

Configurare TACACS+ over TLS 1.3 su un dispositivo IOS XR con ISE

Sommario

[Introduzione](#)

[Panoramica](#)

[Utilizzo della Guida](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Licenze](#)

[Parte 1 - Configurazione 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 XR_RW - Profilo dell'amministratore](#)

[IOS XR_RO - Profilo operatore](#)

[Set di comandi ConfigureTACACS+](#)

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

[CISCO IOS XR RO - Set comandi operatore](#)

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

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

[Configurazioni iniziali](#)

[Configura Trustpoint](#)

[Configurazione di TACACS e AAA con TLS](#)

[Rinnovo certificato](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

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

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

Prerequisiti

Requisiti

Requisiti per configurare TACACS+ over TLS:

- Un'Autorità di certificazione (CA) per firmare il certificato utilizzato da TACACS+ over TLS per firmare i certificati ISE e i 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
- Cisco 8201 Router, versione 25.3.1

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 - Configurazione 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).

Passaggio 2. Passare ad Amministrazione > Sistema > Certificati.



Summary

Endpoints

Guests

Vulner



Administration

System

Identity Management

Deployment

Identities

Licensing

Groups

Certificates

External Identity So

Logging

Identity Source Seq

Maintenance

Settings

Upgrade & Rollback

Health Checks

Feed Service

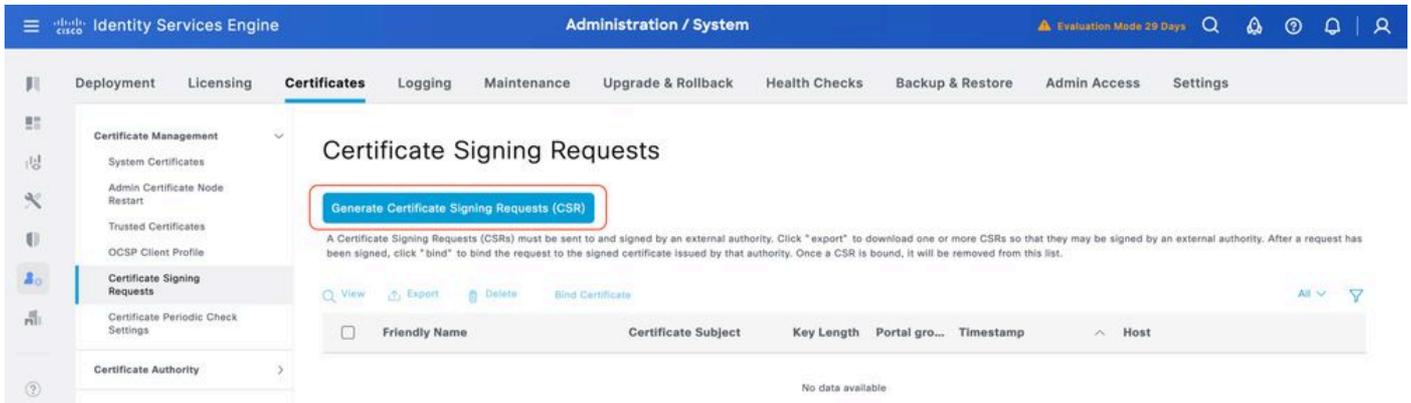
Backup & Restore

Profiler

Admin Access

Settings

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



Passaggio 4. Select TACACS in Usage.

Usage

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

Allow Wildcard Certificates ?

Passaggio 5. Selezionare i PSN per i quali è 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

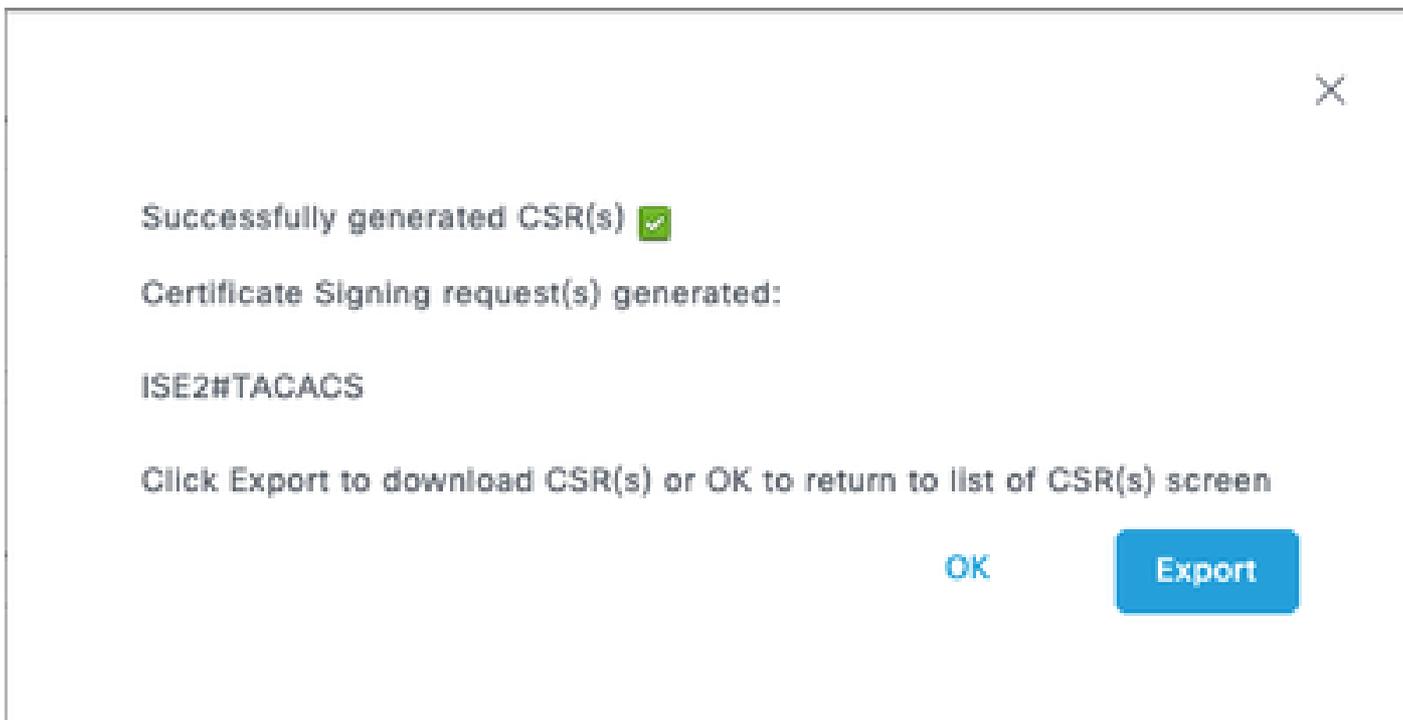
Country (C)
US

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	-	+	

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.

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

Trusted Certificates

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

Edit Import Export Delete View show internal CA certificates

<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 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 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 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 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 il Fiducia 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

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

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System interface. The main navigation bar includes "Administration / System" and "Evaluation Mode 27 Days". The left sidebar shows "Administration" selected. The main content area is titled "Trusted Certificates" and displays a table of certificates. The table has columns for Friendly Name, Trusted For, Serial Number, Issued To, Issued By, Valid From, and Expiration Date. One certificate is listed with a Friendly Name of "CN=SVS LabCA, OU=SVS, O=Cisco, L=..." and an Issued To of "SVS LabCA".

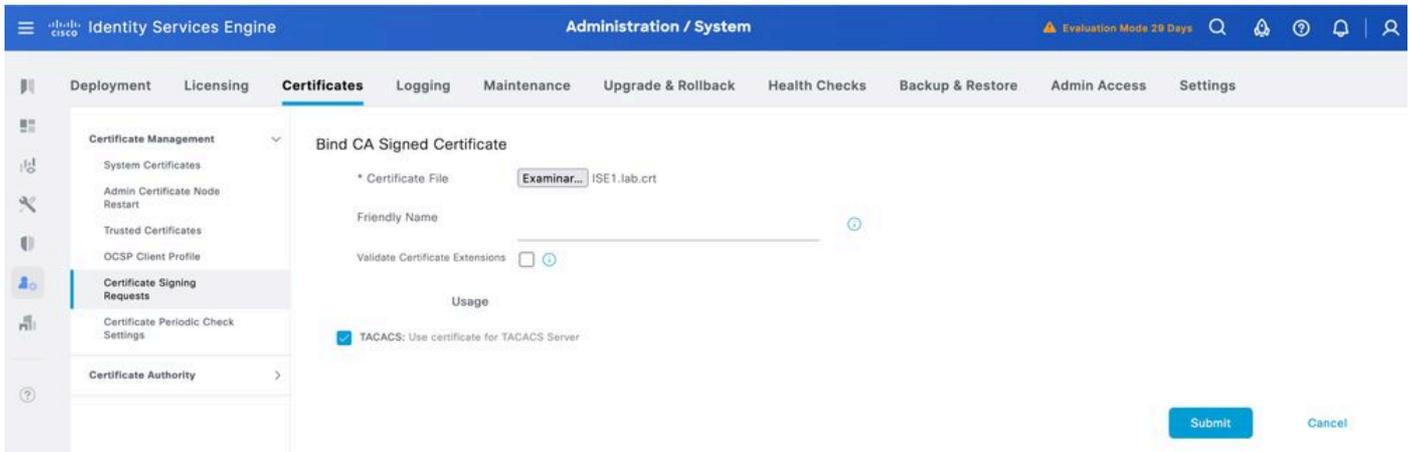
Associare la richiesta di firma del certificato (CSR) firmata a ISE

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

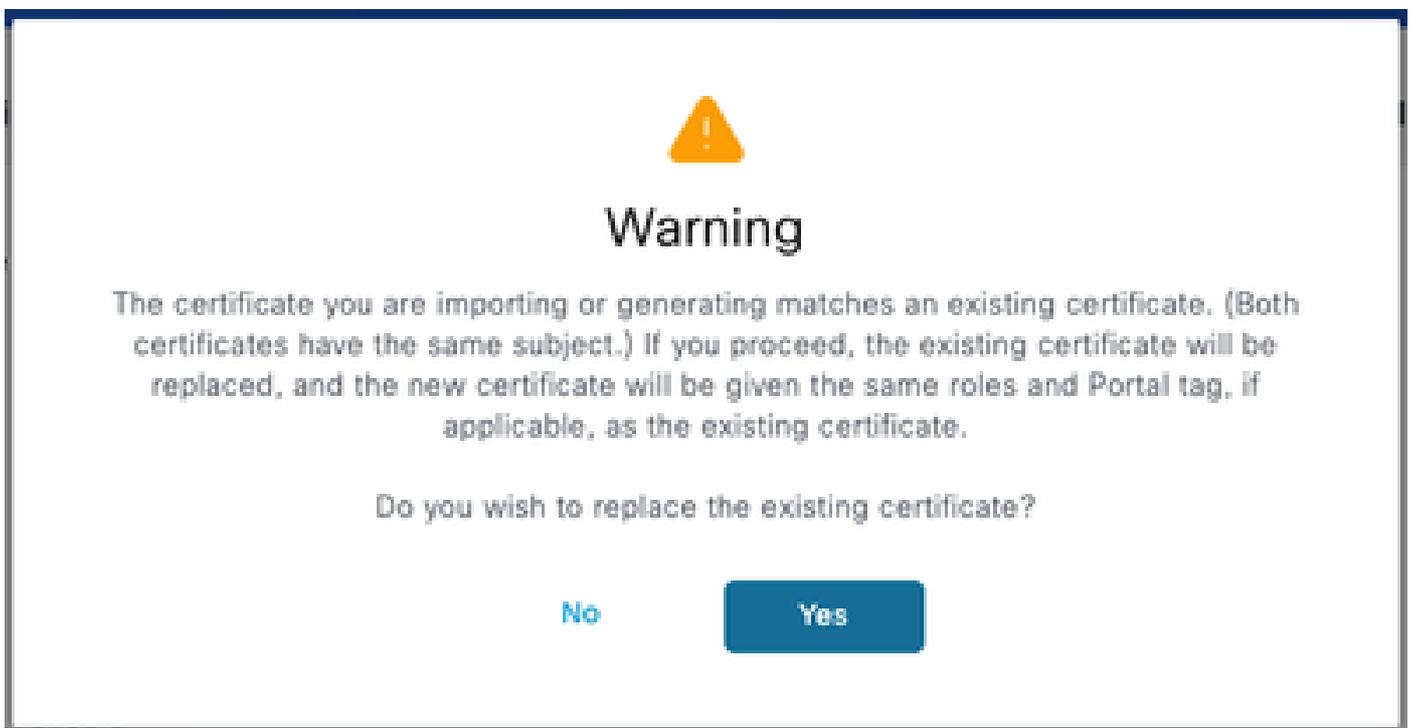
Passaggio 1. Passare a Amministrazione > Sistema > Certificati. In Richieste di firma del certificato, selezionare il CSR TACACS generato nel passaggio precedente e fare clic su Associa certificato.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System interface. The main navigation bar includes "Administration / System" and "Evaluation Mode 29 Days". The left sidebar shows "Administration" selected. The main content area is titled "Certificate Signing Requests" and displays a "Generate Certificate Signing Requests (CSR)" button. Below the button, there is a text box explaining that CSR requests must be sent to and signed by an external authority. The "Bind Certificate" button is highlighted with a red box. The table below has columns for Friendly Name, Certificate Subject, Key Length, Portal gro..., Timestamp, and Host.

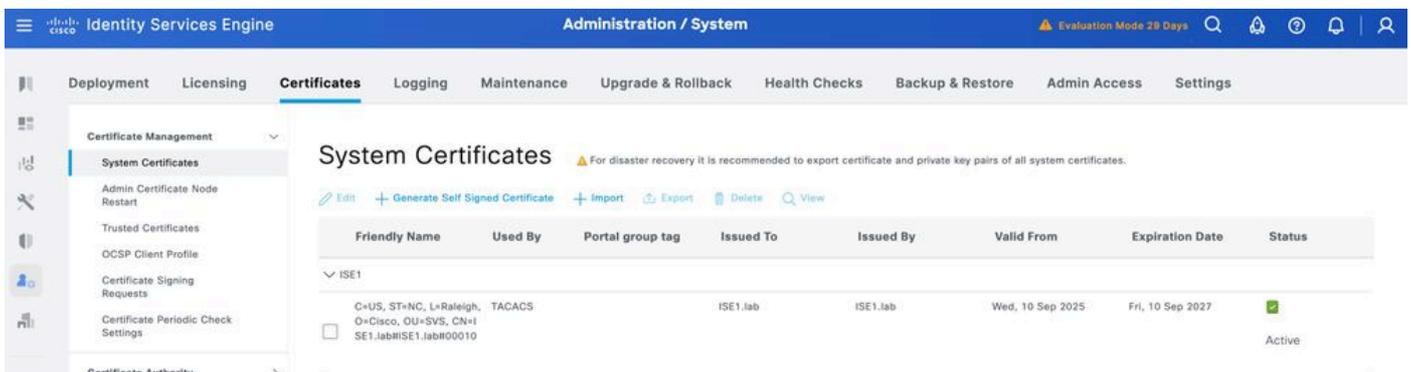
Passaggio 2. Selezionare il certificato firmato e assicurarsi che la casella di controllo TACACS in Uso rimanga selezionata.



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



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



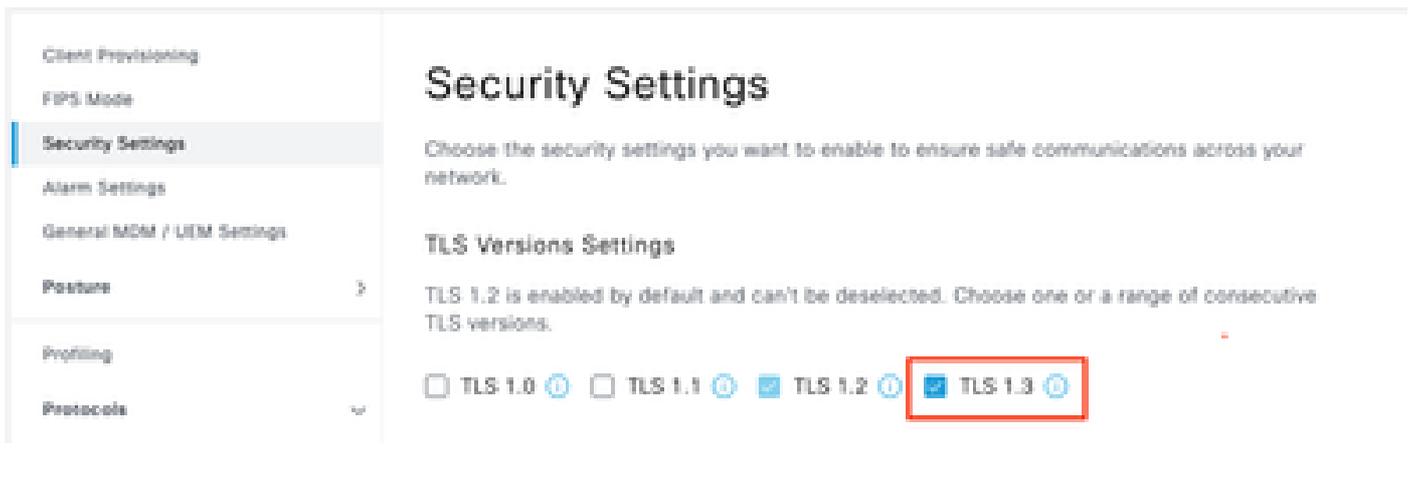
Abilita TLS 1.3

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

Passaggio 1. Passare ad Amministrazione > Sistema > Impostazioni.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar is blue and contains the Cisco logo and the text "Identity Services Engine". Below this, a sidebar on the left lists various navigation options: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (highlighted in blue), Work Centers, and Interactive Help. The main content area is divided into two sections: "Deployment" and "Licensing". Under "Deployment", there is a sub-menu with the following items: Client Provisioning (highlighted with a blue bar), FIPS Mode, Security Settings, and Alarm Settings. Under "Licensing", there is a sub-menu with the following items: System, Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade & Rollback, Health Checks, Backup & Restore, and Admin Access. At the bottom of this sub-menu, the "Settings" option is highlighted in blue and includes a checkmark icon.

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.



The screenshot shows the 'Security Settings' configuration page in Cisco ISE. On the left is a navigation menu with options: Client Provisioning, FIPS Mode, Security Settings (highlighted), Alarm Settings, General MDM / UEM Settings, Posture, Profiling, and Protocols. The main content area is titled 'Security Settings' and includes a sub-section 'TLS Versions Settings'. Below this, there is a note: 'TLS 1.2 is enabled by default and can't be deselected. Choose one or a range of consecutive TLS versions.' At the bottom, there are four checkboxes for TLS versions: TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. The 'TLS 1.3' checkbox is checked and highlighted with a red rectangular box.

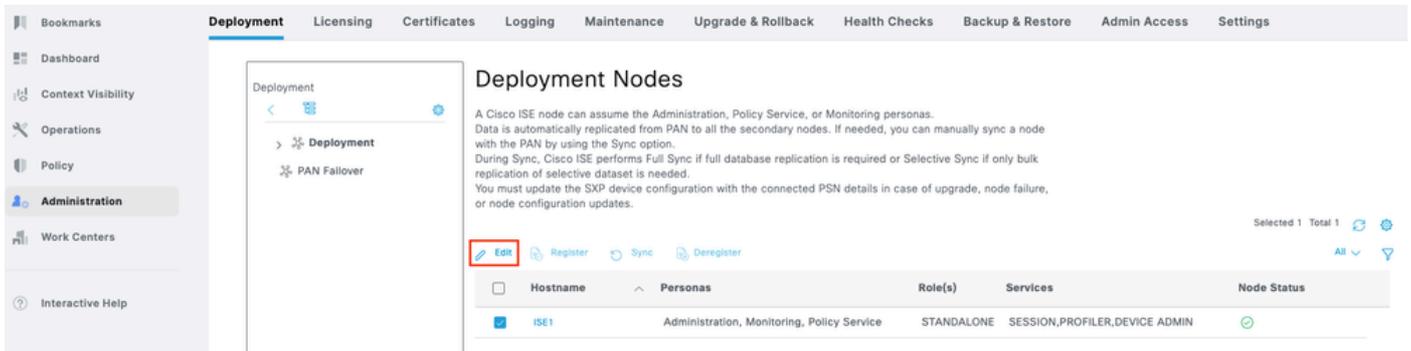


Avviso: Quando si modifica la versione TLS, il server applicazioni Cisco ISE viene riavviato su tutti i computer di implementazione di Cisco ISE.

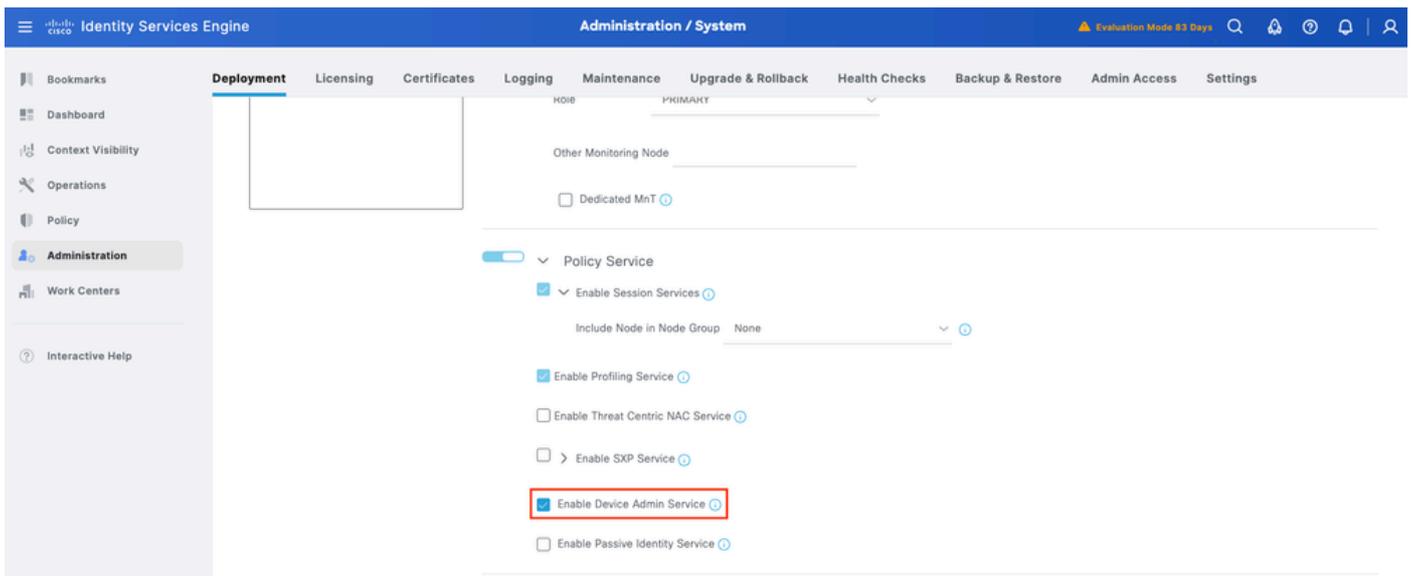
Abilita amministrazione dispositivi su ISE

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



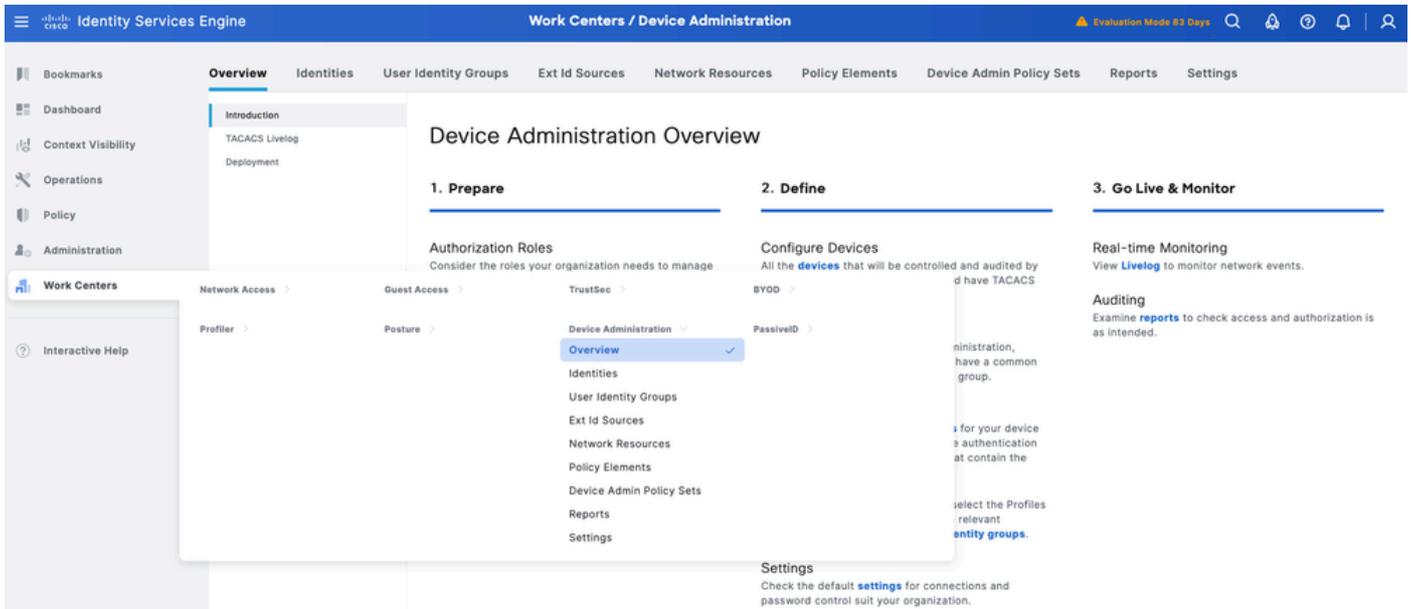
Passaggio 2. In GeneralSettings, scorrere verso il basso e selezionare la casella di controllo accanto a Enable Device Admin Service.



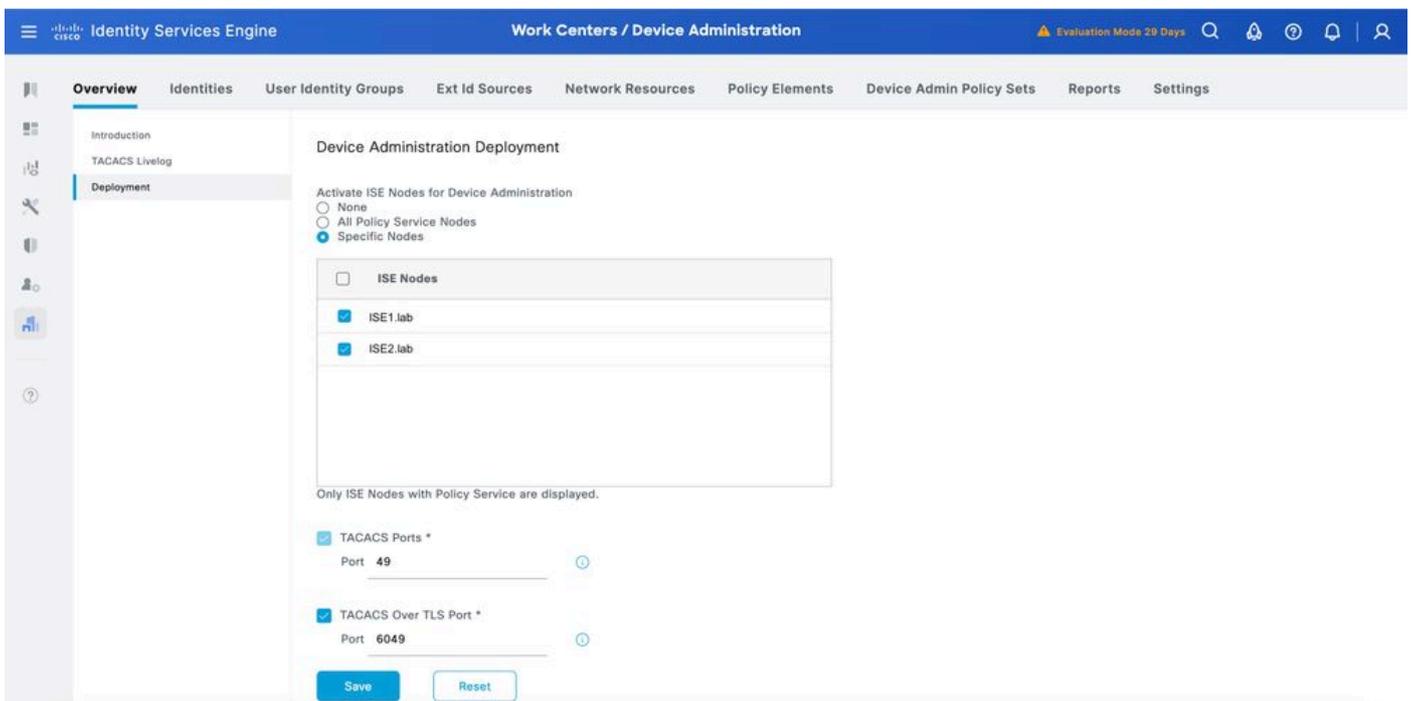
Passaggio 3. Salvare la configurazione. Device Admin Service è ora abilitato su ISE.

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 XR.

Identity Services Engine Work Centers / Device Administration

Overview Identities User

Network Devices

Network Device Groups

Default Devices

TACACS External Servers

TACACS Server Sequence

Edit Group

Name*
IOS-XR

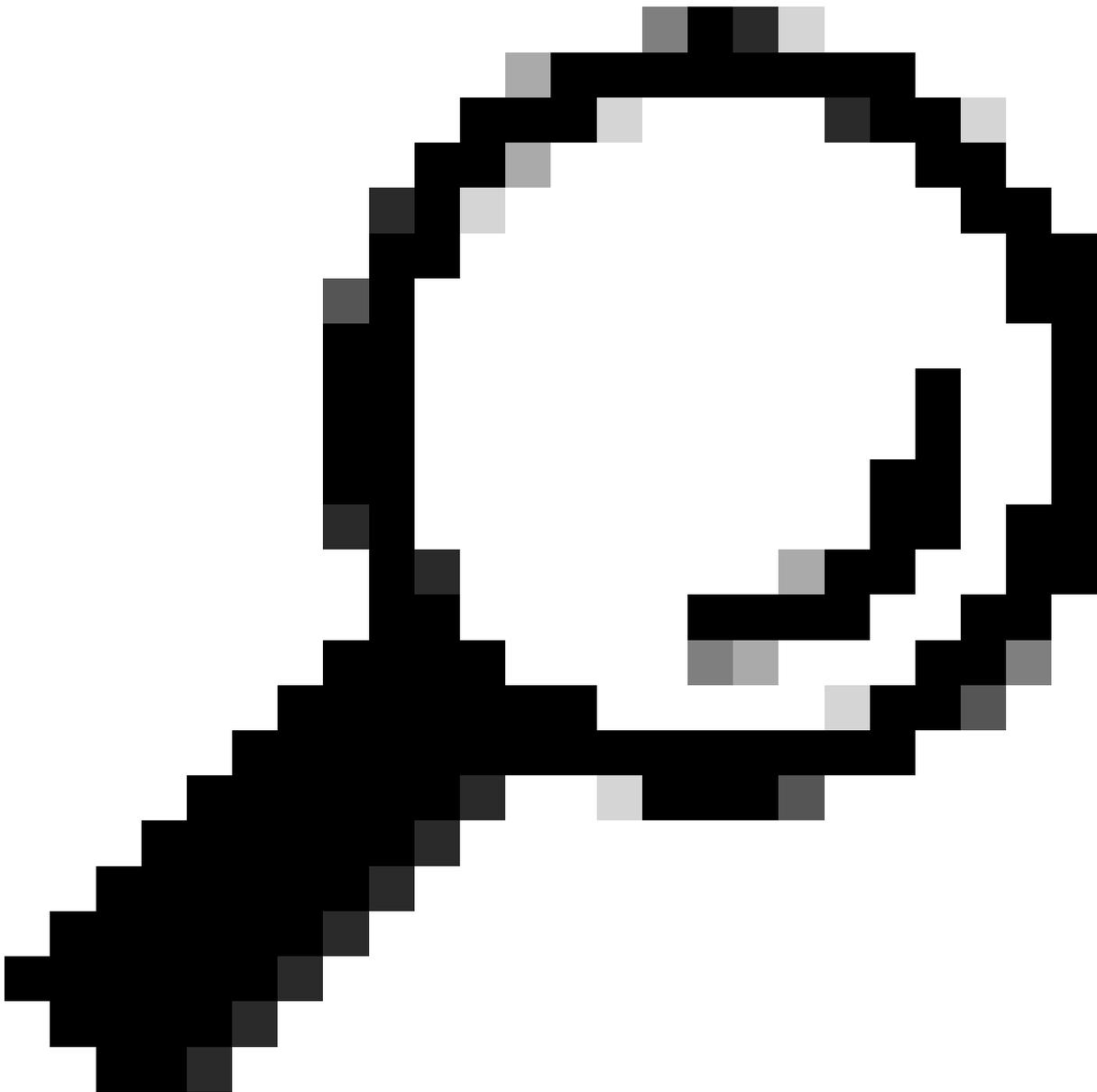
Description

Group Hierarchy
Device Type > All Device Types > IOS-XR

Cancel Save

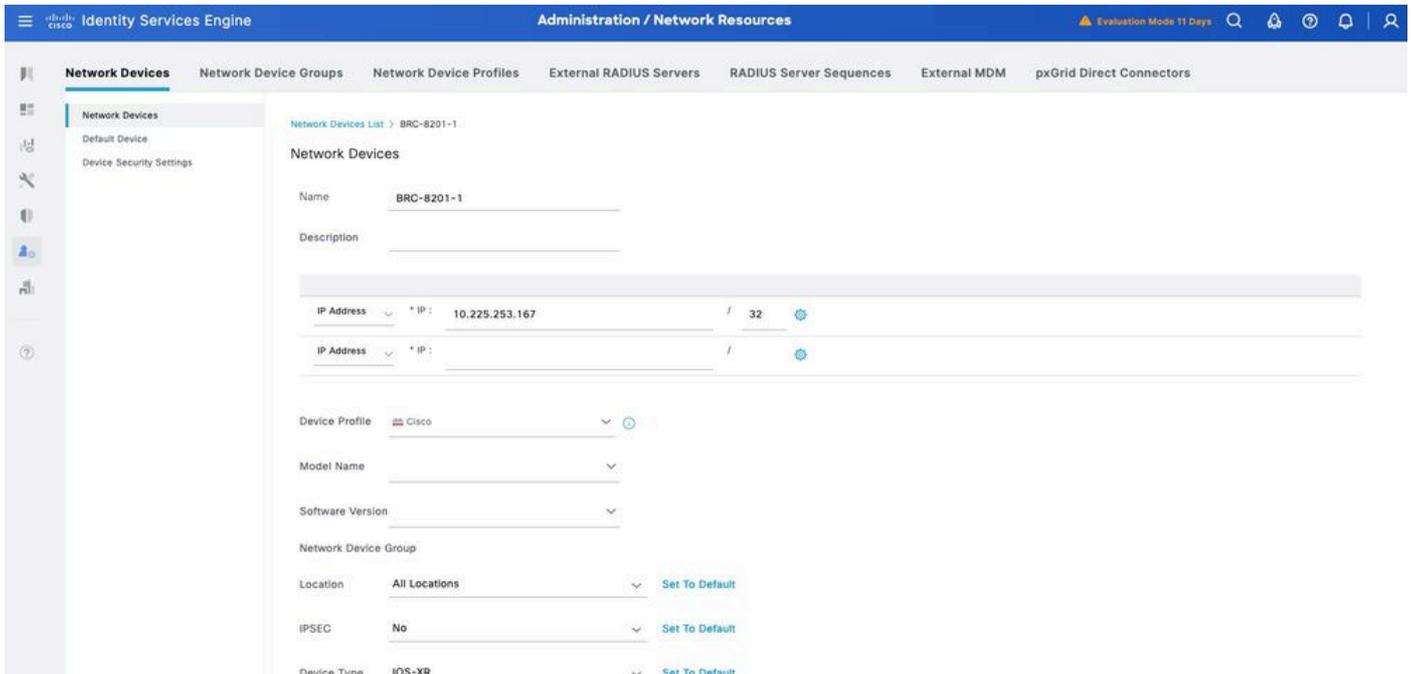
	No. of Network Devices
--	702
	0
	11
ADVA	243

ADVA SyncDirector Network Time Monitoring

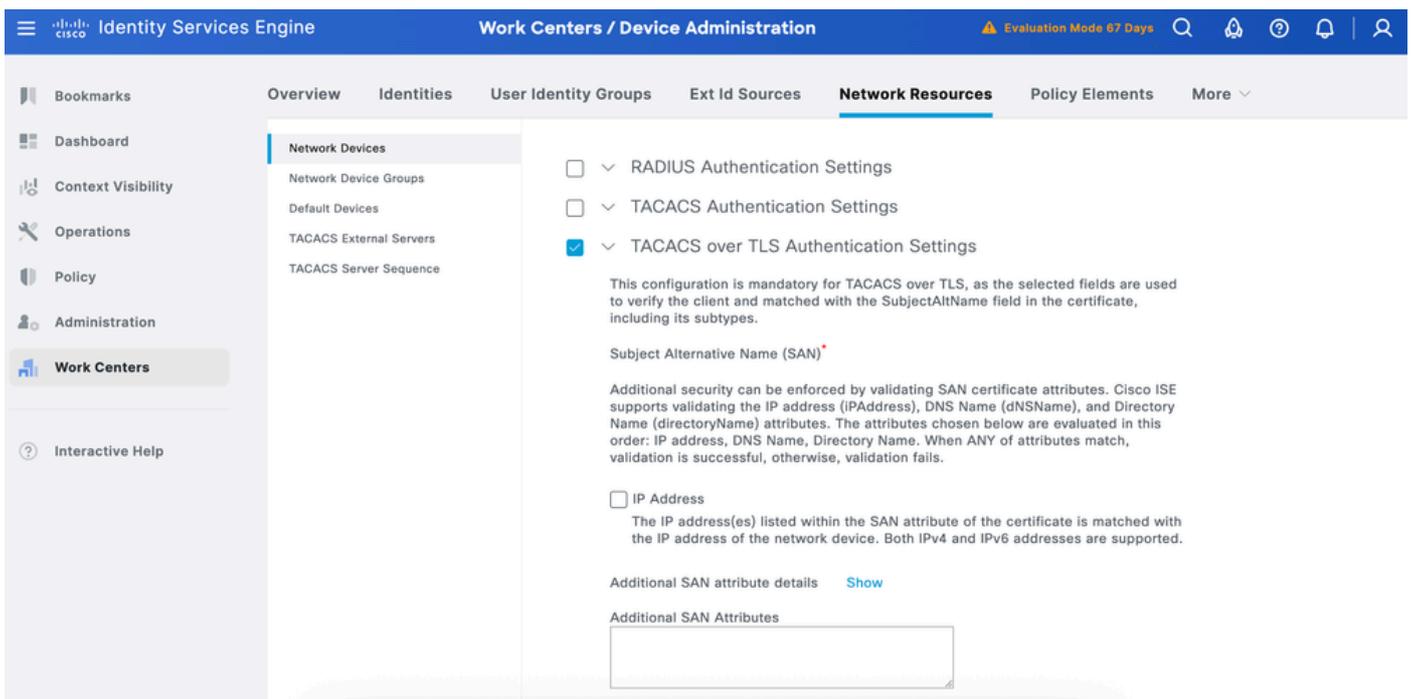


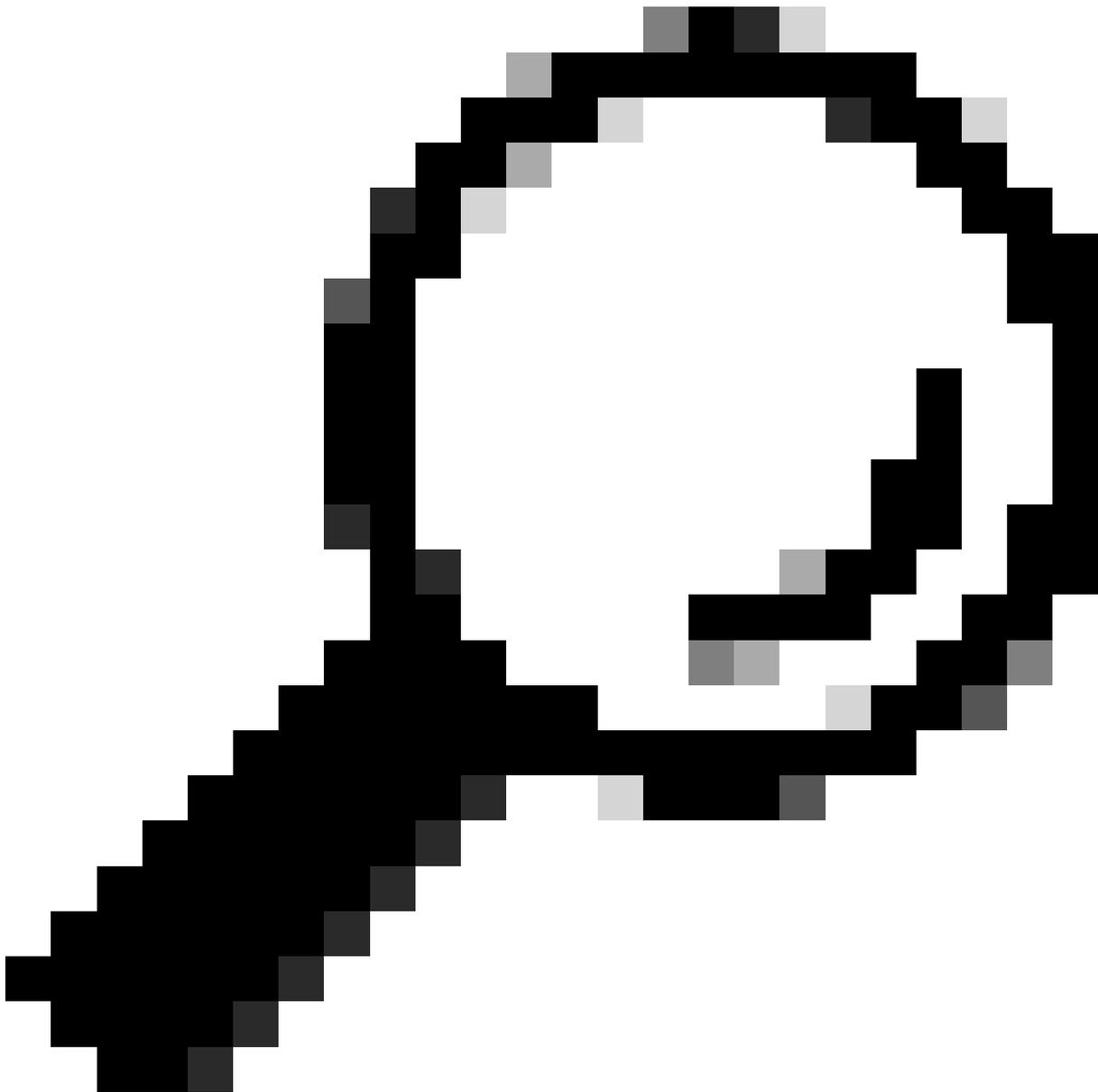
Suggerimento: Tutti i tipi di dispositivo e Tutti i percorsi sono gerarchie predefinite fornite da ISE. È possibile aggiungere gerarchie personalizzate e definire i vari componenti per l'identificazione di un dispositivo di rete che potrà essere utilizzato successivamente nella condizione del criterio

Passaggio 2. Aggiungere ora un dispositivo Cisco IOS XR 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.



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



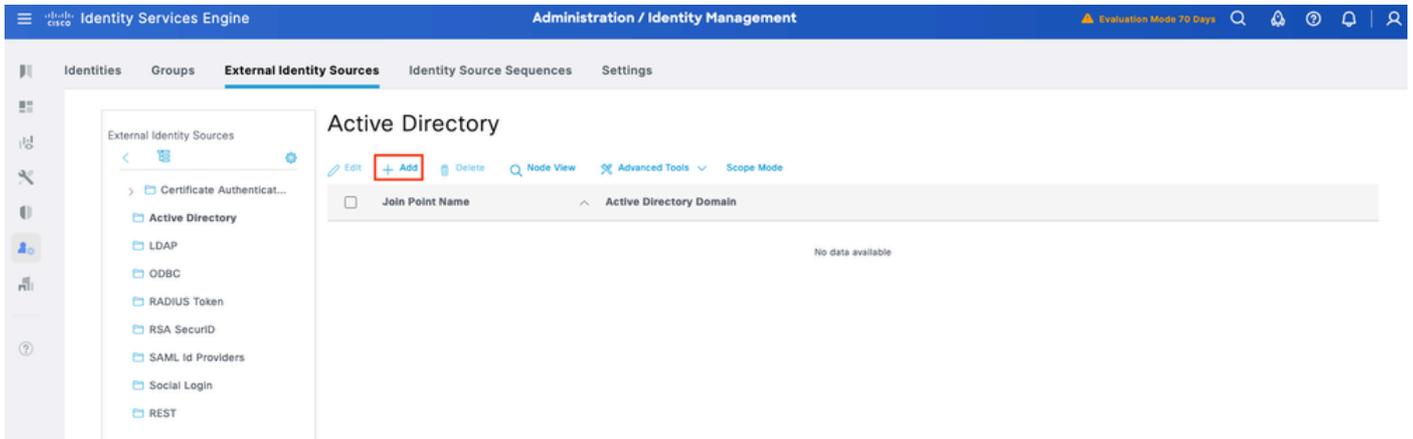


Suggerimento: Per evitare di riavviare la sessione TCP ogni volta che si invia un comando al dispositivo, si consiglia di abilitare la modalità di connessione singola.

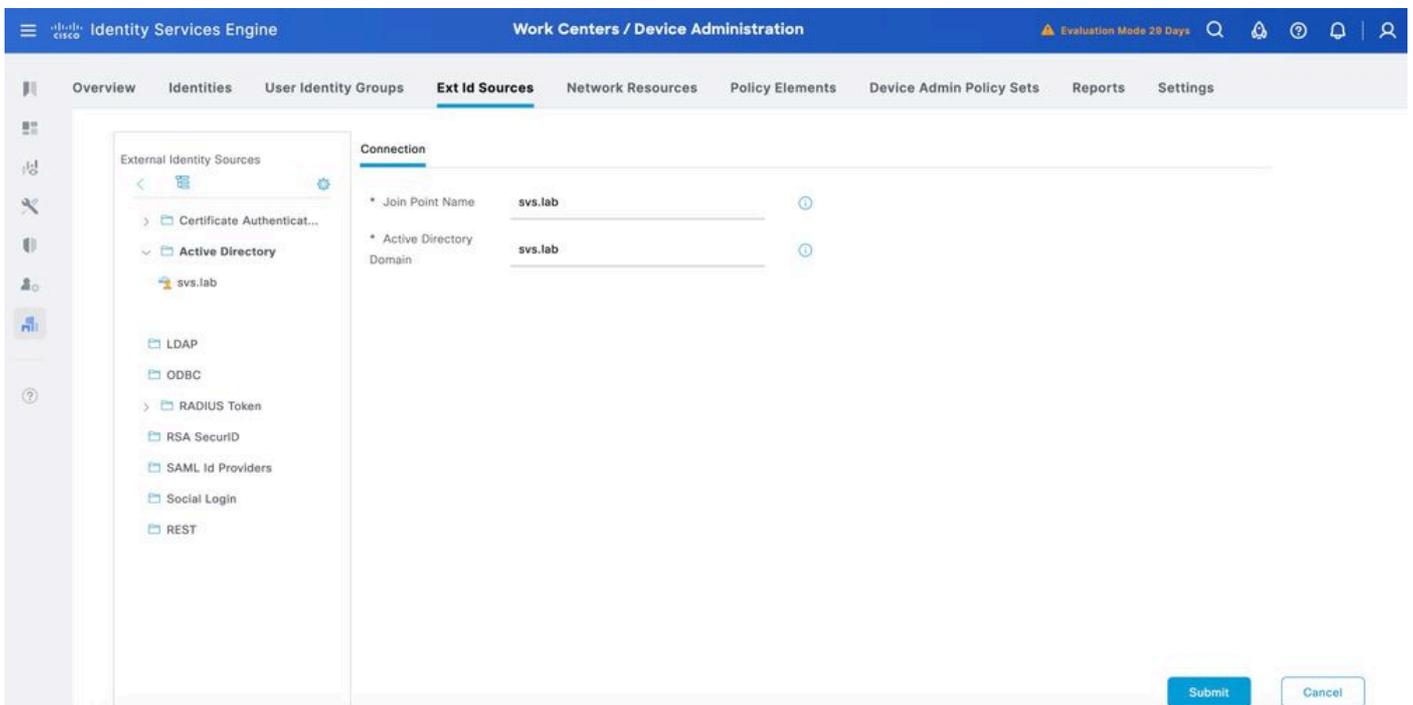
Configura archivi identità

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.

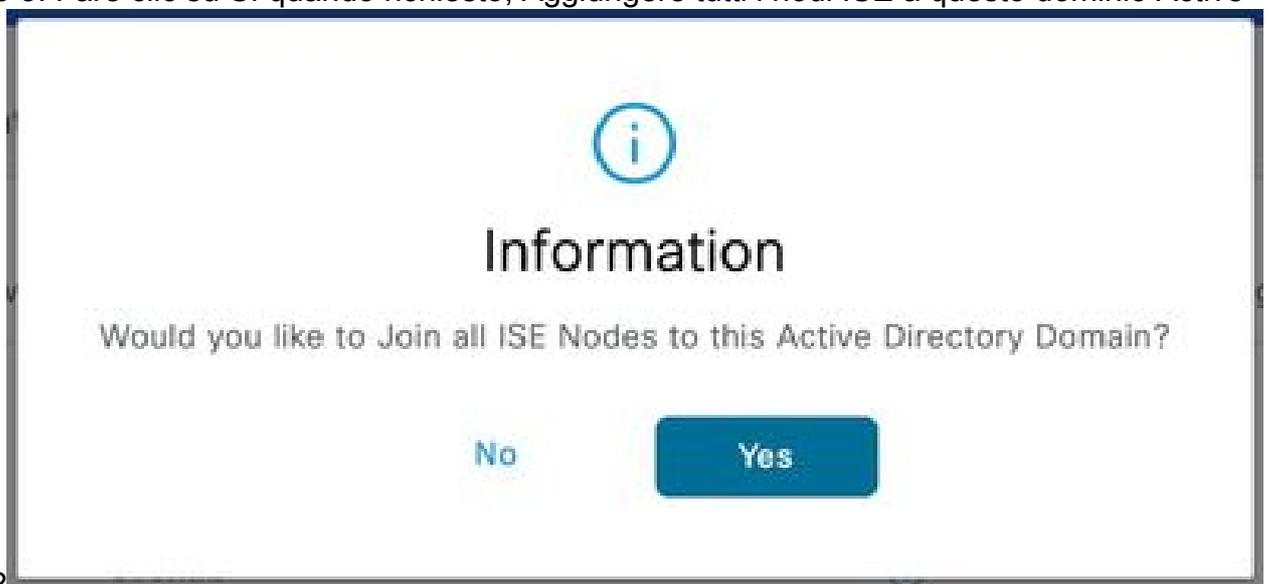
Passaggio 1. Passare ad Amministrazione > Gestione delle identità > Archivi identità esterni > Active Directory. Fare clic su Aggiungi per definire un nuovo punto di giunzione AD.



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

✕

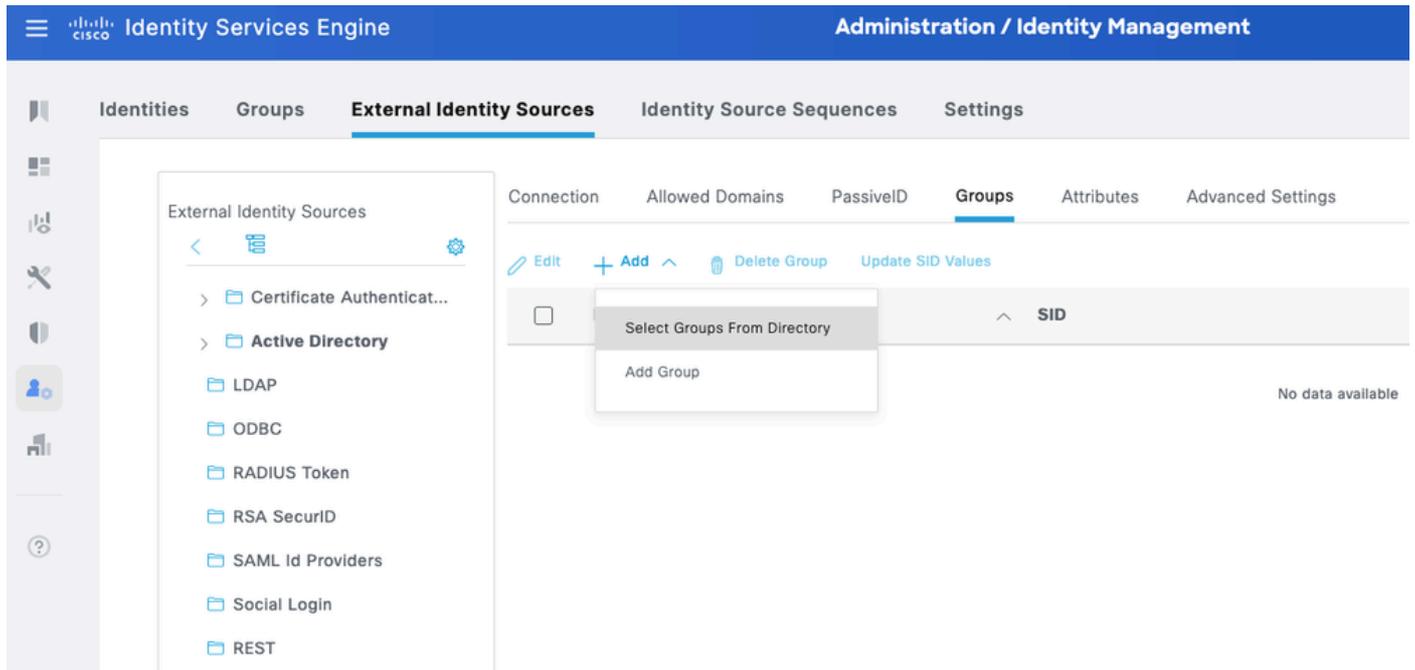
Join Operation Status

Status Summary: Successful

ISE Node	Node Status
ISE1.lab	✔ Completed.

Close

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.



Select Directory Groups

This dialog is used to select groups from the Directory.

Domain svcs.lab

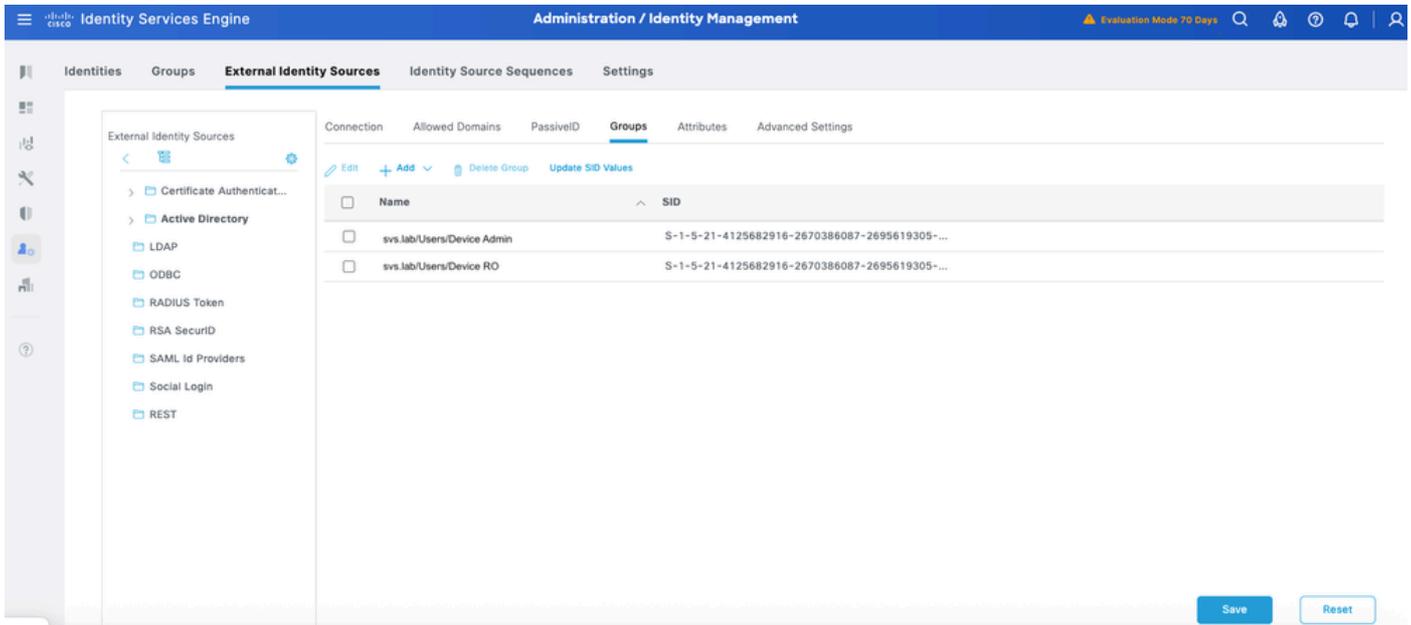
Name Device *
Filter

SID *
Filter

Type ALL
Filter

Retrieve Groups... 2 Groups Retrieved.

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



Configurazione dei profili TACACS+

Mappare i profili TACACS+ ai ruoli utente sui dispositivi Cisco IOS XR. Nell'esempio sono definite le seguenti opzioni:

- 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.

Definire due profili TACACS+: IOSXR_RW e IOSXR_RO.

IOS XR_RW - Profilo dell'amministratore

Passaggio 1. Passare a Centri di lavoro > Amministrazione dispositivi > Elementi della policy > Risultati > Profili TACACS. Aggiungere un nuovo profilo TACACS e denominarlo IOSXR_RW.

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

Passaggio 3. Confermare la configurazione e salvare.

Identity Services Engine Work Centers / Device Administration Evaluation Mode 63 Days

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

Conditions > TACACS Profiles > IOSXR_RW
TACACS Profile

Name: IOSXR_RW

Description: [Empty text area]

Task Attribute View Raw View

Common Tasks

Common Task Type: Shell

- Default Privilege: 15 (Select 0 to 15)
- Maximum Privilege: 15 (Select 0 to 15)
- Access Control List
- Auto Command
- No Escape (Select true or false)

IOS XR_RO - Profilo operatore

Passaggio 1. Passare a Work Center > Device Administration > Policy Elements > Results > TACACS Profiles. Aggiungere un nuovo profilo TACACS e denominarlo IOSXR_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 Evaluation Mode 62 Days

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

Conditions > TACACS Profiles > New
TACACS Profile

Name: IOSXR_RO

Description: [Empty text area]

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
- No Escape

Set di comandi ConfigureTACACS+

Definire i set di comandi TACACS+: Nell'esempio, questi sono definiti CISCO_IOSXR_RW e

CISCO_IOSXR_RO.

CISCO IOS XR 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_IOSXR_RW.

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

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring a TACACS Command Set. The breadcrumb trail is 'TACACS Command Sets > CISCO_IOSXR_RW'. The main configuration area includes the following elements:

- Name:** CISCO_IOSXR_RW
- Description:** (Empty text area)
- Commands:** A checkbox labeled 'Permit any command that is not listed below' is checked.
- Table:** A table with columns 'Grant', 'Command', and 'Arguments'. The 'Grant' column has a checkbox that is currently unchecked.
- Buttons:** 'Add', 'Trash', 'Edit', 'Move Up', 'Move Down', 'Cancel', and 'Save'.

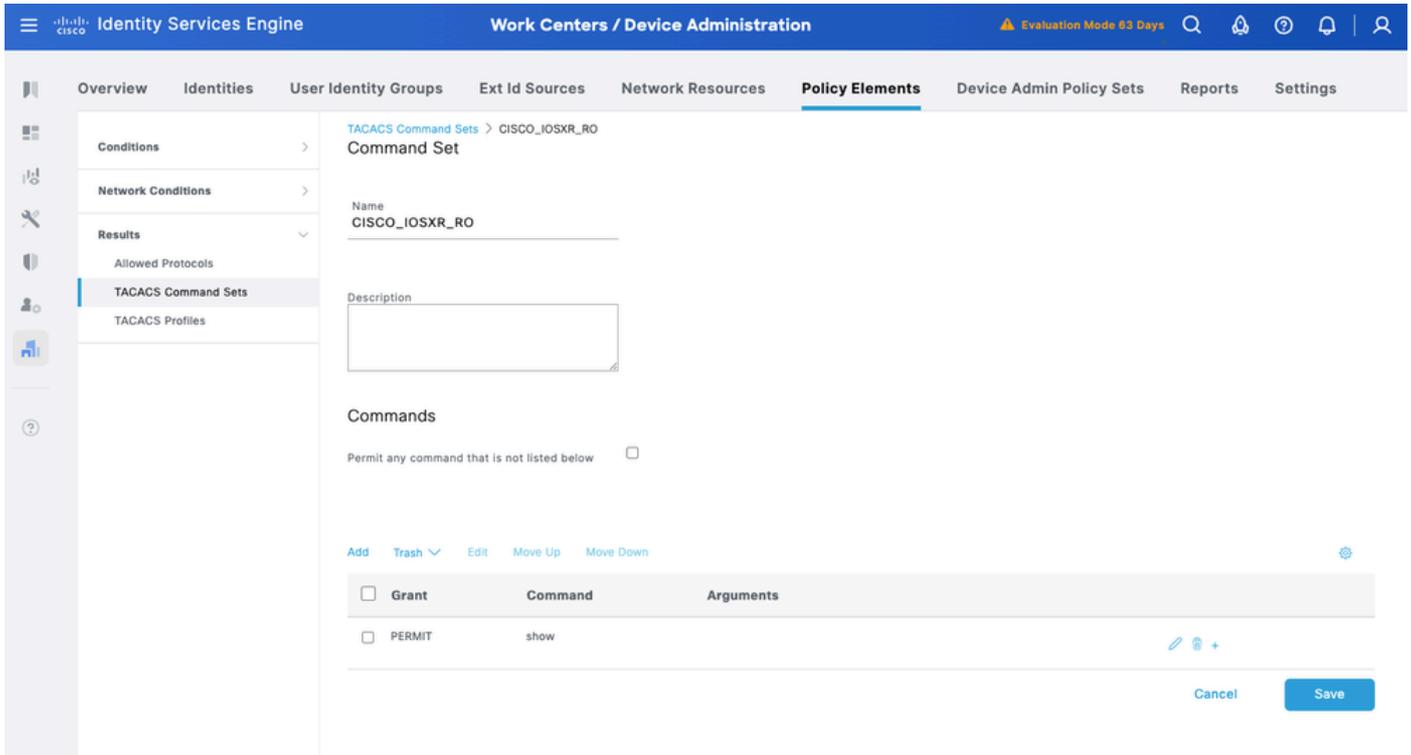
CISCO IOS XR RO - Set comandi operatore

Passaggio 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_IOSXR_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.

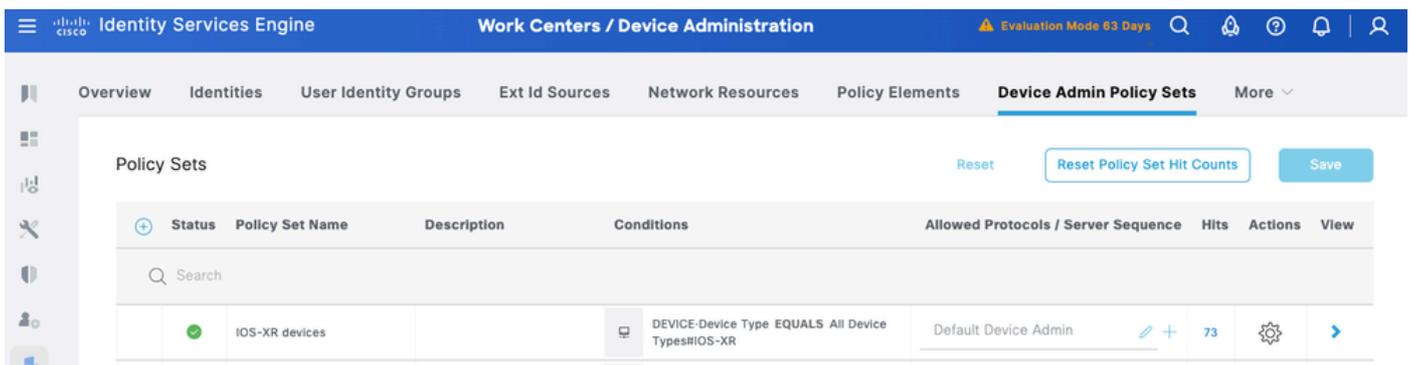
Passaggio 4. Confermare i dati e fare clic su Salva.



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 XR. In questa condizione specificare DEVICE:Device Type EQUALS All Device Types#IOS XR. In Protocolli consentiti, selezionare Amministratore di dispositivo predefinito.



Passaggio 2. Fare clic su Salva e quindi sulla freccia destra per configurare il 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 non trovato (If User not found) e Se processo (If Process fail).

Identity Services Engine Work Centers / Device Administration Evaluation Mode 63 Days

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

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

Authentication Policy(1)

Status	Rule Name	Conditions	Use	Hits	Actions
✔	Default		svs.lab ✎ v	85	⚙

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 della shell IOSXR_RO.
- Agli utenti del gruppo AD Device Admin vengono assegnati il set di comandi CISCO_IOSXR_RW e il profilo della shell IOSXR_RW.

Identity Services Engine Work Centers / Device Administration Evaluation Mode 62 Days

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

Policy Sets → IOS-XR devices Reset Reset Policy Set Hit Counts Save

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

> Authentication Policy(1)

> Authorization Policy - Local Exceptions

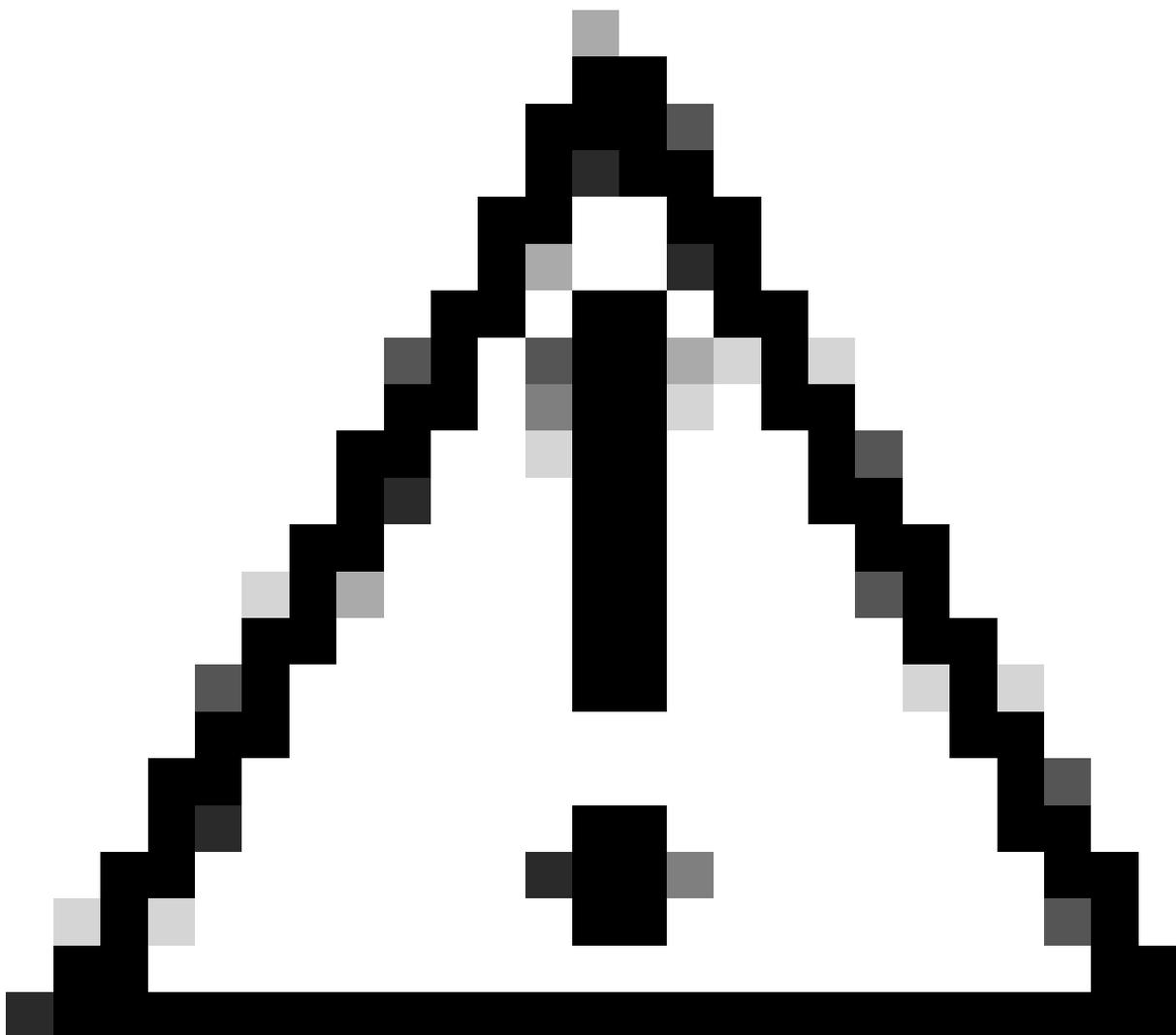
> Authorization Policy - Global Exceptions

∨ Authorization Policy(3)

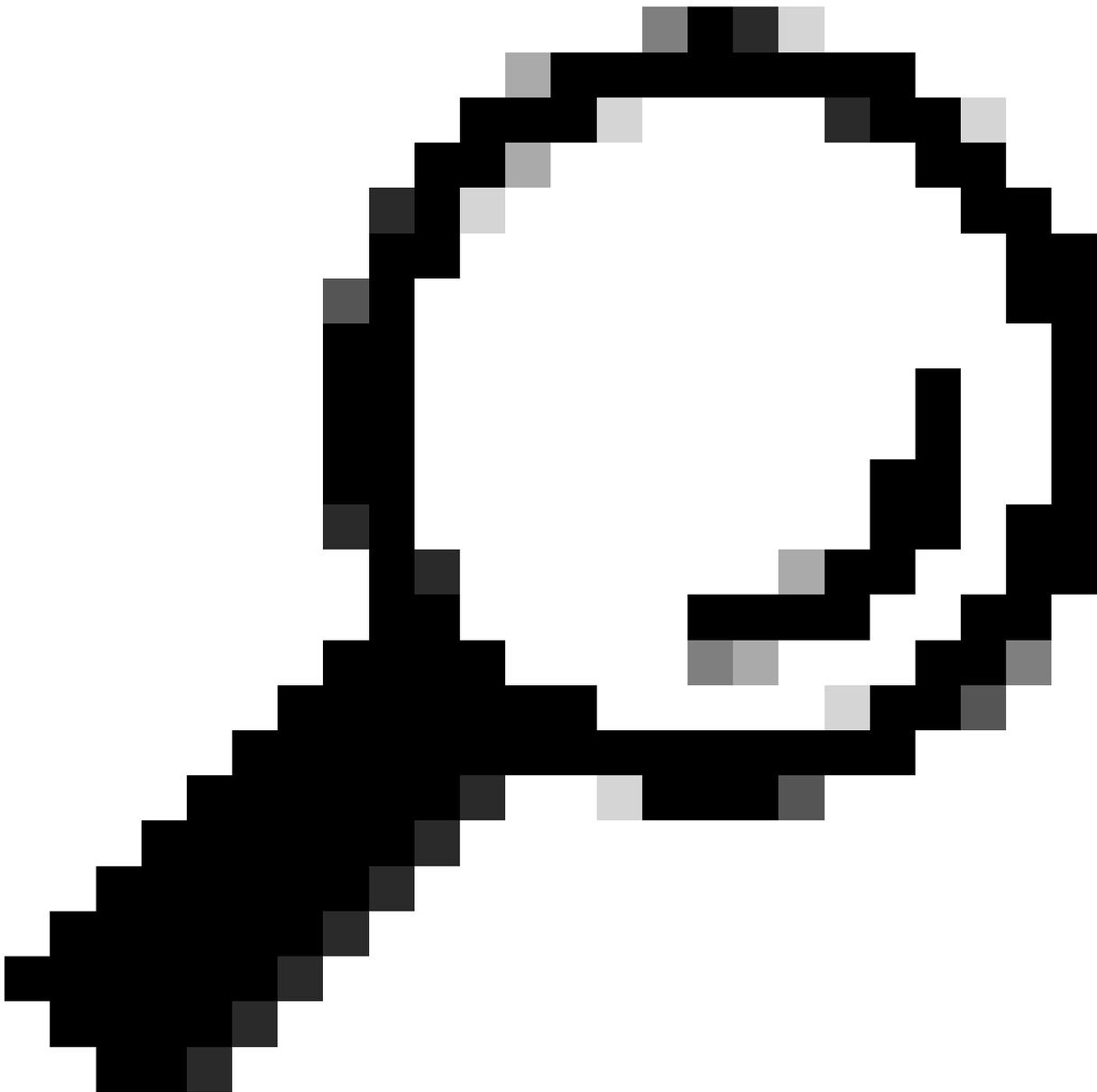
Status	Rule Name	Conditions	Results			Hits	Actions
			Command Sets	Shell Profiles			
✓	Authorization Rule RO	svs.lab-ExternalGroups EQUALS svs.lab /Users/Device RO	CISCO_IOSXR_RO	IOSXR_RO	0	⚙️	
✓	Authorization Rule RW	svs.lab-ExternalGroups EQUALS svs.lab /Users/Device Admin	CISCO_IOSXR_RW	IOSXR_RW	77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

Parte 2 - Configurazione di Cisco IOS XR 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.

Configurazioni iniziali

Passaggio 1. Verificare che il server dei nomi (DNS) sia configurato e che il router sia in grado di risolvere i nomi di dominio qualificati (FQDN) frequenti, in particolare il nome di dominio completo (FQDN) del server ISE.

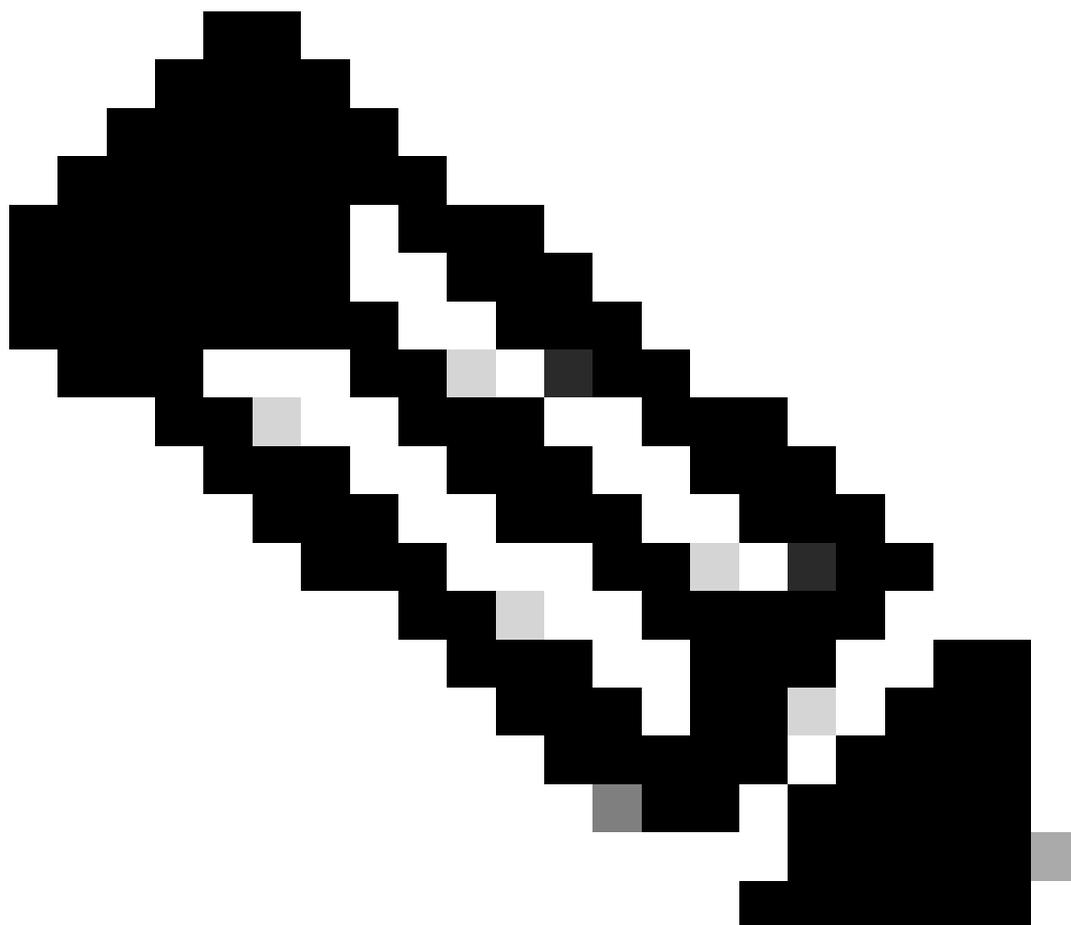
```
domain vrf mgmt name svcs.lab
domain vrf mgmt name-server 10.225.253.247
no domain vrf mgmt lookup disable
```

```
RP/0/RP0/CPU0:BRC-8201-1#ping vrf mgmt ise1.svs.lab
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.225.253.209 timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Passaggio 2. Cancellare tutti i trust point e i certificati vecchi/inutilizzati. Verificare che non siano presenti trust e certificati vecchi. Se vengono visualizzate voci obsolete, rimuoverle o cancellarle.

```
show crypto ca trustpoint
show crypto ca certificates
```

```
(config)# no crypto ca trustpoint <tp-name>
# clear crypto ca certificates <tp-name>
```



Nota: È possibile creare manualmente una nuova coppia di chiavi RSA e collegarla in trustpoint. Se non ne create una, viene utilizzata la coppia di chiavi predefinita. La definizione della coppia di chiavi ECC in trustpoint non è attualmente supportata.

Configura Trustpoint

Passaggio 1. Configurazione della coppia di chiavi (facoltativo).

```
<#root>
```

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

```
crypto key generate rsa
```

```
4096
```

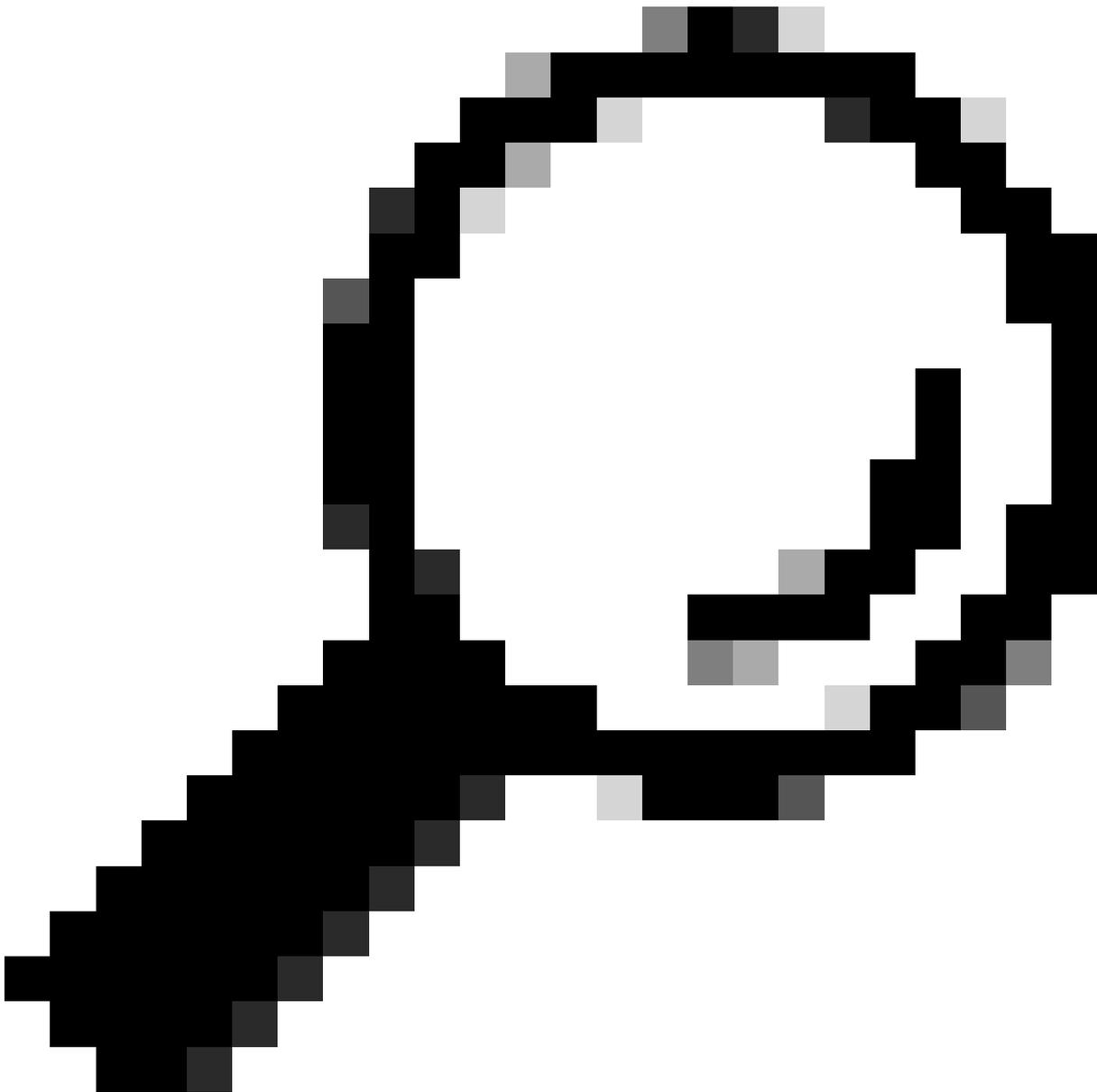
```
RP/0/RP0/CPU0:BRC-8201-1(config)#
```

```
crypto ca trustpoint
```

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

```
rsakeypair
```

Passaggio 2. Creare un trust point.



Suggerimento: La configurazione DNS per il nome alternativo del soggetto è facoltativa (se abilitata su ISE), ma consigliata.

```
<#root>
```

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

```
crypto ca trustpoint svr
```

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

```
vrf mgmt
```

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

```
crl optional
```

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

subject-name C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=brc-8201-1.svs.lab

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

subject-alternative-name IP:10.225.253.167,DNS:brc-8201-1.svs.lab

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

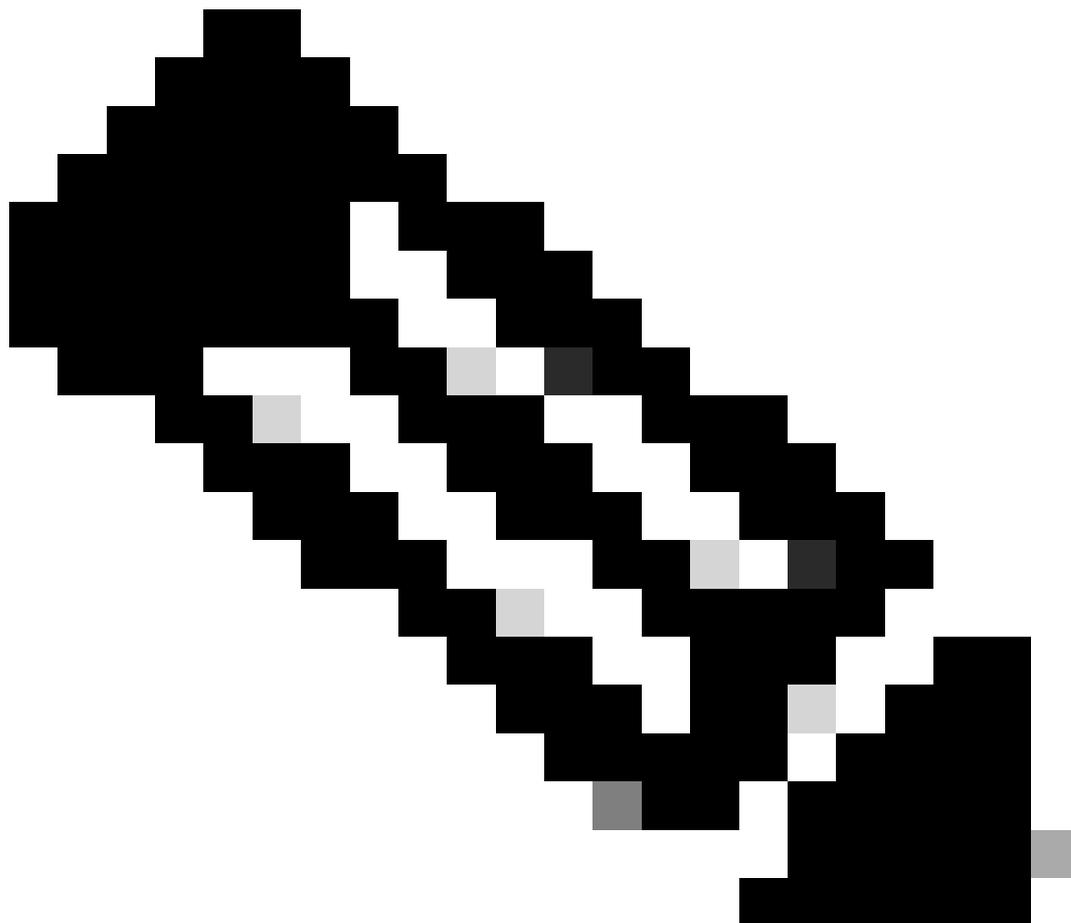
enrollment url terminal

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

rsakeypair svs-4096

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

commit



Nota: Se è necessario utilizzare la virgola in O o in OU, è possibile utilizzare una barra rovesciata (\) prima della virgola. Ad esempio: O=Cisco Systems\, Inc.

Passaggio 3. Autenticare il trust point installando il certificato CA.

```
<#root>
```

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

```
crypto ca authenticate svcs
```

```
Enter the base64/PEM encoded certificate/certificates.  
Please note: for multiple certificates use only PEM.  
End with a blank line or the word "quit" on a line by itself
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIF1DCCA3ygAwIBAgIIIM10AsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE  
BhMCMVVMxZmFzAVBgNVBAGTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo  
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECXMdU1ZTMRIwEAYDVQQDEw1TV1MgTGFi  
Q0EwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV  
UzEXMBUGA1UECBM0MjYyYzEzSH6EkEvxnJTy+kksiFD33GyHQepk7vfp4NFU50tQ4HC7t/A0v9grDa3QW  
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNNTV1MxEjAQBgNVBAMTCVNWUyBYWJDQTC  
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZU0yn2vIn6gKbx3M7vaRq  
2YjwZ1zSH6EkEvxnJTy+kksiFD33GyHQepk7vfp4NFU50tQ4HC7t/A0v9grDa3QW  
VvwV4MBBjHfM3s0J/ejgDYcMZhIAaPy0Zo5WLbo0kXEiKjPLatkXojB8FVrhLF30  
jMBSqwa4/Wlniy5S+7s4FFxsCf20COWfBAsnrs0tatIIhmcnx+VLJP7MRm8f0w4m  
mutNo7IhbJSrgAFXmj1bBjMmgspObULo/wxMHdTbtPBf11HRHTkNIto3qy04UADL2  
WpoGhgT/FaxxBo2UBcnYVaP+jjREONYT973MCbVAAxtNVU6bEBROz+LWniACzupm  
+qh23SL43uW5A3iSw/BuU1E9p7B0e8oDNKU6gX1ojKyLP/gC7j8AeP03ir+KZui8  
b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN  
gJ+kQXe7QtT/u6m1MrtjE3gAEVpl334rTIxy9hpKZIkB86t2ZA3JX8CLsbCa13sA  
z1XC0NX+6a1ekmXuAOI+t3c1sNbn2AtFi4cJovTA01xh60I4QnK+MNQKPtjt/E4  
ydH10rrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVL1783nTc9wYptQEPi5sw  
83g9EMgKV0ARIiVUa/q1AgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAyb4  
QgEBBAQDAgAHMBkGCWCSAGG+EIBDQMFgpTV1MgTGFiIENBMAOGCSqGSIb3DQEB  
CwUAA4ICAQAIT308oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr  
AwXIwFAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oK0dGayi  
iSEkSSX9qyflINHR2JSVqJU6jLsy86X7q7RmIPMS7XfhzuddFNI4YDoXRX67X+v  
0+ja6zTQqj061qJhmrSkyFbYf/ZTpe4d10zJsZjNsN0r8bF9n0A/7qNZLp3Z3cpU  
PU0KdbiSvRqnPw3e8TfITVmAzcx8COI2SrYFMSUazo1VBvDy+xRKxyAtMbneGz6n  
YdykCimThCKoKwp/pWpYBEqIE0f5ay1PKURO/8aj/B7a1uJapXkmnj5qPeGhN0pB  
Q9r14reov4so2EspkXS7CrH9yGfpIyTprokz1UvZBZ8v1oI7YZmjFmem+5rT6Gnk  
eU/1X7nV61SYG5W5K+I8uaKuyBH0Mn7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgrU8  
8ggz1P0dsS/i6Lo7ypYX0eB9HgVDCkzQsLXQuHGj/2WsgPgDRcjkvnyURk4Jx+Ib  
xDrmo7e0XPPSW4172a6K18CR3U2Cr4wsuvndPEq/qd2NRSBWffFOX/AJHQG7STT  
HaXLU9r2Ko603oecu8ysGTwL1It/9T1/F0b0xZRugWcpJrVoTgDGUA==
```

```
-----END CERTIFICATE-----
```

```
quit
```

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

```
Subject:
```

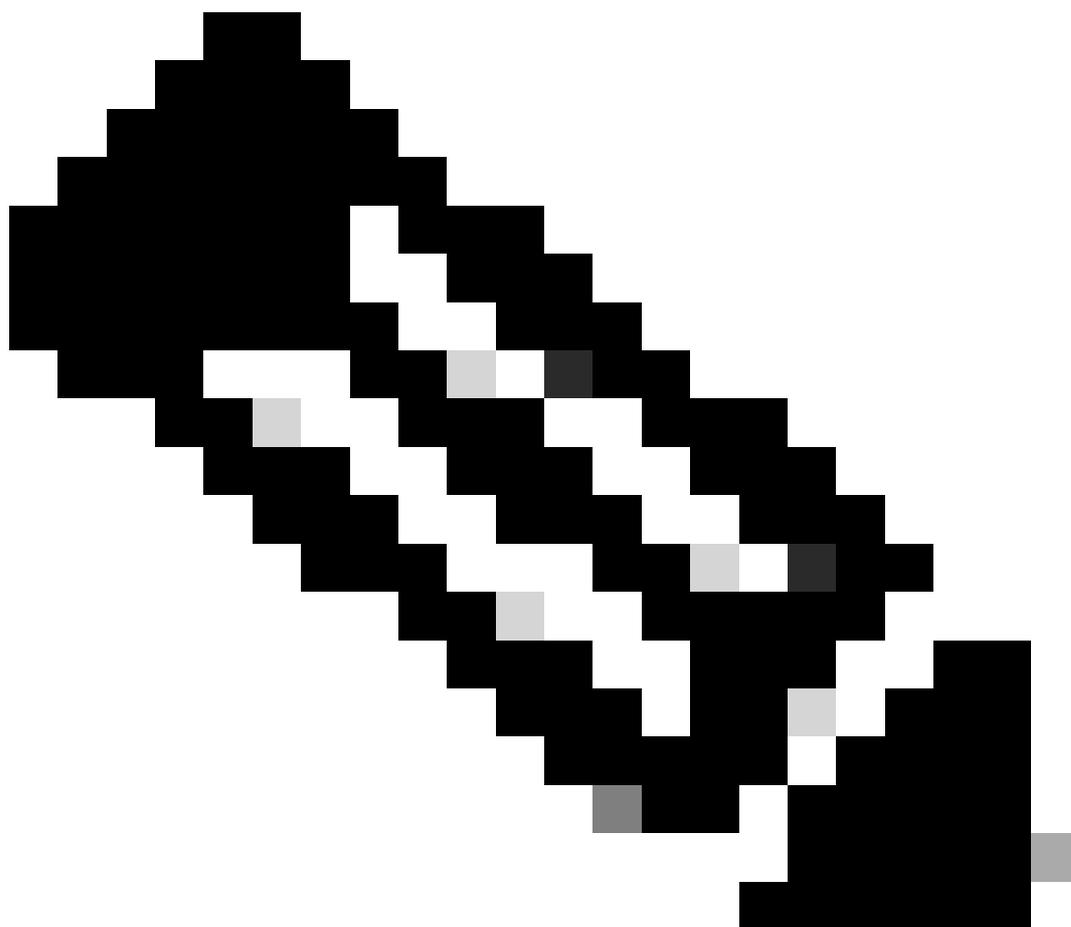
```
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
```

```
Issued By :
```

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

Validity Start : 17:05:00 UTC Mon Apr 28 2025
Validity End : 17:05:00 UTC Sat Apr 28 2035
RP/0/RP0/CPU0:May 9 14:52:20.961 UTC: pki_cmd[66362]: %SECURITY-PKI-6-LOG_INFO_DETAIL : Fingerprint: 2A
SHA1 Fingerprint:
0EB181E95A3ED7803BC5A8059A854A95C83AC737
Do you accept this certificate? [yes/no]:
yes

RP/0/RP0/CPU0:May 9 14:52:23.437 UTC: cepki[153]: %SECURITY-CEPKI-6-INFO : certificate database updated



Nota: Se si dispone di un sistema CA subordinata, è necessario importare sia i certificati CA radice che quelli CA subordinata. Utilizzare lo stesso comando con Sub CA in primo piano e Root CA in secondo piano.

Passaggio 4. Generare una richiesta di firma del certificato (CSR).

<#root>

RP/0/RP0/CPU0:BRC-8201-1#

crypto ca enroll svcs

Fri May 9 14:52:44.030 UTC

% Start certificate enrollment ...

% Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate.

% For security reasons your password will not be saved in the configuration.

% Please make a note of it.

Password:

Re-enter Password:

% The subject name in the certificate will include: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=10.225.253.167

% The subject name in the certificate will include: BRC-8201-1.svs.lab

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

yes

% The serial number in the certificate will be: 4090843b

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

yes

Enter IP Address[]

10.225.253.167

Fingerprint: 36354532 38324335 43434136 42333545

Display Certificate Request to terminal? [yes/no]:

yes

Certificate Request follows:

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

MIIDQTCCAikCAQAwcjELMAKGA1UEBhMCVVMxMzA1BjBGNVBAgMAK5DMQwwCgYDVQQH
DANSVFAXDjAMBGNVBAoMBUNpc2NvMQwwCgYDVQQLDANTV1MxMzA1BjBGNVBAgMAK5DMQwwCgYDVQQH
LjIyNS4yNTMuMTYzMRERDwYDVQQFEWg0MDkwODQzYjCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBALwx9w4DnTtr1oDH9i0ZxPvEDARwN0t4WrPEjaQc1ZUA
6ax6Ccx/0J1QiUf2+eQv+4rKZqAZ1xDhiaIMGqETn00LKpwmtx10IqXL7UYMHhWF
9vRII52zomkWA8a63Wx66UkExaXoeXaf5HkLoqDu68X83U7LPvMe1sMwvmq7Rmy2
DAu30HB/JfY1QChmTVFz3M5fBt86xx4t1nxTFU/41RWMC73UdL5YdKJLjMpBT2tN
E3piZ+kL4p1c9U4RIBkU8/G4drzFbGvHCIkKwI0cb1X2HgtbVQdCXTAwJDMr2O9
zd2ZCa5enTbOKHbNXuHjpy0k8MewKOV2muwxVcQbej8CAwEAAaCBiTAyBqkqhkG
9w0BCQcxCMJQzFzY28uMTIzMG0GCSqGSIb3DQEJJDJFgMF4wDgYDVR0PAQH/BAQD
AgWgMCAGA1UdJQEB/wQWMBQGCSsGAQUFBwMBBggrBgEFBQcDAjA1BjBGNVBRMEAjAA
MB8GA1UdEQQYMBaCDjEwLjIyNS4yNTMuMTYzMRERDwYDVQQFEWg0MDkwODQzYjCCASIwDQYJKoZIhvcNAQEB
A4IBAQBBOXeWF5ZUZ701GFjuQHBBdgYb+31hF0xbYm9psIWfv1uwjKkL297tGHv
Iux7nMyrDVkSj81i5BSTdd9FE6AbSFswj1Yp0+IxmUM971Ejwg2rj+jABDR7I8SU
06Y06mS9x2ZJYqImeq8xwIr19Hi+7tyaLe6apfTI1jdgVxB+Xyz0FJMckI05US3j
T/3aw/115RcXerdrh360MUHEepUjIx/15u9s1c7e1mxACoQE6f90A+fdg2zYt0ME
Z6VAw64cY+YF6iLbYv7c41iz05Zj2NjBUKpeqijkFAKY/1rIxTHypzH/p2ma4zuS
46a+kLXsVHZ716ZMB3WrUzB2ZN00

-----END CERTIFICATE REQUEST-----
---End - This line not part of the certificate request---
Redisplay enrollment request? [yes/no]:

no

Passaggio 5. Importare un certificato firmato dall'autorità di certificazione.

<#root>

RP/0/RP0/CPU0:BRC-8201-1#

crypto ca import svcs certificate

Fri May 9 15:00:35.426 UTC

Enter the base64/PEM encoded certificate/certificates.
Please note: for multiple certificates use only PEM.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIIE3zCCAsEgAwIBAgIINL1NAUzx14UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCMVVMxZzAVBgNVBAGTDk5vbnRoIENhcm9saW5hMRAdDgYDVQQHEwdSYWx1aWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECXMdU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNTA5MTQ1NzAwWhcNMjYwNTA5MTQ1NzAwWjByMQswCQYDVQQGEwJV
UzELMAkGA1UECAwCTMxkDDAKBgNVBACMA1JUUEDEOMAwGA1UECgwFQ21zY28xDDAK
BgNVBAsMA1NWUzEXMBUGA1UEAwwOMTAuMjUwNTA5MTQ1NzAwWjByMQswCQYDVQ
OTA4NDNiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvDH3Dg0d02uW
gMf2I5nE+8QMBHA3S3has8SNpByV1QDprHoLGr/QmVCJR/b55C/7i spmoBnXEOGJ
qIwaoR0c7QsqnCa3HXQipcvtrGwcfAX29Egjnboi aRYDxrdbHrpSQTfpeh5dp/k
eQuio07rxfdzTss+8x7WwzC+artGbLYMC7fQcH819iVAIeZNUXPcz18G3zrHHi3W
fFMVT/iVFYwLvdR0v1h0okuMykFPa00TemJn6QvinVz1ThEgGRTz8bh2vMVsa8cI
iRaTajRxxvFyE1tVB0JdMDAK0avY73N3Zkjr16dNs4ods1e4eOnLSTwx7Ao5Xaa
7DFVxBt6PwIDAQBo4GAMH4wHgYJYZIAYb4QgENBBEWD3hjYSBjZXJ0aWZpY2F0
ZTA0BgNVHQ8BAf8EBAMCBaAwIAAYDVR01AQH/BBYwFAYIKwYBBQUHAWEGCCsGAQUF
BwMCMCAkGA1UdEwQCMAAwHwYDVR0RBBgwFoIOMTAuMjUwNTA5MTQ1NzAwWjByMQsw
DQYJKoZIhvcNAQELBQADggIBAARpS5bEck+oj012106WxedDQ8Vdu0bBtrnOH+Nt
94EA1co7HEe4USf1FiASAX7rNveLpY3ICmLh+tQZYTzRQ93tb9mMTZg7exqN89ZU
V1XoB2UOTri5K10/+izEGgyNq42/yTAP8Y007HR/2jf7gfhovwvR5QN0EHv4o61
Zma5Xio1sBbkA7JB2mpzzG4Zjysv81RGXxxgyt1mwNmb7EiAc81odRcgy7FNh3
F/k9cMMMr51M4Ysvo1tx1k9AeLjzb2syv5/fG6Qu0ZdWwTaaQh0Y2h/cVDiV97wg
0D1mEfdSv6QrxQSujz2R2RzVykKH1tviV2B74pthUuGRBtFHS5XFy7uTTbfGX8M6
ZJw8rX1SADr8tDplrf1ZIRPmv3ZPP7woTB22yWzyd0use+5Ia1b0w70twN4t/Iiw
8CJu6HfnDXLDPZ0jsC8steffrS1opwGccp3j6aZKPFz+I/Purb44a9WxEwa2TA7H
+r1oynBcGmet0HxvLnpt1sC7Q4mN/MDXeGyW+OTNCirNEG/gqcu+dn9EnNkKE2WV
oF5370w+uNHok8Bdt8mqadUT40oUsqY8ArV0Bom05tzbemreVPmQAZ/IahZ7TqKo
3dGNontAFTTESM1iujQ81iRKsikdHySnwCM2ni1CKZrhVq5IB8NK6jKRJZ0eQAX
vMt1
-----END CERTIFICATE-----

quit

Serial Number : C2:F4:AB:34:02:D2:76:74:65:34:FE:D5
Subject:
serialNumber=4090843b,CN=10.225.253.167,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
Issued By :
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US

Validity Start : 14:57:00 UTC Fri May 09 2025
Validity End : 14:57:00 UTC Sat May 09 2026
SHA1 Fingerprint:
21E4DA0B02181D08B6E51F0CC754BCE5B815C792

Verificare che il certificato di identità del router sia registrato.

<#root>

RP/0/RP0/CPU0:BRC-8201-1#

show crypto ca trustpoint svcs detail

Trustpoint :svcs-new

```
=====
KeyPair Label: the_default
CRL:optional
enrollment: terminal
subject name: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=brc-8201-1.svs.lab
```

RP/0/RP0/CPU0:BRC-8201-1#

show crypto ca certificates svcs

Wed May 14 14:55:58.173 UTC

Trustpoint : svcs-new

CA certificate

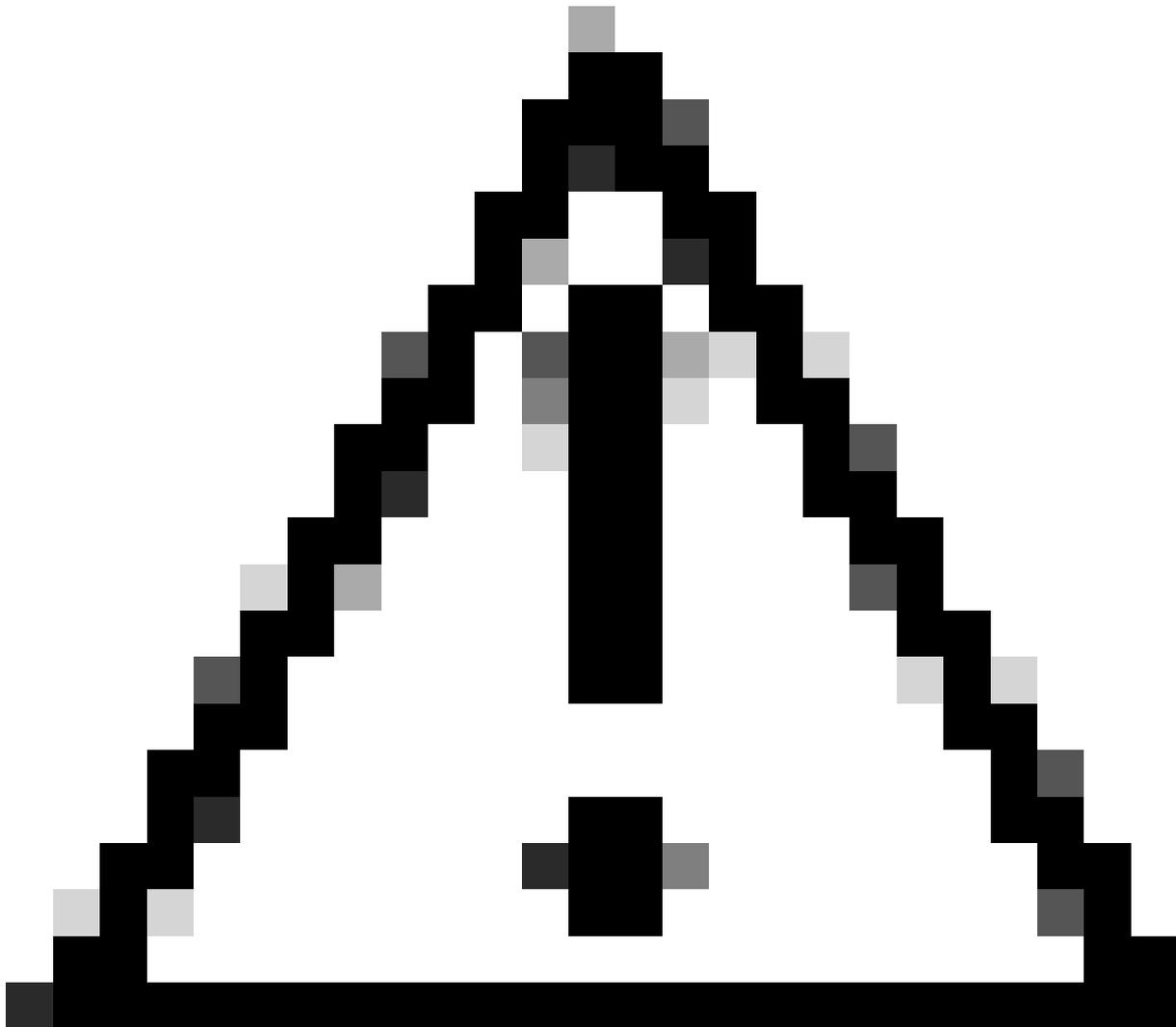
```
Serial Number : 20:01:20:1F:B6:9D:C3:FE:43:78:FF:64
Subject:
  CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
Issued By :
  CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
Validity Start : 17:05:00 UTC Mon Apr 28 2025
Validity End : 17:05:00 UTC Sat Apr 28 2035
SHA1 Fingerprint:
  0EB181E95A3ED7803BC5A8059A854A95C83AC737
```

Router certificate

```
Key usage : General Purpose
Status : Available
Serial Number : FD:AC:20:1F:B6:9D:C3:FE:98:43:ED
Subject:
  serialNumber=4090843b,CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
Issued By :
  CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
Validity Start : 19:59:00 UTC Fri May 09 2025
Validity End : 19:59:00 UTC Sat May 09 2026
SHA1 Fingerprint:
  AC17E4772D909470F753BDBFA463F2DF522CC2A6
```

Associated Trustpoint: svcs

Configurazione di TACACS e AAA con TLS



Attenzione: Eseguire le modifiche alla configurazione tramite la console con le credenziali locali.

Passaggio 1. Configurare il server TACACS+.

```
tacacs source-interface MgmtEth0/RP0/CPU0/0 vrf mgmt
tacacs-server host 10.225.253.209 port 49
key 7 072C705F4D0648574453
```

```
aaa group server tacacs+ tacacs2
server 10.225.253.209
vrf mgmt
```

Passaggio 2. Configurare il gruppo AAA.

```
aaa group server tacacs+ tac_tls_sc
vrf mgmt
server-private 10.225.253.209 port 6049
timeout 10
tls
  trustpoint svr
  !
single-connection
```

Passaggio 2. Configurare AAA.

```
aaa accounting exec default start-stop group tac_tls_sc
aaa accounting system default start-stop group tac_tls_sc
aaa accounting network default start-stop group tac_tls_sc
aaa accounting commands default stop-only group tac_tls_sc
aaa authorization exec default group tac_tls_sc local
aaa authorization commands default group tac_tls_sc none
aaa authentication login default group tac_tls_sc local
```

Rinnovo certificato

Nota: Non è necessario rimuovere il trust point dalla configurazione TACACS+ durante il rinnovo.

Passaggio 1. Verificare le date di validità del certificato correnti.

```
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates svr-new
Thu Aug 14 15:13:37.465 UTC
```

```
Trustpoint : svr-new
```

```
=====
```

```
CA certificate
```

```
Serial Number : 30:A2:10:14:C9:5E:B0:E0:07:CE:0A:24:16:69:90:ED:D1:34:B5:9B
```

```
Subject:
```

```
CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
```

```
Issued By :
```

```
CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
```

```
Validity Start : 22:13:17 UTC Thu Jun 26 2025
```

```
Validity End : 22:13:16 UTC Tue Jun 25 2030
```

CRL Distribution Point

<http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=m9uB1QsZDYy6wxomiFWB5Gv0AZM>

SHA1 Fingerprint:

EA8FB276563B927FCAF0174D9FD1C58F3E8B5FF2

Trusted Certificate Chain

Serial Number : 1F:A6:6E:2E:F8:AB:CE:B4:9C:B8:07:5A:9F:2B:32:02:B4:56:5C:96

Subject:

CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US

Issued By :

CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US

Validity Start : 22:13:17 UTC Thu Jun 26 2025

Validity End : 22:13:16 UTC Sun Jun 24 2035

SHA1 Fingerprint:

E225647FF9BDA176D2998D5A3A9770270F37D2A7

Router certificate

Key usage : General Purpose

Status : Available

Serial Number : 7A:13:EB:C0:6A:8D:66:68:09:0B:32:C7:0C:D8:05:BD:81:72:9B:4E

Subject:

CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US

Issued By :

CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US

Validity Start : 16:38:36 UTC Wed Jul 30 2025

Validity End : 16:38:35 UTC Thu Jul 30 2026

CRL Distribution Point

<http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=X4as2q+6I9Bd4Qg1Qa8g1xoH8GY>

SHA1 Fingerprint:

B562F3CF507CE7F97893F28BC896794CFF6995C1

Associated Trustpoint: svb-new

Passaggio 2. Eliminare il certificato del trust point esistente.

```
RP/0/RP0/CPU0:BRC-8201-1#clear crypto ca certificates KF_TP
```

```
Thu Aug 14 15:25:26.286 UTC
```

```
certificates cleared for trustpoint KF_TP
```

```
RP/0/RP0/CPU0:Aug 14 15:25:26.577 UTC: cepki[382]: %SECURITY-CEPKI-6-INFO : certificate database updated
```

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

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

```
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates KF_TP
```

```
Thu Aug 14 15:25:37.270 UTC
```

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

Passaggio 3. Ripetere l'autenticazione e la registrazione del trust point come descritto nei passaggi in Configurazione del trust point.

Passaggio 4. Verificare che le date di validità del certificato siano aggiornate.

```
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates KF_TP
```

```
Thu Aug 14 15:31:28.309 UTC
```

Trustpoint : KF_TP

=====

CA certificate

Serial Number : 30:A2:10:14:C9:5E:B0:E0:07:CE:0A:24:16:69:90:ED:D1:34:B5:9B
Subject:
CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
Issued By :
CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
Validity Start : 22:13:17 UTC Thu Jun 26 2025
Validity End : 22:13:16 UTC Tue Jun 25 2030

CRL Distribution Point

<http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=m9uB1QsZDYy6wxomiFWB5Gv0AZM>

SHA1 Fingerprint:

EA8FB276563B927FCAF0174D9FD1C58F3E8B5FF2

Trusted Certificate Chain

Serial Number : 1F:A6:6E:2E:F8:AB:CE:B4:9C:B8:07:5A:9F:2B:32:02:B4:56:5C:96
Subject:
CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
Issued By :
CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
Validity Start : 22:13:17 UTC Thu Jun 26 2025
Validity End : 22:13:16 UTC Sun Jun 24 2035

SHA1 Fingerprint:

E225647FF9BDA176D2998D5A3A9770270F37D2A7

Router certificate

Key usage : General Purpose
Status : Available
Serial Number : 1F:B0:AE:44:CF:8E:24:62:83:42:2F:34:BF:D0:82:07:DF:E4:49:0B
Subject:
CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
Issued By :
CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
Validity Start : 15:17:29 UTC Thu Aug 14 2025
Validity End : 15:17:28 UTC Fri Aug 14 2026

CRL Distribution Point

<http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=X4as2q+6I9Bd4Qg1Qa8g1xoH8GY>

SHA1 Fingerprint:

D3CE0AEB51C5E8009F626A1A9FD633FB9AFA96DE

Associated Trustpoint: KF_TP

Verifica

Verifica della configurazione.

```
show crypto ca certificates [detail]  
show crypto ca trustpoint detail  
show tacacs details
```

Debug per TACACS+

```
debug tacacs tls
```

Debug TLS

```
debug ssl error  
debug ssl events
```

Verificare l'utente remoto prima di configurare l'autenticazione AAA.

```
<#root>
```

```
test aaa group tacacs2
```

```
user has been authenticated
```

Risoluzione dei problemi

Cancellazione dei certificati (vengono eliminati tutti i certificati associati a un trust point).

```
clear crypto ca certificate <trustpoint name>
```

Riavvio del processo TACACS (se necessario)

```
process restart tacacsd
```

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).