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

Sommario

Introduzione

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

Panoramica

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

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

Utilizzo della Guida

Questa guida divide le attività in due parti per consentire ad ISE di gestire l'accesso amministrativo per i dispositivi di rete basati su Cisco IOS XE.
· Parte 1 - Configurazione di ISE per l'amministrazione dei dispositivi
· Parte 2 - Configurazione di Cisco IOS XE per TACACS+ over TLS

Prerequisiti

Requisiti

Requisiti per configurare TACACS+ over TLS:

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

Componenti usati

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

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

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

Licenze

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

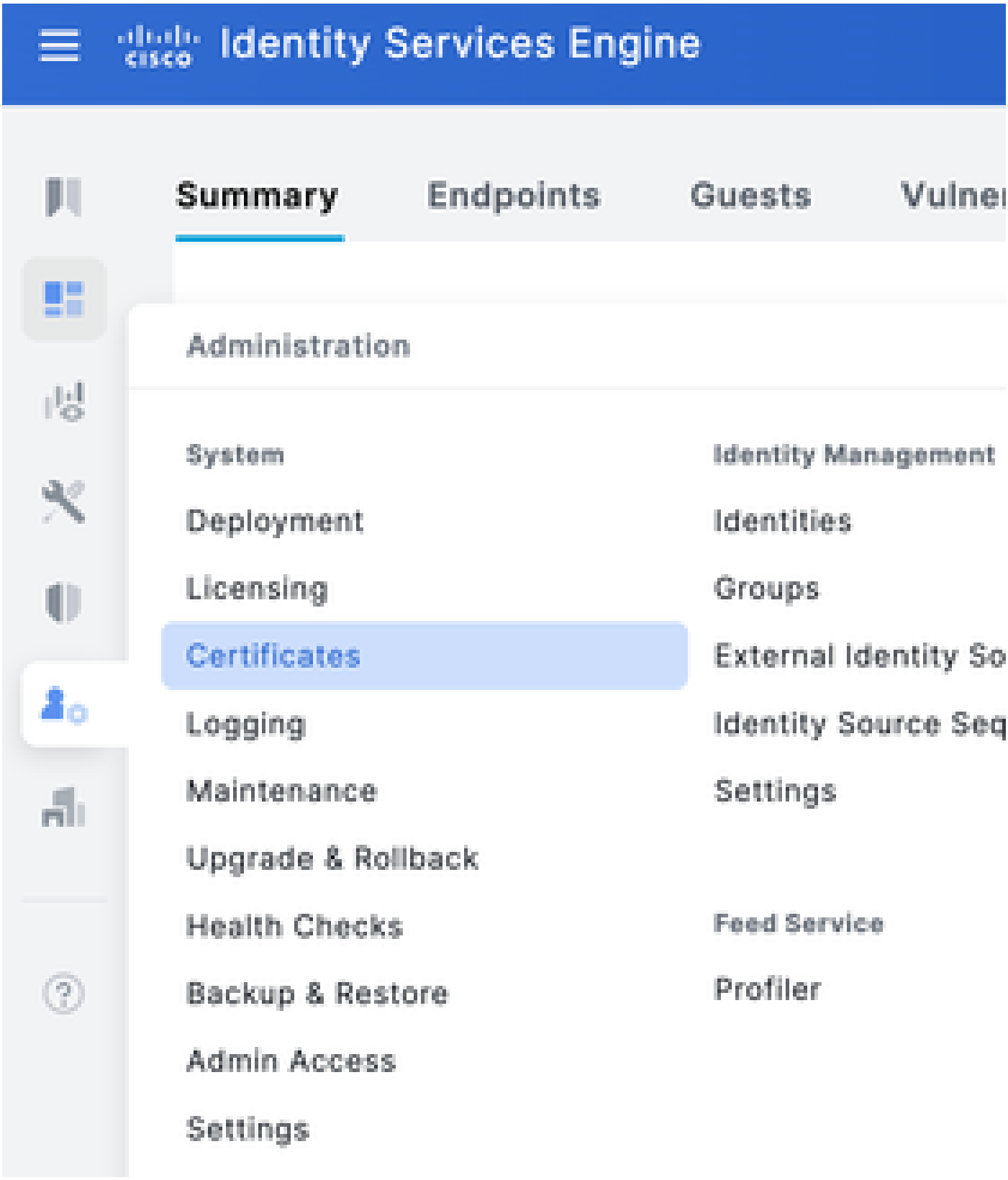
Parte 1 - Configurare ISE per l'amministrazione dei dispositivi

Genera richiesta di firma del certificato per autenticazione server TACACS+

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

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

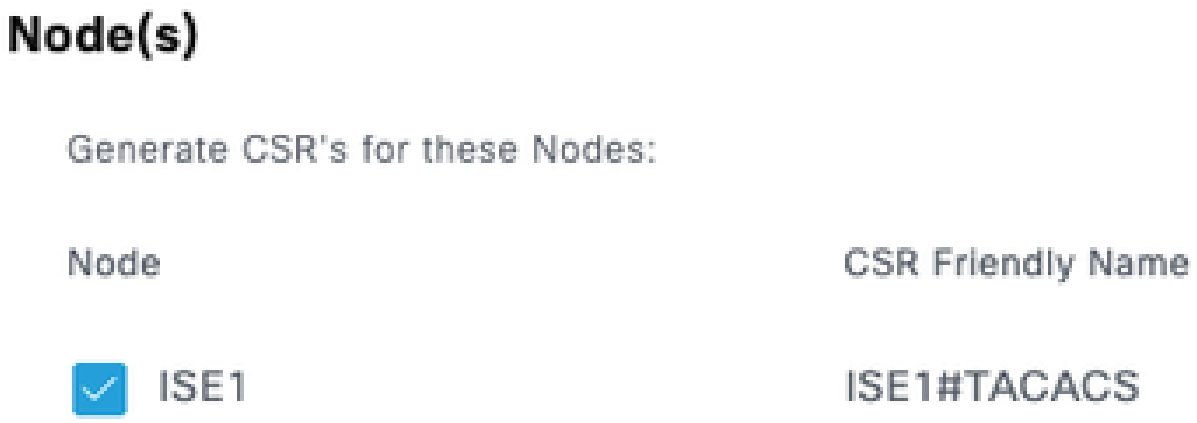
Passare alla fase 2. Passare ad Amministrazione > Sistema > Certificati.



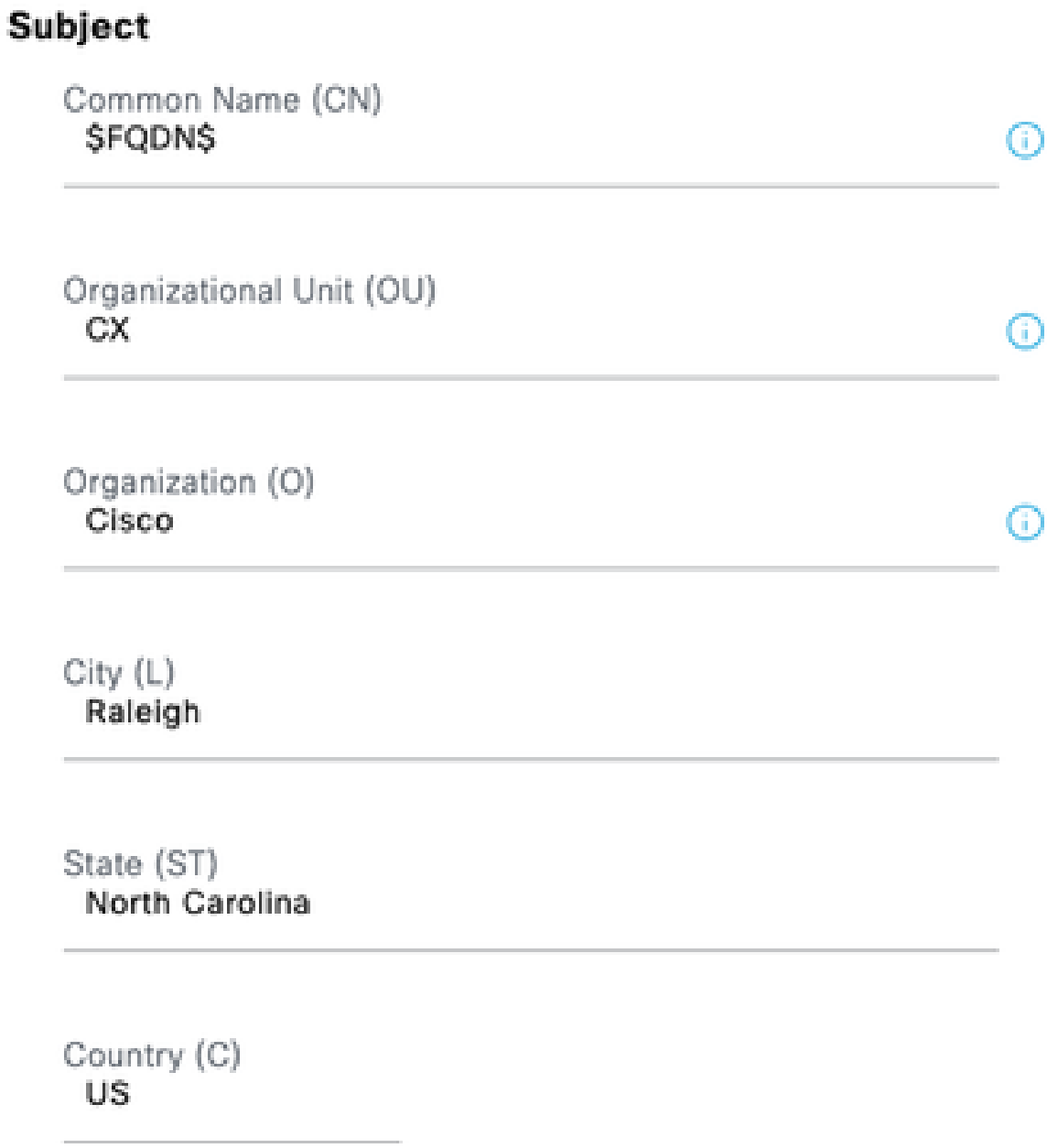
Passaggio 3. In Richieste di firma del certificato fare clic su Genera richiesta di firma del certificato.

Passaggio 4. Selezionare TACACS in Usage.

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

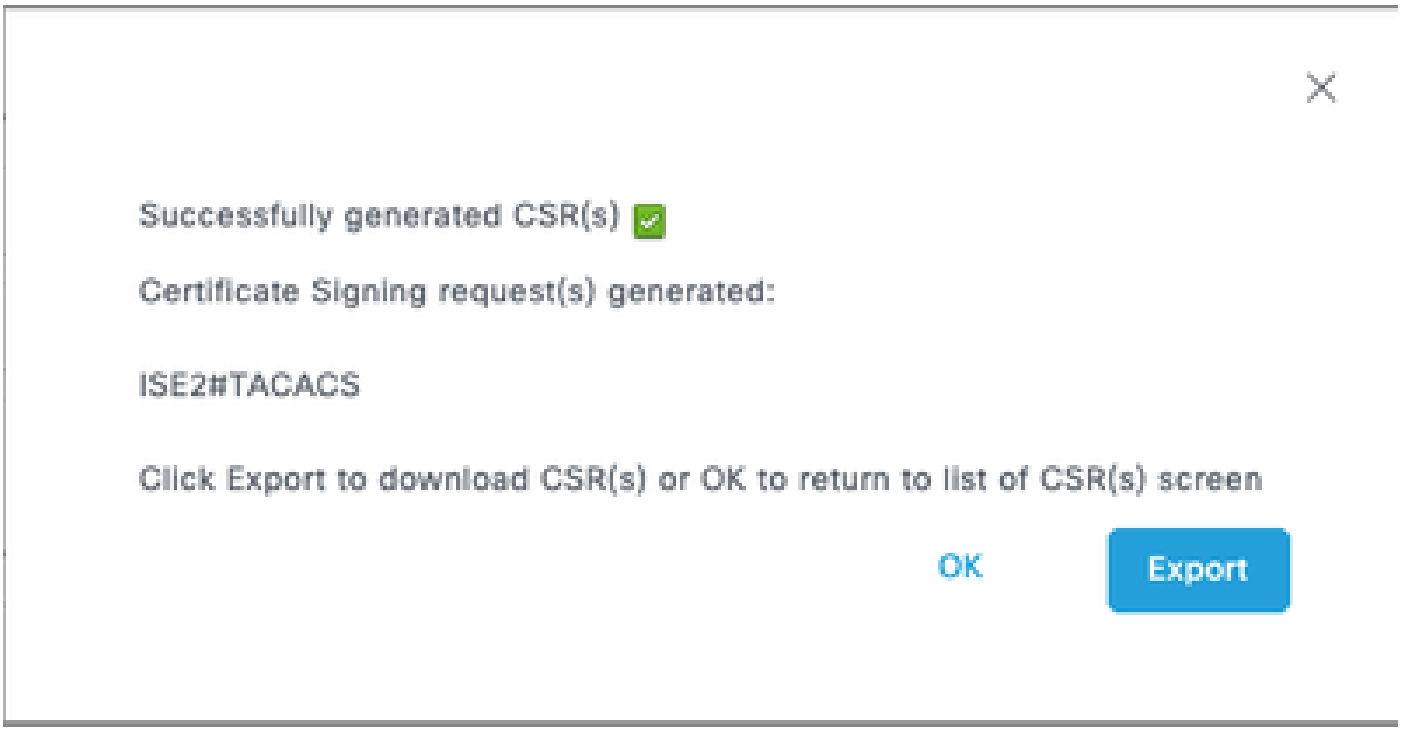


Passaggio 6. Inserire le informazioni appropriate nei campi Oggetto.



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

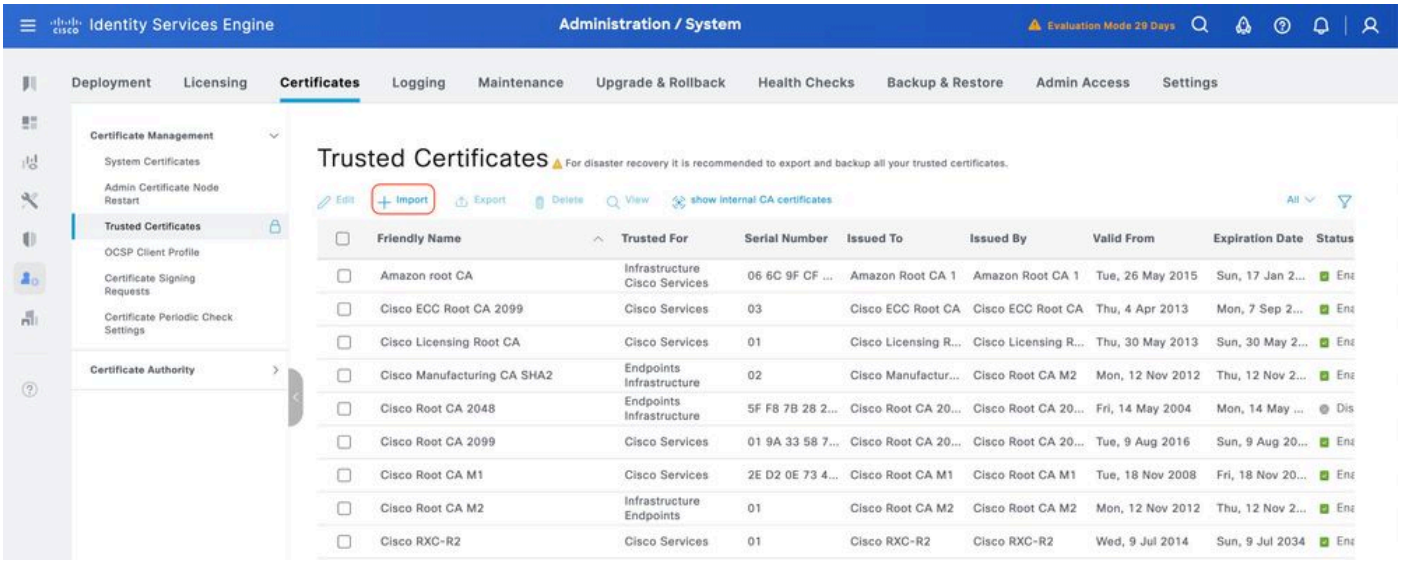
Passaggio 8. Fare clic su Genera, quindi su Esporta.



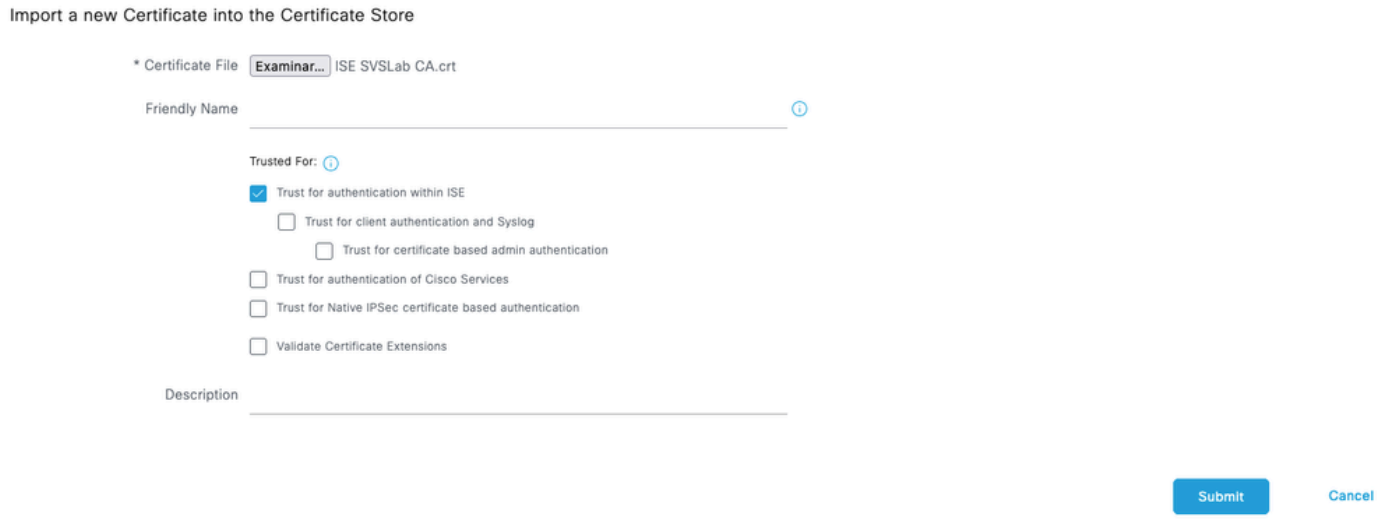
A questo punto, è possibile far firmare il certificato (CRT) all'autorità di certificazione (CA).

Carica certificato CA radice per autenticazione server TACACS+

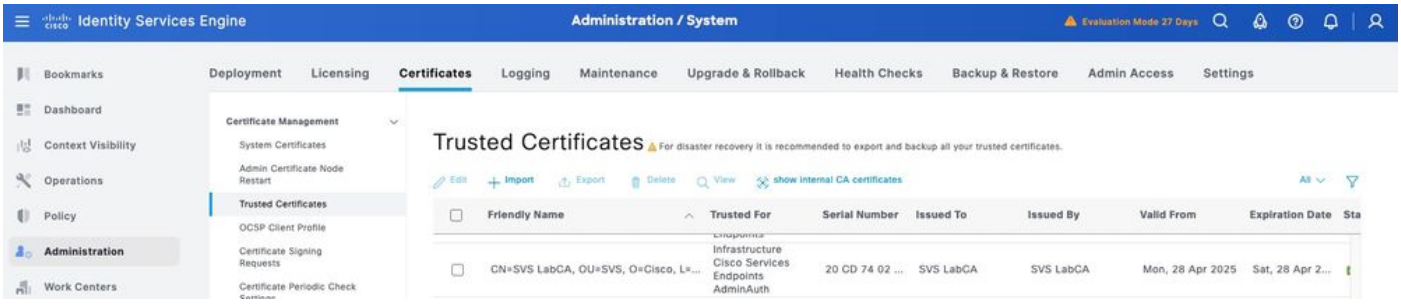
Passaggio 1. Passare ad Amministrazione > Sistema > Certificati. In Certificati attendibili fare clic su Importa.



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



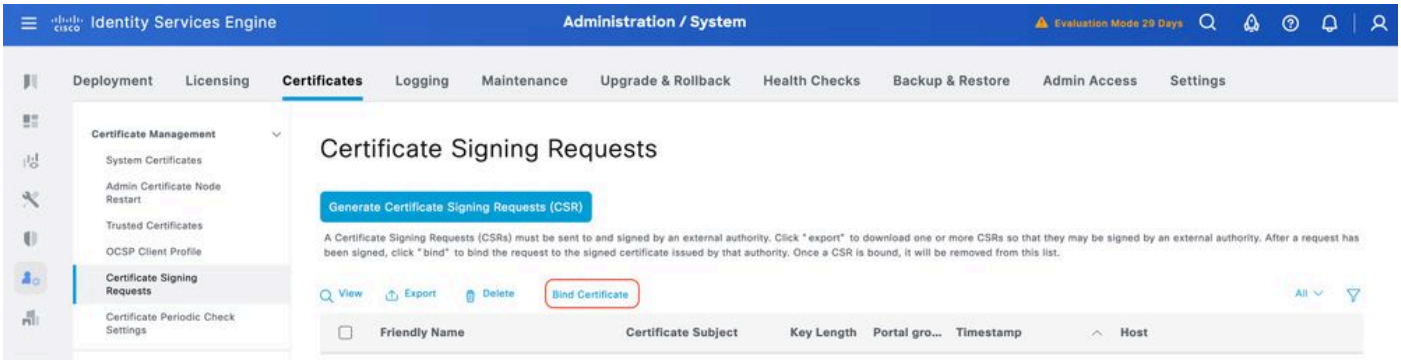
Passaggio 3. Fare clic su Invia. Il certificato deve essere visualizzato in Certificati attendibili.



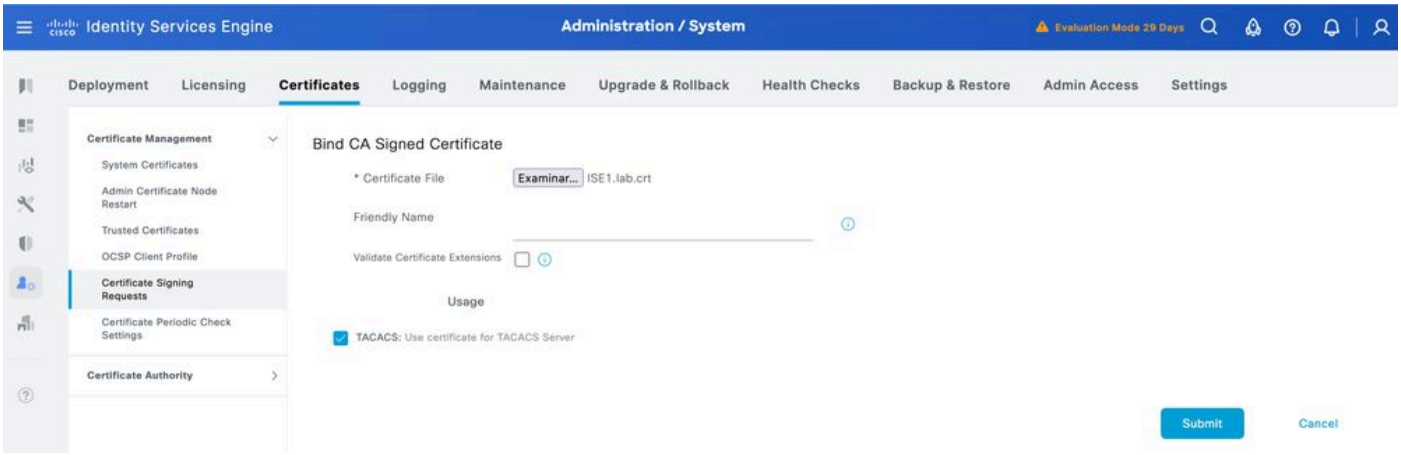
Associare la richiesta di firma del certificato (CSR) firmata a ISE

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.

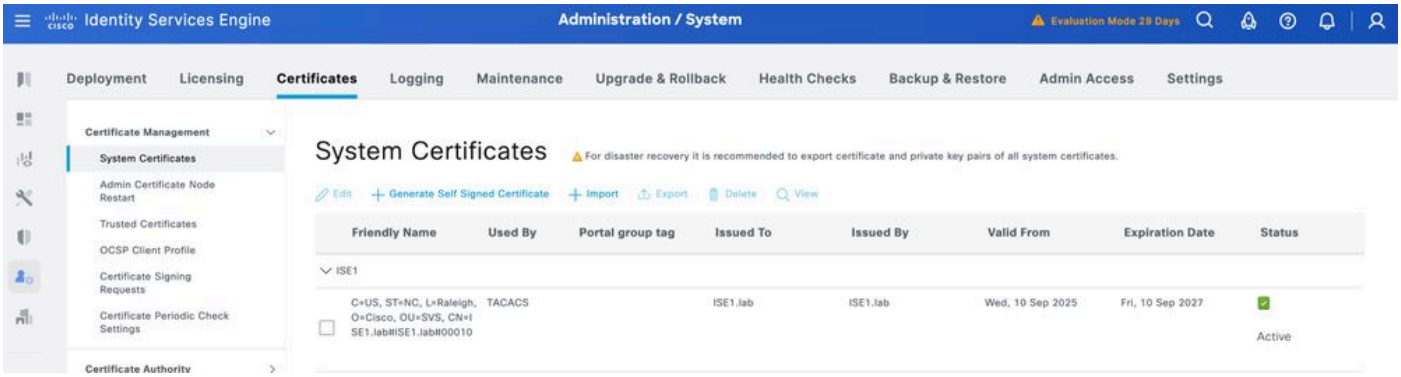


Passaggio 2. Selezionare il certificato firmato e assicurarsi che la casella di controllo TACACS in Uso rimanga selezionata.



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

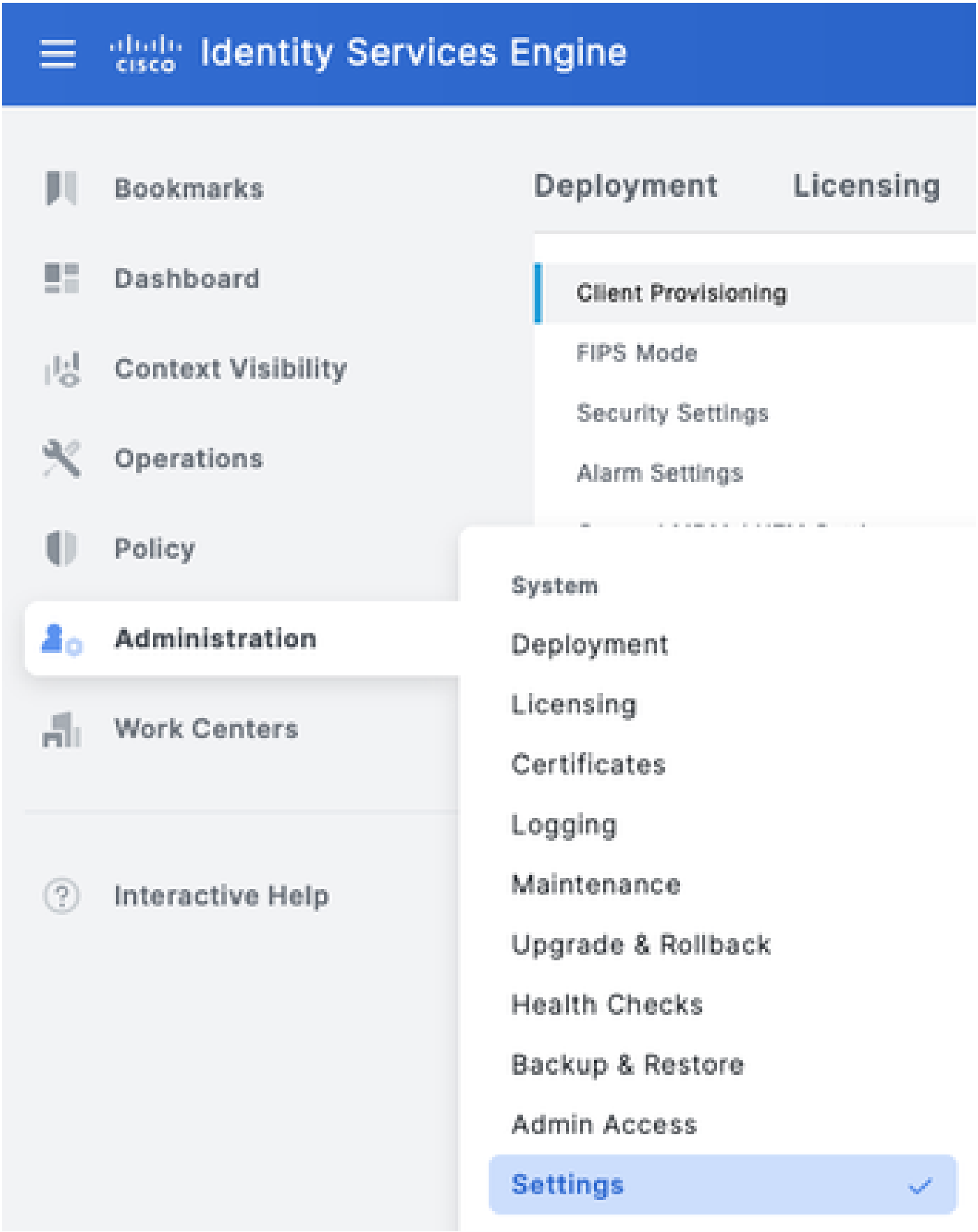
A questo punto è necessario installare correttamente il certificato. È possibile verificare questa condizione in Certificati di sistema.



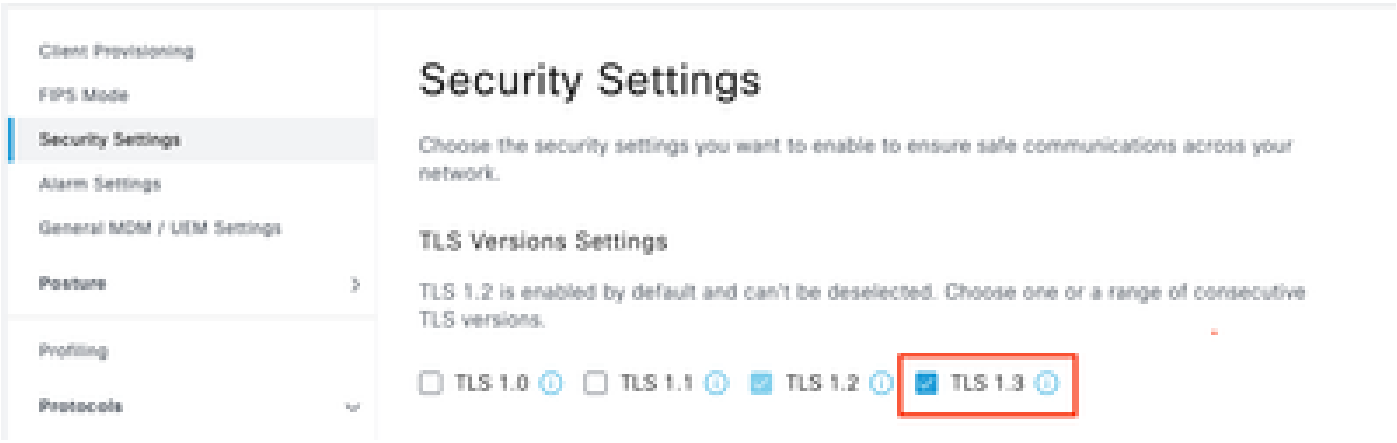
Abilita TLS 1.3

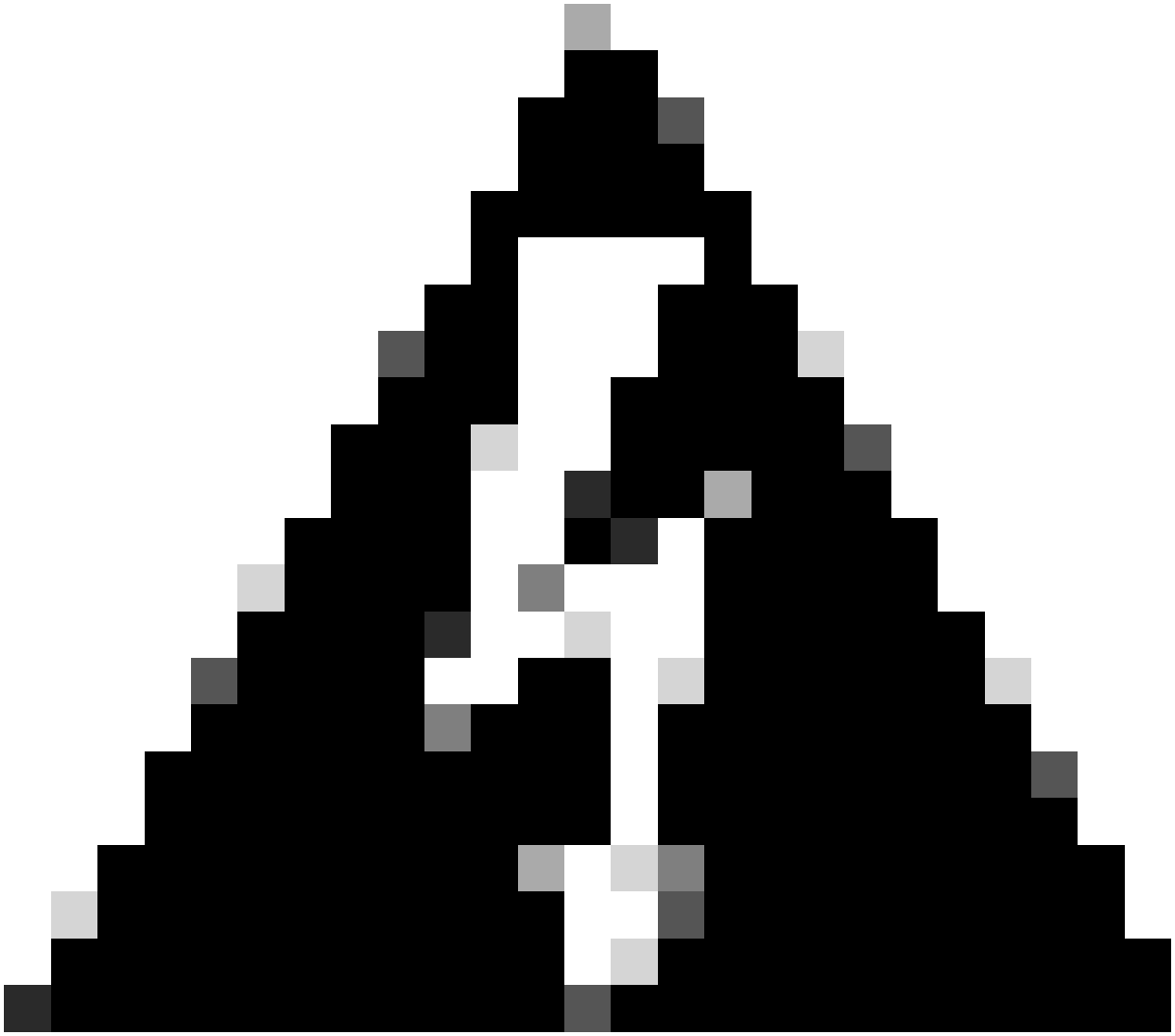
TLS 1.3 non è abilitato per impostazione predefinita in ISE 3.4.x. Deve essere attivata manualmente.

Passaggio 1. Passare a Amministrazione > Sistema > Impostazioni.



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.



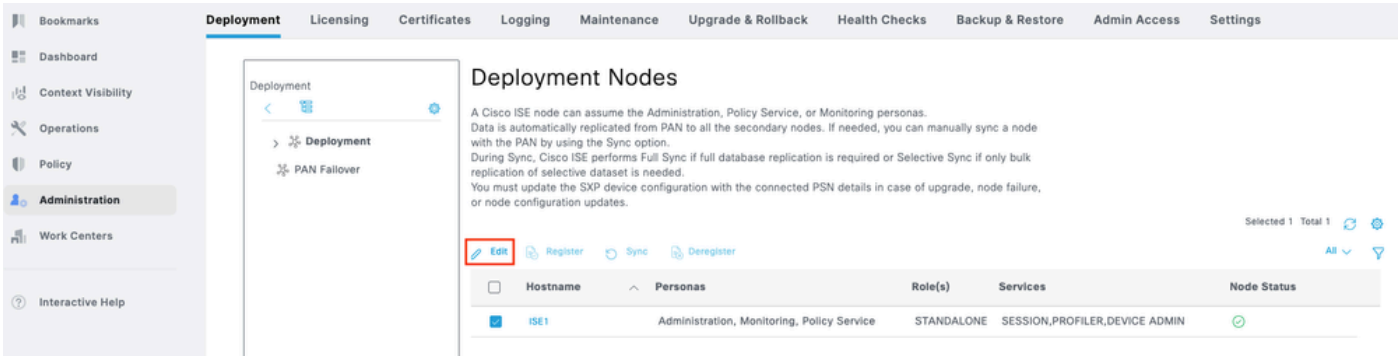


Avviso: Quando si modifica la versione TLS, il server applicazioni Cisco ISE viene riavviato su tutti i computer di implementazione di Cisco ISE.

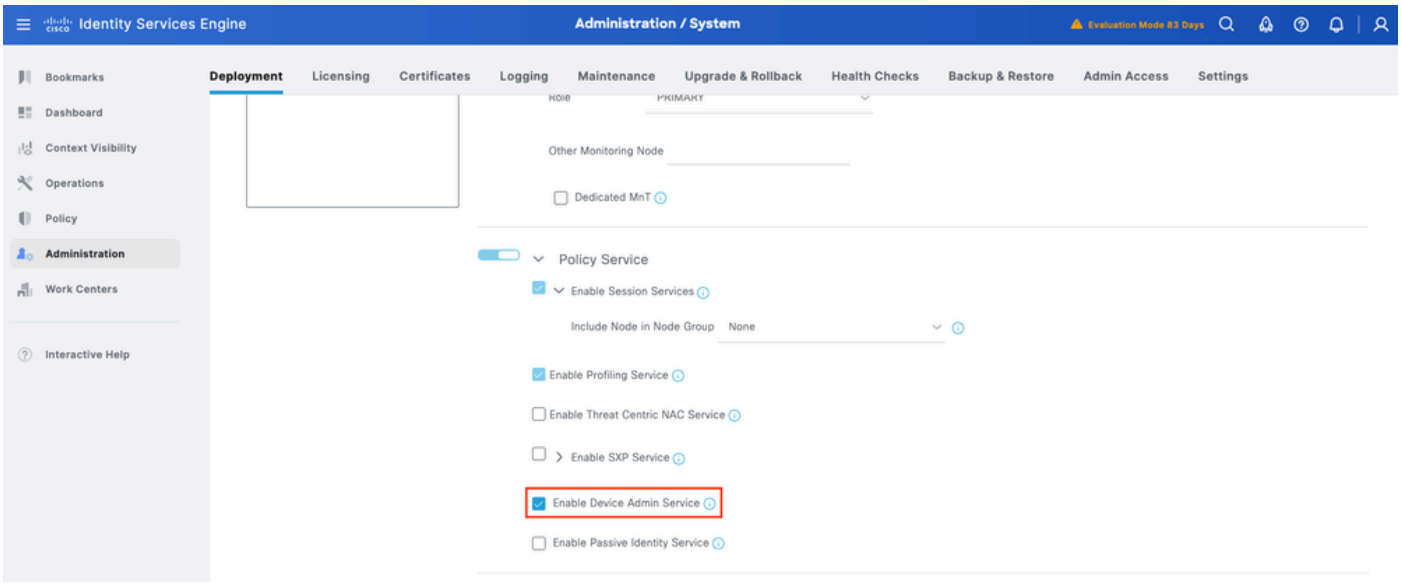
Abilita amministrazione dispositivi su ISE

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

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



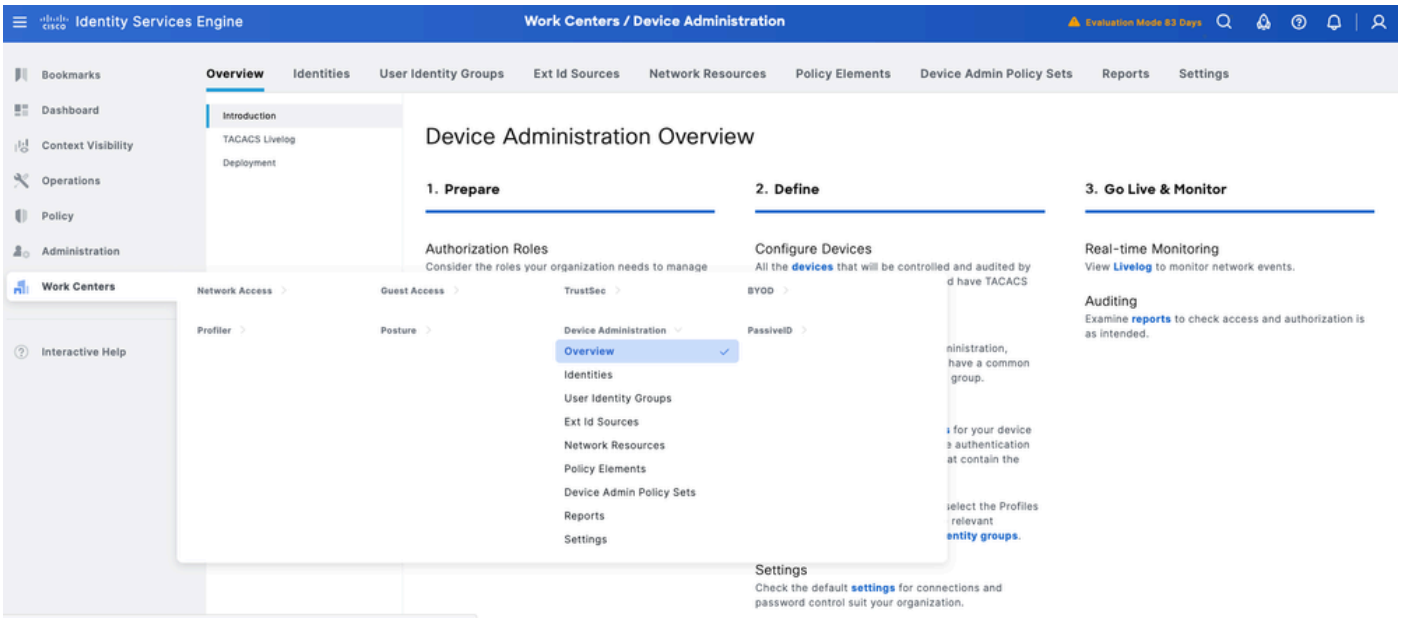
Passaggio 2. In GeneralSettings, scorrere verso il basso e selezionare la casella di controllo accanto a Enable Device Admin Service (Abilita servizio di amministrazione dispositivi).



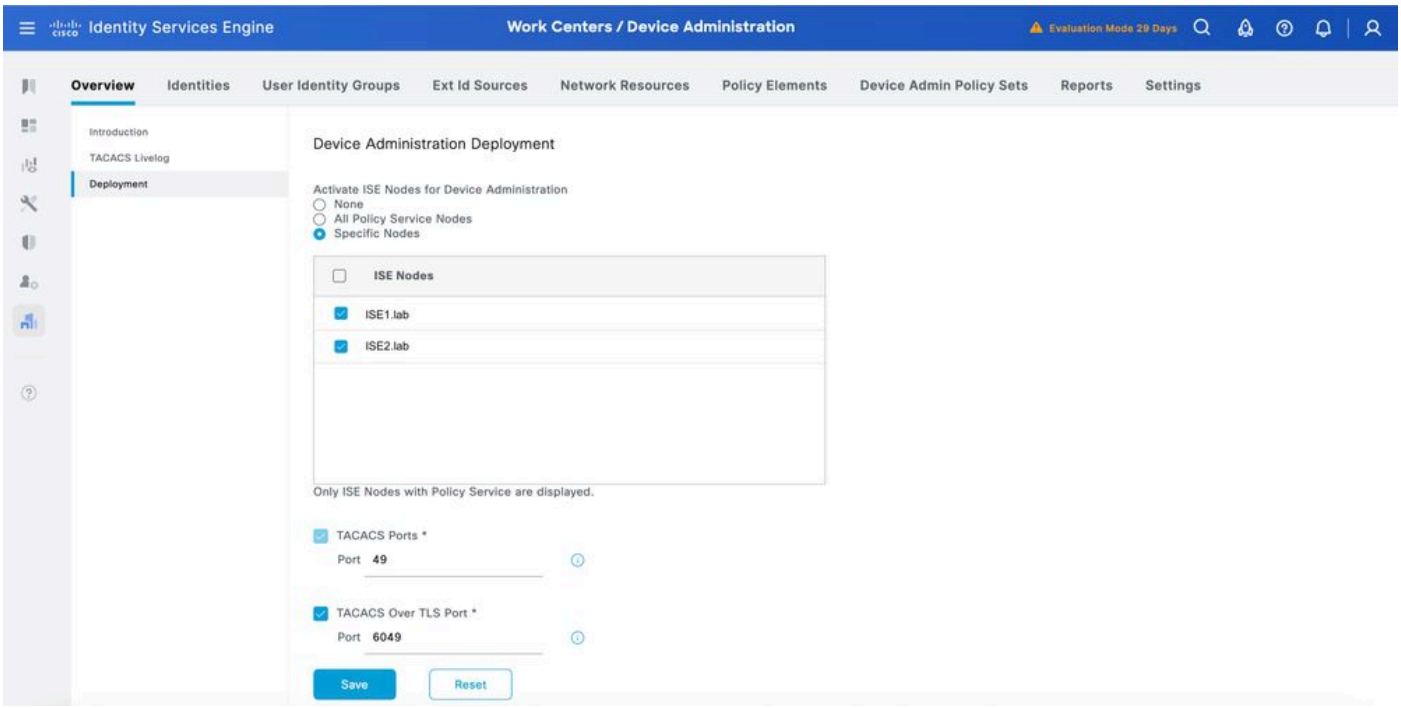
Passaggio 3. Salvare la configurazione. Device Admin Service è ora abilitato su ISE.

Abilita TACACS su TLS

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



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

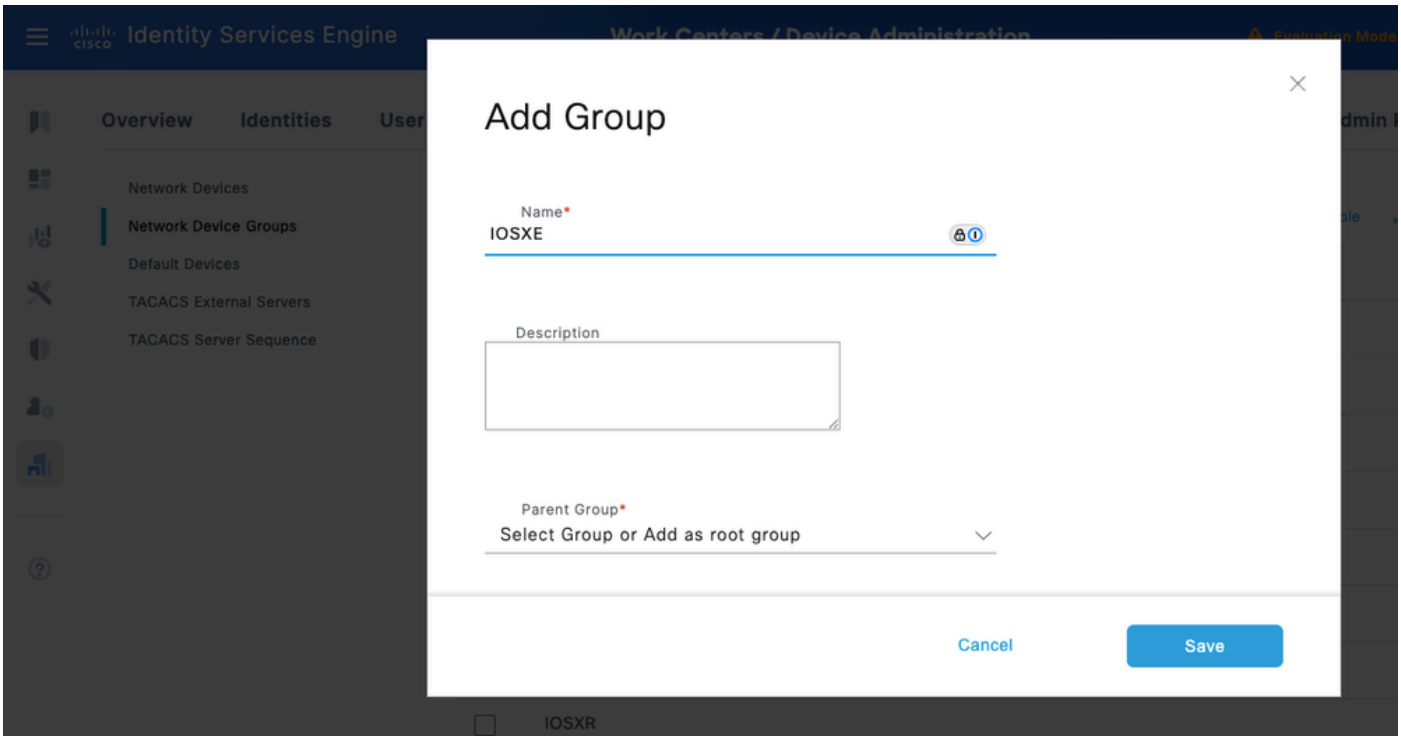


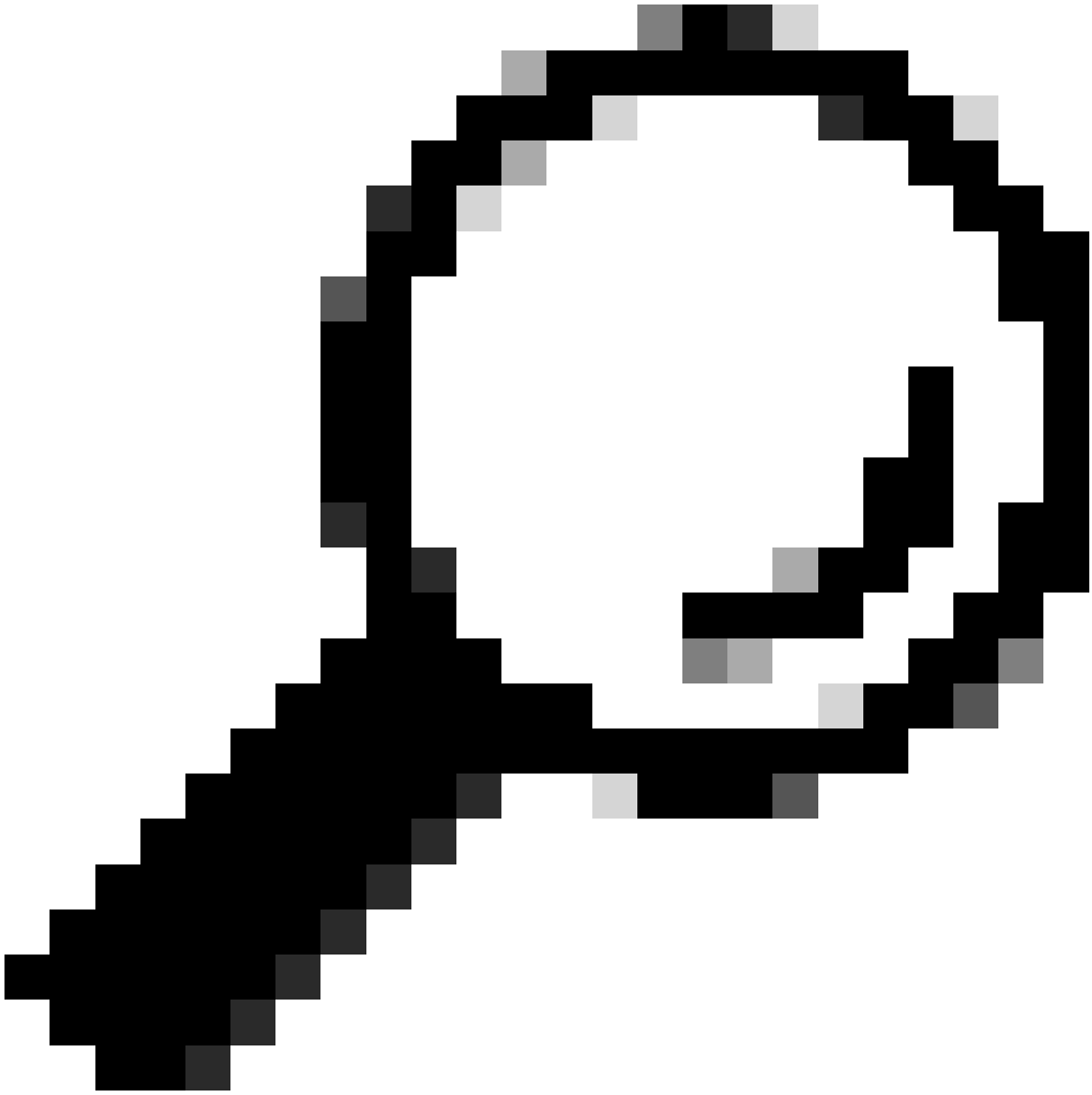
Passaggio 3. Mantenere la porta predefinita 6049 o specificare una porta TCP diversa per TACACS over TLS, quindi fare clic su Save.

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

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

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

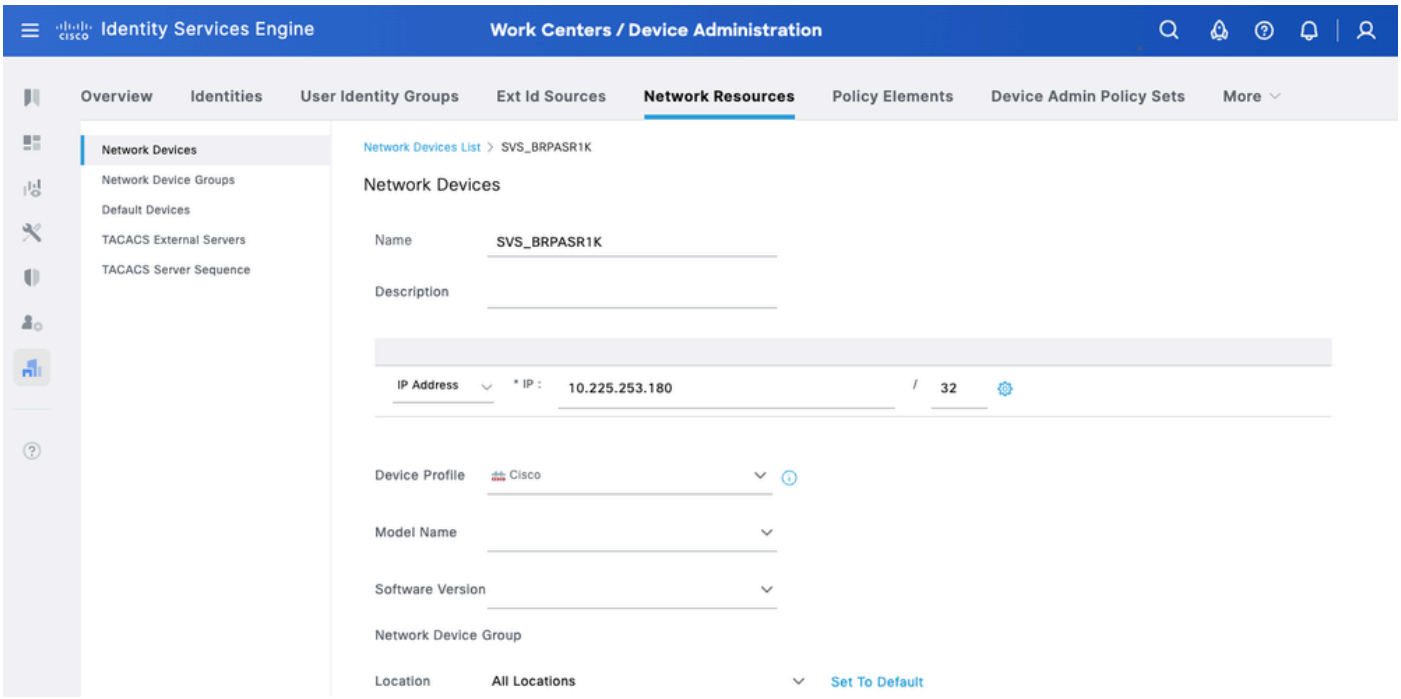

Identity Services Engine
Overview
Identities
Network Devices
Network Device Groups
Default Devices
TACACS External Servers
TACACS Server Sequence
Add Group
Name*
IOSXE
Description
Parent Group*
Select Group or Add as root group
Cancel
Save
IOSXR



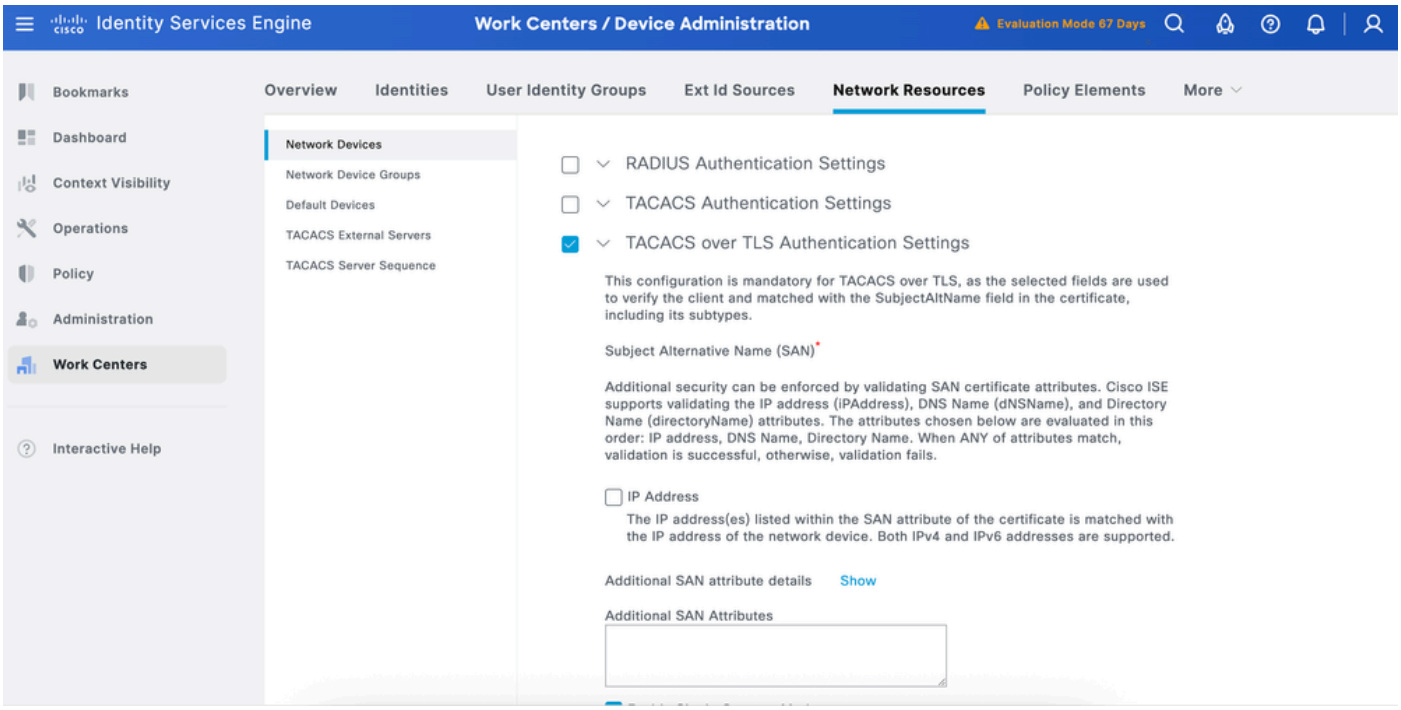
Suggerimento: Tutti i tipi di dispositivo e Tutti i percorsi sono gerarchie predefinite fornite da ISE. È possibile aggiungere gerarchie personalizzate e definire i vari componenti per l'identificazione di un dispositivo di rete che potrà essere utilizzato successivamente nella condizione del criterio

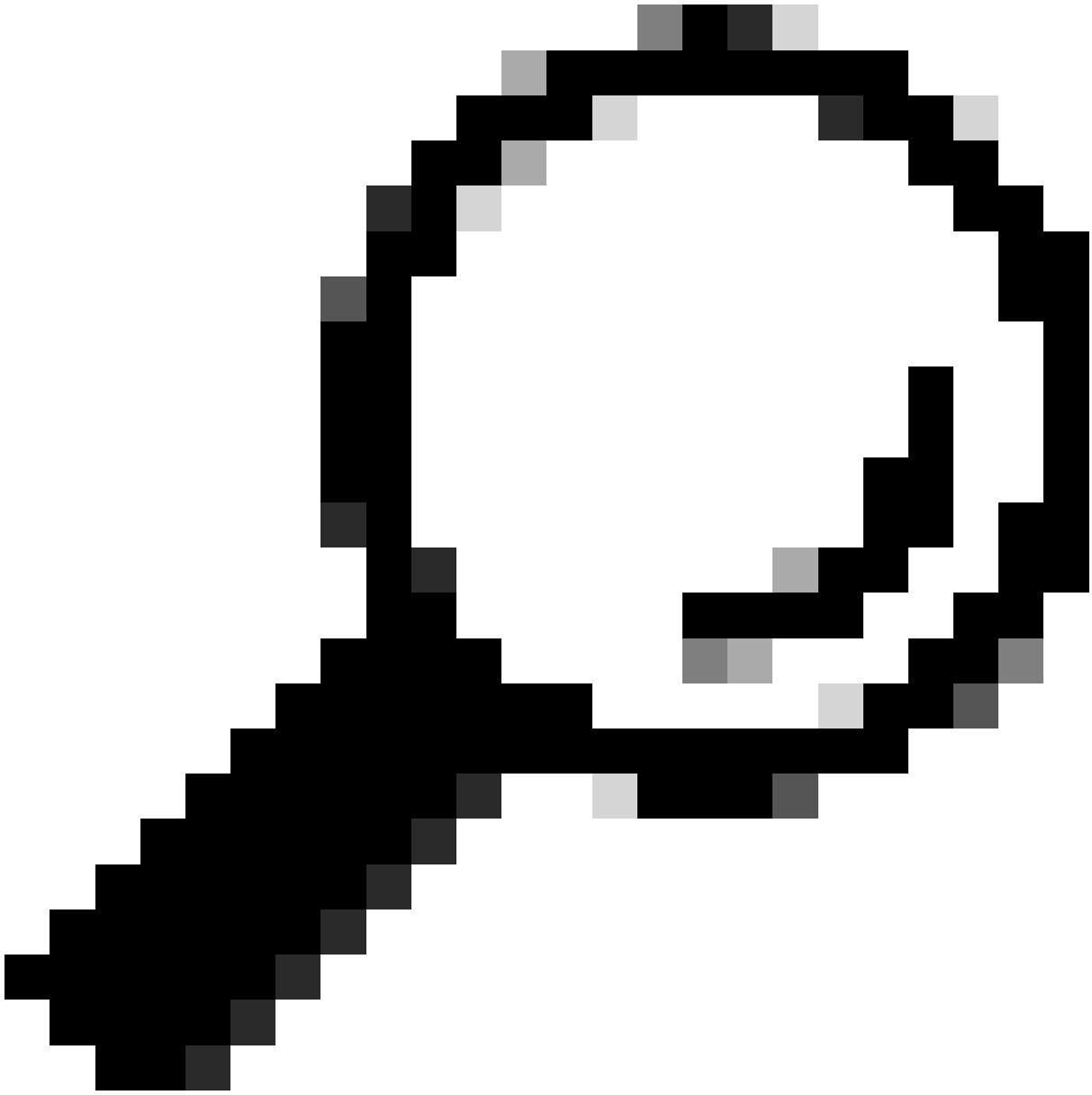
---

Passaggio 2.Aggiungere ora un dispositivo Cisco IOS XE come dispositivo di rete. Passare a Centri di lavoro > Amministrazione dispositivi > Risorse di rete > Dispositivi di rete. Fare clic su Add (Aggiungi) per aggiungere un nuovo dispositivo di rete. Per questo test, sarebbe SVS_BRPASR1K.



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



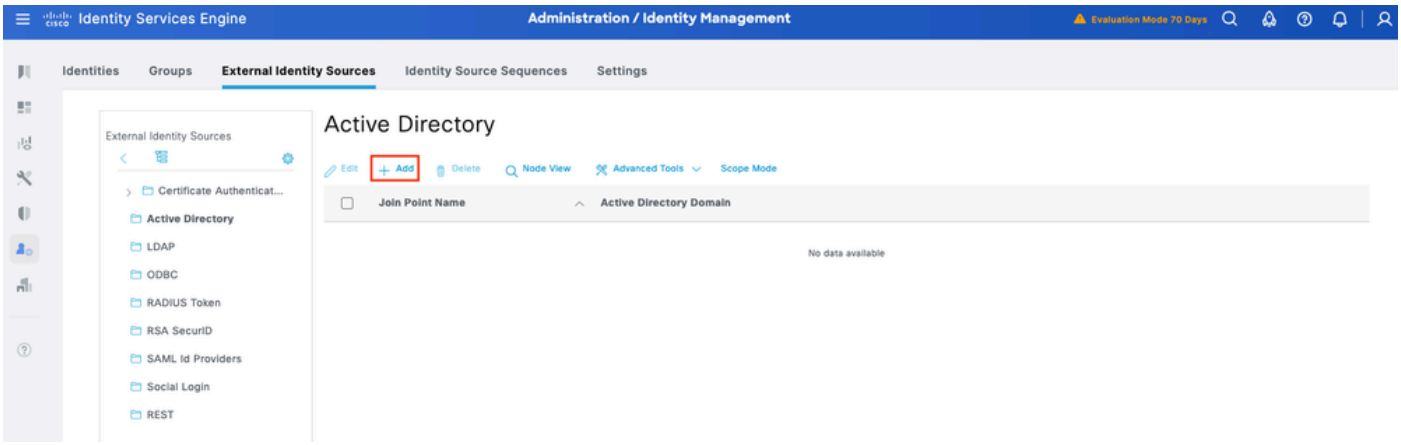


Suggerimento: Per evitare di riavviare la sessione TCP ogni volta che si invia un comando al dispositivo, si consiglia di abilitare la modalità di connessione singola.

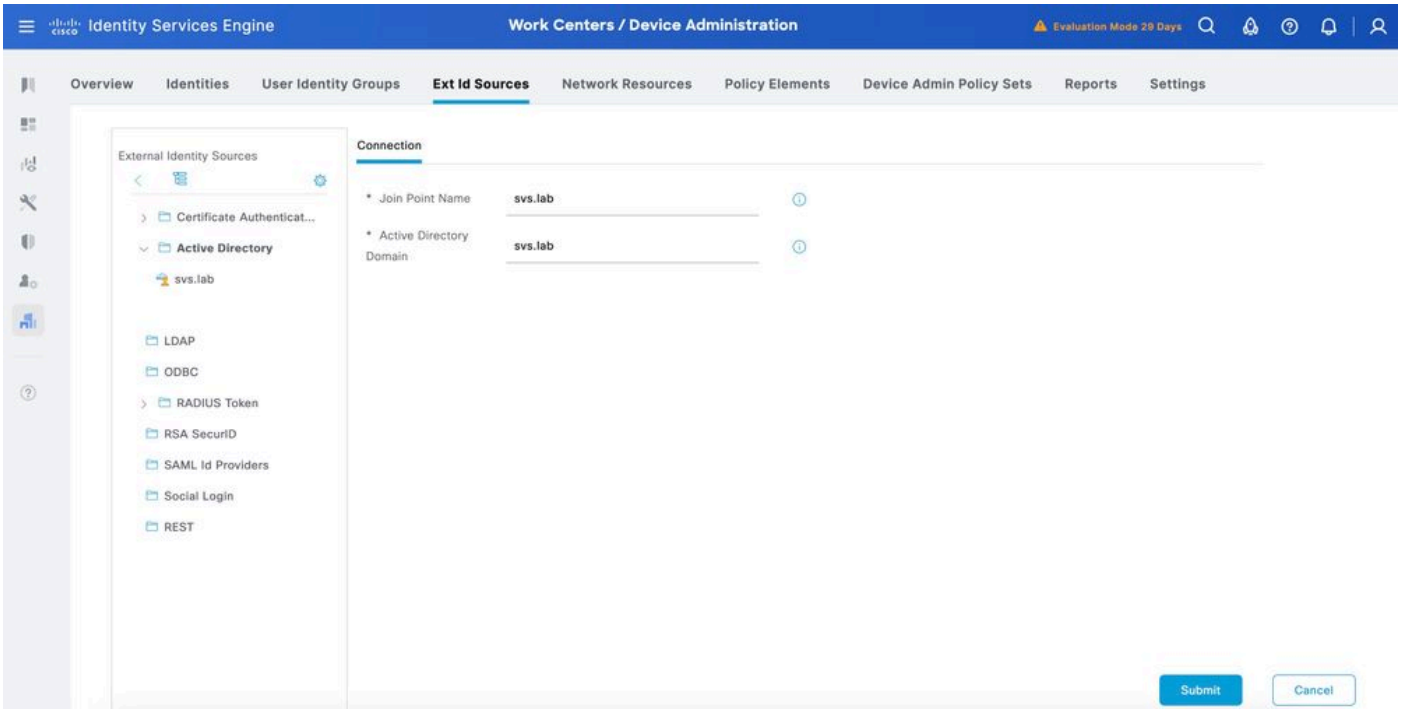
Configura archivi identità

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

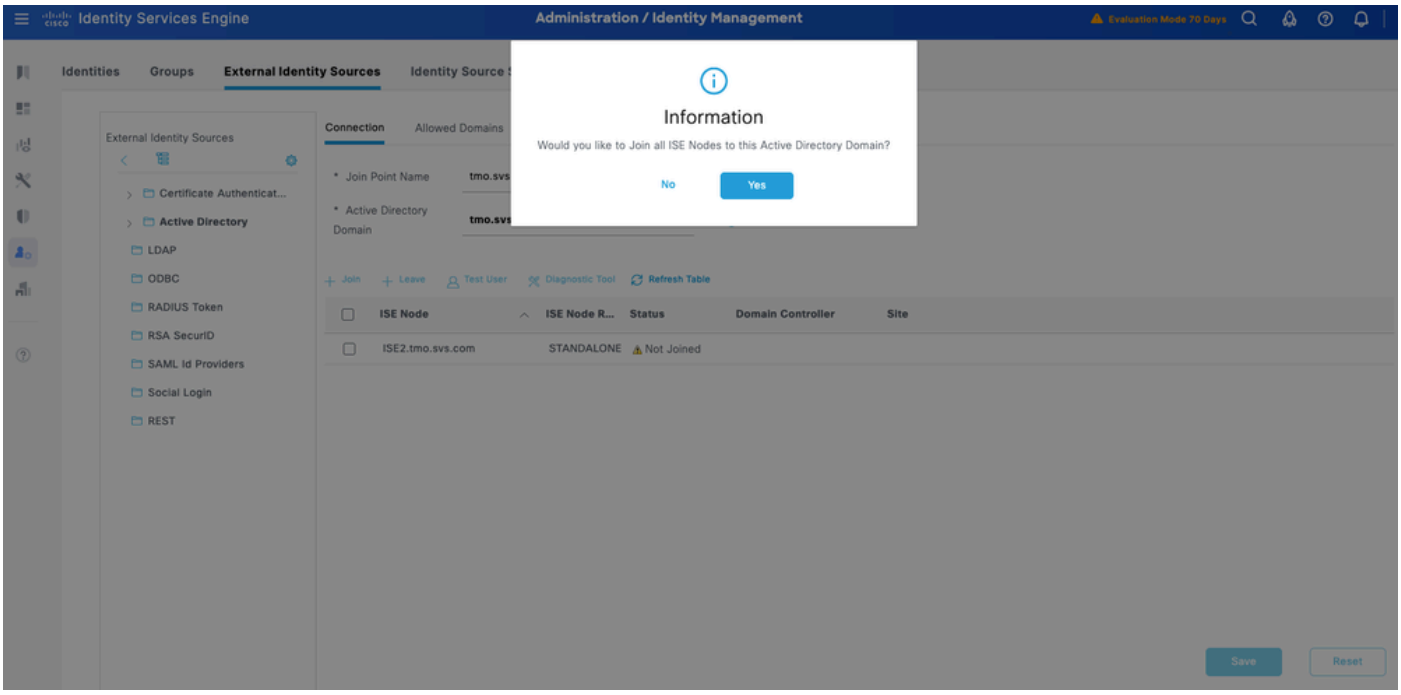
Passaggio 1. Passare a Amministrazione > Gestione delle identità > Archivi identità esterni > Active Directory. Fare clic su Aggiungi per definire un nuovo punto di giunzione AD.



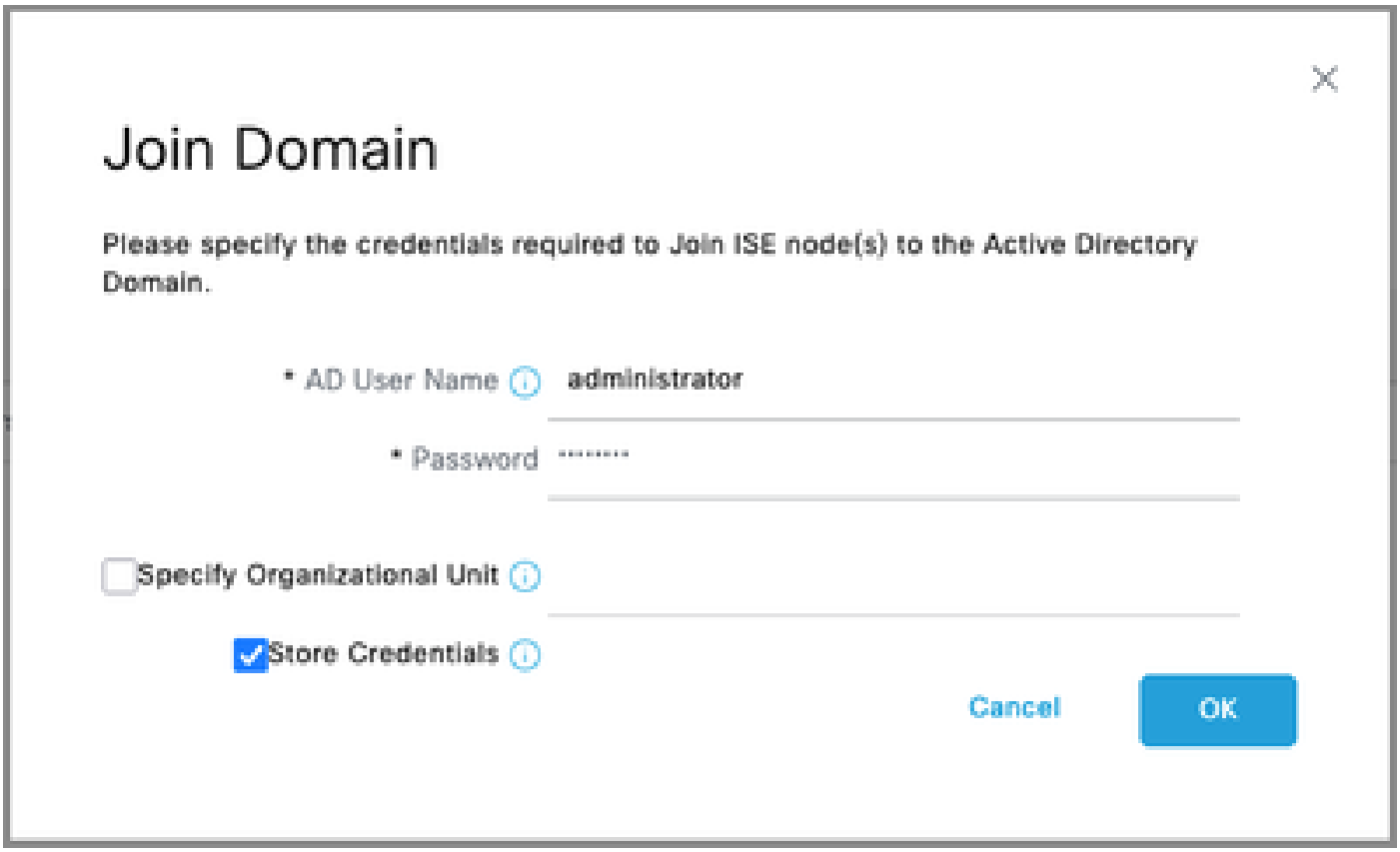
Passaggio 2. Specificare il nome del punto di join e il nome del dominio Active Directory e fare clic su Invia.

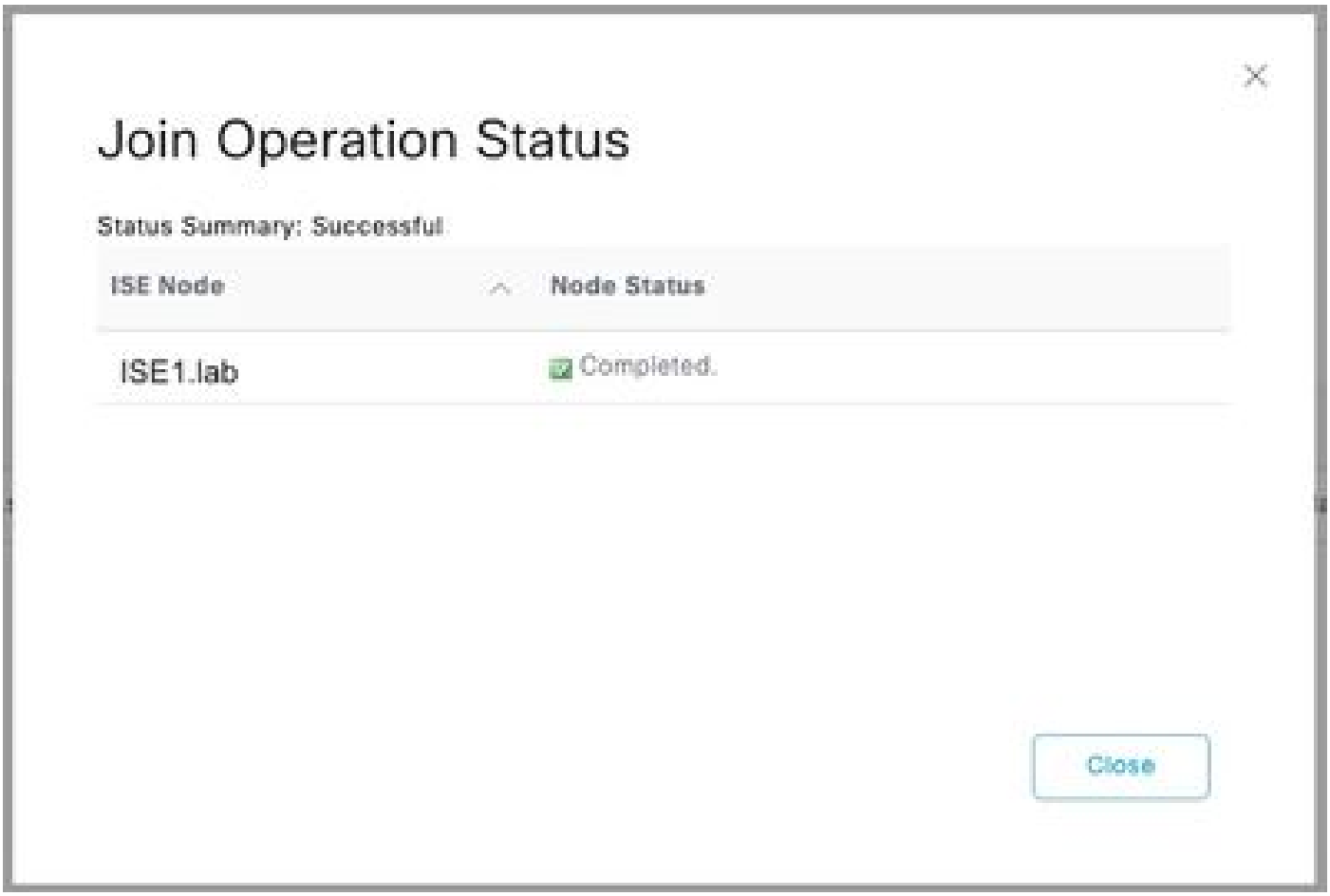


Passaggio 3. Fare clic su Sì quando richiesto Aggiungere tutti i nodi ISE a questo dominio Active Directory?

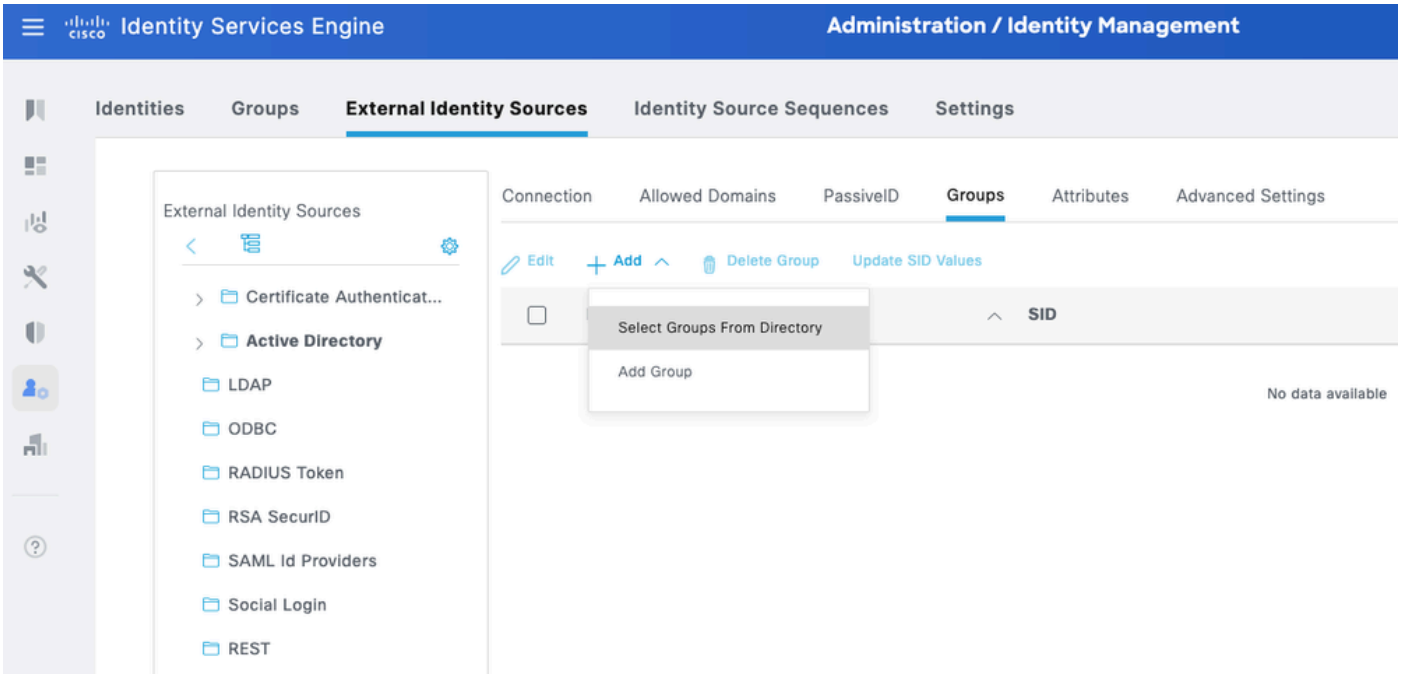


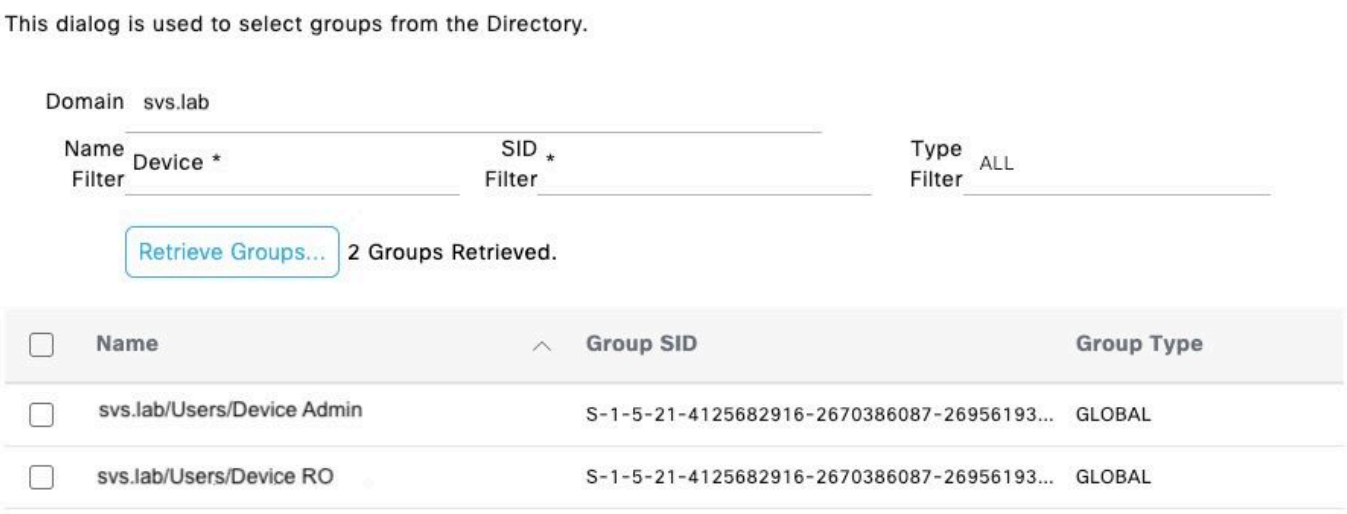
Passaggio 4. Inserire le credenziali con privilegi di join AD e Join ISE to AD. Controllare lo Stato per verificare che sia operativo.

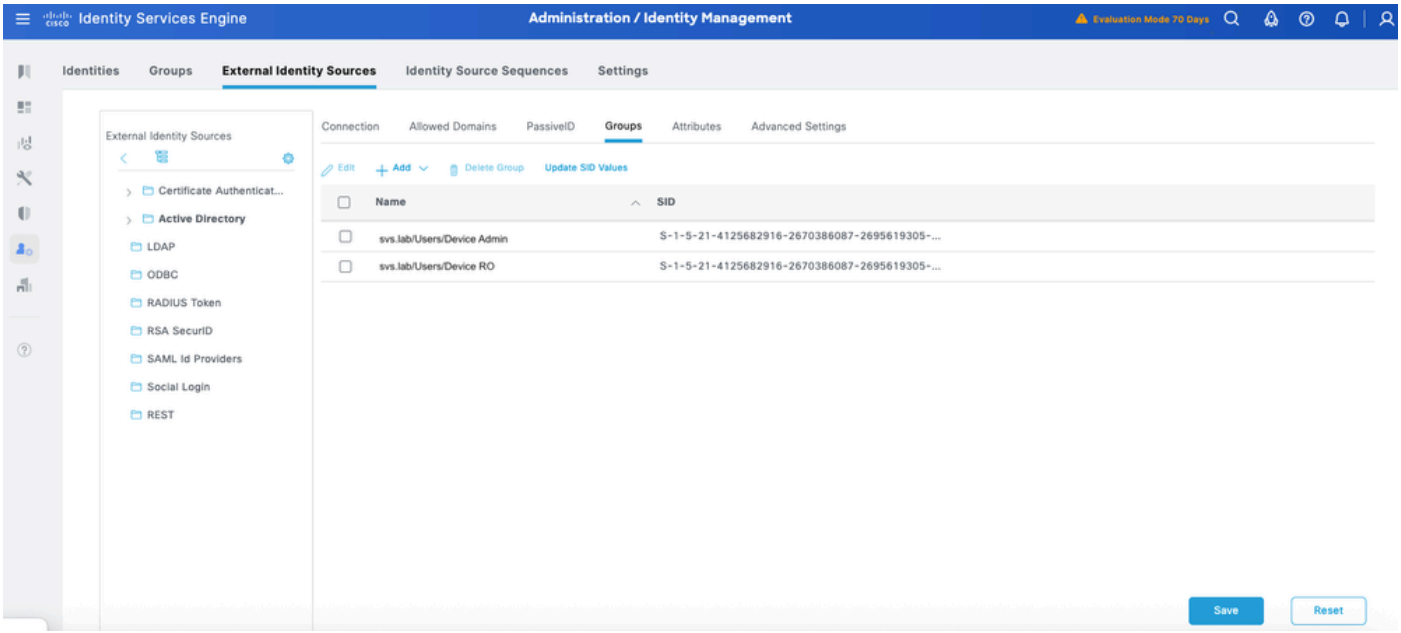




Passaggio 5. Passare alla scheda Gruppi e fare clic su Aggiungi per ottenere tutti i gruppi necessari in base ai quali gli utenti sono autorizzati per l'accesso al dispositivo. In questo esempio vengono illustrati i gruppi utilizzati nei criteri di autorizzazione in questa guida







Configura profili TACACS+

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

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

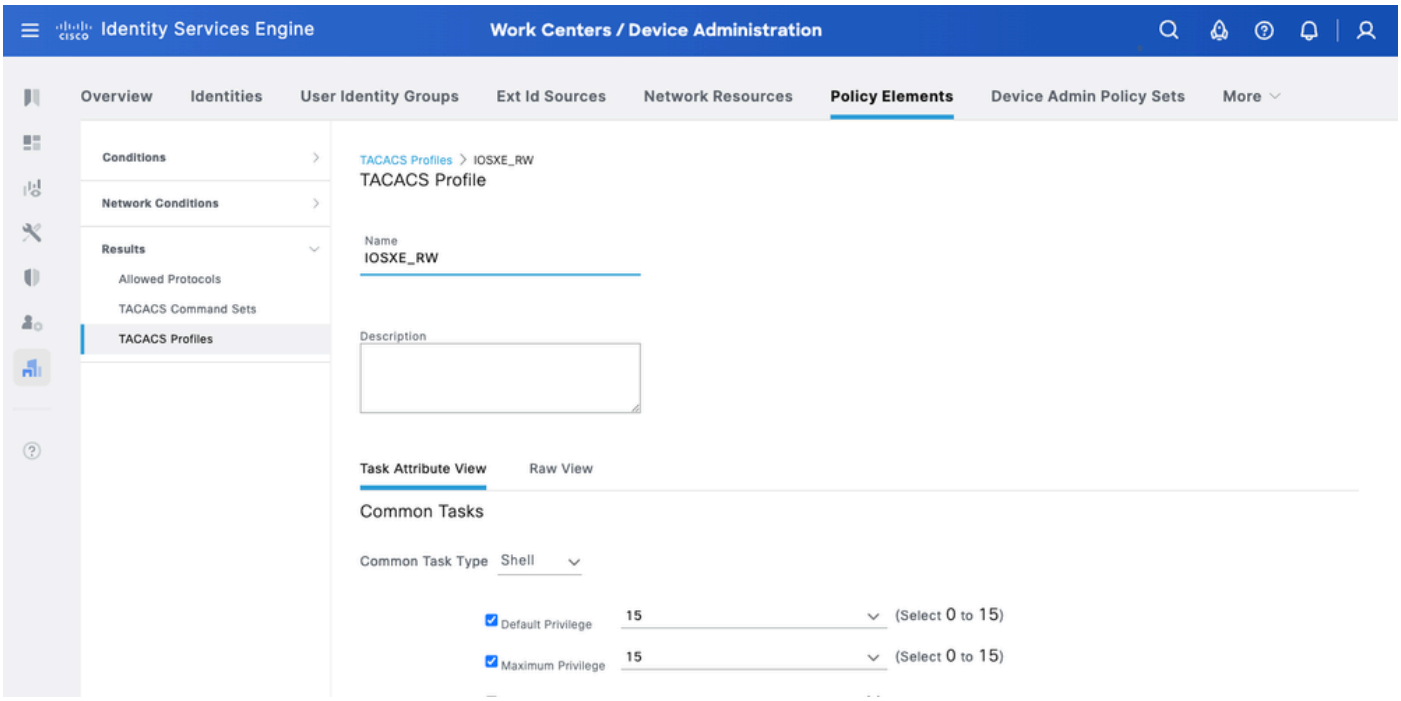
Questi sono definiti come due profili TACACS+: IOS XE_RW e IOSXR_RO.

IOS XE_RW - Profilo dell'amministratore

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

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

Passaggio 3. Confermare la configurazione e salvare.

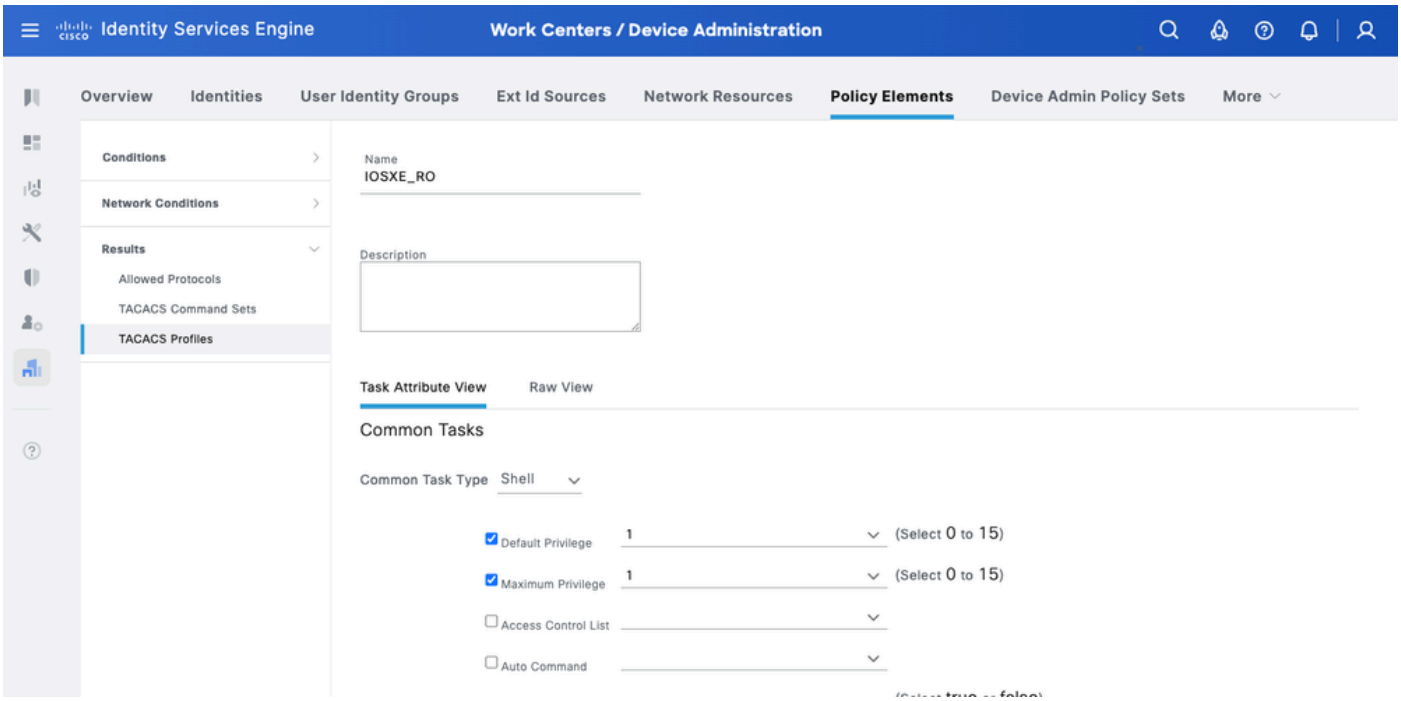


IOS XE_RO - Profilo operatore

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

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

Passaggio 3. Confermare la configurazione e salvare.



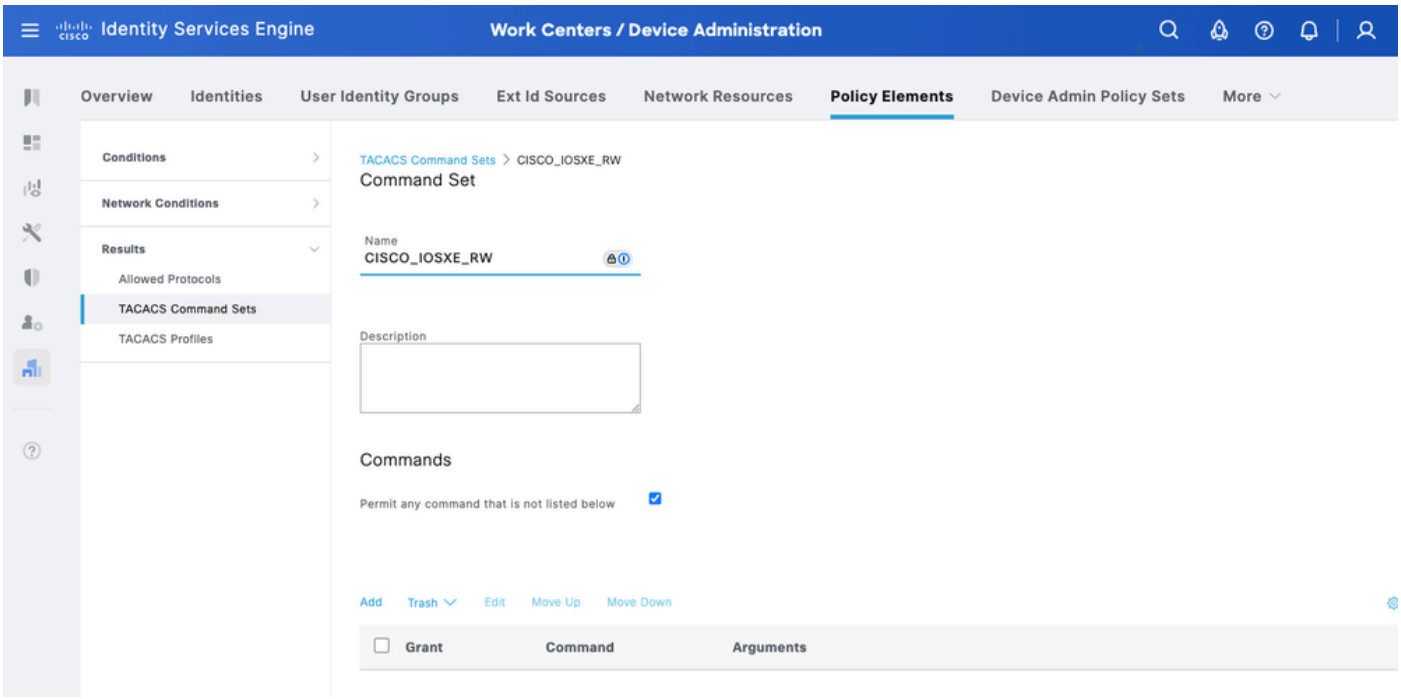
Set di comandi ConfigureTACACS+

questi sono definiti come due set di comandi TACACS+: CISCO_IOS XE_RW e CISCO_IOS XE_RO.

CISCO_IOS XE_RW - Set comandi amministratore

Passaggio 1. Passare a Centri di lavoro > Amministrazione dispositivi > Elementi dei criteri > Risultati > Set di comandi TACACS. Aggiungere un nuovo set di comandi TACACS e denominarlo CISCO_IOS XE_RW.

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



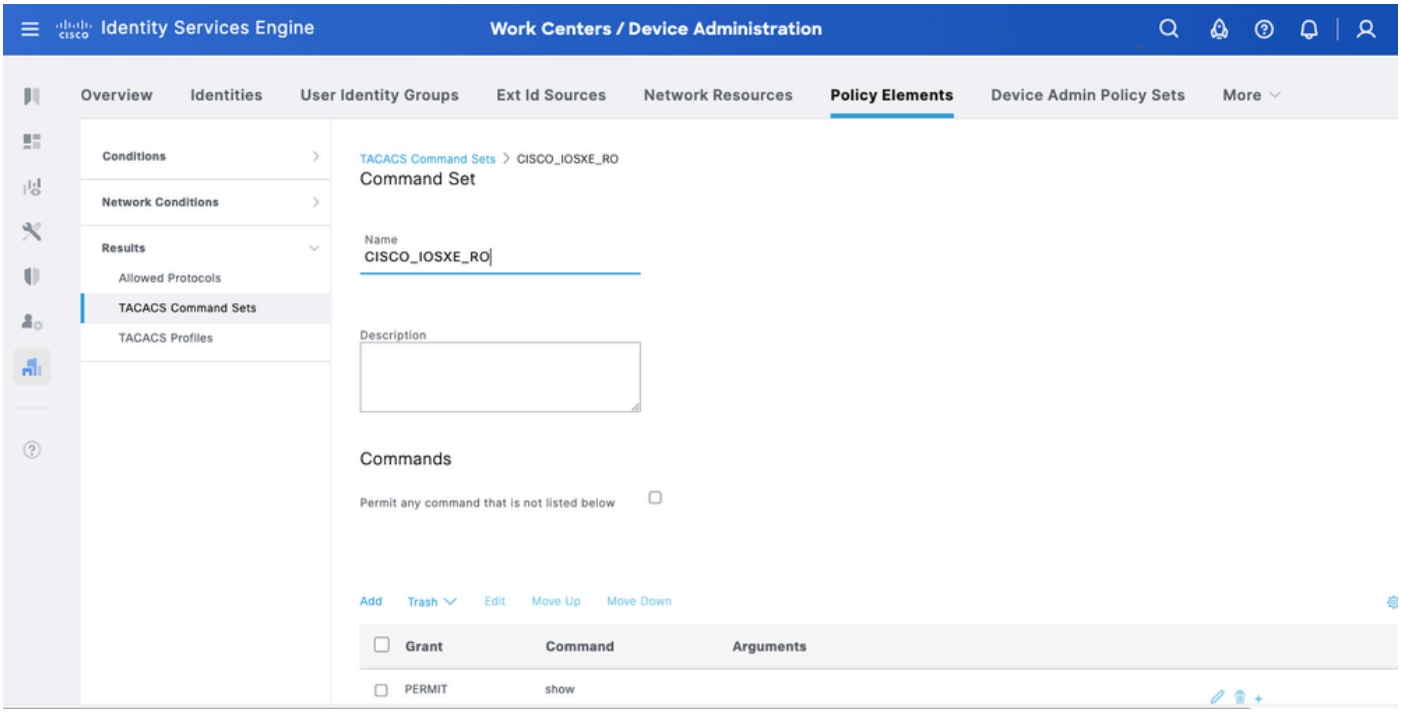
CISCO_IOS XE_RO - Set di comandi dell'operatore

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

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

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

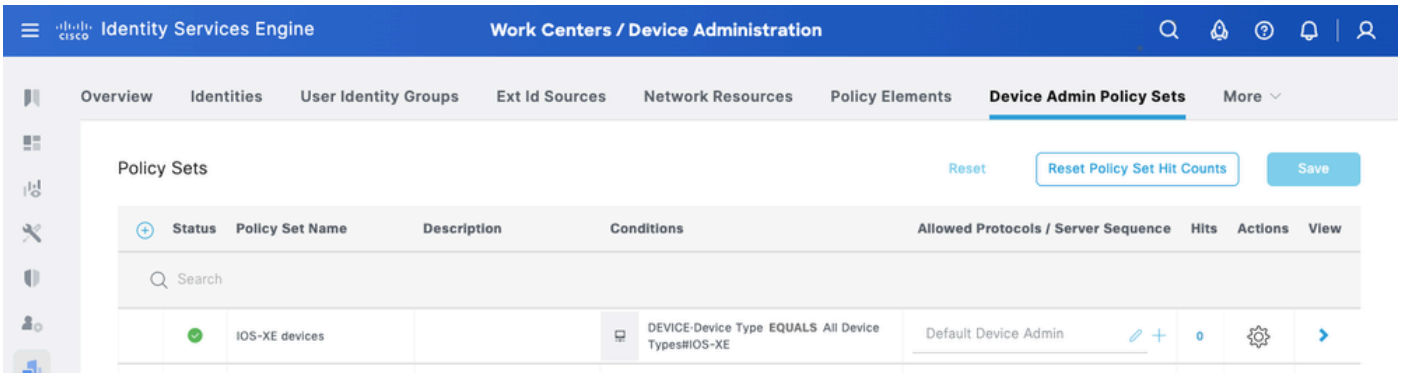
Passaggio 4. Confermare i dati e fare clic su Salva.



Set di criteri di amministrazione del dispositivo

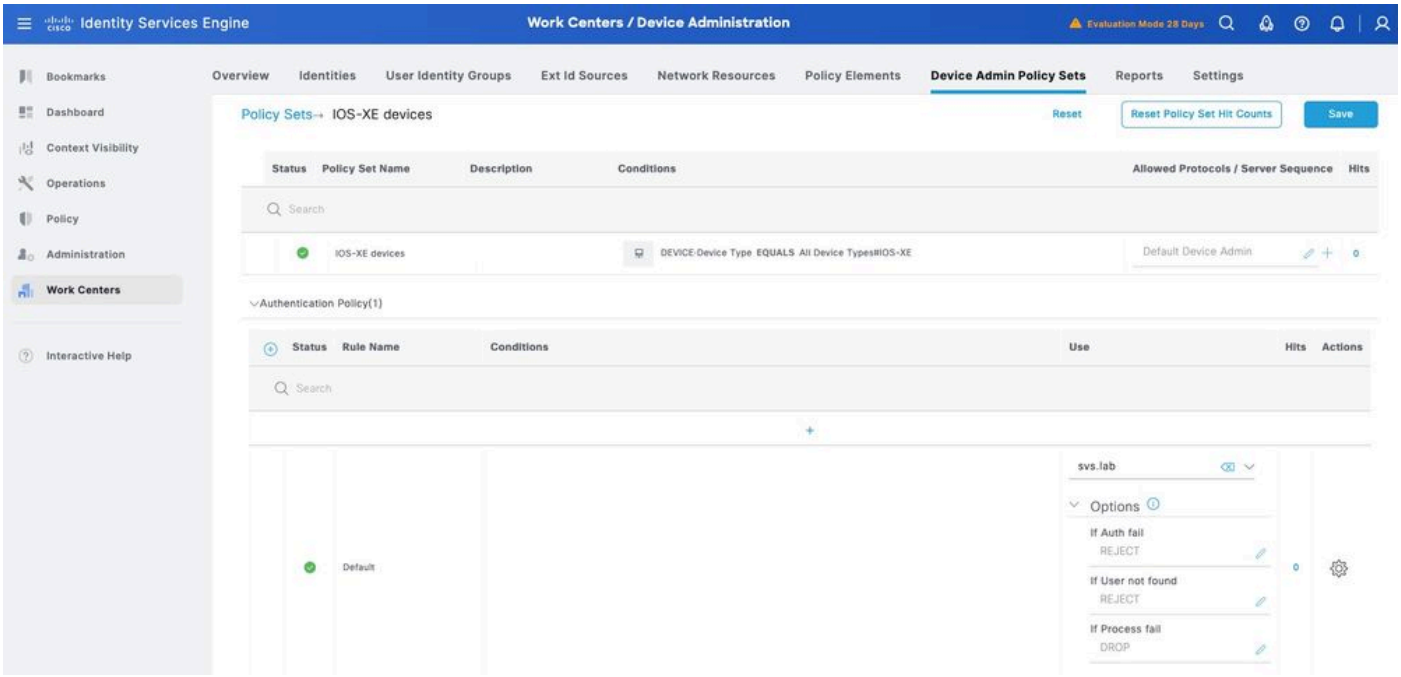
I set di criteri sono attivati per impostazione predefinita per l'amministrazione dei dispositivi. I set di criteri possono dividere i criteri in base ai tipi di dispositivo in modo da semplificare l'applicazione dei profili TACACS.

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



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

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



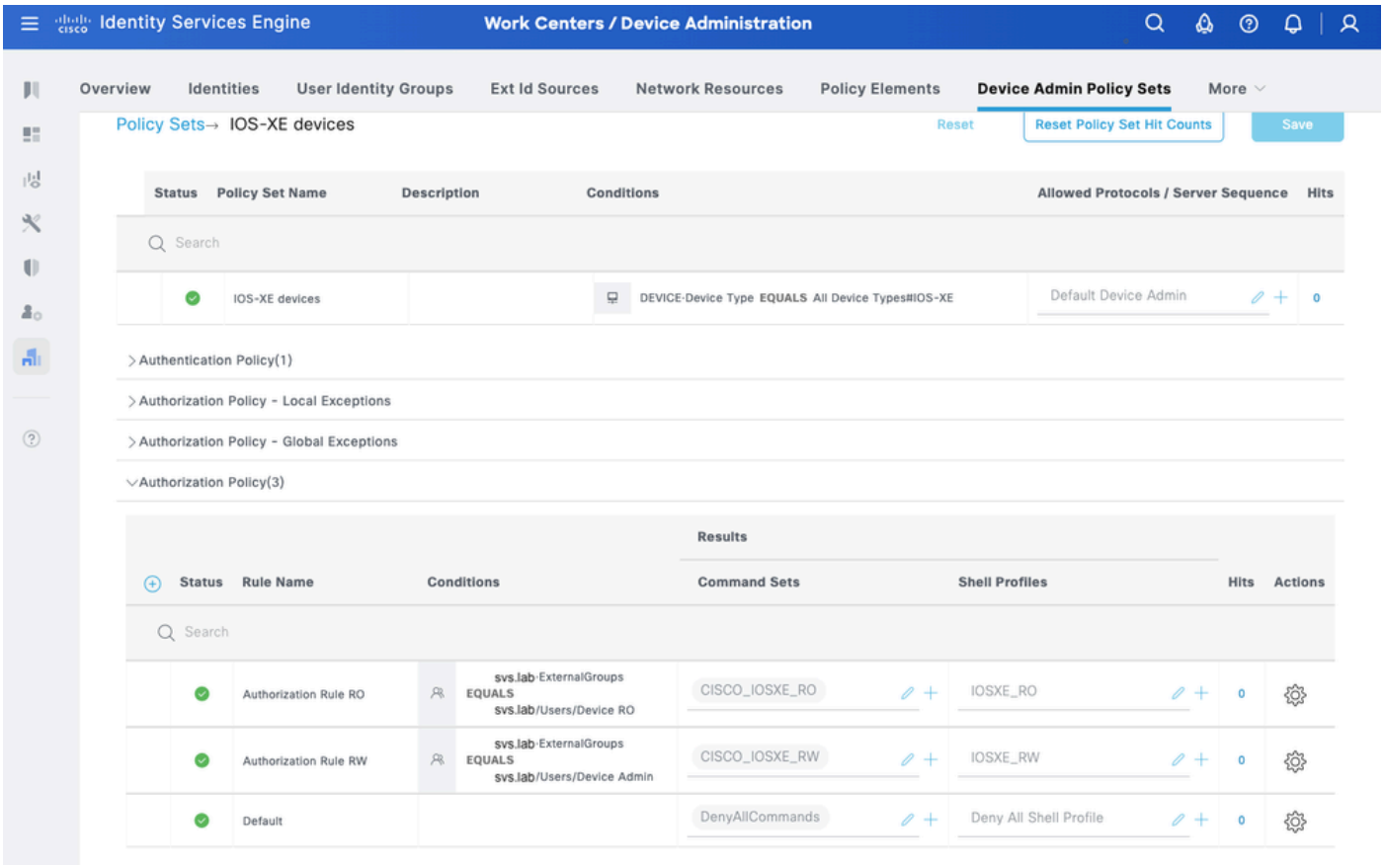
Passaggio 4. Definire il criterio di autorizzazione.

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

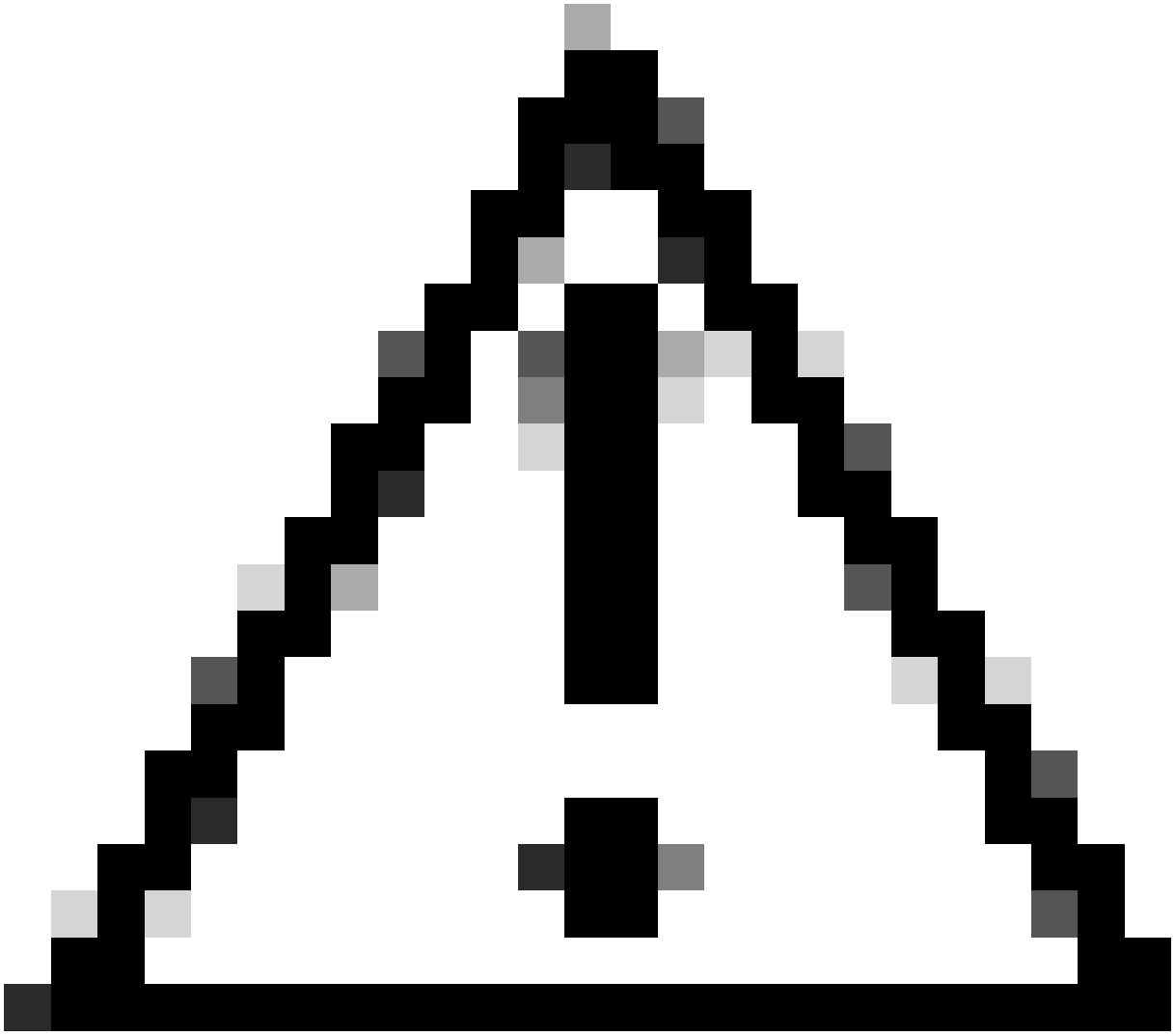
Ad esempio:

· Agli utenti del gruppo AD Device RO viene assegnato il set di comandi CISCO_IOSXR_RO e il profilo di IOSXR_RO Shell.

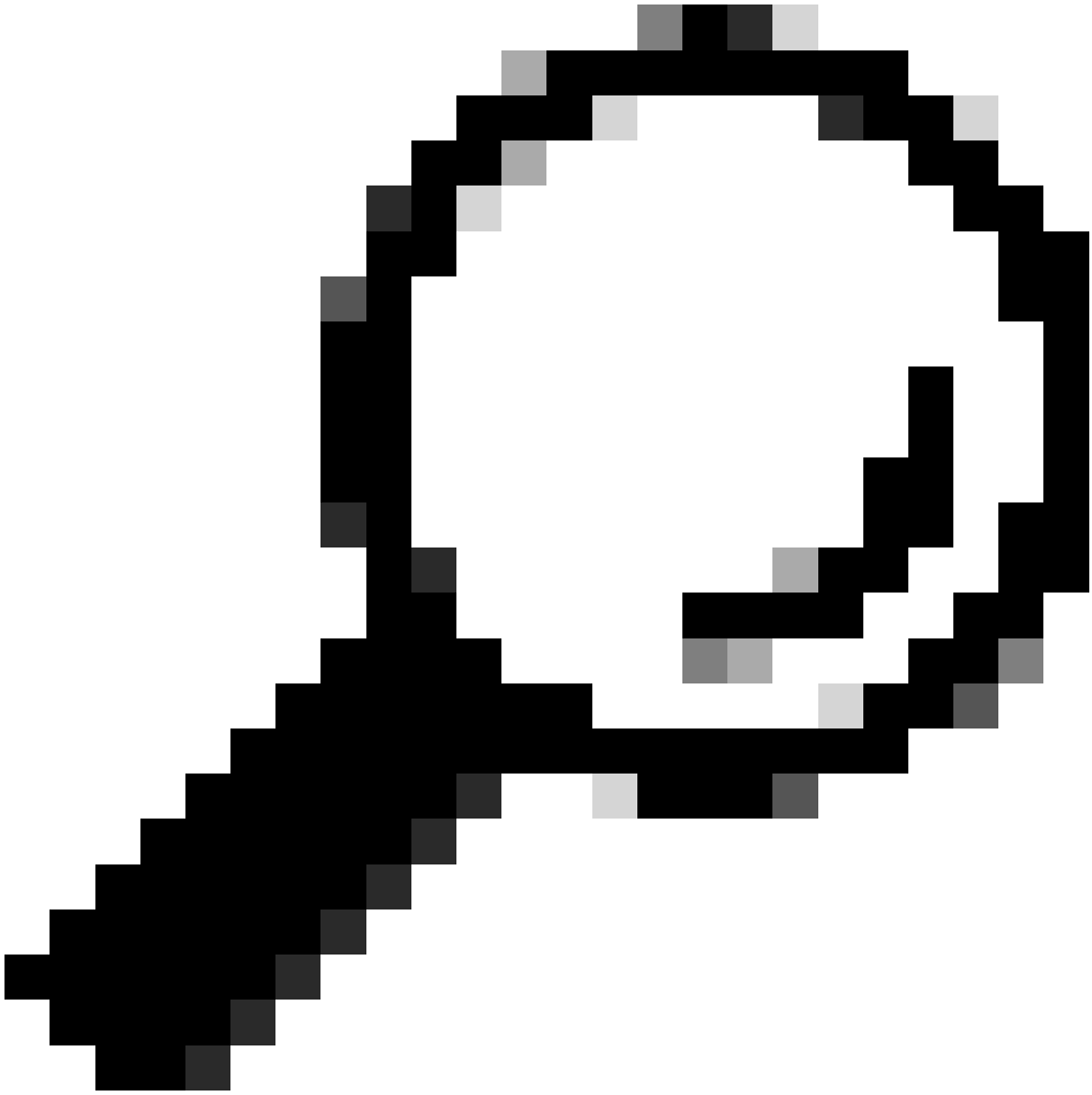
· Agli utenti del gruppo AD Device Admin viene assegnato il set di comandi CISCO_IOSXR_RW e il profilo della shell IOSXR_RW.



Parte 2 - Configurazione di Cisco IOS XE per TACACS+ su TLS 1.3



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



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

Metodo di configurazione 1 - Coppia di chiavi generata dal dispositivo

Configurazione server TACACS+

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

```
ip domain name svs.lab

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

Configurazione del punto di trust

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

```
crypto pki trustpoint svs_cat9k
  enrollment terminal pem
  subject-name C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=cat9k.svs.lab
  serial-number none
  ip-address none
  revocation-check none
  eckeypair svs-256ec-key
```

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

<#root>

```
cat9k(config)#
```

crypto pki authenticate svs_cat9k

```
Enter the base 64 encoded CA certificate.

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

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

MIIFlDCCA3ygAwIBAgIIIM1OAsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
QOEwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUGA1UECBMOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBAcTB1JhbGVpZ2gxDjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTVlMxEjAQBgNVBAMTCVNWUyBMYWJDQTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZUOyn2vIn6gKbx3M7vaRq
2YjwZlzSH6EkEvxnJTy+kksiFD33GyHQepk7vfp4NFU5OtQ4HC7t/AOv9grDa3QW
VwvV4MBbJhFM3s0J/ejgDYcMZhIAaPyOZo5WLboOkXEiKjPLatkXojB8FVrhLF3O
jMBSqwa4/Wlniy5S+7s4FFxsCf2OCOWfBAsnrs0tatIIhmcnx+VLJP7MRm8fOw4m
mutNo7IhbJSrgAFXmjlbBjMmgspObULo/wxMHdTbtPBf11HRHTkNIo3qyO4UADL2
WpoGhgT/FaxxBo2UBcnYVaP+jjRE0NYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7BOe8oDNKU6gXlojKyLP/gC7j8AePO3ir+KZui8
b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
```

```
gJ+kQXe7QtT/u6m1MrtjE3gAEVpL334rTIxy9hpKZIkB86t2ZA3JX8CLsbCa13sA
z1XCoONX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTA01xh6OI4QnK+MNQKpTjt/E4
ydHl0rrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVLl783nTc9wYptQEPi5sw
83g9EMgKV0ARIiVUa/qlAgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAYb4
QgEBBAQDAgAHMBkGCWCGSAGG+EIBDQQMFgpTVlMgTGFiIENBMA0GCSqGSIb3DQEB
CwUAA4ICAQAIT3O8oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oKOdGayi
iSEkSSX9qyfLfINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXRX67X+v
O+ja6zTQqjO6lqJhmrSkyFbYf/ZTpe4d1OzJsZjNsNOr8bF9nOA/7qNZLp3Z3cpU
PUOKdbiSvRqnPw3e8TfITVmAzcx8COI2SrYFMSUazolVBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIEOf5ay1PKURO/8aj/B7aluJapXkmnj5qPeGhNOpB
Q9r14reov4so2EspkXS7CrH9yGfpIyTprokz1UvZBZ8vloI7YZmjFmem+5rT6Gnk
eU/lX7nV61SYG5W5K+I8uaKuyBHOMn7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggzlPOdsS/i6Lo7ypYXOeB9HgVDCkzQsLXQuHGj/2WsgPgdRcjkvnyURk4Jx+Ib
xDrmo7eOXPpSW4l72a6Kl8CR3U2Cr4wsuvndPEq/qd2NRSBWffF0XE/AJHQG7STT
HaXLU9r2Ko6O3oecu8ysGTwLlIt/9T1/FOb0xZRugWcpJrVoTgDGuA==

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

Certificate has the following attributes:
   Fingerprint MD5: D9C4O4B2 ECO8A26O EC3539E7 F54ED17D
   Fingerprint SHA1: OEB181E9 5A3ED78O 3BC5A8O5 9A854A95 C83AC737

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

yes

```
Trustpoint CA certificate accepted.
% Certificate successfully imported

cat9k(config)#
```

Passaggio 3. Generare una richiesta di firma del certificato (CSR).

```
<#root>

cat9k(config)#
```

crypto pki enroll svs_cat9k

```
% Start certificate enrollment ..

% The subject name in the certificate will include: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=cat9k.svs.lab
% The subject name in the certificate will include: cat9k.svs.lab
Display Certificate Request to terminal? [yes/no]:
```

yes

```
Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
MIIBfDCCASMCAQAwgYQxGjAYBgNVBAMTEWNhdDlrLnRtby5zdnMuY29tMQwwCgYD
VQQLEwNTVlMxDjAMBgNVBAoTBUNpc2NvMQwwCgYDVQQHEwNSVFAxCzAJBgNVBAgT
Ak5DMQswCQYDVQQGEwJVUzEgMB4GCSqGSIb3DQEJAhYRY2F0OWsudG1vLnN2cy5j
b20wWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATpYE7atscrtl4ddevCh3UgxjYi
4N4oBGWrpJBctKy4so8V5i6RXDt7kHgPzp14Qnf20bcXVODE1wtTAHHBrIXqoDww
OgYJKoZIhvcNAQkOMSOwKzAcBgNVHREEFTATghFjYXQ5ay5ObW8uc3ZzLmNvbTAL
```

```
BgNVHQ8EBAMCB4AwCgYIKoZIzj0EAwQDRwAwRAIgZqP2QTwM3ZZrmIphJ7+jSTER
40kTx2DiVs1c1Xf+vR4CIBcSb18DIYz84DmgMHUaf778/cmpe9cWakvdaxMWseBH
-----END CERTIFICATE REQUEST-----

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]:
```

no

```
cat9k(config)#
```

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

<#root>

```
cat9k(config)#
```

crypto pki import svs_cat9k certificate

```
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIID8zCCAdugAwIBAgIIKfdYWg5WpskwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
QOEwHhcNMjUwNTE0MTUxMjAwWhcNMjYwNTE0MTUxMjAwWjCBhDEaMBgGA1UEAxMR
Y2F0OWsudG1vLnN2cy5jb20xDDAKBgNVBAsTA1NWUzEOMAwGA1UEChMFQ2lzY28x
DDAKBgNVBAcTA1JUUDELMAkGA1UECBMCTkMxCzAJBgNVBAYTAlVTMSAwHgYJKoZI
hvcNAQkCFhFjYXQ5ay5ObW8uc3ZzLmNvbTBZMBMGByqGSM49AgEGCCqGSM49AwEH
A0IABOlgTtq2xyu2Xh1168KHdSDGNiLg3igEZaukkFyOrLiyjxXmLpFcO3uQeA/O
nXhCd/bRtxdU4MTXC1MAccGsheqjTTBLMB4GCWCGSAGG+EIBDQQRFg94Y2EgY2Vy
dGlmaWNhdGUwHAYDVR0RBBUwE4IRY2F0OWsudG1vLnN2cy5jb20wCwYDVR0PBAQD
AgeAMA0GCSqGSIb3DQEBCwUAA4ICAQBObgKVykeyVC9UsvuuOAUsGaZHGwy2H9Yd
m5vIaui6PJczkCzIoAIghHPGQhIgpEcRqtGyXPZ2r8TCJP11WXNN/G73sFyWAhzY
RtmIM5KIojiDHLtifPayxv9juDuOZRx+wYR2PIQ5eLv1bafg7K8E82sqOCfOtcPr
Oc0NU8UCxqObdOgu4XsdBN1+wcWFqeQSDLmP7nxvhOOm/LXwCWUHwgVioOAuU2Fe
k5NthtvdxNAhRAImQdTyq6u/yB7vwTwJHcRiJc5USsyzCsTBb6RvL+HsXqBgXGc5
lxCSoLtYOdUxFIpJyK2MOZBY2zq2cNSc8Xbso5/OEQmnHtpWPvij4rSPUhQSY+4m
Qq2Sn3iqf4mGh/AO8T4iXfWDWfNezh7ZxMsCSCK/ZRlELZ2hj6OfzwX1H27Uf8XU
ecr0Wx+WzRn7LVRCaGQzFkukfi8S4DLLNtxnNHfsLBVX5yHXCLEL+CQ7n8Z/pxcB
VVrPitwN3ZbO9poZyWiRLTnBsb42xNaWiL9bjQznAOiTDfmfFFourBsaAioz7ouY
2r1Mh+OpE83Uu+4lOTMawDgGiEv7iaiJ6xWc95EC+AdmOx3FvBXMtIM9qr7WwHW6
3C2hVYHJH254elV5+H8iiz7rovEPm8ZDsnvYpJn4Km3iDvBNqp/vvAHOFcyXrvG6
3i/1b9erGQ==
-----END CERTIFICATE-----

% Router Certificate successfully imported

cat9k(config)#
```

TACACS e AAA con configurazione TLS

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

```
tacacs server svs_tacacs
 address ipv4 10.225.253.209
 single-connection
 tls port 6049
 tls idle-timeout 60
 tls connection-timeout 60
 tls trustpoint client svs_cat9k
 tls ip tacacs source-interface GigabitEthernet0/0
 tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ svs_tls
 server name svs_tacacs
 ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request
```

Passaggio 2. Configurare i metodi AAA.

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

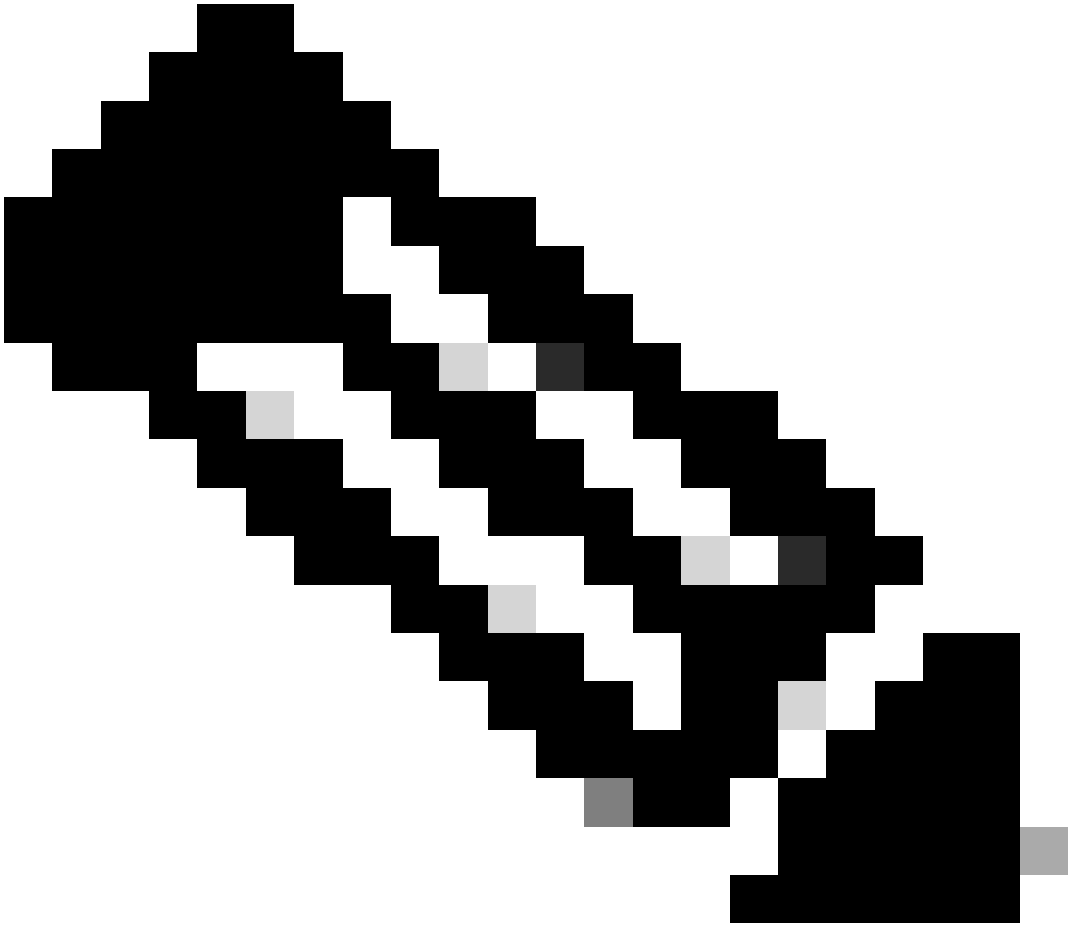
Metodo di configurazione 2 - Coppia di chiavi generata dalla CA

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

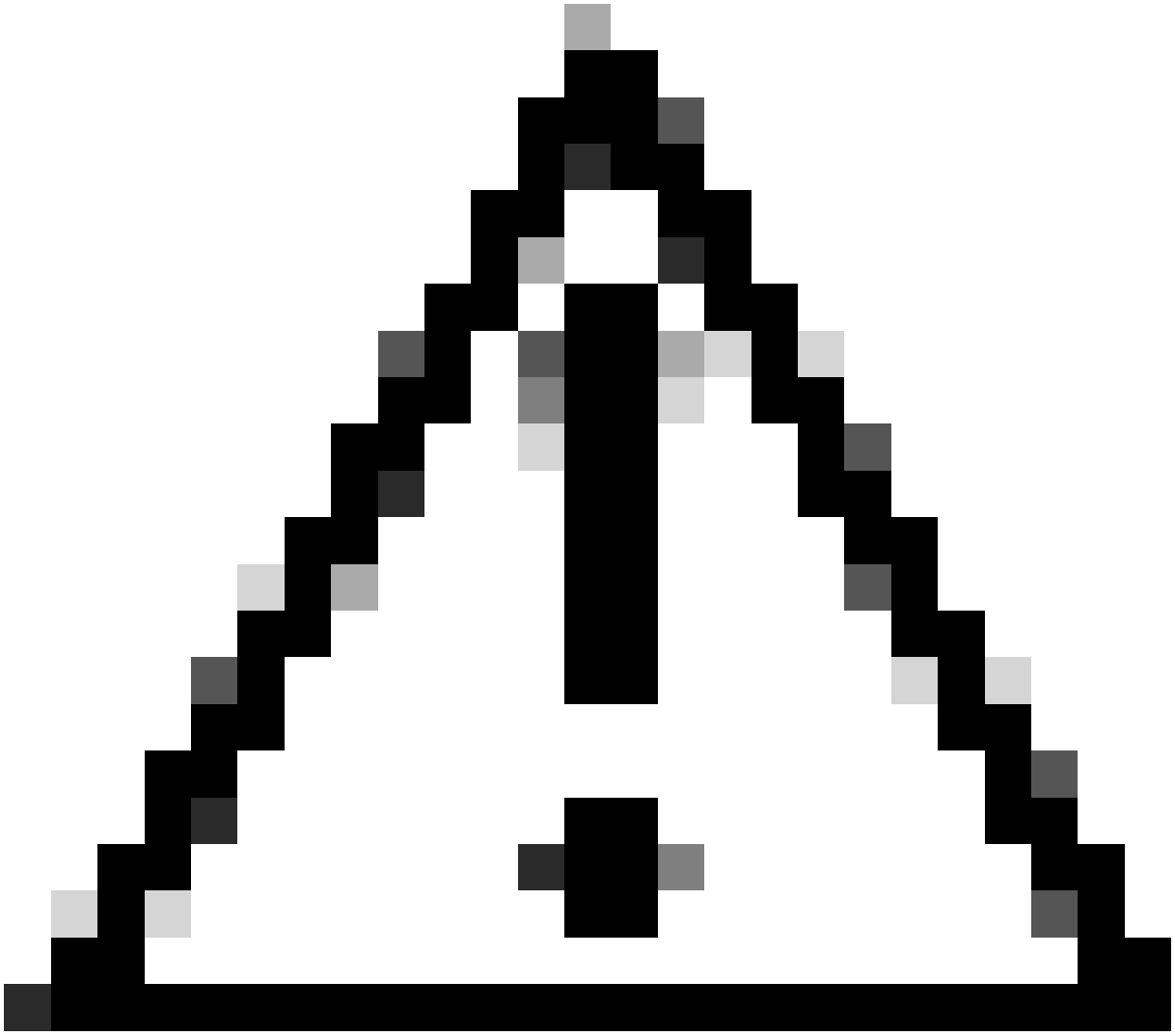
Passaggio 1. Creare un trust point client.

```
cat9k(config)#crypto pki trustpoint svs_cat9k_25jun17
cat9k(ca-trustpoint)#revocation-check none
```

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



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



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

<#root>

```
cat9k#

copy sftp bootflash: vrf Mgmt-vrf


Address or name of remote host [10.225.253.247]?
Source username [svs-user]?
Source filename [cat9k.svs.lab.pfx]? /home/svs-user/upload/cat9k-25jun17.pfx
Destination filename [cat9k-25jun17.pfx]?
Password:
!
2960 bytes copied in 3.022 secs (979 bytes/sec)
```

Passaggio 3. Importare il file PKCS#12 utilizzando il comando import.

<#root>

```
cat9k#

crypto pki import svs_cat9k_25jun17 pkcs12 bootflash:cat9k-25jun17.pfx

 password C1sco.123
% Importing pkcs12...Reading file from bootflash:cat9k-25jun17.pfx
CRYPTO_PKI: Imported PKCS12 file successfully.
cat9k#

cat9k#

show crypto pki certificates svs_cat9k_25jun17


Certificate
  Status: Available
  Certificate Serial Number (hex): 586OBF33A2O33365
  Certificate Usage: General Purpose
  Issuer:
    cn=SVS LabCA
    ou=SVS
    o=Cisco
    l=Raleigh
    st=North Carolina
    c=US
  Subject:
    Name: cat9k.svs.lab
    e=pkalkur@cisco.com
    cn=cat9k.svs.lab
    ou=svs
    o=cisco
    l=rtp
    st=nc
    c=us
  Validity Date:
    start date: 17:56:00 UTC Jun 17 2025
    end   date: 17:56:00 UTC Jun 17 2026
  Associated Trustpoints: svs_cat9k_25jun17

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 2OCD74O2C4DA37F5
  Certificate Usage: General Purpose
  Issuer:
    cn=SVS LabCA
    ou=SVS
    o=Cisco
    l=Raleigh
    st=North Carolina
    c=US
  Subject:
    cn=SVS LabCA
    ou=SVS
    o=Cisco
    l=Raleigh
    st=North Carolina
    c=US
  Validity Date:
    start date: 17:05:00 UTC Apr 28 2025
    end   date: 17:05:00 UTC Apr 28 2035
  Associated Trustpoints: svs_cat9k_25jun17 svs_cat9k
```

```
  Storage: nvram:SVSLabCA#37F5CA.cer
```

TACACS e AAA con configurazione TLS

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

```
tacacs server svs_tacacs
 address ipv4 10.225.253.209
 single-connection
 tls port 6049
 tls idle-timeout 60
 tls connection-timeout 60
 tls trustpoint client svs_cat9k
 tls ip tacacs source-interface GigabitEthernet0/0
 tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ svs_tls
 server name svs_tacacs
 ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request
```

Passaggio 2. Configurare i metodi AAA.

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

Verifica

Verifica della configurazione.

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

Debug per AAA e TACACS+.

```
debug aaa authentication
debug aaa authorization
debug aaa accounting
debug aaa subsys
debug aaa protocol local
debug tacacs authentication
debug tacacs authorization
debug tacacs accounting
debug tacacs events
debug tacacs packet
debug tacacs
debug tacacs secure

! Below debugs will be needed only if there is any issue with SSL Handshake
debug ip tcp transactions
debug ip tcp packet
debug crypto pki transactions
debug crypto pki API
debug crypto pki messages
debug crypto pki server
debug ssl openssl errors
debug ssl openssl msg
debug ssl openssl states
clear logging
```

Informazioni su questa traduzione

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