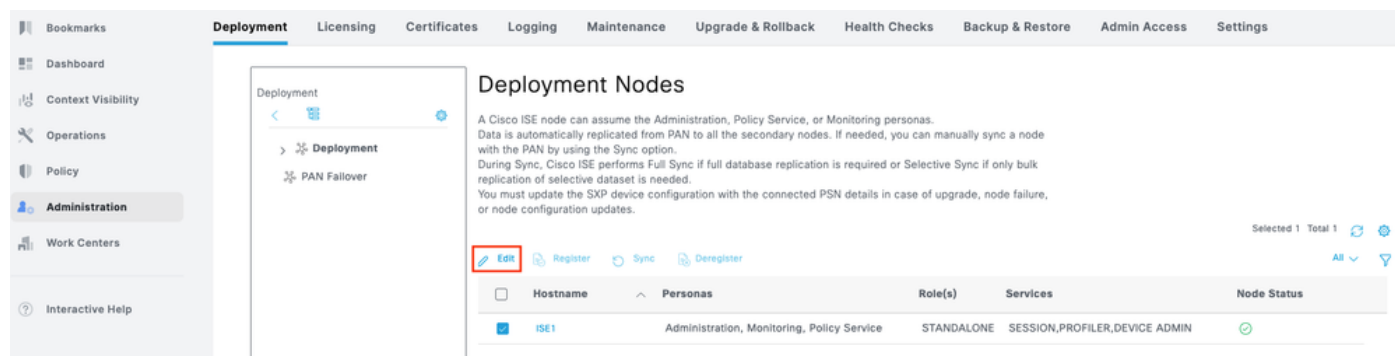


Avviso: Quando si modifica la versione TLS, il server applicazioni Cisco ISE viene riavviato su tutti i computer di implementazione di Cisco ISE.

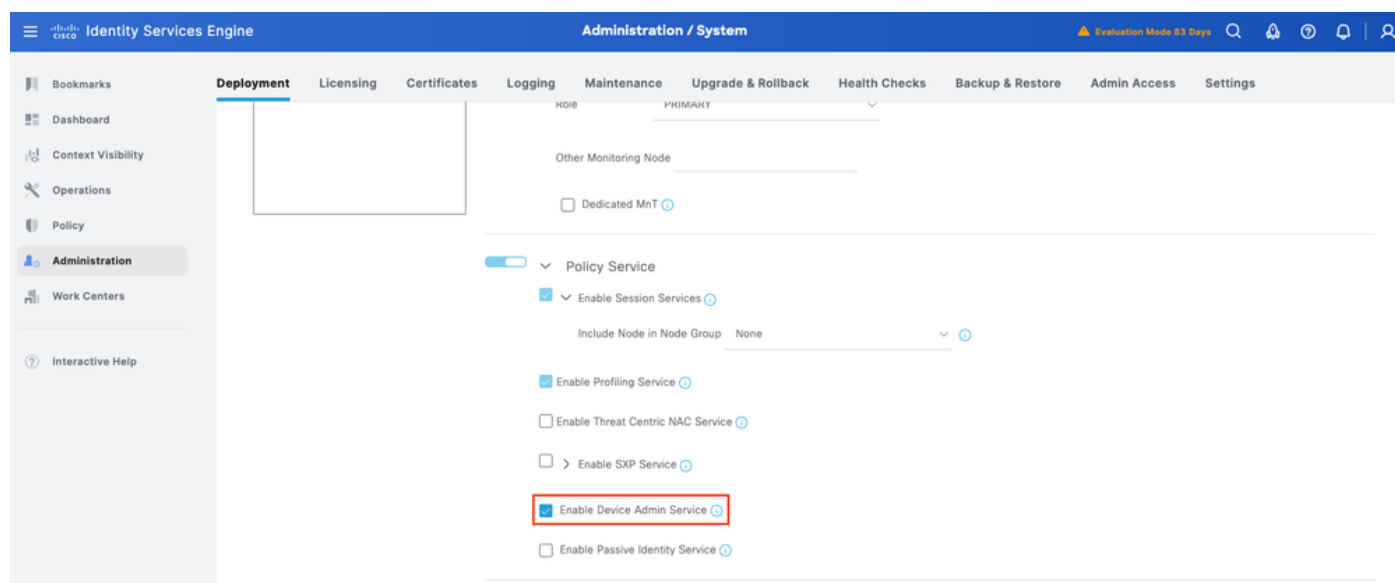
## Abilita amministrazione dispositivi su ISE

Il servizio Device Administration (TACACS+) non è abilitato per impostazione predefinita su un nodo ISE. Abilitare TACACS+ su un nodo PSN.

Passaggio 1. Passare a Amministrazione > Sistema > Distribuzione. Selezionare la casella di controllo accanto al nodo ISE e fare clic su Modifica.



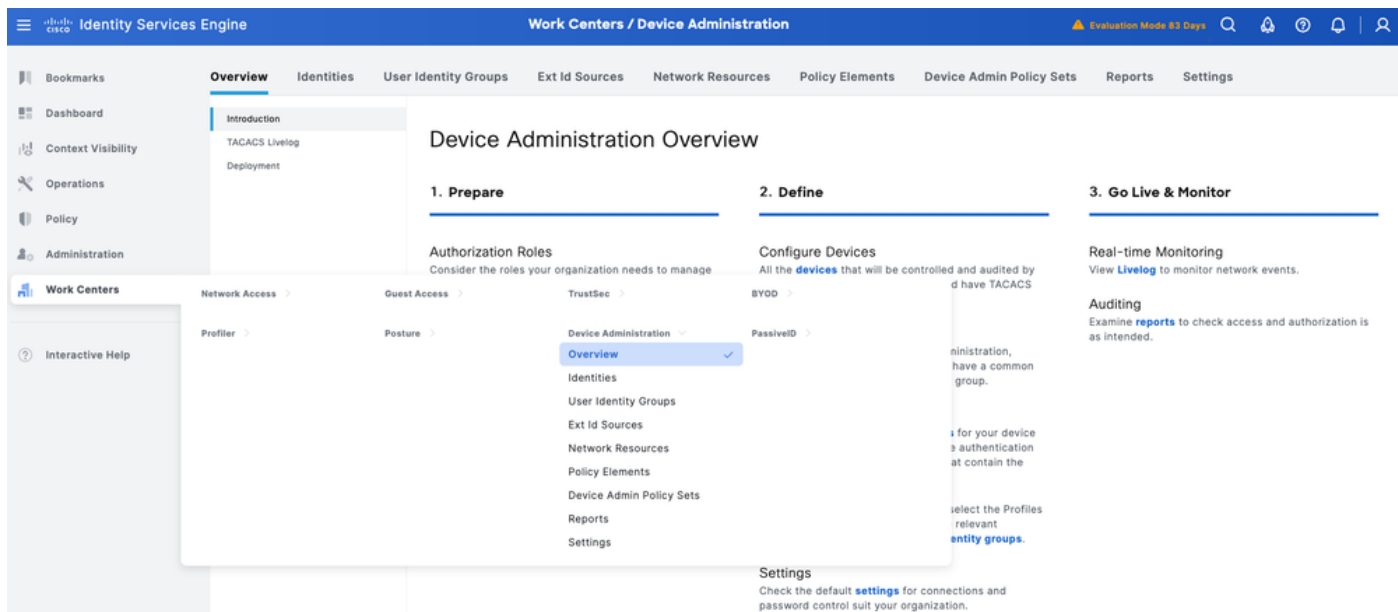
Passaggio 2. In GeneralSettings, scorrere verso il basso e selezionare la casella di controllo accanto a Enable Device Admin Service (Abilita servizio di amministrazione dispositivi).



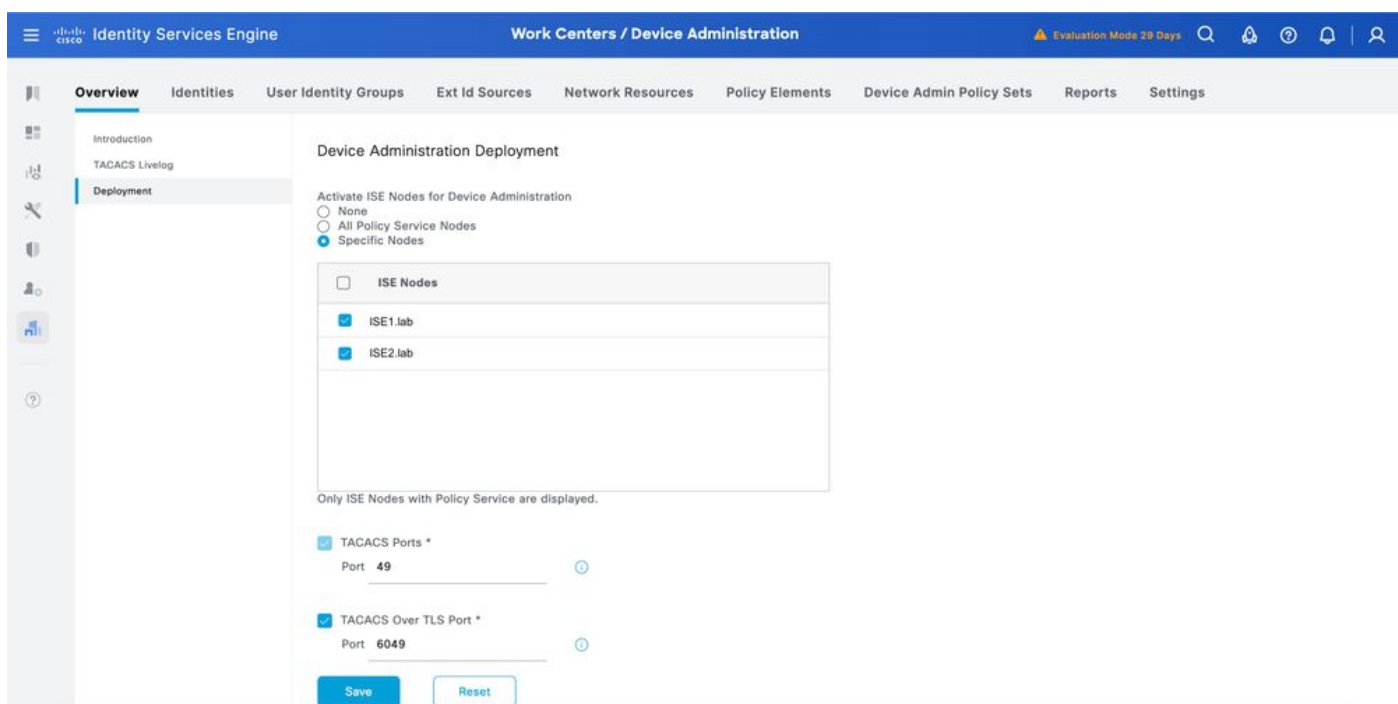
Passaggio 3. Salvare la configurazione. Device Admin Service è ora abilitato su ISE.

## Abilita TACACS su TLS

Passaggio 1. Passare a Centri di lavoro > Amministrazione dispositivi > Panoramica.



Passaggio 2. Fare clic su Distribuzione. Selezionare i nodi PSN in cui si desidera abilitare TACACS su TLS.



Passaggio 3. Mantenere la porta predefinita 6049 o specificare una porta TCP diversa per TACACS over TLS, quindi fare clic su Save.

## Creazione di gruppi di dispositivi di rete e di dispositivi di rete

ISE fornisce un potente raggruppamento di dispositivi con più gerarchie di gruppi di dispositivi. Ogni gerarchia rappresenta una classificazione distinta e indipendente dei dispositivi di rete.

Passaggio 1. Passare a Centri di lavoro > Amministrazione dispositivi > Risorse di rete. Fare clic su Gruppi di dispositivi di rete e creare un gruppo denominato IOS XE.

Identity Services Engine

Work Centers / Device Administration

Evaluation Mode

OverviewIdentitiesUsers

Network Devices

Network Device Groups

Default Devices

TACACS External Servers

TACACS Server Sequence

×

Add Group

Name\*

IOSXE

Description

Parent Group\*

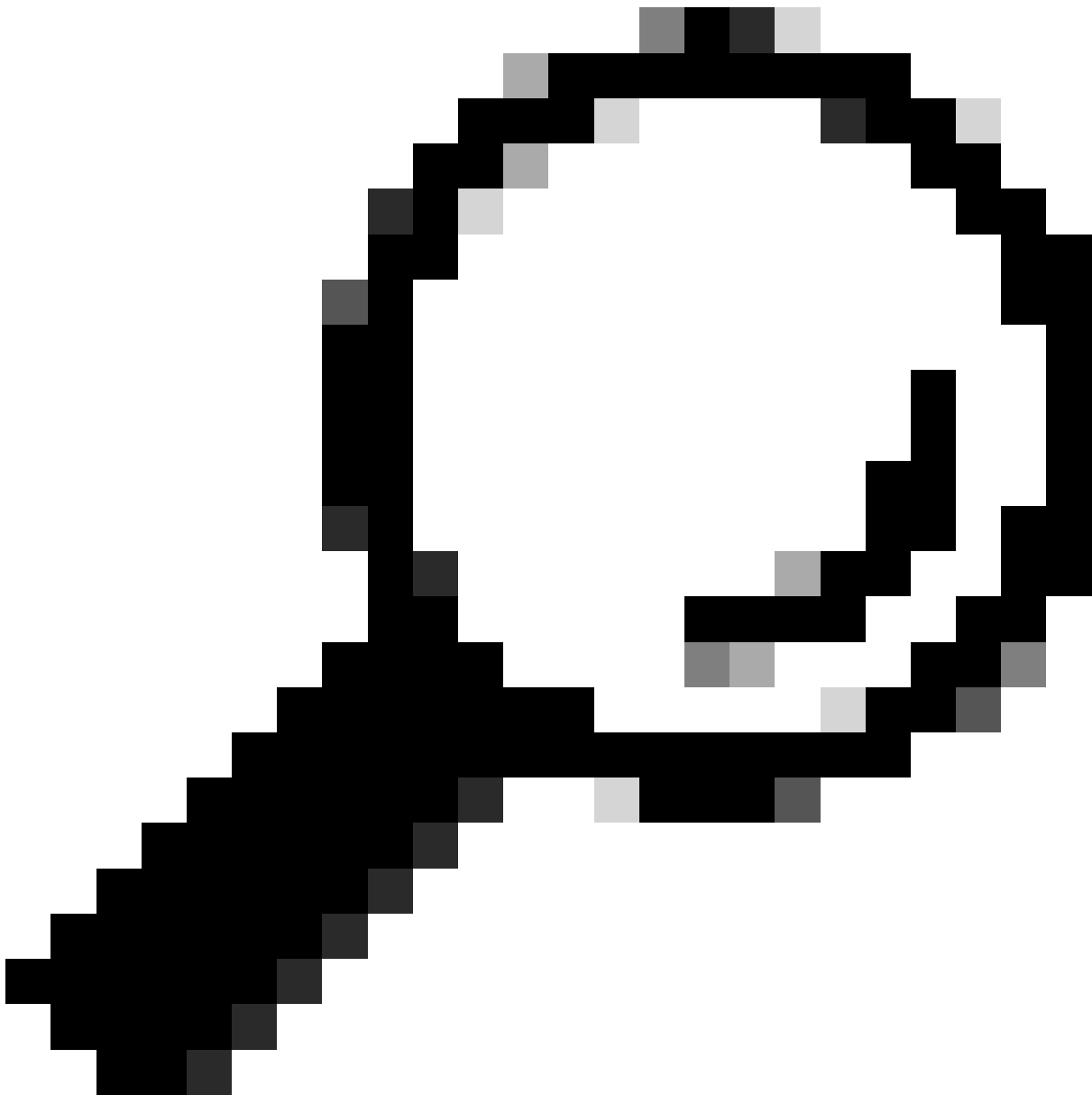
Select Group or Add as root group

Cancel

Save

☐

IOSXR



Suggerimento: Tutti i tipi di dispositivo e Tutti i percorsi sono gerarchie predefinite fornite da ISE. È possibile aggiungere gerarchie personalizzate e definire i vari componenti per l'identificazione di un dispositivo di rete che potrà essere utilizzato successivamente nella condizione del criterio

---

Passaggio 2. Aggiungere ora un dispositivo Cisco IOS XE come dispositivo di rete. Passare a Centri di lavoro > Amministrazione dispositivi > Risorse di rete > Dispositivi di rete. Fare clic su Add (Aggiungi) per aggiungere un nuovo dispositivo di rete. Per questo test, sarebbe SVS\_BRPASR1K.

Identity Services Engine

Work Centers / Device Administration

Overview

Identities

User Identity Groups

Ext Id Sources

Network Resources

Policy Elements

Device Admin Policy Sets

More

Network Devices

Network Device Groups

Default Devices

TACACS External Servers

TACACS Server Sequence

Network Devices List > SVS\_BRPASR1K

Network Devices

Name

SVS\_BRPASR1K

Description

IP Address

\* IP :

10.225.253.180

/ 32

Device Profile

Cisco

Model Name

Software Version

Network Device Group

Location

All Locations

Set To Default

Passaggio 3. Immettere l'indirizzo IP del dispositivo e accertarsi di mappare la posizione e il tipo di dispositivo (IOS XE) per il dispositivo. Infine, abilitare le impostazioni di autenticazione TACACS+ over TLS.

Identity Services Engine

Work Centers / Device Administration

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.

☐

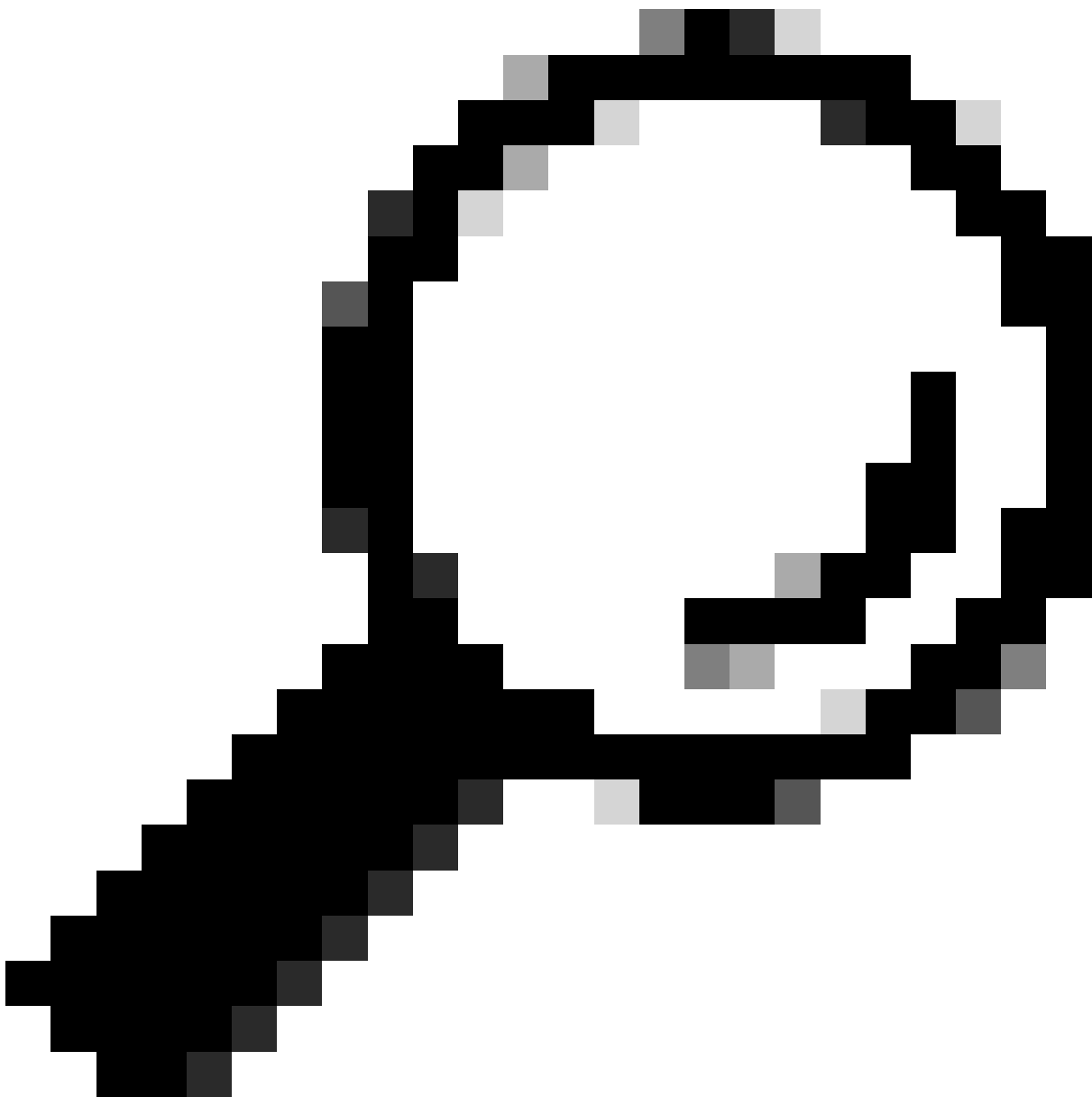
IP Address

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



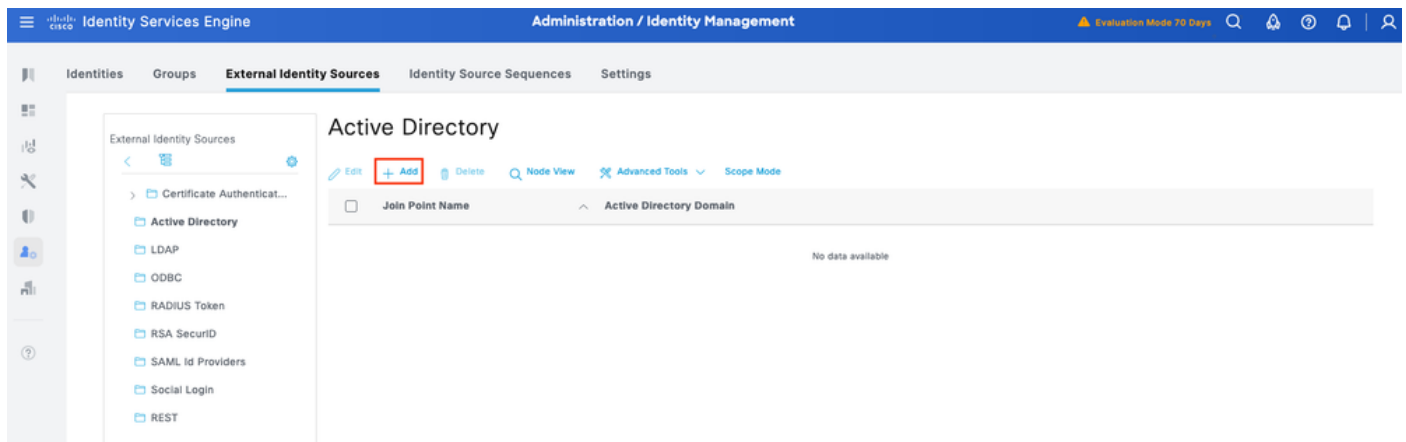
Suggerimento: Per evitare di riavviare la sessione TCP ogni volta che si invia un comando al dispositivo, si consiglia di abilitare la modalità di connessione singola.

---

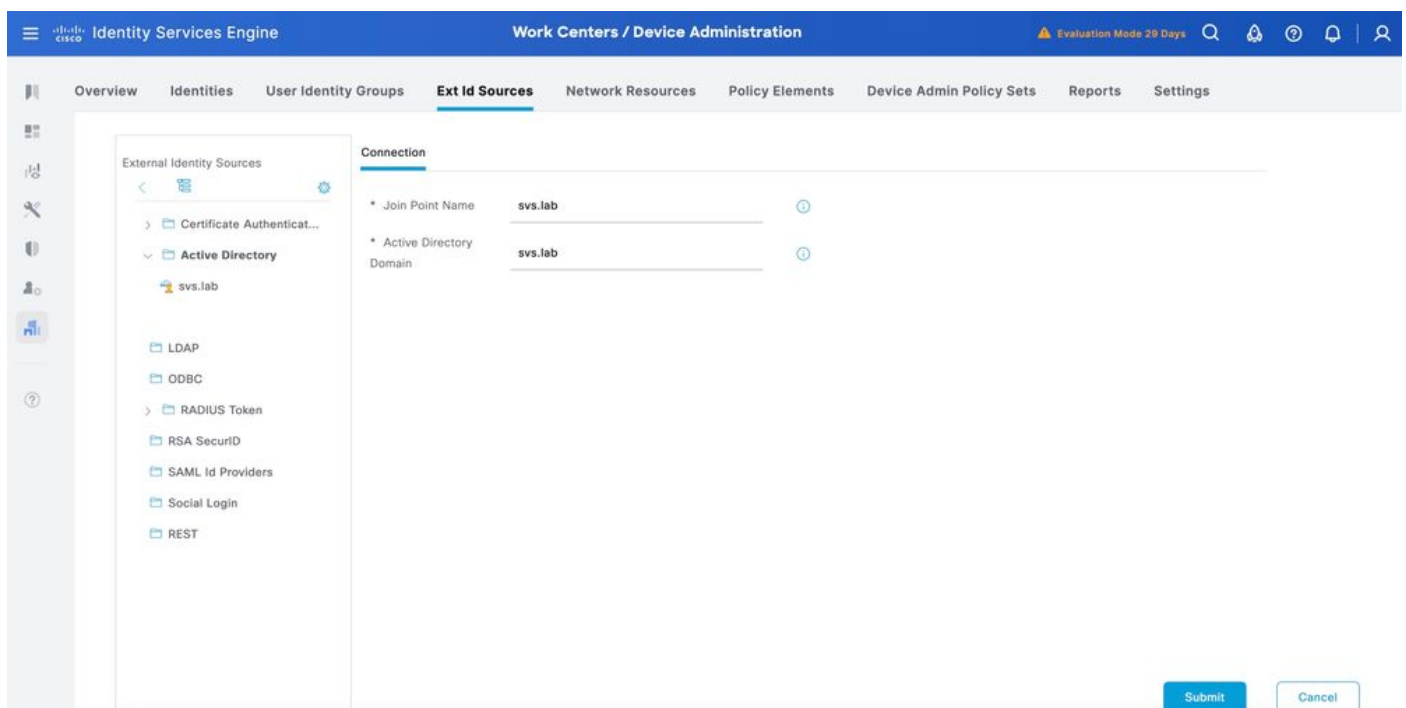
## Configura archivi identità

In questa sezione viene definito un archivio identità per gli amministratori dei dispositivi, che può essere costituito dagli utenti interni ISE e da qualsiasi origine identità esterna supportata. In questo esempio viene utilizzato Active Directory (AD), un'origine identità esterna.

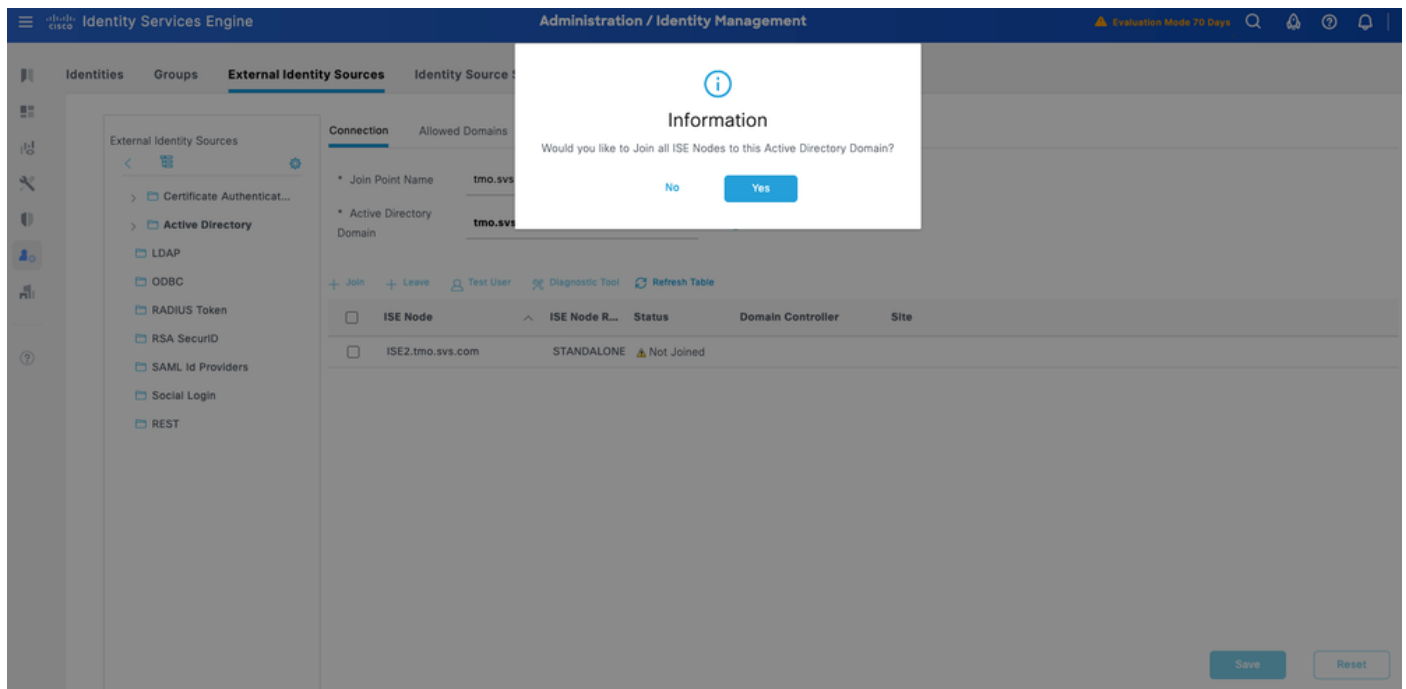
Passaggio 1. Passare a Amministrazione > Gestione delle identità > Archivi identità esterni > Active Directory. Fare clic su Aggiungi per definire un nuovo punto di giunzione AD.



Passaggio 2. Specificare il nome del punto di join e il nome del dominio Active Directory e fare clic su Invia.



Passaggio 3. Fare clic su Sì quando richiesto Aggiungere tutti i nodi ISE a questo dominio Active Directory?



Passaggio 4. Inserire le credenziali con privilegi di join AD e Join ISE to AD. Controllare lo Stato per verificare che sia operativo.

×

## Join Domain

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

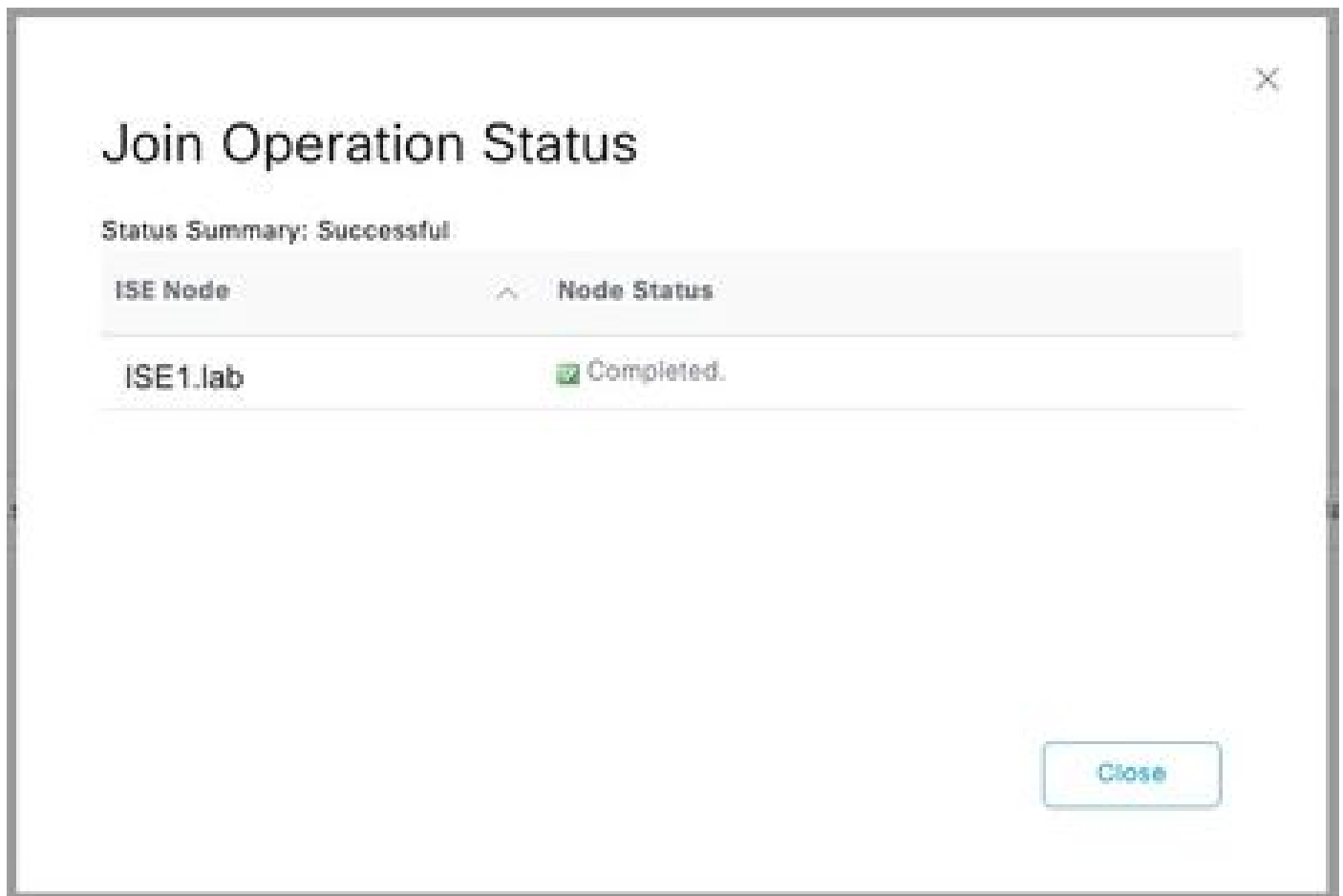
\* AD User Name ⓘ administrator

\* Password .....  
.....

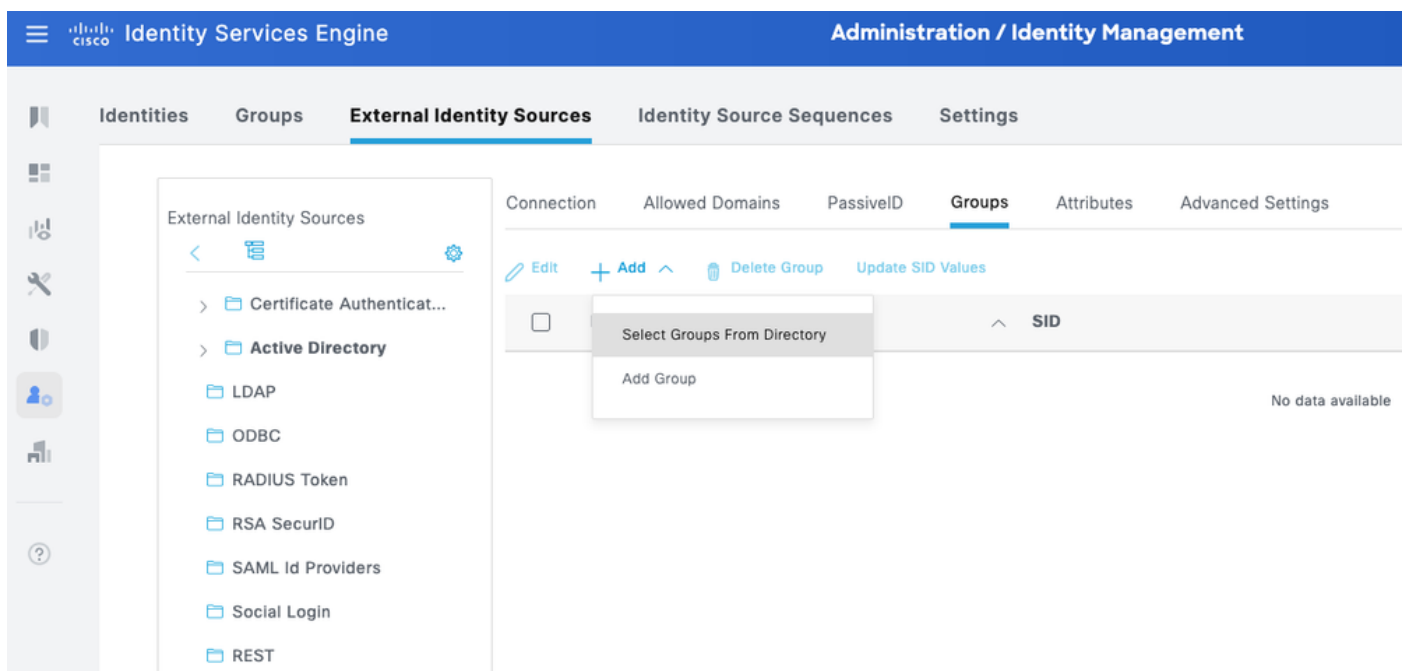
☐ Specify Organizational Unit ⓘ

☒ Store Credentials ⓘ

Cancel OK



Passaggio 5. Passare alla scheda Gruppi e fare clic su Aggiungi per ottenere tutti i gruppi necessari in base ai quali gli utenti sono autorizzati per l'accesso al dispositivo. In questo esempio vengono illustrati i gruppi utilizzati nei criteri di autorizzazione in questa guida



# Select Directory Groups

This dialog is used to select groups from the Directory.

Domain

Name

SID

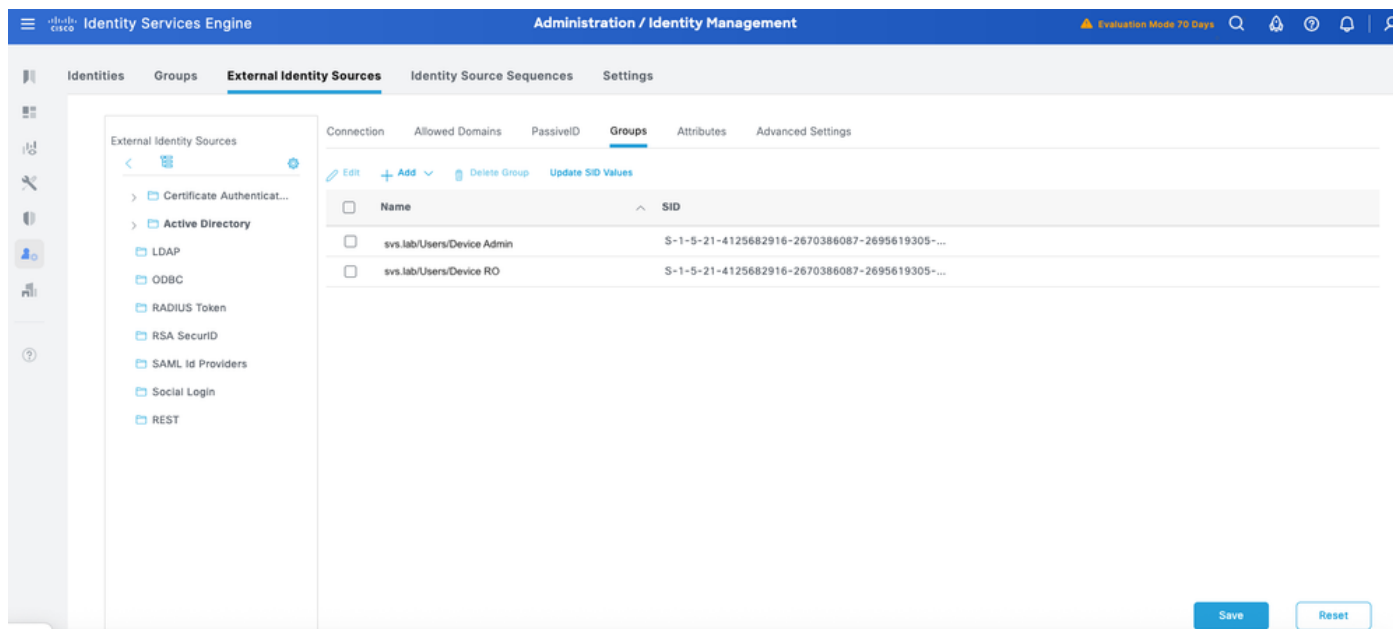
Type

Filter

Retrieve Groups...

2 Groups Retrieved.

| <input type="checkbox"/> | Name                       | Group SID                                  | Group Type |
|--------------------------|----------------------------|--------------------------------------------|------------|
| <input type="checkbox"/> | svs.lab/Users/Device Admin | S-1-5-21-4125682916-2670386087-26956193... | GLOBAL     |
| <input type="checkbox"/> | svs.lab/Users/Device RO    | S-1-5-21-4125682916-2670386087-26956193... | GLOBAL     |



## Configura profili TACACS+

Si sta per mappare i profili TACACS+ ai due ruoli utente principali sui dispositivi Cisco IOS XE:

- Amministratore di sistema principale - È il ruolo con i privilegi più elevati nel dispositivo. L'utente con il ruolo di amministratore di sistema radice dispone di accesso amministrativo completo a tutti i comandi di sistema e alle funzionalità di configurazione.
- Operatore: questo ruolo è destinato agli utenti che necessitano di accesso in sola lettura al sistema a scopo di monitoraggio e risoluzione dei problemi.

Questi sono definiti come due profili TACACS+: IOS\_XE\_RW e IOSXR\_RO.

IOS\_XE\_RW - Profilo dell'amministratore

1. Accedere a Work Center > Device Administration > Policy Elements > Results > TACACS Profiles. Aggiungere un nuovo profilo TACACS e denominarlo IOS\_XE\_RW.

Passaggio 2. Selezionare e impostare Privilegio predefinito e Privilegio massimo su 15.

Passaggio 3. Confermare la configurazione e salvare.

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 'Policy Elements' section is expanded, showing 'Conditions', 'Network Conditions', 'Results' (with sub-items 'Allowed Protocols', 'TACACS Command Sets', and 'TACACS Profiles' selected), and 'TACACS Profiles'. The main content area displays the configuration for a 'TACACS Profile' named 'IOSXE\_RW'. It includes a 'Name' field with the value 'IOSXE\_RW' and a 'Description' text area. 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'. Below this, there are two rows of configuration: 'Default Privilege' and 'Maximum Privilege', both set to '15' with a dropdown arrow and a note '(Select 0 to 15)'. Both rows have a checked checkbox on the left.

## IOS\_XE\_RO - Profilo operatore

1. Accedere a Work Center > Device Administration > Policy Elements > Results > TACACS Profiles. Aggiungere un nuovo profilo TACACS e denominarlo IOS\_XE\_RO.

Passaggio 2. Selezionare e impostare Privilegio predefinito e Privilegio massimo su 1.

Passaggio 3. Confermare la configurazione e salvare.

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

## Set di comandi ConfigureTACACS+

questi sono definiti come due set di comandi TACACS+: CISCO\_IOS XE\_RW e CISCO\_IOS XE\_RO.

CISCO\_IOS XE\_RW - Set comandi amministratore

Passaggio 1. Passare a Centri di lavoro > Amministrazione dispositivi > Elementi dei criteri > Risultati > Set di comandi TACACS. Aggiungere un nuovo set di comandi TACACS e denominarlo CISCO\_IOS XE\_RW.

Passaggio 2. Selezionare la casella di controllo Consenti qualsiasi comando non elencato di seguito (consente qualsiasi comando per il ruolo di amministratore) e fare clic su Salva.

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

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 - Set di comandi dell'operatore

1. Dall'interfaccia utente di ISE, selezionare Work Center > Device Administration > Policy Elements > Results > TACACS Command Sets. Aggiungere un nuovo set di comandi TACACS e denominarlo CISCO\_IOS XE\_RO.

Passaggio 2. Nella sezione Comandi, aggiungere un nuovo comando.

Passaggio 3. Selezionare Permit dall'elenco a discesa della colonna Grant (Concedi) e immettere show nella colonna Command; e fare clic sulla freccia check.

Passaggio 4. Confermare i dati e fare clic su Salva.

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

TACACS Command Sets > CISCO\_IOSXE\_RO

Command Set

Name  
CISCO\_IOSXE\_RO

Description

Commands

Permit any command that is not listed below ☐

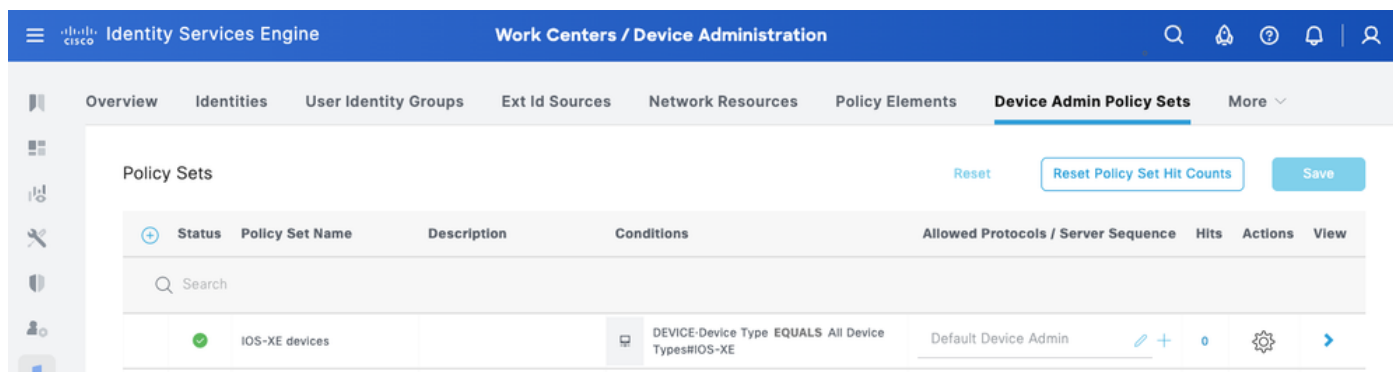
Add Trash Edit Move Up Move Down

| Grant                           | Command | Arguments |
|---------------------------------|---------|-----------|
| <input type="checkbox"/> PERMIT | show    |           |

## Set di criteri di amministrazione del dispositivo

I set di criteri sono attivati per impostazione predefinita per l'amministrazione dei dispositivi. I set di criteri possono dividere i criteri in base ai tipi di dispositivo in modo da semplificare l'applicazione dei profili TACACS.

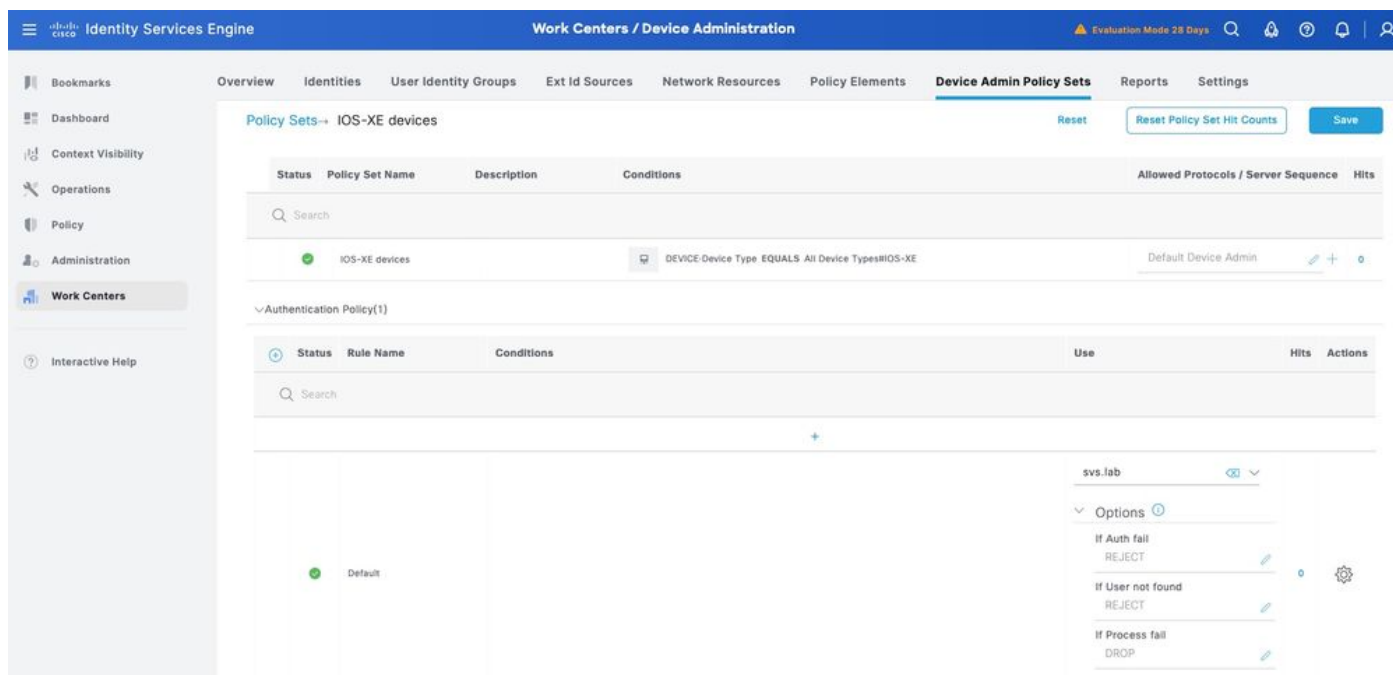
Passaggio 1. Passare a Centri di lavoro > Amministrazione dispositivi > Set di criteri di amministrazione dispositivi. Aggiungere un nuovo set di criteri per i dispositivi IOS XE. In questa condizione specificare `DEVICE:Device Type EQUALS All Device Types#IOS XE`. In Protocolli consentiti, selezionare Amministratore di dispositivo predefinito.



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

Passaggio 2. Fare clic su Save e sulla freccia destra per configurare questo set di criteri.

Passaggio 3. Creare il criterio di autenticazione. Per l'autenticazione, utilizzare AD come archivio ID. Accettare le opzioni di default in Se autenticazione (If Auth fail), Se utente (If User) non è stato trovato e Se processo (Process fail).



| Status | Rule Name | Conditions | Use | Hits | Actions |
|--------|-----------|------------|-----|------|---------|
| ✓      | Default   |            |     | 0    |         |

**Options**

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

Passaggio 4. Definire il criterio di autorizzazione.

Creare i criteri di autorizzazione in base ai gruppi di utenti in Active Directory (AD).

Ad esempio:

- Agli utenti del gruppo AD Device RO viene assegnato il set di comandi CISCO\_IOSXR\_RO e il profilo di IOSXR\_RO Shell.
- Agli utenti del gruppo AD Device Admin viene assegnato il set di comandi CISCO\_IOSXR\_RW e il profilo della shell IOSXR\_RW.

The screenshot displays the Cisco Identity Services Engine (ISE) interface, specifically the 'Work Centers / Device Administration' section. The 'Device Admin Policy Sets' tab is active, showing a table of policy sets for 'IOS-XE devices'. The table includes columns for Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, and Hits. Below the main table, there are expandable sections for 'Authentication Policy(1)', 'Authorization Policy - Local Exceptions', 'Authorization Policy - Global Exceptions', and 'Authorization Policy(3)'. The 'Authorization Policy(3)' section is expanded, showing a detailed table of authorization rules. This table includes columns for Status, Rule Name, Conditions, Command Sets, Shell Profiles, Hits, and Actions. The rules listed are 'Authorization Rule RO', 'Authorization Rule RW', and 'Default'.

| 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

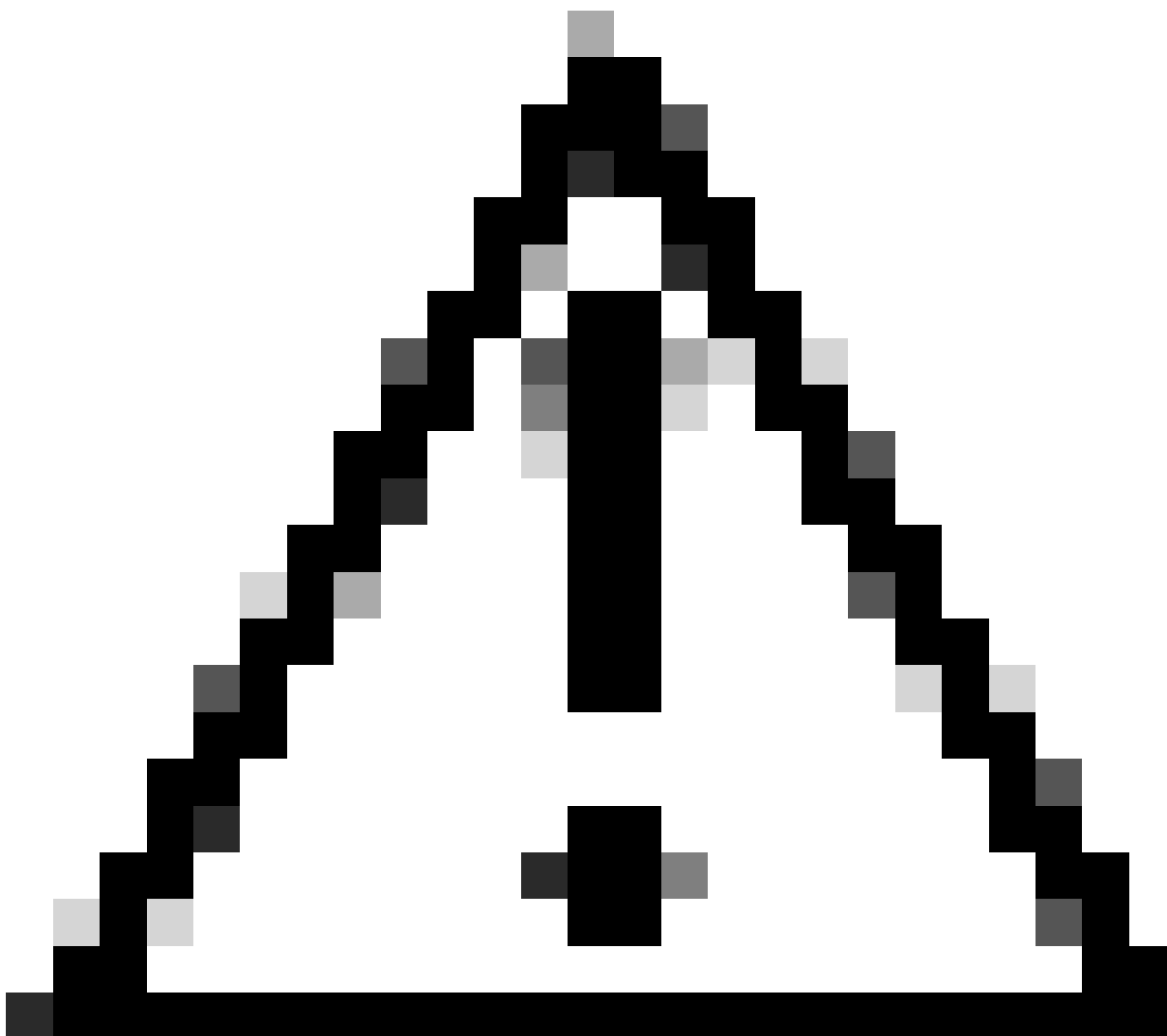
> Authorization Policy - Global Exceptions

✓ Authorization Policy(3)

| Status | Rule Name             | Conditions                                               | Results         |                        |   | Hits | Actions |
|--------|-----------------------|----------------------------------------------------------|-----------------|------------------------|---|------|---------|
|        |                       |                                                          | Command Sets    | Shell Profiles         |   |      |         |
| ✓      | 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 |      |         |

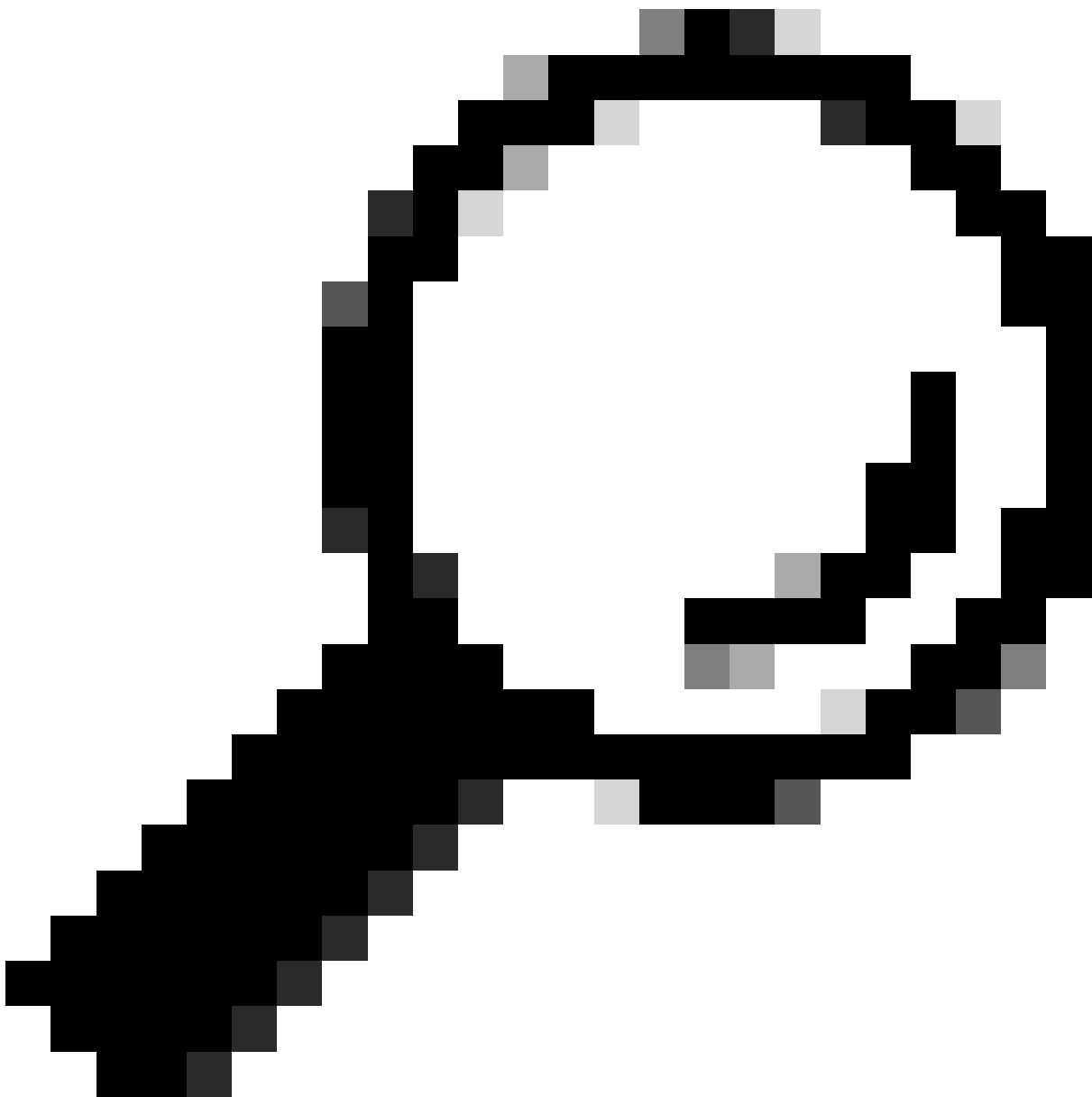
## Parte 2 - Configurazione di Cisco IOS XE per TACACS+ su TLS

### 1.3



Attenzione: Verificare che la connessione alla console sia raggiungibile e funzioni correttamente.

---



Suggerimento: Per evitare di essere bloccati dal dispositivo, si consiglia di configurare un utente temporaneo e modificare i metodi di autenticazione e autorizzazione AAA in modo da usare le credenziali locali anziché TACACS durante le modifiche alla configurazione.

---

## Metodo di configurazione 1 - Coppia di chiavi generata dal dispositivo

### Configurazione server TACACS+

Passaggio 1 Configurare il nome di dominio e generare una coppia di chiavi utilizzata per il trust router.

```
ip domain name svS.lab
```

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

## Configurazione del punto di trust

1. Creare un trustpoint del router e associare la coppia di chiavi.

```
crypto pki trustpoint svS_cat9k
  enrollment terminal pem
  subject-name C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=cat9k.svS.lab
  serial-number none
  ip-address none
  revocation-check none
  eckeypair svS-256ec-key
```

Passaggio 2. Autenticare il trust point installando il certificato CA.

<#root>

```
cat9k(config)#
```

```
crypto pki authenticate svS_cat9k
```

Enter the base 64 encoded CA certificate.

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

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

```
MIIF1DCCA3ygAwIBAgIIIM10AsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZzAVBgNVBAGTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECXMdu1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUgA1UECBMOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBACTB1JhbGVpZ2gxDjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTV1MxEjAQBgNVBAMTCVNWUyBMWJJDQTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZU0yn2vIn6gKbx3M7vaRq
2YjwZ1zSH6EkEvxnJTjy+kksIFD33GyHQepk7vfp4NFU50tQ4HC7t/A0v9grDa3QW
VwvV4MBBjHFM3s0J/ejgDYcMZhIAaPy0Zo5WLboOkXEiKjPLatKXojB8FVrhLF3O
jMBSqwa4/Wlniy5S+7s4FFxsCf20COWfBAsnrs0tatIIhmcnx+VLJP7MRm8f0w4m
mutNo7IhbJSrgAFxmjlBjMmgspObULo/wxMHdTbtPBf11HRHTkNIo3qy04UADL2
WpoGhgT/FaxxBo2UBcnYVaP+jjREONYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7B0e8oDNKU6gX1ojKyLP/gC7j8AeP03ir+KZui8
b8X4iYn/67SbzZFhwn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
```

```
gJ+kQXe7QtT/u6m1MrtjE3gAEVpL334rTIxy9hpKZIkB86t2ZA3JX8CLsbCa13sA
z1XCoONX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTA01xh60I4QnK+MNQKpTjt/E4
ydHl0rrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVL1783nTc9wYptQEPi5sw
83g9EMgKV0ARIiVUa/q7AgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAyb4
QgEBBAQDAgAHMBkGCWCGSAGG+EIBDQMFgptV1MgTGF1IENBMAOGCSqGSIb3DQEB
CwUAA4ICAQAIT308oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oK0dGayi
iSEkSSX9qyfLFINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXRX67X+v
O+ja6zTQqj06lqJhmrSkyFbYf/ZTpe4d10zJsZjNsN0r8bF9nOA/7qNZLp3Z3cpU
PU0KdbiSvRqnPw3e8TfITVmAzcx8COI2SrYFMSUazo1VBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIEOf5ay1PKURO/8aj/B7a1uJapXkmnj5qPeGhN0pB
Q9r14reov4so2EspkXS7CrH9yGfpIyTprokz1UvZBZ8v1oI7YZmjFmem+5rT6Gnk
eU/1X7nV61SYG5W5K+I8uaKuyBHOMn7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggz1P0dsS/i6Lo7ypYX0eB9HgVDCkzQsLXQuHGj/2WsgPgDRcjkvnyURk4Jx+Ib
xDrmo7e0XPpSW4l72a6K18CR3U2Cr4wsuvndPEq/qd2NRSBWffFOXe/AJHQG7STT
HaXLU9r2Ko603oecu8ysGTwLlIt/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)#

Passaggio 3. Generare una richiesta di firma del certificato (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
VQQLewNTV1MxDjAMBgNVBAoTBUNpc2NmMQwwCgYDVQQHEwNSVFAXCzAJBgNVBAGT
Ak5DMQswCQYDVQQGEwJVUzEgMB4GCSqGSIb3DQEJAhYRY2F0OWsudG1vLnN2cy5j
b20wWTATBgqhkJOPQIBBggqhkJOPQMBBwNCAATpYE7atscrt14ddevCh3UgxjYi
4N4oBGWrpJBctKy4so8V5i6RXDt7kHgPzp14Qnf20bcXVODE1wtTAHHBrIXqoDww
OgYJKoZIhvcNAQkOMS0wKzAcBgNVHREFTATghFjYXQ5ay50bW8uc3ZzLmNvbTAL
```

```
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)#

Passaggio 4. Importare un certificato firmato dall'autorità di certificazione.

<#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
BhMCVVMxZzFzAVBgNVBAGTDk5vbnRoIENhcm9saW5hMRwwDgYDVQQHEwdSYWx1aWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECXMdU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNTEOMTUxMjAwWWhcNMjUwNTEOMTUxMjAwWjCBhDEaMBGGA1UEAxMR
Y2F0OWsudG1vLnN2cy5jb20xDDAKBgNVBAsTA1NWUzEOMAwGA1UEChMFQ21zY28x
DDAKBgNVBAcTA1JUUEDEMAkGA1UECBMCTkMxZzFzAVBgNVBAYTA1VTMSAwHgYJKoZI
hvcNAQkCFhFjYXQ5ay50bW8uc3ZzLmNvbTBZMBMGByqGSM49AgEGCCqGSM49AwEH
A0IAB01gtTq2xyu2Xh1168KHdSDGNiLg3igEZaukkFy0rLiYjXmLpFc03uQeA/O
nXhCd/bRtxdU4MTXC1MAccGsheqjTTBLMB4GCWCGSAGG+EIBDQRRFg94Y2EgY2Vy
dG1maWNhdGUwHAYDVR0RBBUwE4IRY2F0OWsudG1vLnN2cy5jb20wCwYDVR0PBAQD
AgeAMAOGCSqGSIb3DQEBGwUAA4ICAQB0bgKVykeyVC9Usvuu0AUsGaZHGwy2H9Yd
m5vIau6PjczkCzIoAIghHPGQhIgpEcRqtGyXPZ2r8TCJP11WXNN/G73sFyWAHzY
RtmIM5KIojiDHLtiFpayxv9juDu0ZRx+wYR2PIQ5eLv1bafg7K8E82sq0Cf0tcPr
Oc0NU8UCxq0bd0gu4XsdBN1+wcWFqeQSDLP7nxvh00m/LXwCWUhwgVio0AuU2Fe
k5NthtvdXNAhRAImQdTyq6u/yB7vwTwJHcRiJc5USsyZCsTBb6RvL+HsXqBgXGc5
1xCS0LtY0dUxFipJyK2MOZBY2zq2cNSc8Xbso5/OEQmnHtpWPvjj4rSPUHQSY+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 e AAA con configurazione TLS

Passaggio 1. Creare i gruppi TACACS server e AAA, associare il trust point client (router).

```
tacacs server svcs_tacacs
address ipv4 10.225.253.209
single-connection
tls port 6049
tls idle-timeout 60
tls connection-timeout 60
tls trustpoint client svcs_cat9k
tls ip tacacs source-interface GigabitEthernet0/0
tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ svcs_tls
server name svcs_tacacs
ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request
```

Passaggio 2. Configurare i metodi AAA.

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

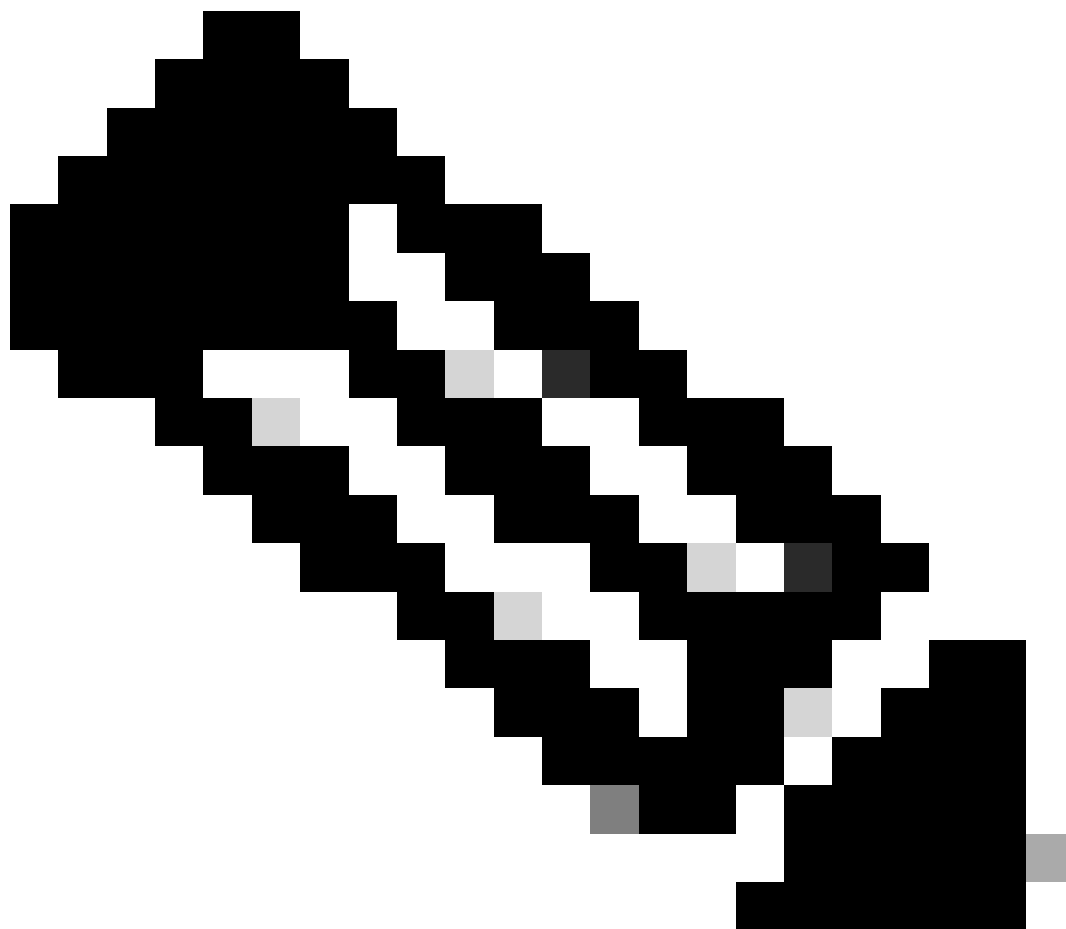
## Metodo di configurazione 2 - Coppia di chiavi generata dalla CA

Se si importano le chiavi, nonché i certificati dei dispositivi e delle CA direttamente in formato PKCS#12 anziché in formato CSR, è possibile utilizzare questo metodo.

Passaggio 1. Creare un trust point client.

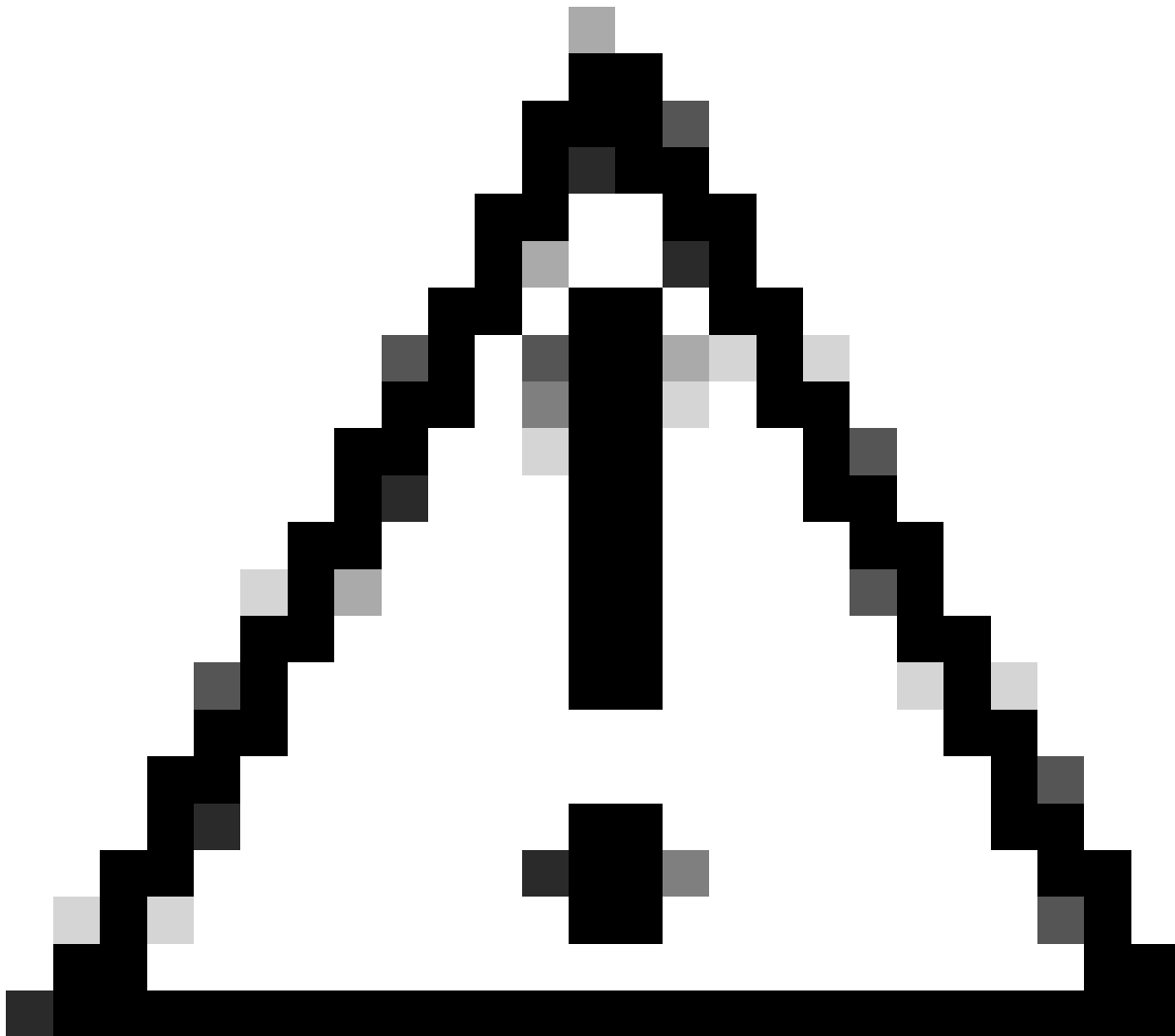
```
cat9k(config)#crypto pki trustpoint svcs_cat9k_25jun17
cat9k(ca-trustpoint)#revocation-check none
```

Passaggio 2. Copiare il file PKCS#12 in bootflash.



Nota: Verificare che il file PKCS#12 contenga la catena di certificati completa e la chiave privata come file crittografato.

---



Attenzione: Le chiavi nel PKCS#12 importato devono essere di RSA (ad esempio: RSA 2048), non 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)
```

Passaggio 3. Importare il file PKCS#12 utilizzando il 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 e AAA con configurazione TLS

Passaggio 1. Creare i gruppi di server e AAA TACACS, associare il trustpoint del client (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
```

Passaggio 2. Configurare i metodi 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
```

## Verifica

Verifica della configurazione.

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

## Debug per AAA e 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
```

### Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).