

Configurazione di TACACS+ over TLS 1.3 su un dispositivo Nexus con ISE

Sommario

[Introduzione](#)

[Panoramica](#)

[Utilizzo della Guida](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Licenze](#)

[Configurare ISE per Device Admin](#)

[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](#)

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

[Configura archivi identità](#)

[Configura profili shell TACACS+](#)

[Amministratore NX-OS](#)

[HelpDesk NX-OS](#)

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

[Configurazione di Cisco NX-OS per TACACS+ over TLS](#)

[Configurazione server TACACS+](#)

[Configurazione del punto di trust](#)

[Configurazione TACACS+ TLS](#)

[Configurazione AAA](#)

[Test e risoluzione dei problemi di accesso utente per NX-OS](#)

[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 NX-OS 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 NX-OS.

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

Prerequisiti

Requisiti

Prerequisiti 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.
- Switch Nexus 9000 modello C9364D-GX2A, Cisco NX-OS versione 10.5(3t).

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.

Configurare ISE per Device Admin

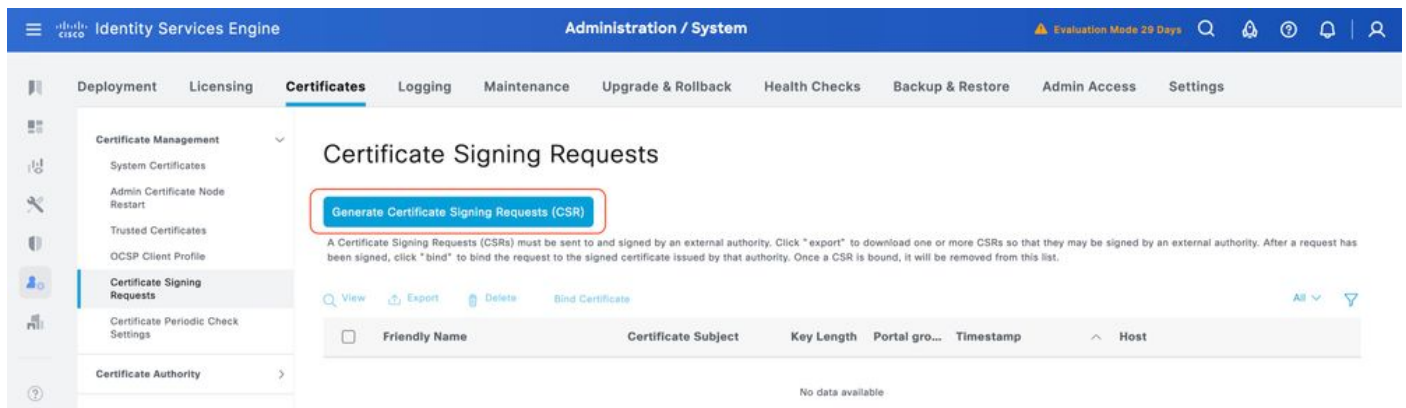
Genera richiesta di firma del certificato per autenticazione server TACACS+

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.

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 PSN con TACACS+ abilitato.

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☒ 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

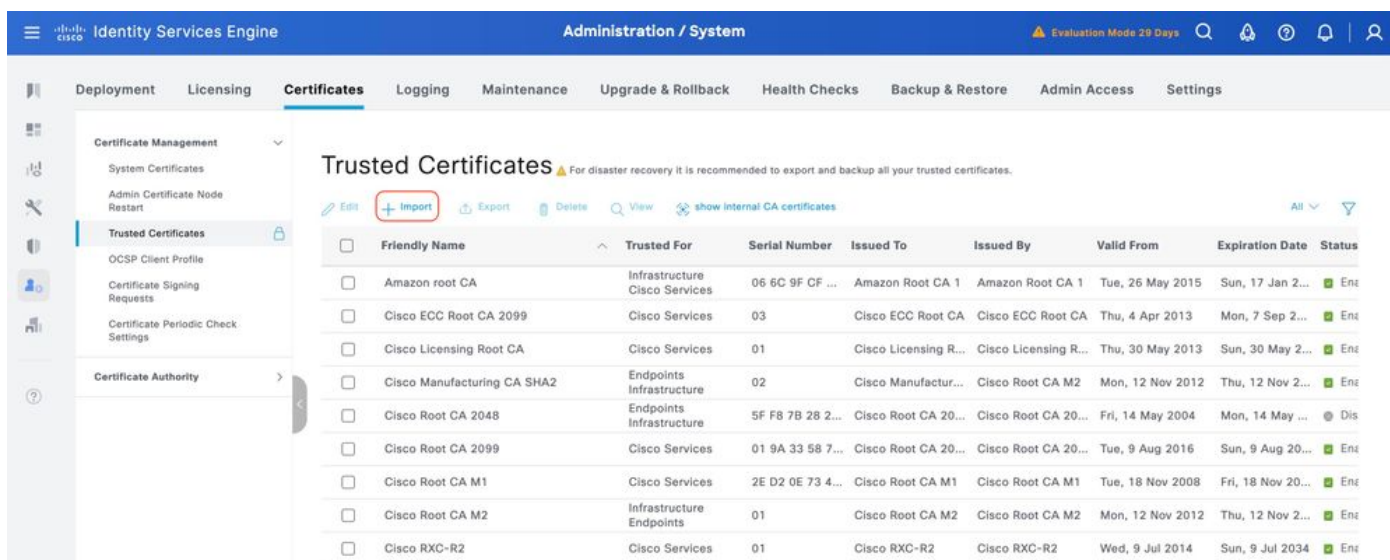
Passaggio 8. Fare clic su Genera, quindi su Esporta.



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.



Passaggio 2. Selezionare il certificato emesso dall'Autorità di certificazione (CA) che ha firmato la richiesta TACACS di firma del certificato (CSR). Assicurarsi che l'opzione Trust for Authentication in ISE sia abilitata.

Import a new Certificate into the Certificate Store

* Certificate File **Examinar...** 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

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 a menu with options like Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade & Rollback, Health Checks, Backup & Restore, Admin Access, and Settings. 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, Expiration Date, and Status. The first row is highlighted with a red box, showing a certificate for "CN=SVS LabCA, OU=SVS, O=Cisco, L=..." issued by "SVS LabCA".

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

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 ad 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 a menu with options like Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade & Rollback, Health Checks, Backup & Restore, Admin Access, and Settings. The main content area is titled "Certificate Signing Requests" and displays a button "Generate Certificate Signing Requests (CSR)". Below the button, there is a text box explaining that CSR requests must be sent to and signed by an external authority. At the bottom, there is a table with columns for Friendly Name, Certificate Subject, Key Length, Portal gro..., Timestamp, and Host. The "Bind Certificate" button is highlighted with a red box.

Friendly Name	Certificate Subject	Key Length	Portal gro...	Timestamp	Host
---------------	---------------------	------------	---------------	-----------	------

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

Identity Services Engine Administration / System

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 Sottometti. 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

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

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

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 ad Amministrazione > Sistema > Impostazioni.



Identity Services Engine



Bookmarks



Dashboard



Context Visibility



Operations



Policy



Administration



Work Centers



Interactive Help

Deployment

Licensing

Client Provisioning

FIPS Mode

Security Settings

Alarm Settings

System

Deployment

Licensing

Certificates

Logging

Maintenance

Upgrade & Rollback

Health Checks

Backup & Restore

Admin Access

Settings ✓

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

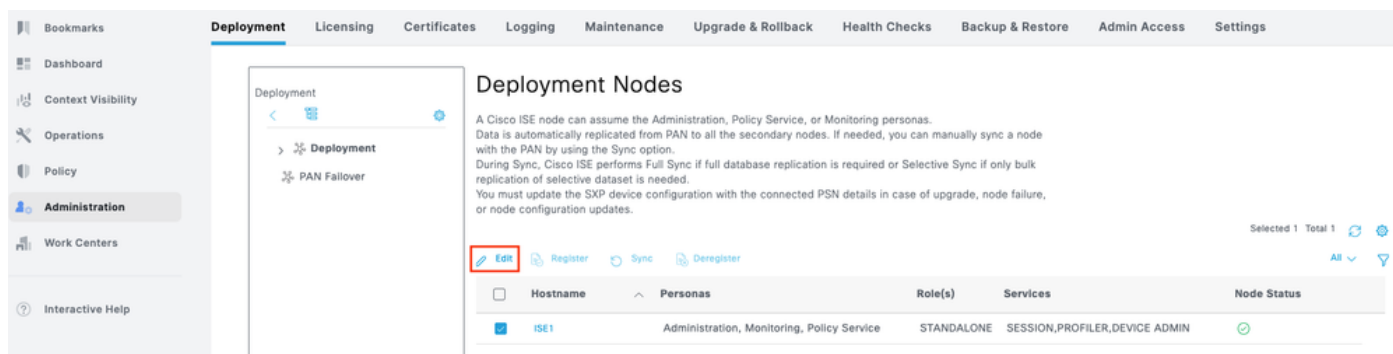
☒ TLS 1.3



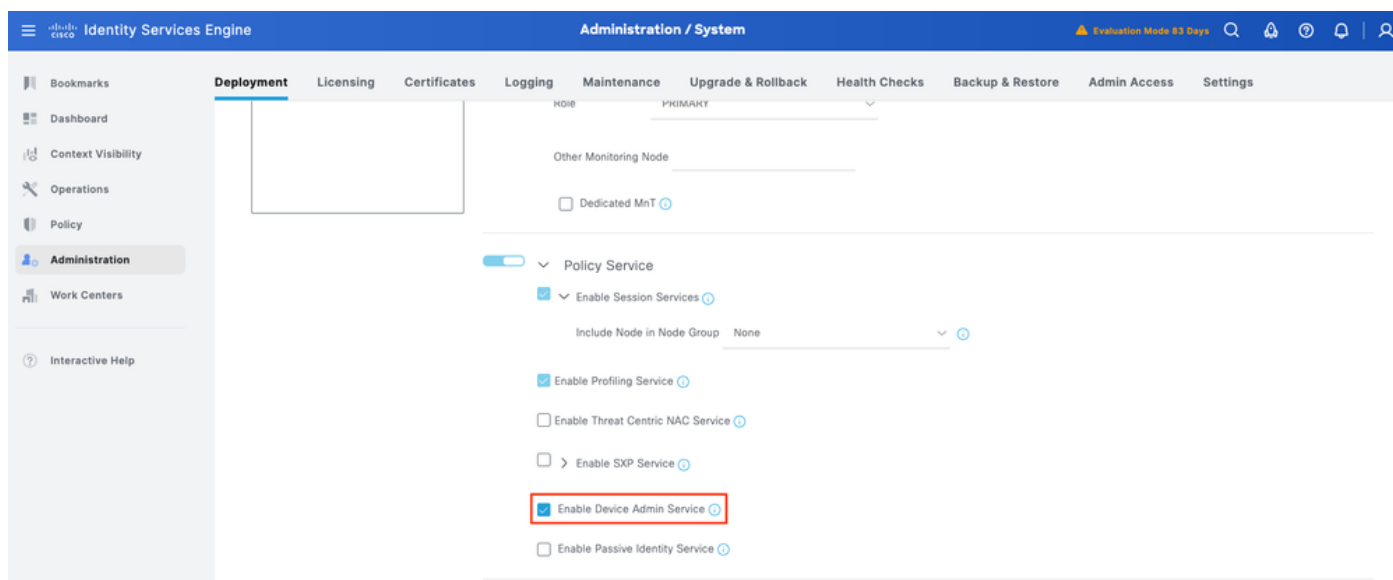
Avviso: Quando si modifica la versione TLS, il server applicazioni Cisco ISE viene riavviato su tutti i computer di implementazione di Cisco ISE.

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.



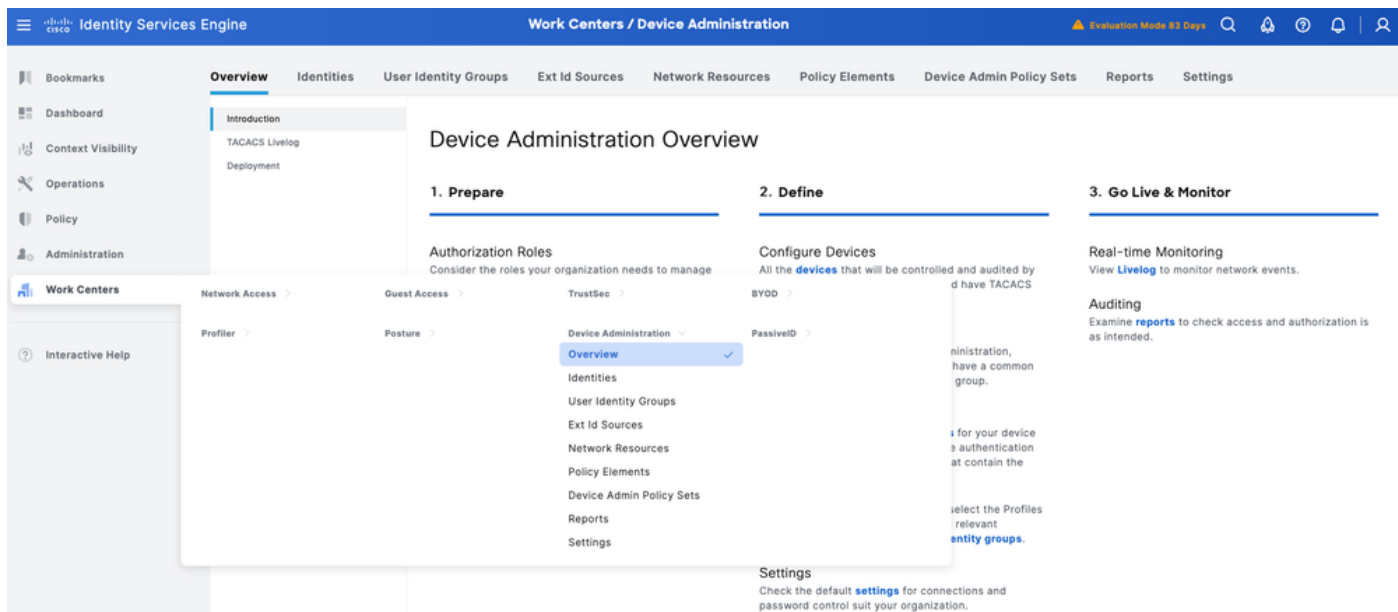
Passaggio 2. In General Settings, scorrere verso il basso e selezionare la casella di controllo accanto a Enable Device Admin Service.



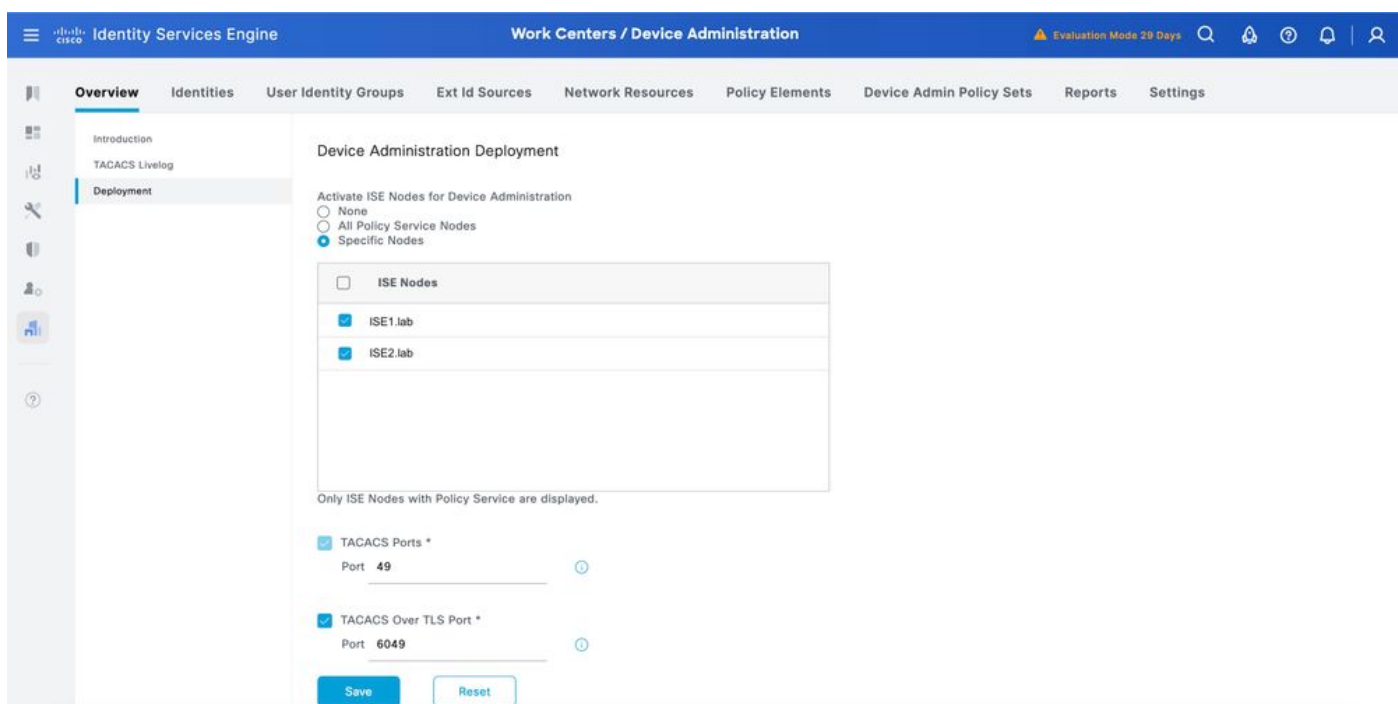
Passaggio 3. Salvare la configurazione. Device Admin Service è ora abilitato su ISE.

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 (Salva).

Dispositivi di rete e gruppi 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 > Risorsa di rete. Fare clic su Gruppi di dispositivi di rete.

Work Centers / Device Administration

Network Resources

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

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 NS-OX come dispositivo di rete. Passare a Centri di lavoro > Amministrazione dispositivi > Risorse di rete. Fare clic su Add (Aggiungi) per aggiungere un nuovo dispositivo di rete POD2IPN2.

Administration / Network Resources

Network Devices

Network Devices List > POD2IPN2

Network Devices

Name: **POD2IPN2**

Description:

IP Address: 10.225.253.177 / 32

Device Profile: Cisco

Model Name: C9364D-GX2A

Software Version: 10.5(3t)

Network Device Group

Location: Atlanta (Set To Default)

IPSEC: No (Set To Default)

Device Type: NXOS (Set To Default)

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

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

Network Devices

Network Device Groups

Network Device Profiles

External RADIUS Servers

RADIUS Server Sequences

External MDM

More

Network Devices

Default Device

Device Security Settings

☐ RADIUS Authentication Settings

☐ TACACS Authentication Settings

☒ TACACS over TLS Authentication Settings

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

Subject Alternative Name (SAN) *

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

☐ IP Address

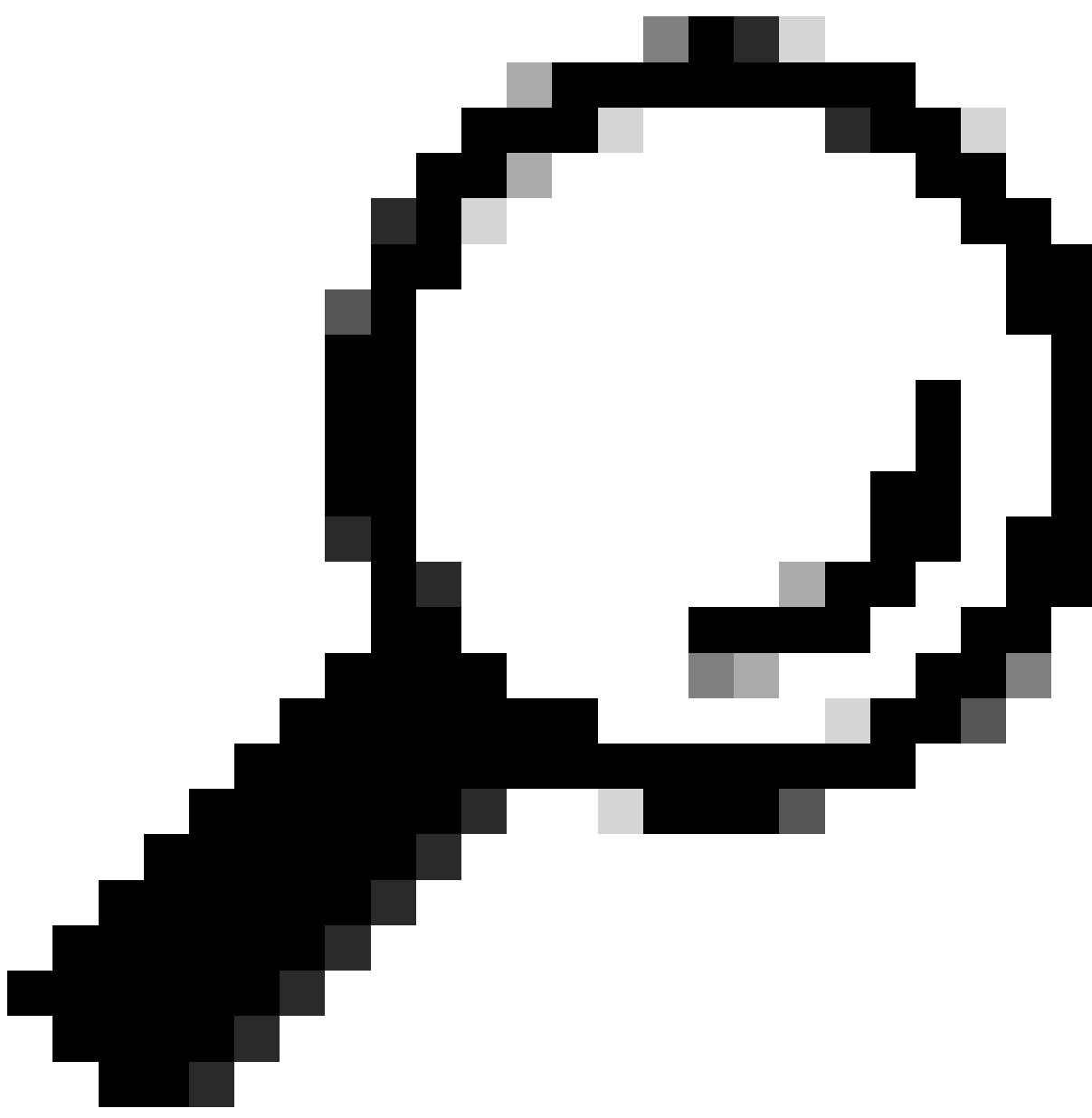
The IP address(es) listed within the SAN attribute of the certificate is matched with the IP address of the network device. Both IPv4 and IPv6 addresses are supported.

Additional SAN attribute details [Show](#)

Additional SAN Attributes

☒ Enable Single Connect Mode

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

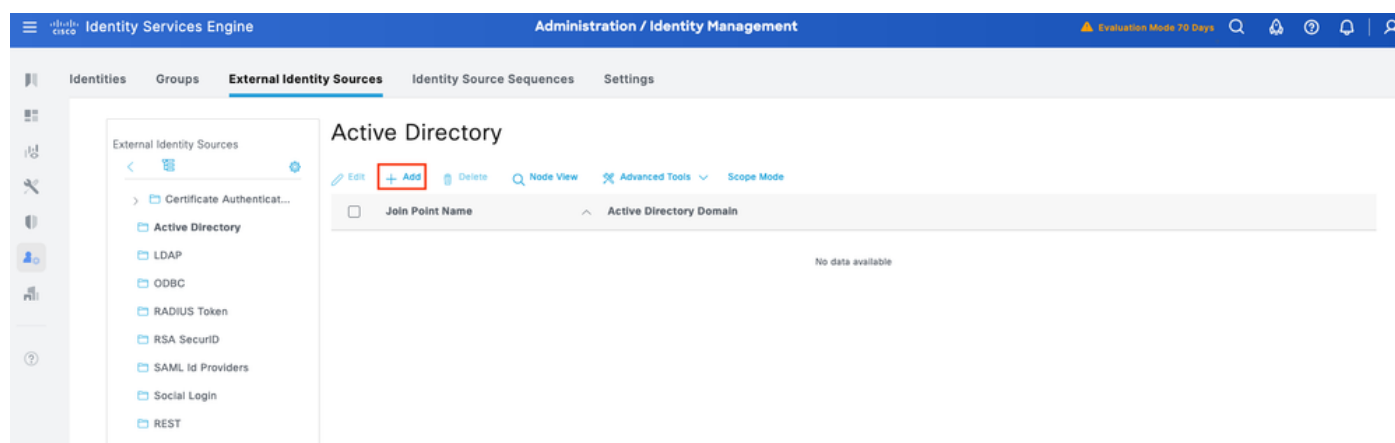


Suggerimento: Per evitare di riavviare la sessione TCP ogni volta che si invia un comando al dispositivo, si consiglia di abilitare la modalità di connessione singola.

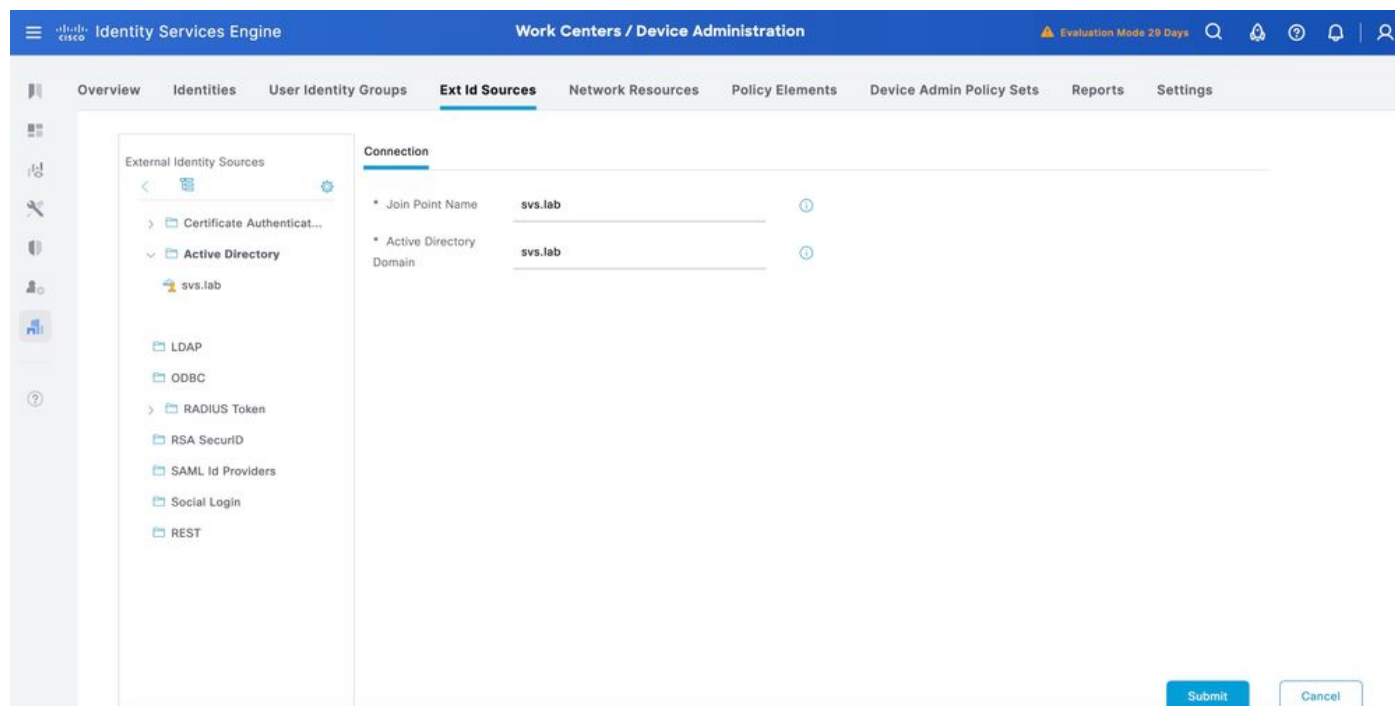
Configura archivi identità

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 viene richiesto se si desidera aggiungere tutti i nodi ISE a questo dominio Active Directory.



Information

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

No

Yes

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

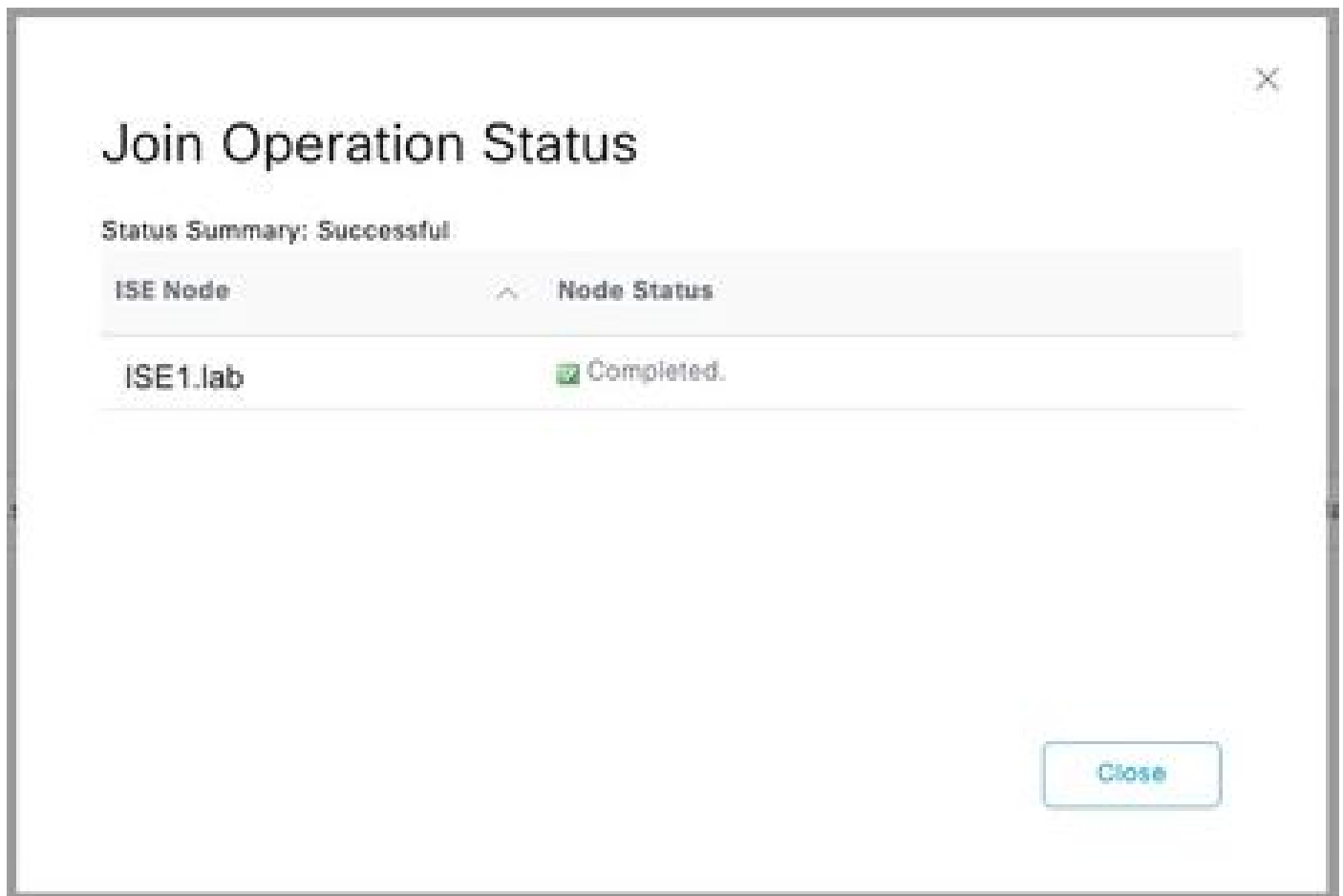
* Password

☐ Specify Organizational Unit ⓘ

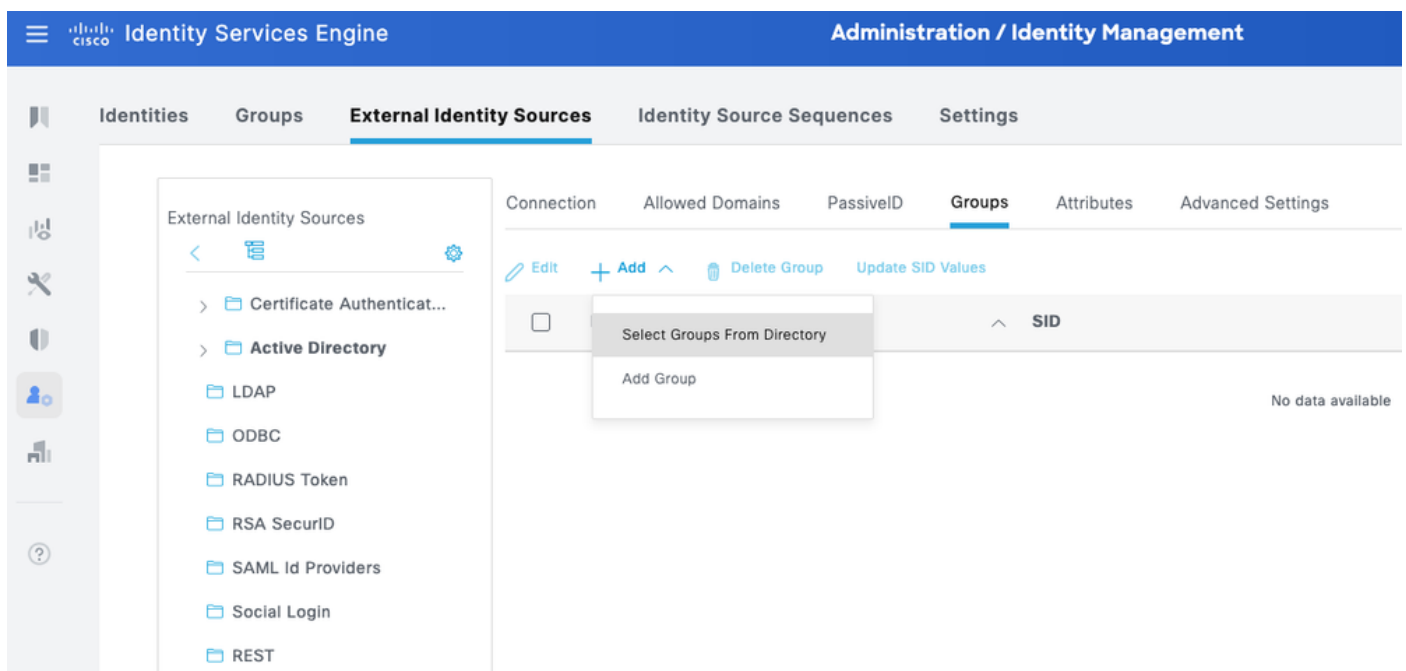
☒ Store Credentials ⓘ

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

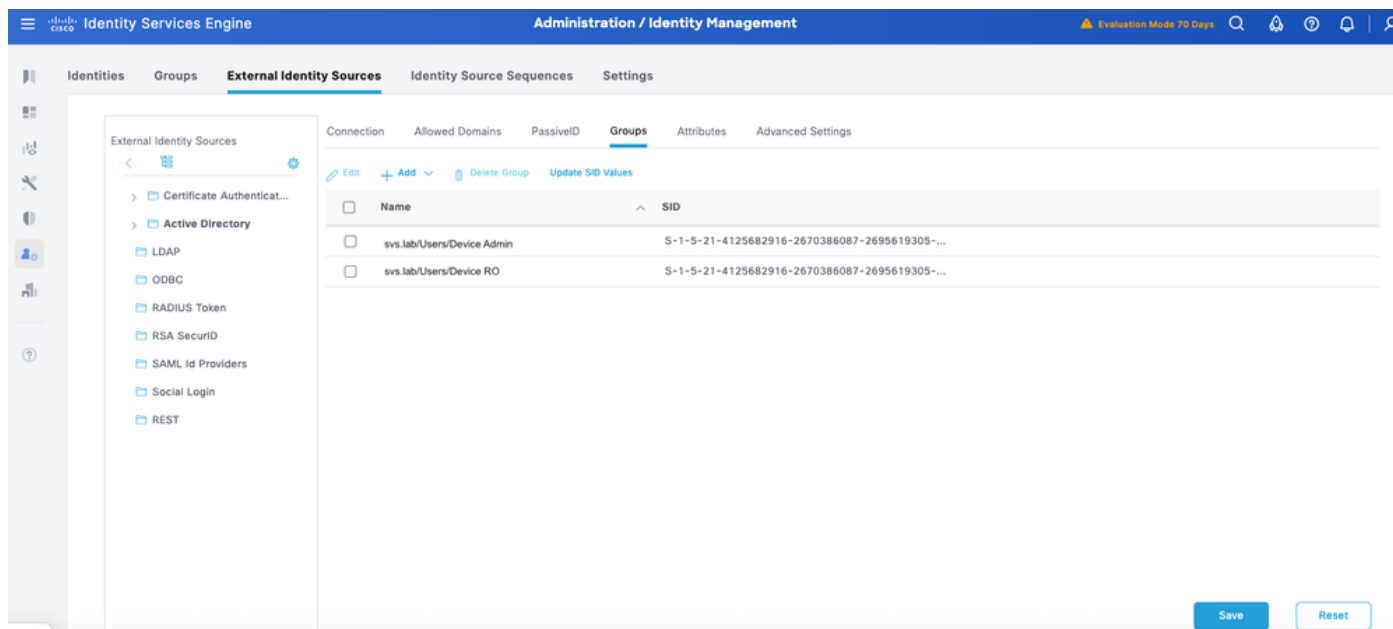
Type

Filter

Retrieve Groups...

2 Groups Retrieved.

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



Configurazione dei profili della shell TACACS+

A differenza dei dispositivi Cisco IOS, che utilizzano i livelli di privilegio per l'autorizzazione, i dispositivi Cisco NX-OS implementano il controllo degli accessi basato sui ruoli (RBAC). In ISE, è possibile mappare i profili TACACS+ ai ruoli utente sui dispositivi Cisco NX-OS usando le attività comuni di tipo Nexus.

I ruoli predefiniti sui dispositivi NX-OS variano a seconda della piattaforma NX-OS. Due comuni sono:

- network-admin - il ruolo predefinito network admin dispone dell'accesso in lettura e scrittura completo a tutti i comandi sullo switch; disponibile nel contesto di dispositivo virtuale predefinito (VDC) solo se i dispositivi (ad esempio, Nexus 7000) dispongono di più VDC. Utilizzare il comando CLI di NX-OS `show cli syntax roles network-admin` per visualizzare

l'elenco completo dei comandi disponibili per questo ruolo.

- operatore di rete - il ruolo amministratore di rete predefinito ha accesso in lettura completo a tutti i comandi sullo switch; disponibile nel VDC predefinito solo se i dispositivi (ad esempio, Nexus 7000) dispongono di più VDC. Utilizzare il comando NX-OS CLI show cli syntax roles network-operator per visualizzare l'elenco completo dei comandi disponibili per questo ruolo.

Successivamente, vengono definiti due profili TACACS: NXOS Admin e NXOS HelpDesk.

Amministratore NX-OS

Passaggio 1. Aggiungere un altro profilo e denominarlo NX-OS Admin.

Passo 2: selezionare Obbligatorio dall'elenco a discesa Imposta attributi come. Selezionare Administrator da Network-role in Common Tasks.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine' and 'Work Centers / Device Administration'. The left sidebar shows a tree view with 'TACACS Profiles' selected. The main content area displays the configuration for a TACACS Profile named 'NXOS Admin'. The 'Name' field is 'NXOS Admin'. The 'Description' field is empty. The 'Task Attribute View' tab is active, showing 'Common Tasks'. Under 'Common Task Type', 'Nexus' is selected. The 'Set attributes as' dropdown is set to 'Mandatory'. The 'Network role' section has three radio buttons: 'None', 'Operator (Read Only)', and 'Administrator (Read Write)', with 'Administrator (Read Write)' selected. The 'VDC role' section has three radio buttons: 'None', 'Operator (Read Only)', and 'Administrator (Read Write)', with 'None' selected.

Passaggio 3. Fare clic su Invia per salvare il profilo.

HelpDesk NX-OS

Passaggio 1. Dall'interfaccia utente di ISE, selezionare Work Center > Device Administration > Policy Elements > Results > TACACS Profiles. Aggiungere un nuovo profilo TACACS e denominarlo NXOS HelpDesk. Andare all'elenco a discesa Tipo di task comune e scegliere Nexus.

È possibile visualizzare le modifiche del modello specifiche del ruolo utente. È possibile selezionare queste opzioni corrispondenti al ruolo utente da configurare.

Passo 2: selezionare Obbligatorio dall'elenco a discesa Imposta attributi come. Selezionare Operatore da ruolo di rete in Operazioni comuni.

Identity Services Engine Work Centers / Device Administration Evaluation Mode 90 Days

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

Conditions > TACACS Profiles > NXOS HelpDesk
TACACS Profile

Results
Allowed Protocols
TACACS Command Sets
TACACS Profiles

Name: NXOS HelpDesk

Description:

Task Attribute View Raw View

Common Tasks

Common Task Type: Nexus

Set attributes as: Optional

Network role
☐ None
☒ Operator (Read Only)
☐ Administrator (Read Write)

VDC role
☒ None
☐ Operator (Read Only)
☐ Administrator (Read Write)

Passaggio 3. Fare clic su Salva per salvare il profilo.

Configura set di criteri di amministrazione dispositivi

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. Ad esempio, i dispositivi Cisco IOS utilizzano livelli di privilegi e/o set di comandi, mentre i dispositivi Cisco NX-OS utilizzano attributi personalizzati.

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

Identity Services Engine Work Centers / Device Administration Evaluation Mode 90 Days

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

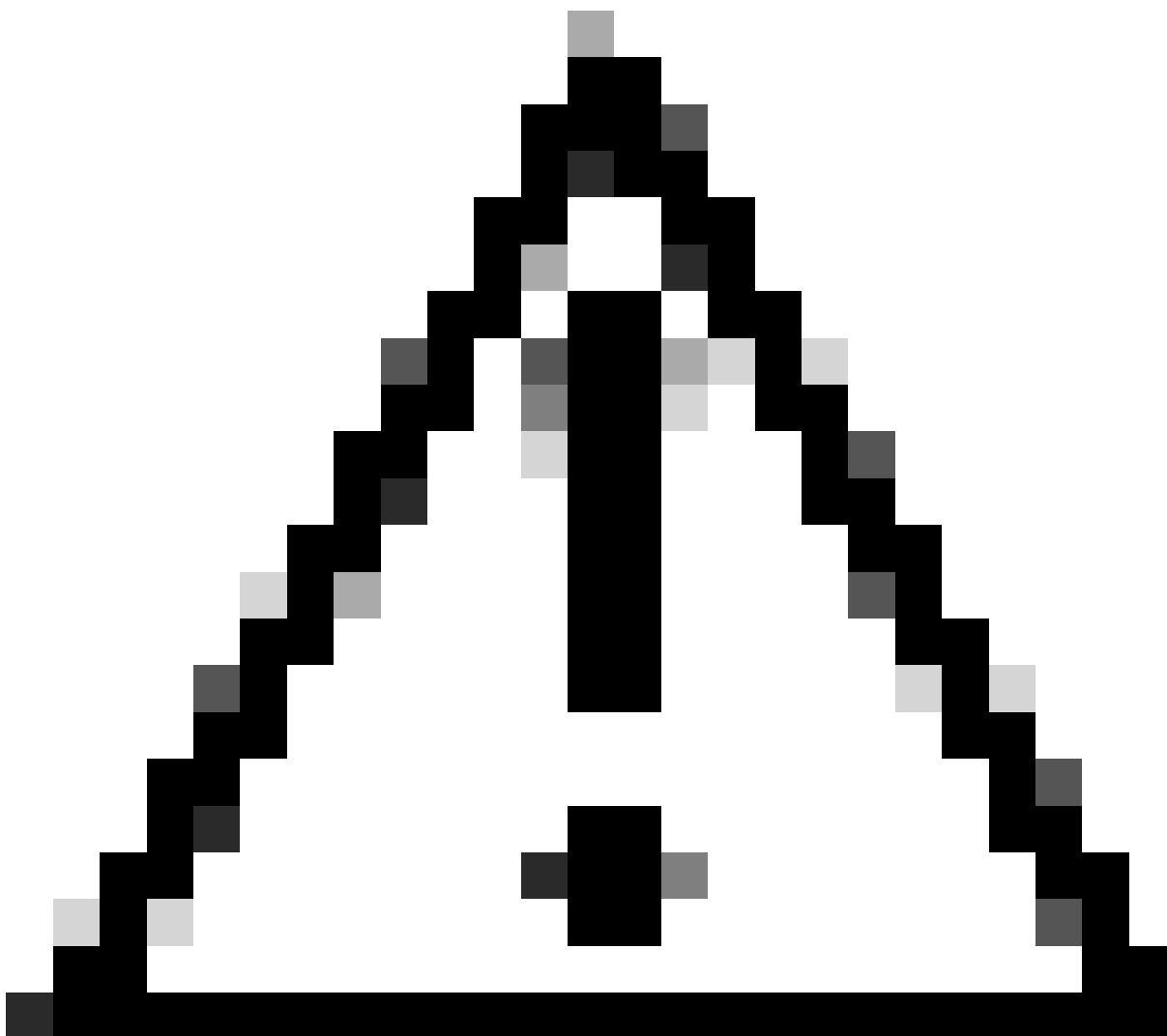
Policy Sets

Reset Reset Policy Set Hit Counts Save

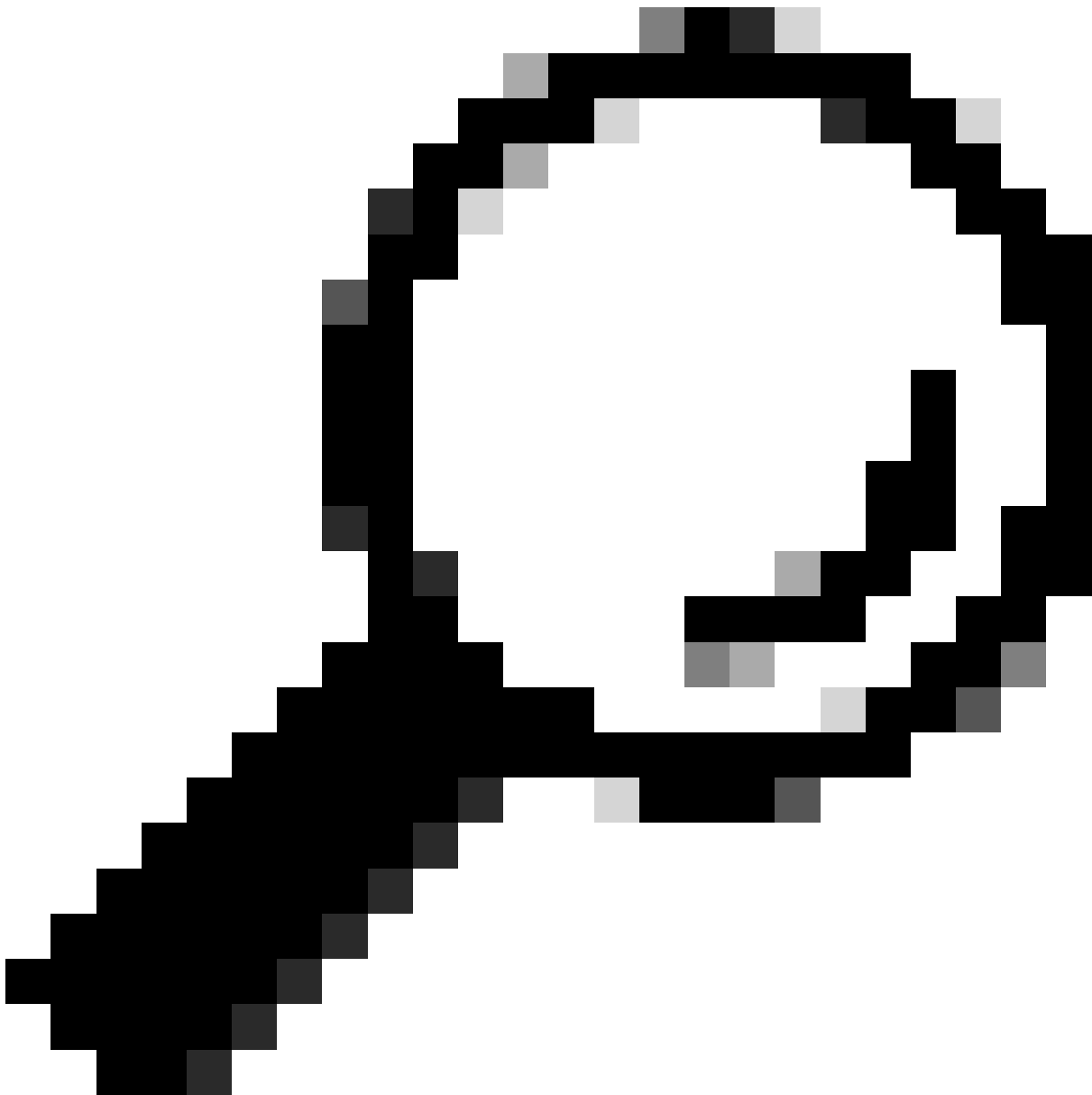
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
+	NX-OS Devices		DEVICE:Device Type EQUALS All Device Types#NXOS	Default Device Admin	0	+ ⚙	>

Passaggio 2. Fare clic su Salva 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 not found) e Se processo (If Process fail).



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.

Configurazione server TACACS+

Passaggio 1. Configurazione iniziale.

```
POD2IPN2# sho run tacacs
```

```
feature tacacs+
```

```
tacacs-server host 10.225.253.209 key 7 "F1whg.123"  
aaa group server tacacs+ tacacs2
```

```
server 10.225.253.209
use-vrf management
```

Configurazione del punto di trust

Passaggio 1. Creare un'etichetta di chiave, nel caso specifico utilizzare una coppia di chiavi ECC.

```
<#root>
```

```
POD2IPN2(config)#
```

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

Passaggio 2. Associare il punto di trust.

```
<#root>
```

```
POD2IPN2(config)#
```

```
crypto ca trustpoint ec521-tp
```

```
POD2IPN2(config-trustpoint)#
```

```
ecckeypair ec521-label
```

Passaggio 3. Installare la chiave pubblica CA.

```
<#root>
```

```
POD2IPN2(config)#
```

```
crypto ca authenticate ec521-tp
```

```
input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----BEGIN CERTIFICATE-----
```

```
MIIFlDCCA3ygAwIBAgIIIM10AsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZzAVBgNVBAGTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECXMdU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUGA1UECBM0Tm9ydGggQ2Fyb2xpbmExEDAOBgNVBACTB1JhbGVpZ2gxDjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTV1MxEjAQBgNVBAMTCVNWUyBMWJJDQTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZU0yn2vIn6gKbx3M7vaRq
2YjwZ1zSH6EkEvxnJTy+kksiFD33GyHQepk7vfp4NFU50tQ4HC7t/A0v9grDa3QW
VwvV4MBbJhFM3s0J/ejgDYcMZhIAaPy0Zo5WLboOkXEiKjPLatkXojB8FVrhLF3O
jMBSqwa4/Wlniy5S+7s4FFxsCf20COWfBAsnrs0tatIIhmcnx+VLJP7MRm8f0w4m
mutNo7IhbJSrgAFXmj1bBjMmgspObULO/wxMHdTbtPBf11HRHTkNIo3qy04UADL2
WpoGhgT/FaxxBo2UBcnYVaP+jjREONYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7B0e8oDNKU6gX1ojKyLP/gC7j8AeP03ir+KZui8
```

```
b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
gJ+kQXe7QtT/u6m1MrtjE3gAEVpL334rTIxy9hpKZIkB86t2ZA3JX8CLsbCa13sA
z1XCoONX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTA01xh60I4QnK+MNQKpTjt/E4
ydH10rrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVL1783nTc9wYptQEPi5sw
83g9EMgKV0ARIiVUa/q7AgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAyb4
QgEBBAQDAgAHMBkGCWCGSAGG+EIBDQQMFGpTV1MgTGF1IENBMAOGCSqGSIb3DQEB
CwUAA4ICAQAIT308oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oK0dGayi
iSEkSSX9qyfLFINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXRX67X+v
O+ja6zTQqj06lqJhmrSkyFbYf/ZTpe4d10zJsZjNsN0r8bF9nOA/7qNZLp3Z3cpU
PU0KdbiSvRqnPw3e8TFITVmAzcX8COI2SrYFMSUazo1VBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIEOf5ay1PKURO/8aj/B7a1uJapXkmnj5qPeGhN0pB
Q9r14reov4so2EspkXS7CrH9yGfPiYtprokz1UvZBZ8v1oI7YZmjFmem+5rT6Gnk
eU/1X7nV61SYG5W5K+I8uaKuyBHOMn7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggz1POdsS/i6Lo7ypYX0eB9HgVDckzQsLXQuHGj/2WsgPgDRcjkvnyURk4Jx+Ib
xDrmo7e0XPpSW4172a6K18CR3U2Cr4wsuvndPEq/qd2NRSBWffFOX/AJHQG7STT
HaXLU9r2Ko603oecu8ysGTWl1It/9T1/F0b0xZRugWcpJrVoTgDGuA==
-----END CERTIFICATE-----
```

END OF INPUT

Fingerprint(s): SHA1

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

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

POD2IPN2(config)#

POD2IPN2(config)#

show crypto ca certificates ec521-tp

Trustpoint: ec521-tp

CA certificate 0:

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

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

serial=20CD7402C4DA37F5

notBefore=Apr 28 17:05:00 2025 GMT

notAfter=Apr 28 17:05:00 2035 GMT

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

purposes: sslserver sslclient

POD2IPN2(config)#

Passaggio 4. Generare la richiesta del certificato di identità del commutatore.

<#root>

POD2IPN2(config)#

crypto ca enroll ec521-tp

Create the certificate request ..

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

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

Please make a note of it.

Password:Cisco.123

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

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

yes

The serial number in the certificate will be: FD026490P4T
Include an IP address in the subject name [yes/no]:

yes

ip address:10.225.253.177
Include the Alternate Subject Name ? [yes/no]:

no

The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
MIIBtjCCARcCAQAwKTERMA8GA1UEAwIUE9EMk1QTjIxFDASBgNVBAUTC0ZETzI2
NDkwUDRUMIGbMBAGByqGSM49AgEGBSuBBAAjA4GGAAQBGYT0iw7OvqIKQ/a22Lkg
Na9IhqWQvetjxKq485gqTSBEo6Lzpk0hPAGE4jBveNHxYeIA7PfNwvJ7xTBWjDNX
/IYBm6E7Hd7q420mCe8Mef+bqJBdJ9wzpyEjhI21IIoXt4814nBx0bkIWwYR5cZN
IiXtLk8P4IMZvPq8jRnELRxd8RGgSTAYBgkqhkiG9w0BCQcxCwwJQzFzY28uMTIz
MCOGCSqGSIB3DQEJJDjEgMB4wHAYDVRORAQH/BBIwEIIIUE9EMk1QTjKHBArh/bEw
CgYIKoZIZj0EAWIDgYwAMIGIAkIAtzQ/knrW2ovCVoHAuq1v2cr0n3NenS/441u1
+3H1y52vn4Rm4CGU3wkzXU3qG03YjhNjCXjhp3+uN2afFf1Wf3ECQgC4bumHVsfj
b5rwPIC5tvXS/A8upqIzqc0yt30hpaDDOTwzzvZY7qFf1C015p6pvUpHigqoZNg5
9xhNdM1CQSyk0g==
-----END CERTIFICATE REQUEST-----

Passaggio 5. Importare il certificato di identità dello switch firmato dall'autorità di certificazione.

<#root>

POD2IPN2(config)#

crypto ca import ec521-tp certificate

input (cut & paste) certificate in PEM format:

-----BEGIN CERTIFICATE-----
MIIDzTCCABwGAWIBAgIIC6zS76XYDm8wDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZmFzAVBGNVBAgTdk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWx1aWdo
MQ4wDAYDVQQKEwVDAxNjBzEMMAoGA1UECXMdU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcnNMjUwNTA3MTkxMDAwWhcnNMjUwNTA3MTkxMDAwWjApMREwDwYDVQQDDAhQ
TOQySVBOMjEUMBIGA1UEBRMLRkRPMjY0OTBQNFQwgZswEAYHkoZIZj0CAQYFK4EE
ACMDgYYABAEZhPSLDS6+ogpD9rbYuSA1r0iGpZC962PEqrjzmCpNIESjov0mQ6E8
AYTiMG940fFh4gDs981a8nvFMFaMM1f8hgGboTsd3urjY6YJ7wx5/5uokF0n3D0n
ISOEjaUgihe3jzXicHE5uQhZbJH1xk0iJdMuTw/ggxm8+ryNGCQtHF3xEaNAMD4w
HgYJYIZIAyb4QgENBBEWD3hjYSBjZXJ0aWZpY2F0ZTAzBgNVHREBAf8EEjAQgghQ
TOQySVBOMocECuH9sTANBgkqhkiG9w0BAQsFAAOCAgEANWGb6zm9TDPaM1yhPMx7
8uai/pF7VQC8NScdOKqr4w4+695ZjJuzqFL3msod0QK0EdgxpQ4+pEa5msRtK0i8
mms2X/Px3/EShxoHrZ01PUXNTyZidXpGd/yTrdQA15JzpW4pEudrbCJMZEETqoP
wD+40E8vKoYEgyW1DrpRZ0ZG1usZczuUhLZ8orkjXMhWC26Q5aqiCKkyg10Nt6nb
1iToeYy2Q0cTesSZCKvRBv6Ewj5JuSLeMURyB4GHY+LT+A9UNmEUM2n+OSVEL329
3hS0qd/YVaEuxjjlg7jNiZb+UsW7IRx3Q8Rouo++ISACpH/PJ61Ln1VxhXombiS6
INoa0GvQONr1+1FT8ADidZ/Ukd5Ubhc9bh/sYzf4MwtK1wV016Hv7vGpSMYonD6
a271im+tJPYKneezQ60yKz1GqsL/Ta6J0dip/fEYp8UmRq9InDh23gDjqrojWL7k
1R/bZpc+baMYXd/2pohHMSN0sKN3zNrJT1nuk5KCqFx//4P7mAoyZYiTiDp1pkYS
VK65fJKD+pYxIhSP9wN8rnwtzSCWb0Z78sg006Y6wIXyTP0UB3FWhD+GxtTkmEce
ZnAQbgxpgrg51hpAEVabpC/zRU4UzTuBmv/WoY12zwXCr5WLXEOWtIe8CwFjSnch

```
1fKuuebdZkbwz72r70yyX/U=
-----END CERTIFICATE-----
POD2IPN2(config)#
```

Verificare che il certificato di identità dello switch sia registrato.

```
<#root>
```

```
POD2IPN2(config)#
```

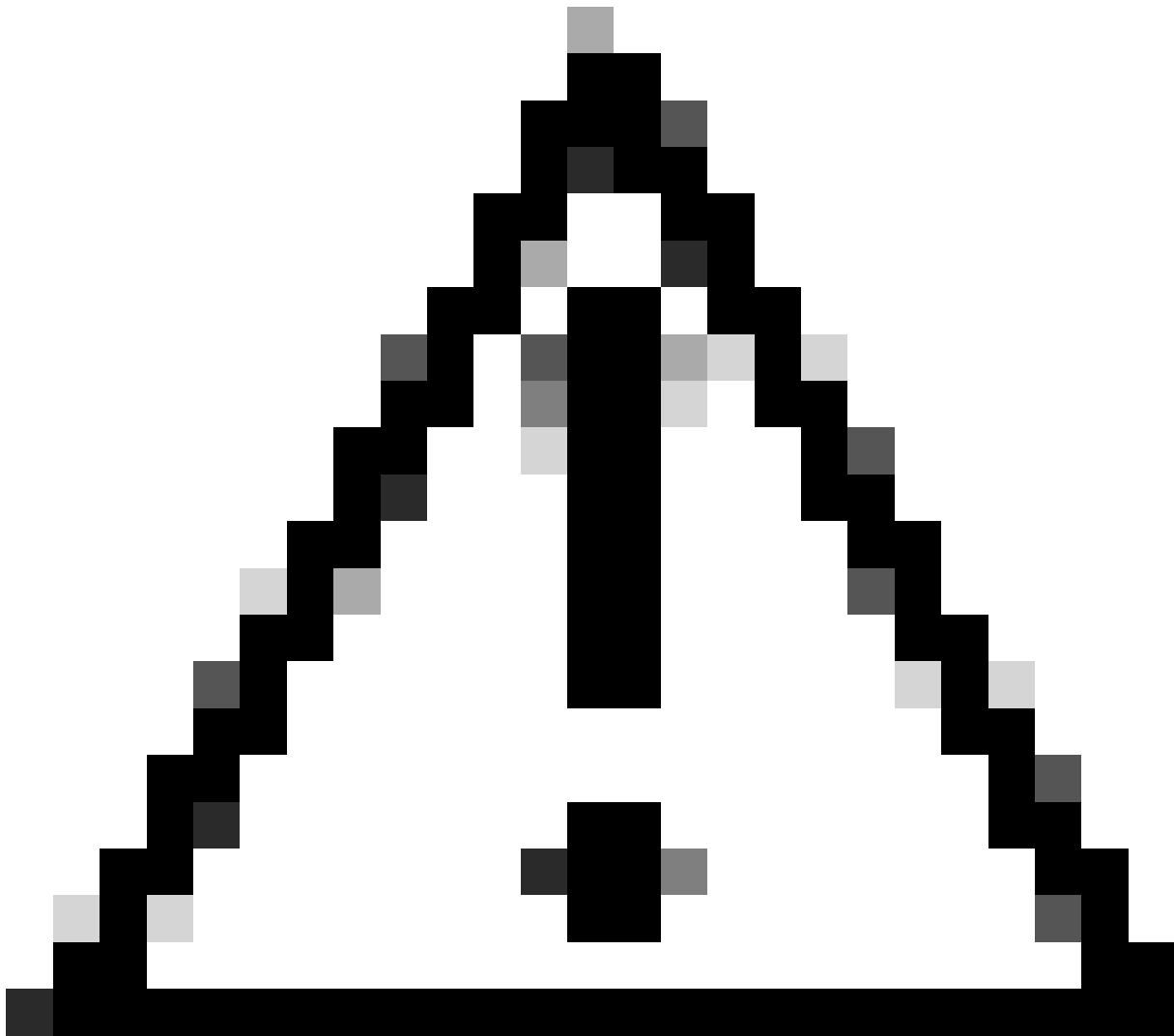
```
show crypto ca certificates ec521-tp
```

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

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

```
POD2IPN2(config)#
```

Configurazione TACACS+ TLS



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

Passaggio 1. Configurare i TAC globali.

```
<#root>
```

```
POD2IPN2(config)#
```

```
tacacs-server secure tls
```

Passaggio 2. Modificare la porta ISE in porta TLS con cui è configurato il server ISE.

```
<#root>
```

```
POD2IPN2(config)#
```

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

Passaggio 3. Associare il server ISE configurato sullo switch al trust point per la connessione TLS.

```
<#root>
```

```
POD2IPN2(config)#
```

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

Passaggio 4. Creare il gruppo di server TACACS.

```
<#root>
```

```
POD2IPN2(config)#
```

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

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

```
server 10.225.253.209
```

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

```
use-vrf management
```

Passaggio 5. Verificare la configurazione.

```
<#root>
```

```
POD2IPN2#
```

```
sho run tacacs
```

```
feature tacacs+
```

```
tacacs-server secure tls
```

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

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

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

```
server 10.225.253.209
```

```
use-vrf management
```

Passaggio 6. Verificare l'utente remoto prima di configurare l'autenticazione AAA.

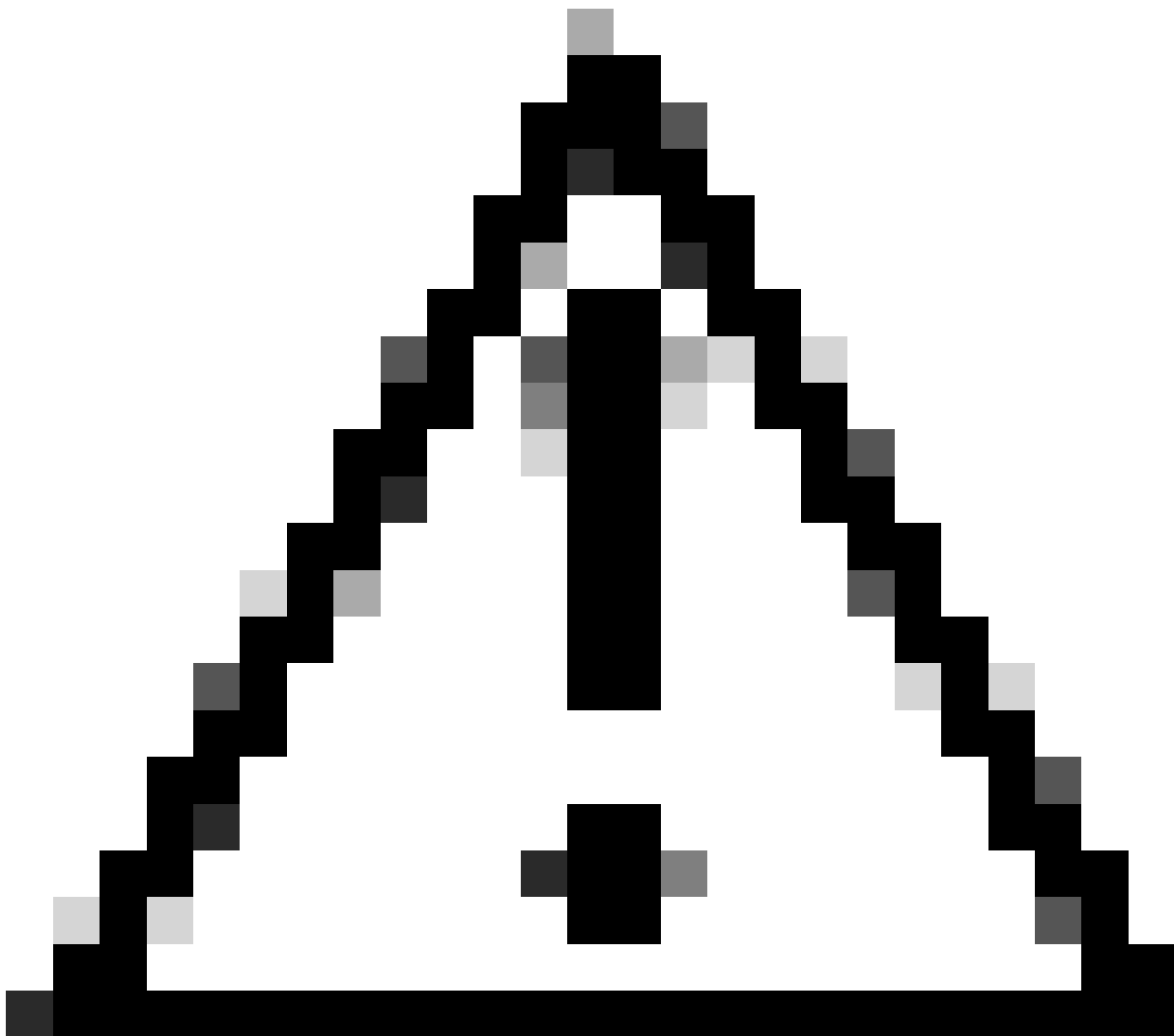
```
<#root>
```

POD2IPN2#

test aaa group tacacs2

user has been authenticated
POD2IPN2#

Configurazione AAA



Attenzione: Accertarsi che l'autenticazione dell'utente remoto sia stata eseguita

correttamente prima di procedere con le configurazioni AAA.

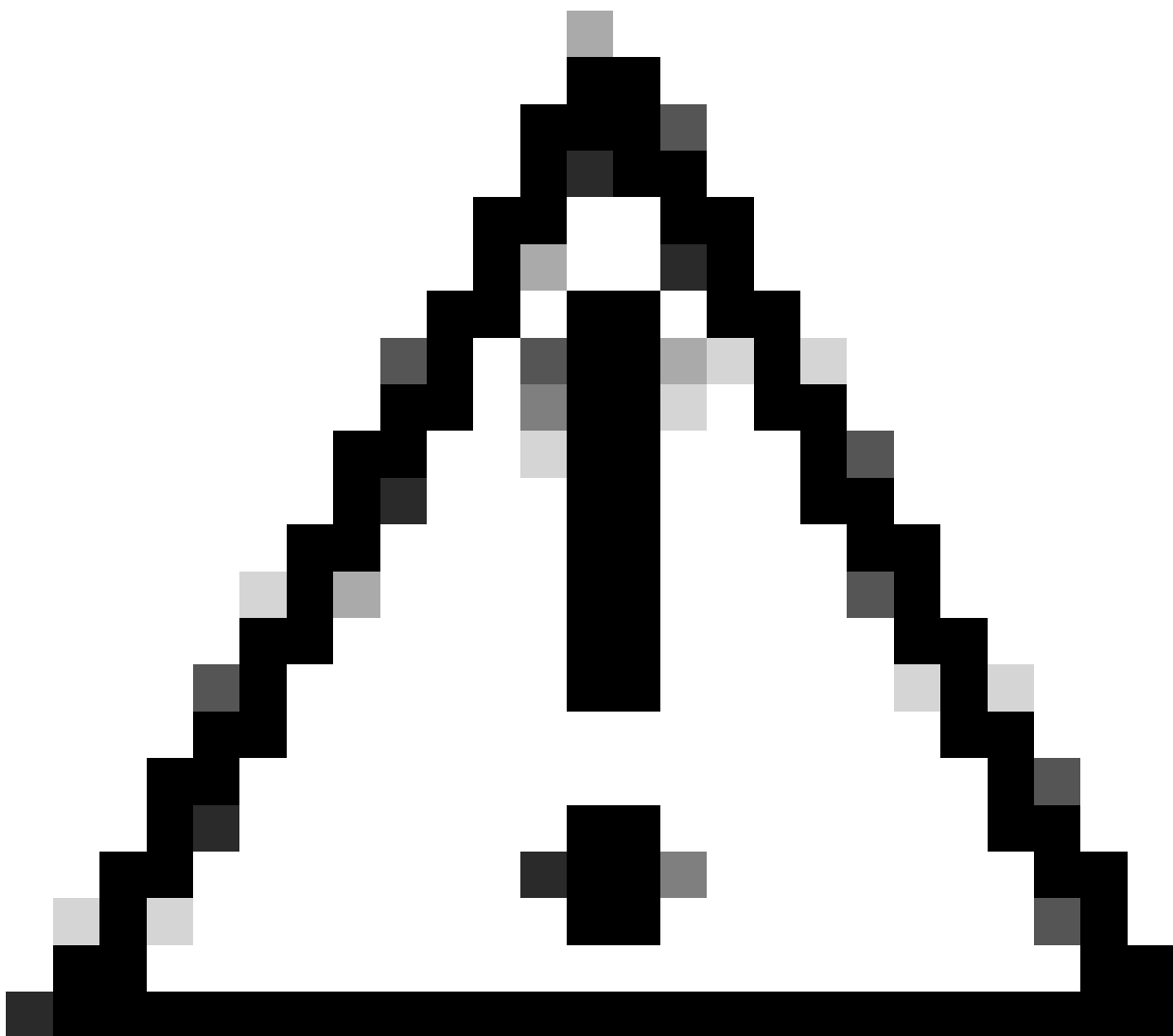
Passaggio 1. Configurare l'autenticazione remota AAA.

```
<#root>
```

```
POD2IPN2(config)#
```

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

Passaggio 2. Configurare l'autorizzazione remota AAA dopo aver verificato il comando.



Attenzione: Accertarsi di visualizzare authorization-status come "AAA_AUTHOR_STATUS_PASS_ADD.

```
<#root>
```

```
POD2IPN2#
```

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

```
command "feature bgp"
```

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

Passaggio 3. Configurare il comando AAA e l'autorizzazione config-command.

```
<#root>
```

```
POD2IPN2(config)#
```

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

```
POD2IPN2(config)#
```

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

Test e risoluzione dei problemi di accesso utente per NX-OS

Verifica

Configurazione per l'amministrazione dei dispositivi per Cisco NX-OS completata. È necessario convalidare la configurazione.

Passaggio 1. SSH e accedere ai dispositivi NX-OS come ruoli diversi.

Passaggio 2. Nell'interfaccia della riga di comando (CLI) del dispositivo, verificare che l'utente abbia accesso ai comandi corretti. Ad esempio, un utente dell'help desk deve essere in grado di eseguire il ping di un indirizzo IP normale (ad esempio, 10.225.253.129), ma gli viene negato di visualizzare la configurazione corrente.

```
POD2IPN1# ping 10.225.253.129 vrf management  
PING 10.225.253.129 (10.225.253.129): 56 data bytes  
64 bytes from 10.225.253.129: icmp_seq=0 ttl=254 time=0.817 ms  
64 bytes from 10.225.253.129: icmp_seq=1 ttl=254 time=0.638 ms  
64 bytes from 10.225.253.129: icmp_seq=2 ttl=254 time=0.642 ms  
64 bytes from 10.225.253.129: icmp_seq=3 ttl=254 time=0.651 ms  
64 bytes from 10.225.253.129: icmp_seq=4 ttl=254 time=0.712 ms
```

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

Risoluzione dei problemi

Convalida della configurazione NX-OS.

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

Per visualizzare le connessioni utente e i ruoli, utilizzare questi comandi.

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

Di seguito vengono riportati alcuni utili debug per la risoluzione dei problemi relativi a TACACS+:

```
debug TACACS+ aaa-request
2016 Jan 11 03:03:08.652514 TACACS[6288]: process_aaa_tplus_request:Checking for state of mgmt0 port w
2016 Jan 11 03:03:08.652543 TACACS[6288]: process_aaa_tplus_request: Group demoTG found. corresponding
2016 Jan 11 03:03:08.652552 TACACS[6288]: process_aaa_tplus_request: checking for mgmt0 vrf:management
2016 Jan 11 03:03:08.652559 TACACS[6288]: process_aaa_tplus_request:port_check will be done
2016 Jan 11 03:03:08.652568 TACACS[6288]: state machine count 0
2016 Jan 11 03:03:08.652677 TACACS[6288]: is_intf_up_with_valid_ip(1258):Proper IOD is found.
2016 Jan 11 03:03:08.652699 TACACS[6288]: is_intf_up_with_valid_ip(1261):Port is up.
2016 Jan 11 03:03:08.653919 TACACS[6288]: debug_av_list(797):Printing list
2016 Jan 11 03:03:08.653930 TACACS[6288]: 35 : 4 : ping
2016 Jan 11 03:03:08.653938 TACACS[6288]: 36 : 12 : 10.1.100.255
2016 Jan 11 03:03:08.653945 TACACS[6288]: 36 : 4 : <cr>
2016 Jan 11 03:03:08.653952 TACACS[6288]: debug_av_list(807):Done printing list, exiting function
2016 Jan 11 03:03:08.654004 TACACS[6288]: tplus_encrypt(659):key is configured for this aaa sessin.
2016 Jan 11 03:03:08.655054 TACACS[6288]: num_inet_addrs: 1 first s_addr: -1268514550 10.100.1.10 s6_a
```

```
2016 Jan 11 03:03:08.655065 TACACS[6288]: non_blocking_connect(259):interface ip_type: IPV4
2016 Jan 11 03:03:08.656023 TACACS[6288]: non_blocking_connect(369): Proceeding with bind
2016 Jan 11 03:03:08.656216 TACACS[6288]: non_blocking_connect(388): setsockopt success error:22
2016 Jan 11 03:03:08.656694 TACACS[6288]: non_blocking_connect(489): connect() is in-progress for serv
2016 Jan 11 03:03:08.679815 TACACS[6288]: tplus_decode_authen_response: copying hostname into context
```

Abilitare il debug SSL.

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

Mostra contenuto file di debug.

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

Dalla GUI di ISE, selezionare Operations > TACACS LiveLog. In questa sezione vengono acquisite tutte le richieste di autenticazione e autorizzazione TACACS e il pulsante Dettagli fornisce informazioni dettagliate sul motivo per cui una particolare transazione ha avuto esito positivo o negativo.

Identity Services Engine

Operations / TACACS

Evaluation Mode 80 Days

Live Logs

Refresh Every 10 sec... Show Latest 20 reco... Within Last 3 hours

Export To Filter

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device...	Network Di
			Identity		Authentication Policy	Authorization Policy	Ise Node	Network Device N	Network Dev
May 15, 2025 07:39:57.081 PM	✓	🔒	Admin-ro	Authorization		Test NXOS >> Authorization Rule RD	ISE1	POD2IPN1	10.225.253.1
May 15, 2025 07:39:57.061 PM	✓	🔒	Admin-ro	Authentication	Test NXOS >> Default		ISE1	POD2IPN1	10.225.253.1
May 15, 2025 07:39:54.462 PM	✓	🔒	pamemart	Authorization		Test NXOS >> Authorization Rule RW	ISE1	POD2IPN1	10.225.253.1
May 15, 2025 07:39:54.443 PM	✓	🔒	pamemart	Authentication	Test NXOS >> Default		ISE1	POD2IPN1	10.225.253.1

Per i rapporti storici: Passare a Centri di lavoro > Amministrazione dispositivi > Report > Amministrazione dispositivi per ottenere i report di autenticazione, autorizzazione e accounting.

Overview

Identities

User Identity Groups

Ext Id Sources

Network Resources

Policy Elements

Device Admin Policy Sets

Reports

Settings

Export Summary

My Reports

Reports

Device Administration Reports

TACACS Authentication

TACACS Authorization

TACACS Command Accounting

Top N Authentication by Failure Reason

Top N Authentication by Network Device

Top N Authentication by User

Scheduled Reports

TACACS Authentication

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

Reports exported in last 7 days 0

Add to My Reports

Export To

Schedule

Filter

Refresh

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

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).