Konfigurieren von TACACS+ über TLS 1.3 auf einem IOS XE-Gerät mit der ISE

Inhalt

Einleitung

In diesem Dokument wird ein Beispiel für TACACS+ über TLS mit Cisco Identity Services Engine (ISE) als Server und einem Cisco IOS® XE-Gerät als Client beschrieben.

Überblick

Das Terminal Access Controller Access-Control System Plus (TACACS+) Protocol [RFC8907] ermöglicht die zentrale Geräteverwaltung für Router, Netzwerkzugriffsserver und andere Netzwerkgeräte über einen oder mehrere TACACS+ Server. Es bietet AAA-Services (Authentication, Authorization und Accounting), die speziell auf Anwendungsfälle der Geräteadministration zugeschnitten sind.

TACACS+ über TLS 1.3 [RFC8446] erweitert das Protokoll durch die Einführung einer sicheren Transportschicht, die hochsensible Daten schützt. Diese Integration gewährleistet Vertraulichkeit, Integrität und Authentifizierung für die Verbindung und den Netzwerkverkehr zwischen TACACS+-Clients und -Servern.

Verwendung dieses Handbuchs

In diesem Leitfaden werden die Aktivitäten in zwei Teile unterteilt, damit die ISE den administrativen Zugriff für Cisco IOS XE-basierte Netzwerkgeräte verwalten kann.
- Teil 1: Konfigurieren der ISE für den Geräteadministrator
- Teil 2: Konfigurieren von Cisco IOS XE für TACACS+ über TLS

Voraussetzungen

Anforderungen

Voraussetzungen für die Konfiguration von TACACS+ über TLS:

- Eine Zertifizierungsstelle (Certificate Authority, CA) zum Signieren des Zertifikats, das von TACACS+ über TLS zum Signieren der Zertifikate von ISE- und Netzwerkgeräten verwendet wird.
- Das Stammzertifikat der Zertifizierungsstelle.
- Netzwerkgeräte und die ISE sind über DNS erreichbar und können Hostnamen auflösen.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- ISE Virtuelle VMware-Appliance, Version 3.4 Patch 2
- Cisco IOS XE Software, Version 17.15+

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Lizenzierung

Mit einer Device Administration-Lizenz können Sie TACACS+-Dienste auf einem Policy Service-Knoten verwenden. In einer Standalone-Bereitstellung mit hoher Verfügbarkeit (HA) ermöglicht eine Device Administration-Lizenz die Verwendung von TACACS+-Services auf einem einzelnen Policy Service-Knoten im HA-Paar.

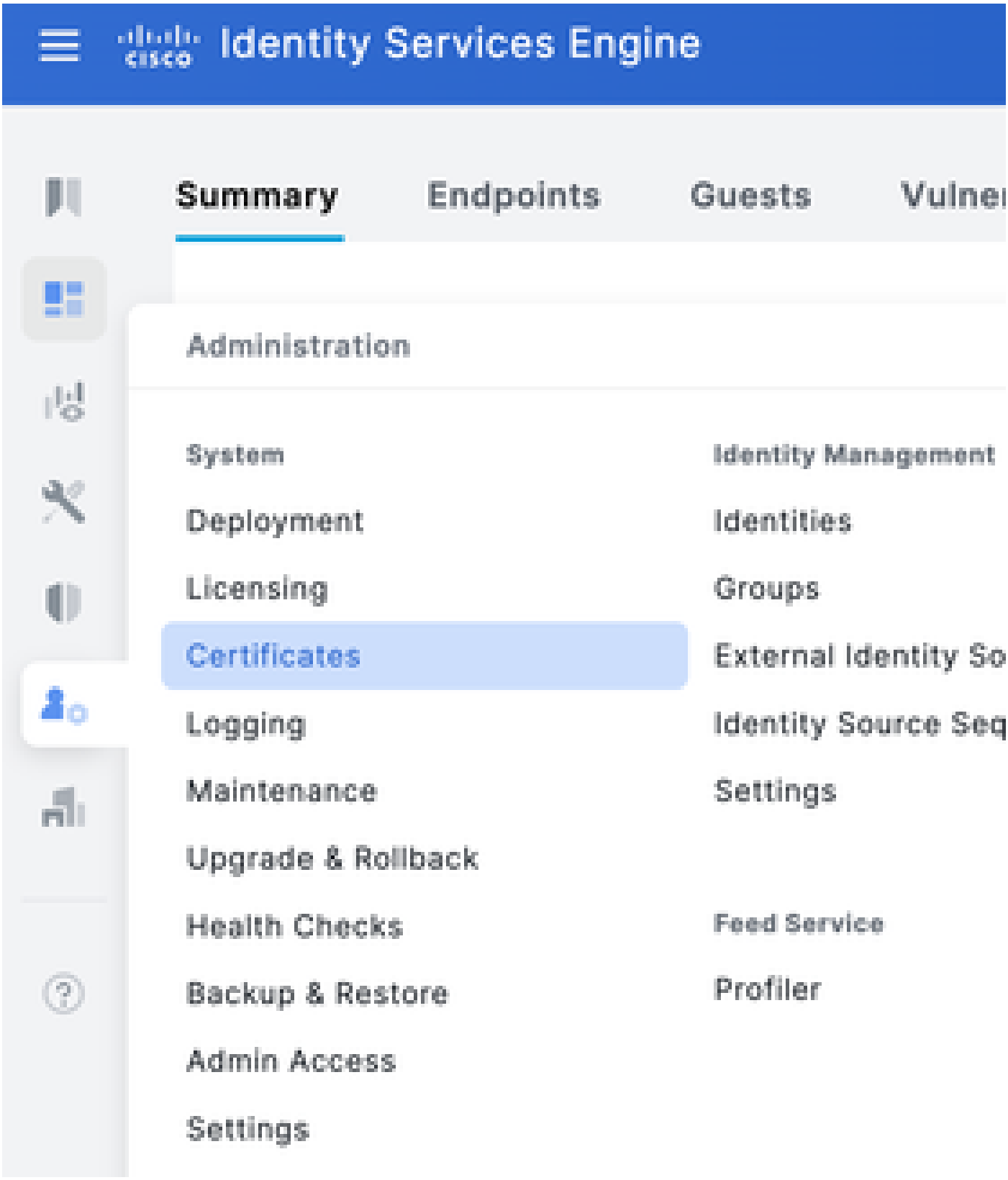
Teil 1: Konfigurieren der ISE für die Geräteverwaltung

Zertifikatsignierungsanforderung für TACACS+-Serverauthentifizierung generieren

Schritt 1: Melden Sie sich mit einem der unterstützten Browser beim ISE-Admin-Webportal an.

Standardmäßig verwendet die ISE ein selbstsigniertes Zertifikat für alle Dienste. Der erste Schritt besteht darin, eine CSR-Anfrage (Certificate Signing Request) zu erstellen, damit sie von unserer Zertifizierungsstelle (Certificate Authority, CA) signiert wird.

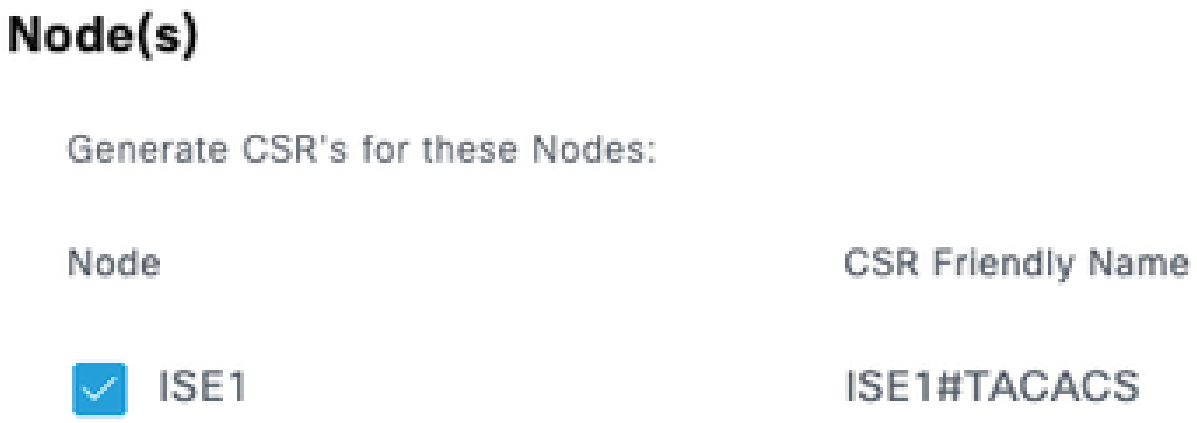
Schritt 2:Navigieren Sie zu Administration > System > Certificates.



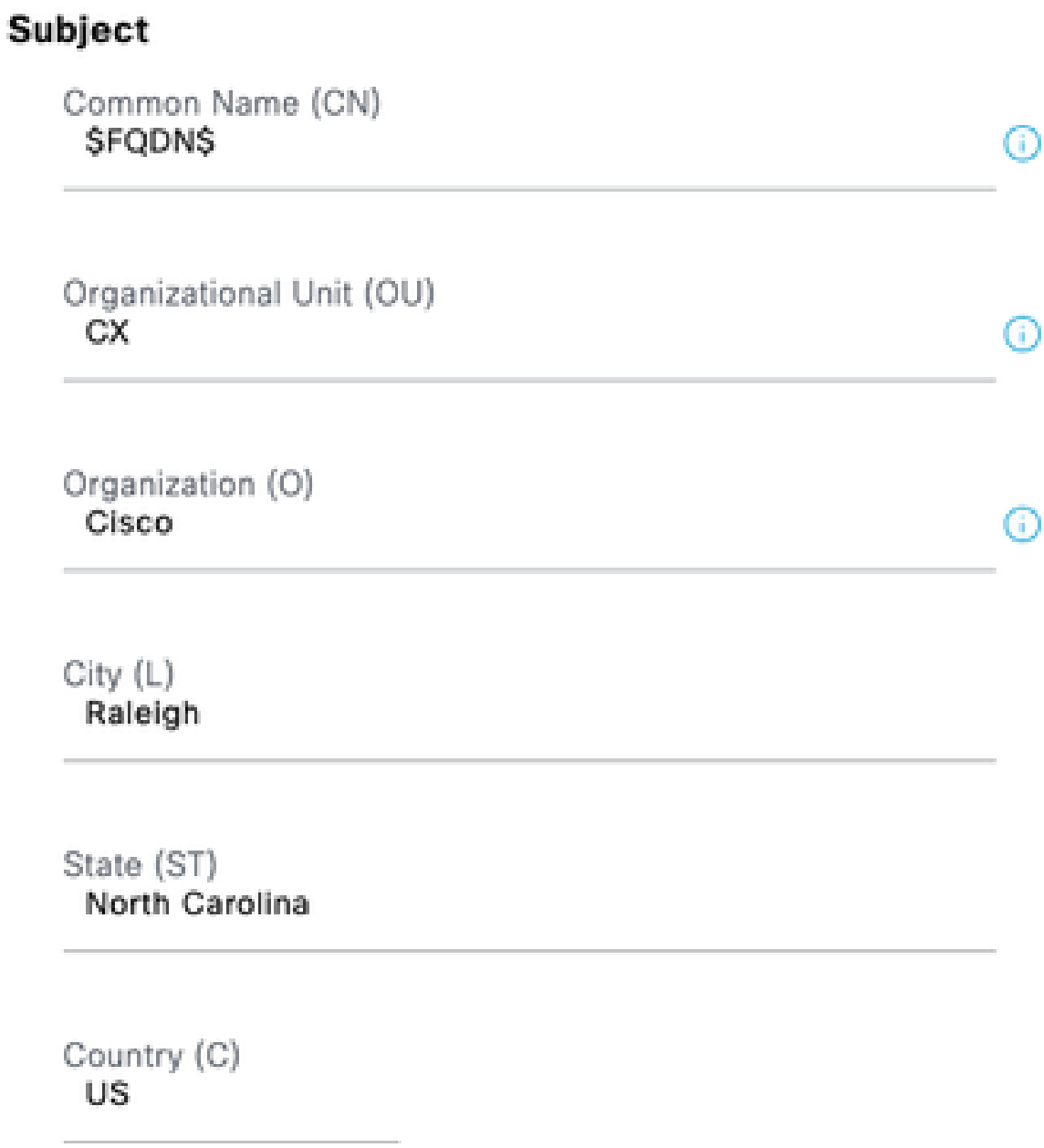
Schritt 3: Klicken Sie unter Zertifikatsignierungsanforderungen auf Zertifikatsignierungsanforderung generieren.

Schritt 4:Wählen Sie TACACS inUsage.

Schritt 5:Wählen Sie die PSNs aus, für die TACACS+ aktiviert ist.

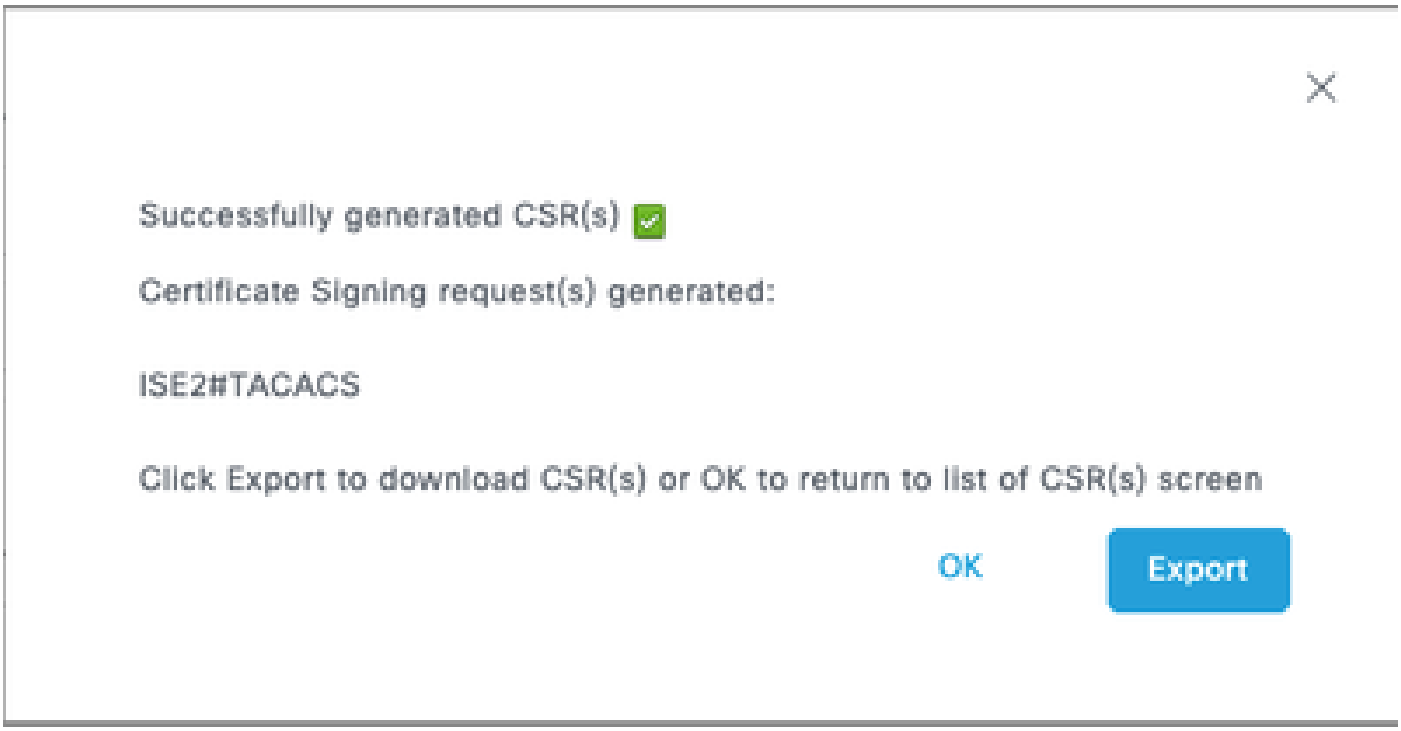


Schritt 6. Füllen Sie die Felder Betreff mit den entsprechenden Informationen aus.



Schritt 7: Fügen Sie den DNS-Namen und die IP-Adresse unter Alternativer Antragstellername (SAN) hinzu.

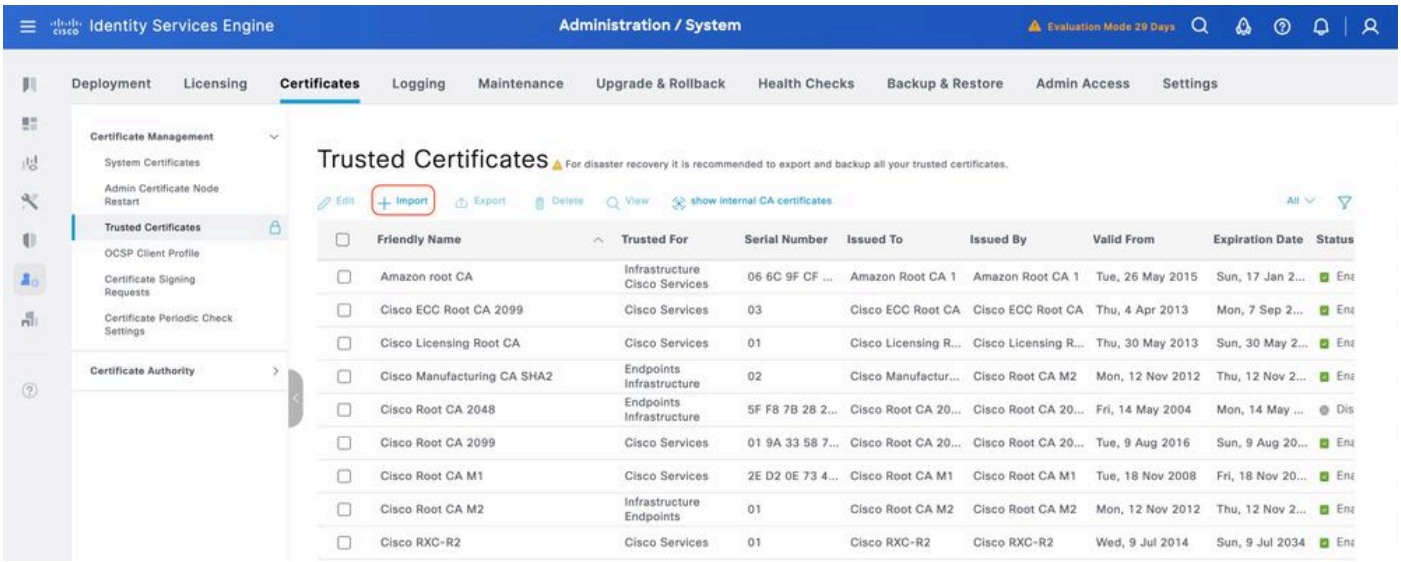
Schritt 8: Klicken Sie auf Generieren und dann auf Exportieren.



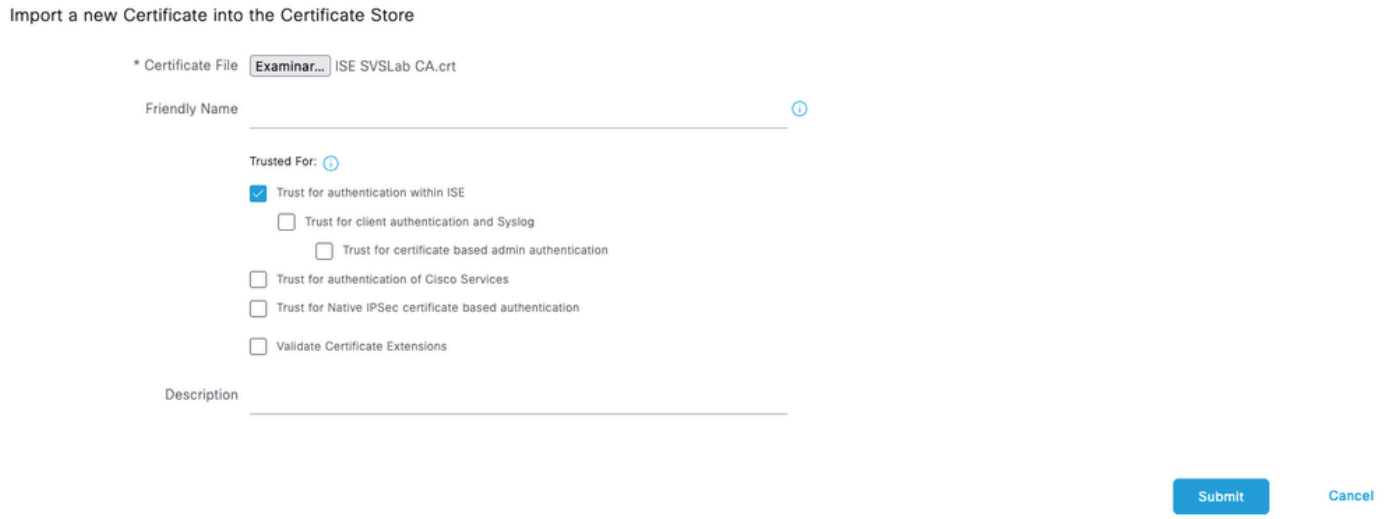
Jetzt können Sie das Zertifikat (CRT) von Ihrer Zertifizierungsstelle (Certificate Authority, CA) signieren lassen.

Hochladen des Zertifikats der Stammzertifizierungsstelle für die TACACS+-Serverauthentifizierung

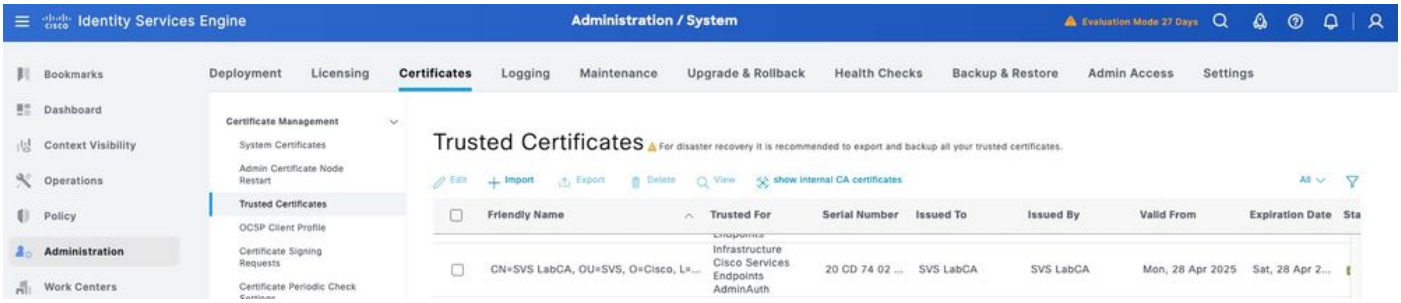
Schritt 1: Navigieren Sie zu Administration > System > Certificates. Klicken Sie unter Vertrauenswürdige Zertifikate auf Importieren.



Schritt 2: Wählen Sie das Zertifikat aus, das von der Zertifizierungsstelle ausgestellt wurde, die Ihre TACACS-Zertifikatsignierungsanfrage (Certificate Signing Request, CSR) signiert hat. Stellen Sie sicher, dassAuthentifizierung innerhalb der ISE vertrauenswürdig ist aktiviert.



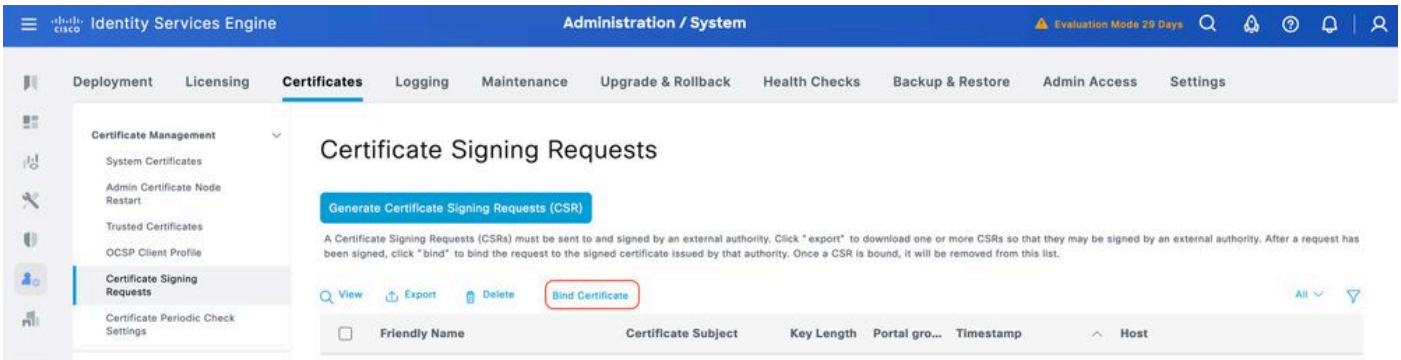
Schritt 3: Klicken Sie auf Senden. Das Zertifikat muss jetzt unter Vertrauenswürdige Zertifikate angezeigt werden.



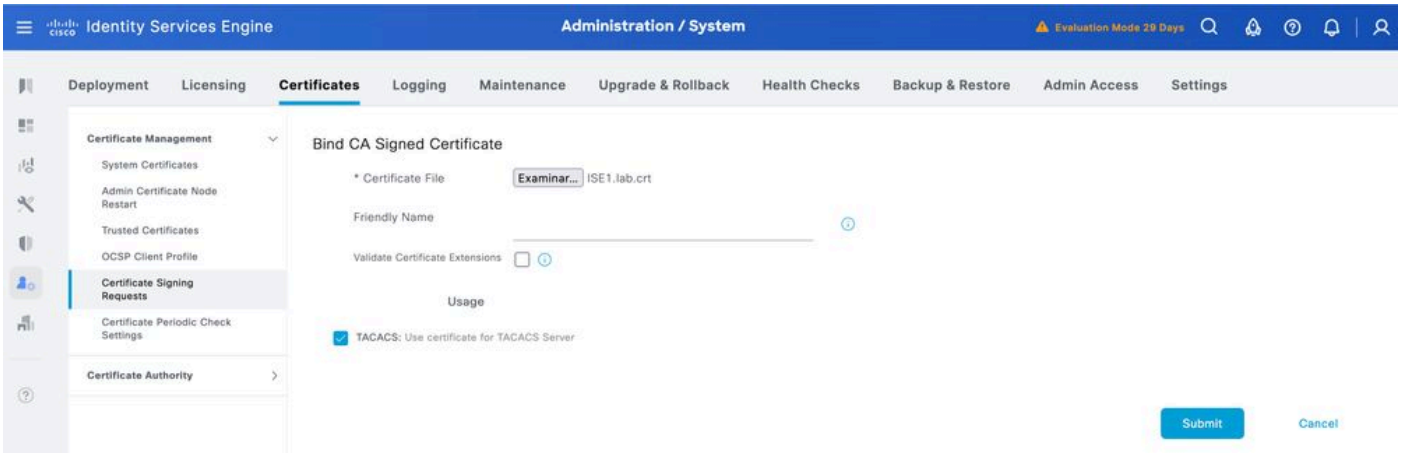
Signierte Zertifikatsanforderung (CSR) an ISE binden

Sobald die CSR-Anforderung (Certificate Signing Request) signiert ist, können Sie das signierte Zertifikat auf der ISE installieren.

Schritt 1:Navigieren Sie zu Administration > System > Certificates. Wählen Sie unter Zertifikatsignierungsanforderungen die im vorherigen Schritt generierte TACACS-CSR aus, und klicken Sie auf Zertifikat binden.

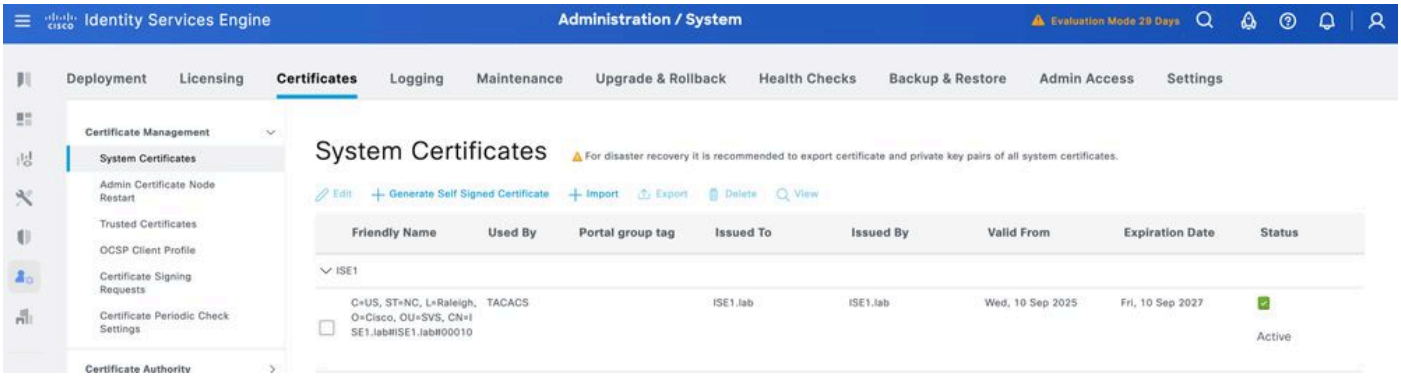


Schritt 2:Wählen Sie das signierte Zertifikat aus, und stellen Sie sicher, dass das Kontrollkästchen TACACS unter Usage (Verwendung) aktiviert bleibt.



Schritt 3: Klicken Sie auf Senden. Wenn Sie eine Warnung bezüglich des Ersetzens des vorhandenen Zertifikats erhalten, klicken Sie auf Ja, um fortzufahren.

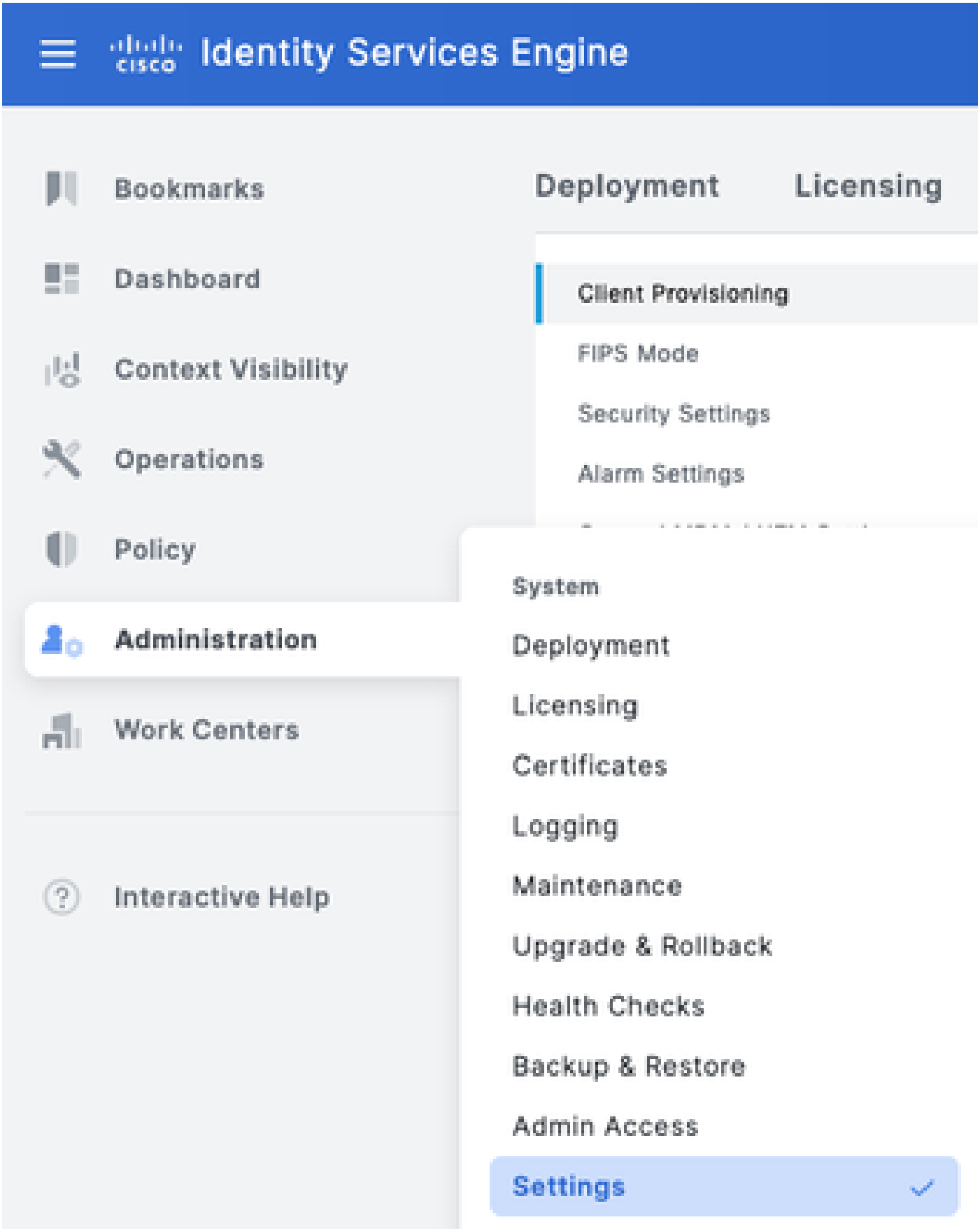
Das Zertifikat muss nun korrekt installiert sein. Sie können dies unter Systemzertifikate überprüfen.



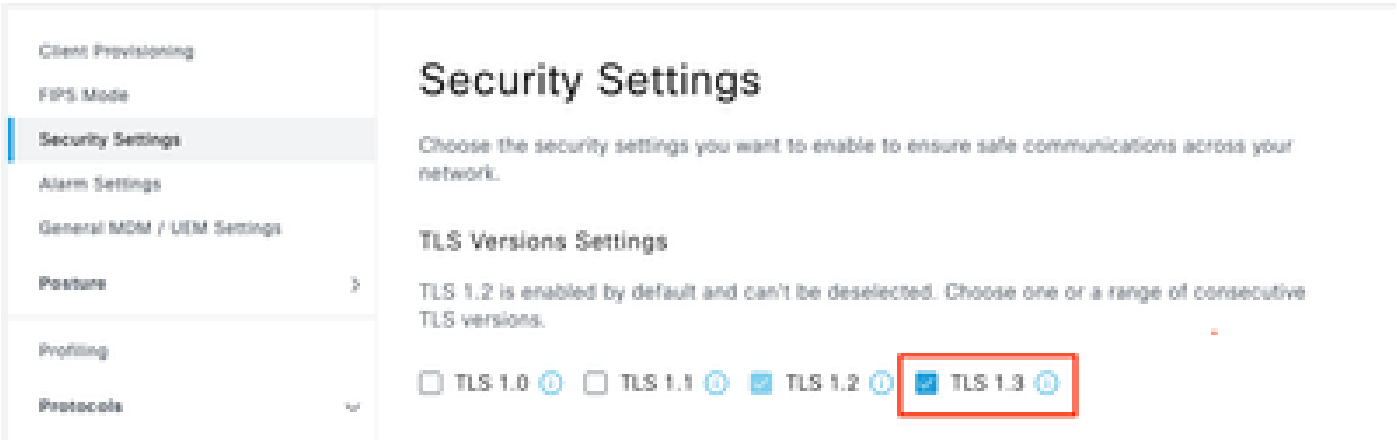
TLS 1.3 aktivieren

TLS 1.3 ist in ISE 3.4.x nicht standardmäßig aktiviert. Sie muss manuell aktiviert werden.

Schritt 1:Navigieren Sie zu Administration > System > Settings.



Schritt 2.Klicken Sie auf Sicherheitseinstellungen, aktivieren Sie das Kontrollkästchen neben TLS1.3 unter TLS-Versionseinstellungen, und klicken Sie dann auf Speichern.

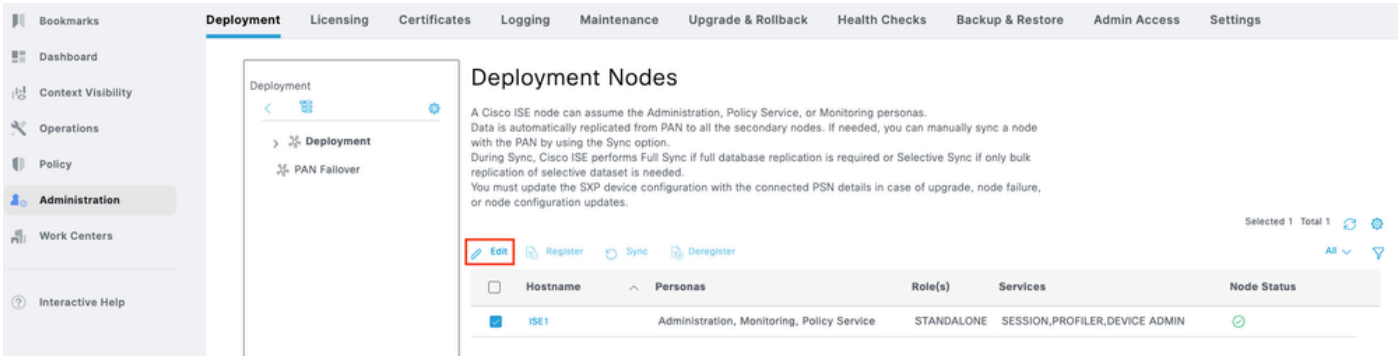


Warnung: Wenn Sie die TLS-Version ändern, wird der Cisco ISE-Anwendungsserver auf allen Cisco ISE-Bereitstellungssystemen neu gestartet.

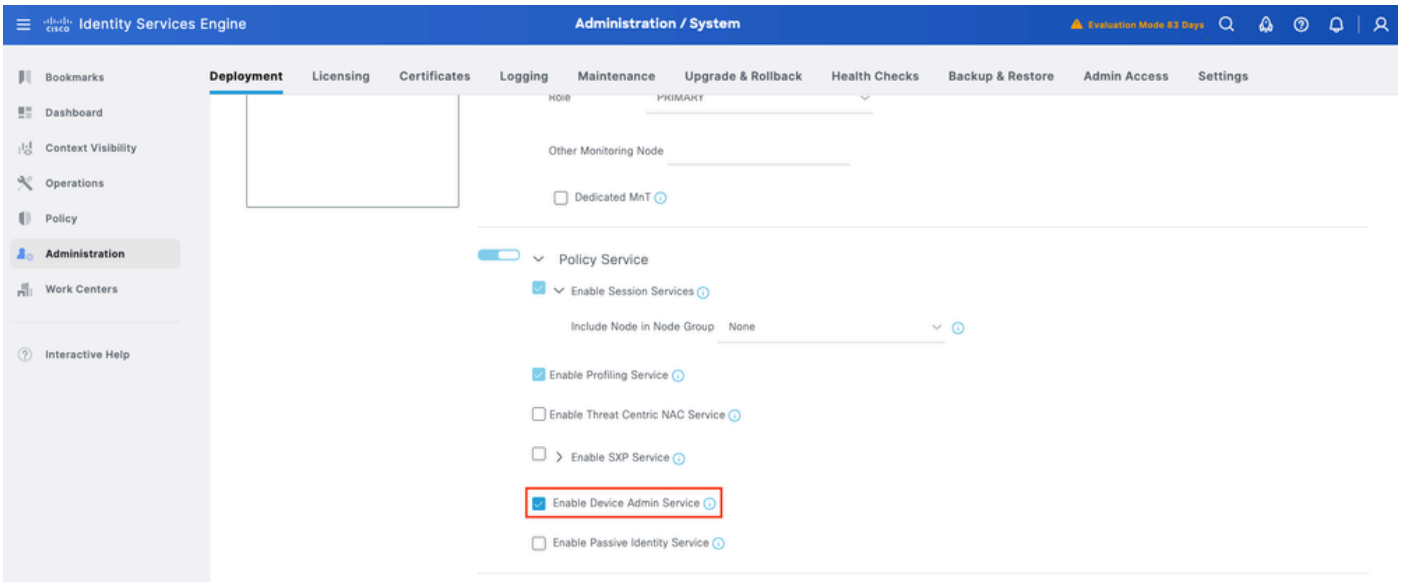
Geräteadministration auf ISE aktivieren

Der Device Administration Service (TACACS+) ist auf einem ISE-Knoten nicht standardmäßig aktiviert. Aktivieren Sie TACACS+ auf einem PSN-Knoten.

Schritt 1:Navigieren Sie zu Administration > System > Deployment. Aktivieren Sie das Kontrollkästchen neben dem ISE-Knoten, und klicken Sie auf Edit.



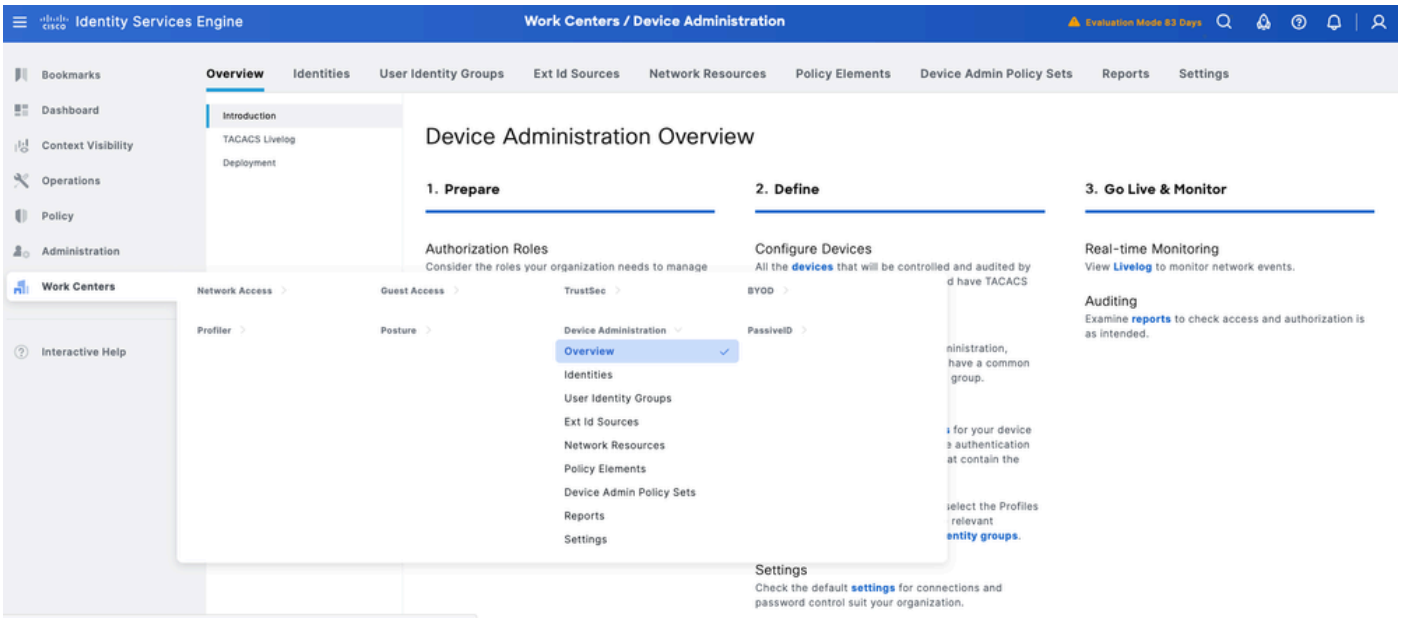
Schritt 2: Blättern Sie unter General Settings nach unten, und aktivieren Sie das Kontrollkästchen neben Enable Device Admin Service.



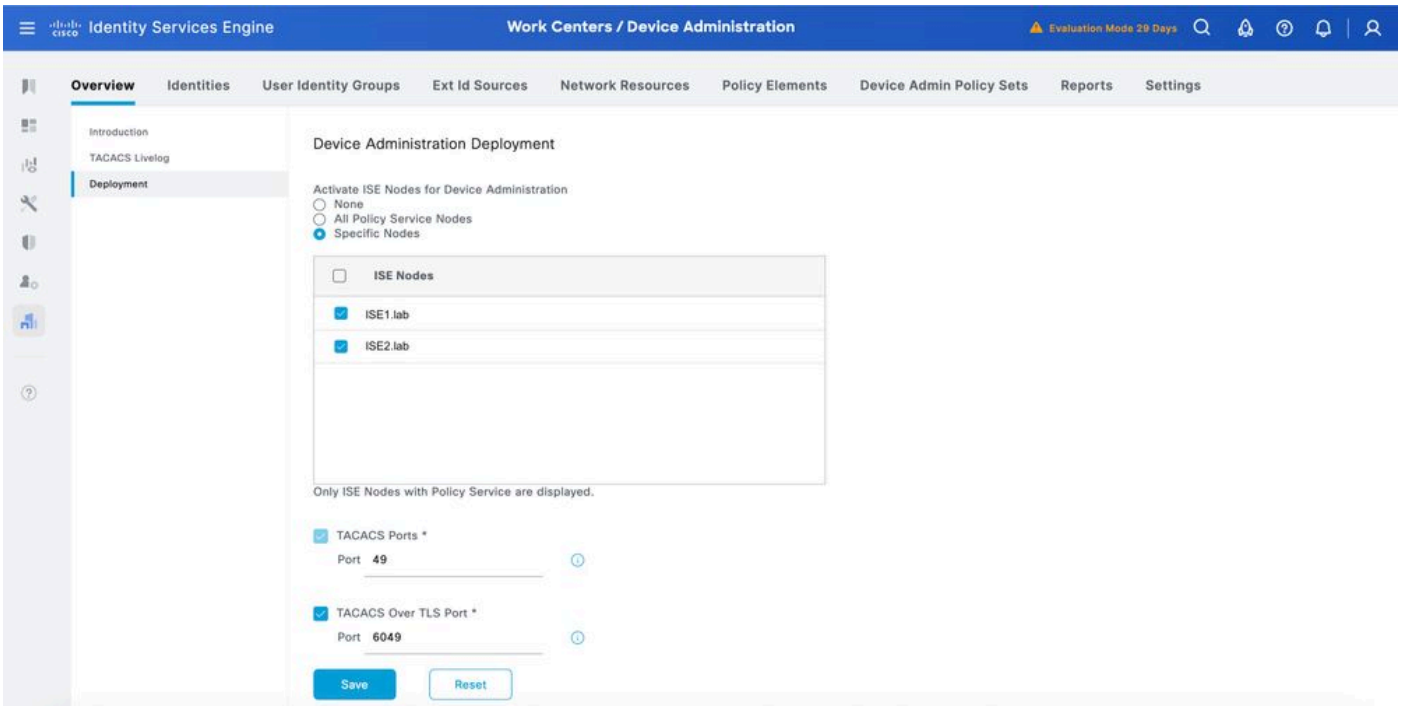
Schritt 3: Speichern der Konfiguration Der Geräteverwaltungsdienst ist jetzt auf der ISE aktiviert.

Aktivieren von TACACS über TLS

Schritt 1:Navigieren Sie zu Work Centers > Device Administration > Overview.



Schritt 2: Klicken Sie auf Bereitstellung. Wählen Sie die PSN-Knoten aus, bei denen TACACS über TLS aktiviert werden soll.



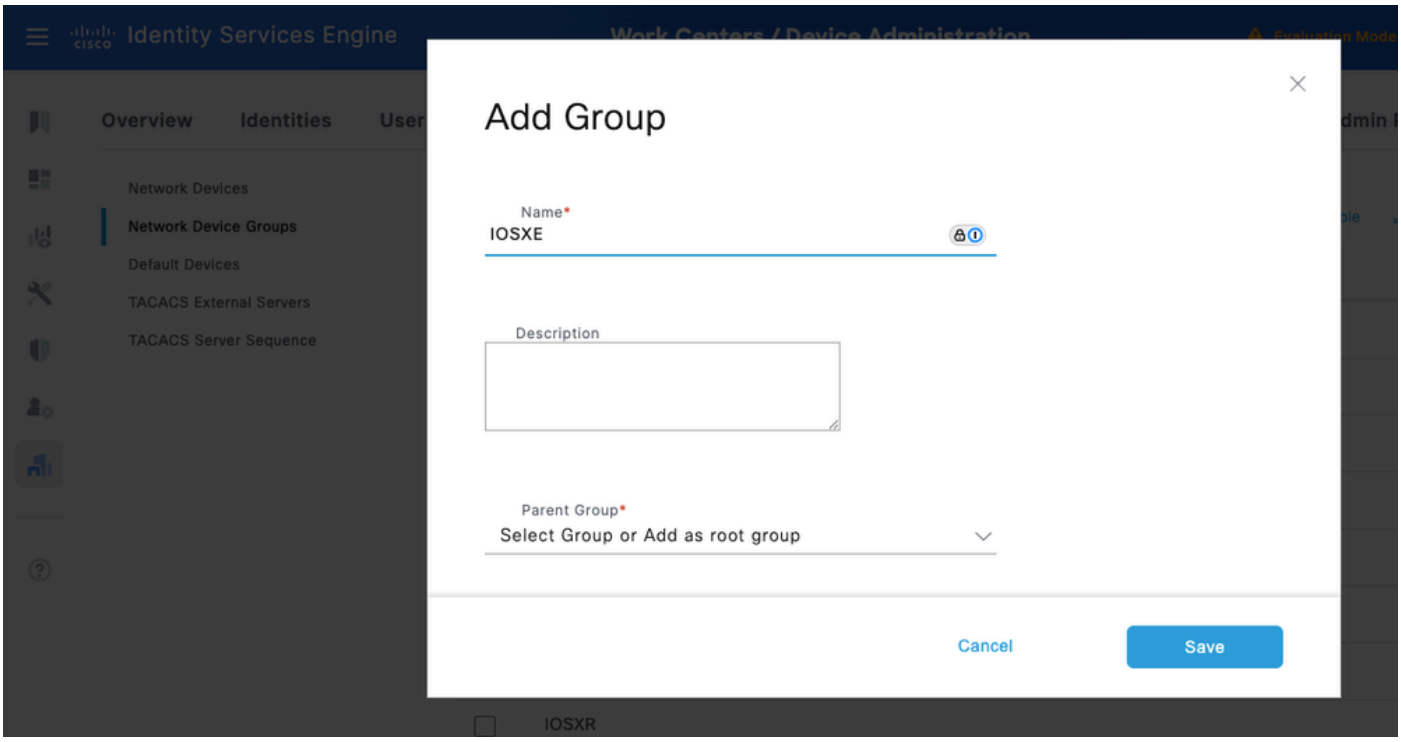
Schritt 3:Behalten Sie den Standardport 6049 bei, oder geben Sie einen anderen TCP-Port für TACACS über TLS an, und klicken Sie dann auf Save.

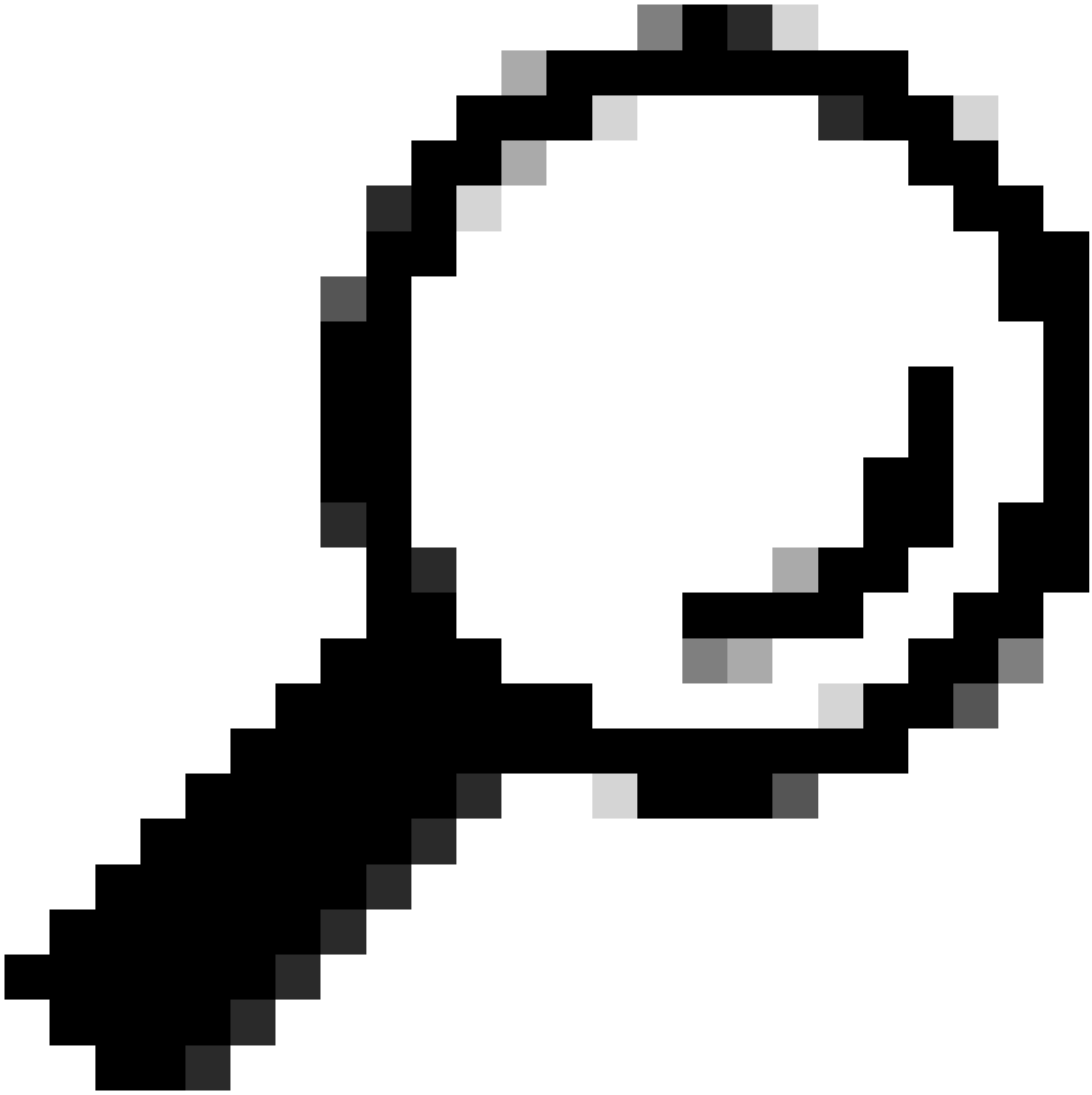
Netzwerkgeräte- und Netzwerkgerätegruppen erstellen

Die ISE ermöglicht eine leistungsstarke Gruppierung von Geräten mit mehreren Hierarchien von Gerätegruppen. Jede Hierarchie stellt eine eigene und unabhängige Klassifizierung von Netzwerkgeräten dar.

Schritt 1: Navigieren Sie zu Work Centers > Device Administration > Network Resources.Klicken Sie auf Network Device Groups (Netzwerkgerätegruppen), und erstellen Sie eine Gruppe mit dem

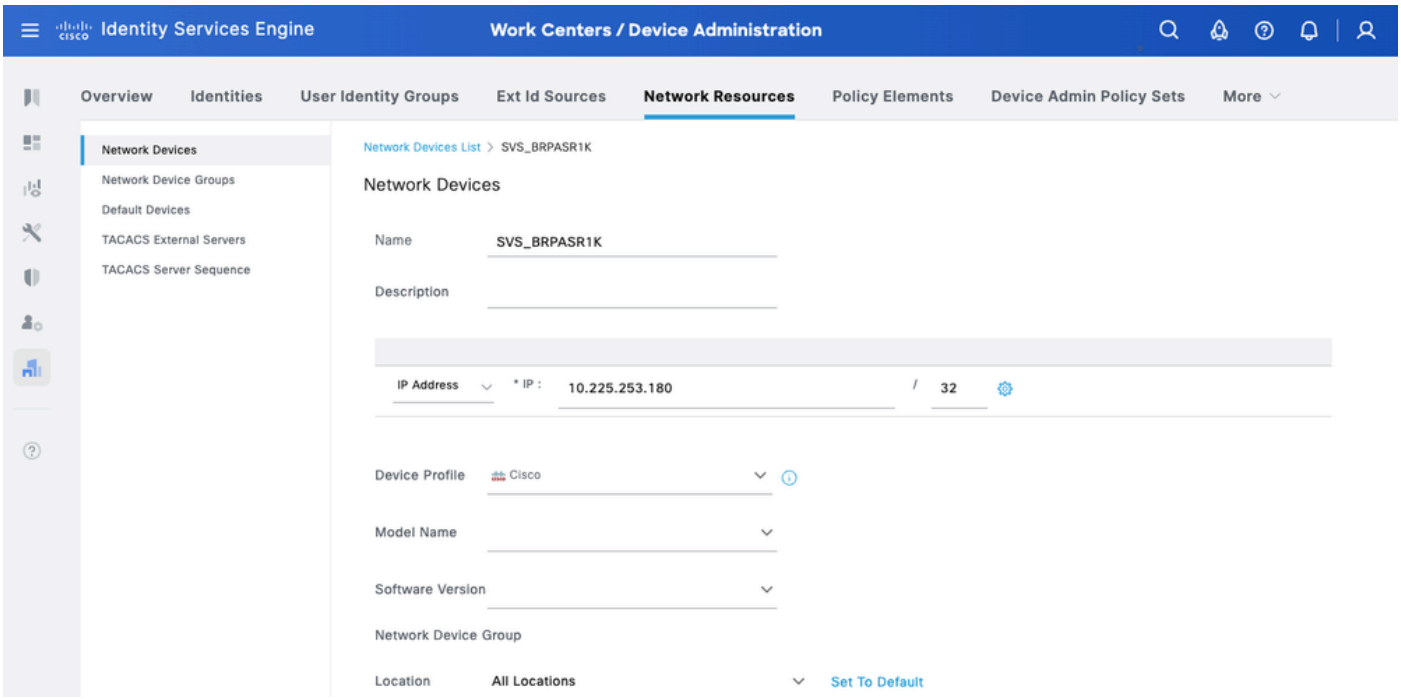
Namen IOS XE.


Identity Services Engine
Work Centers / Device Administration
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

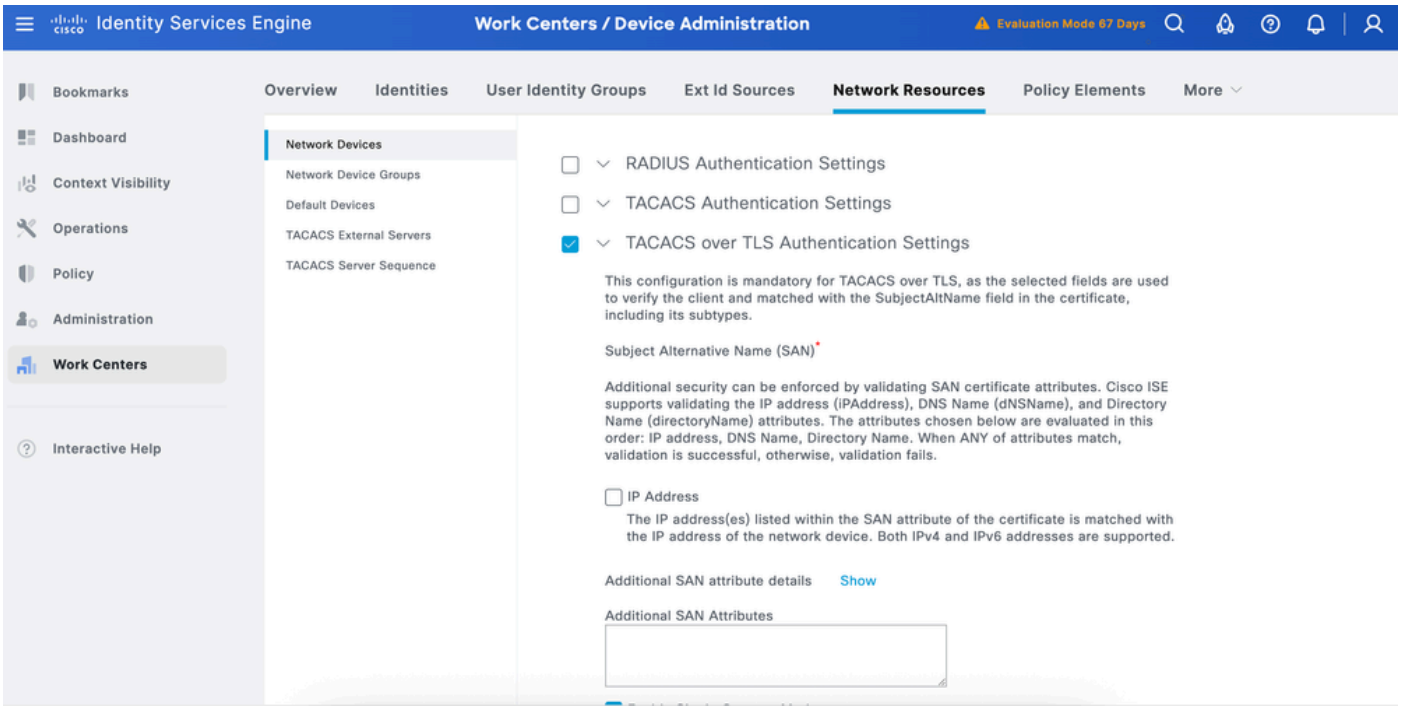


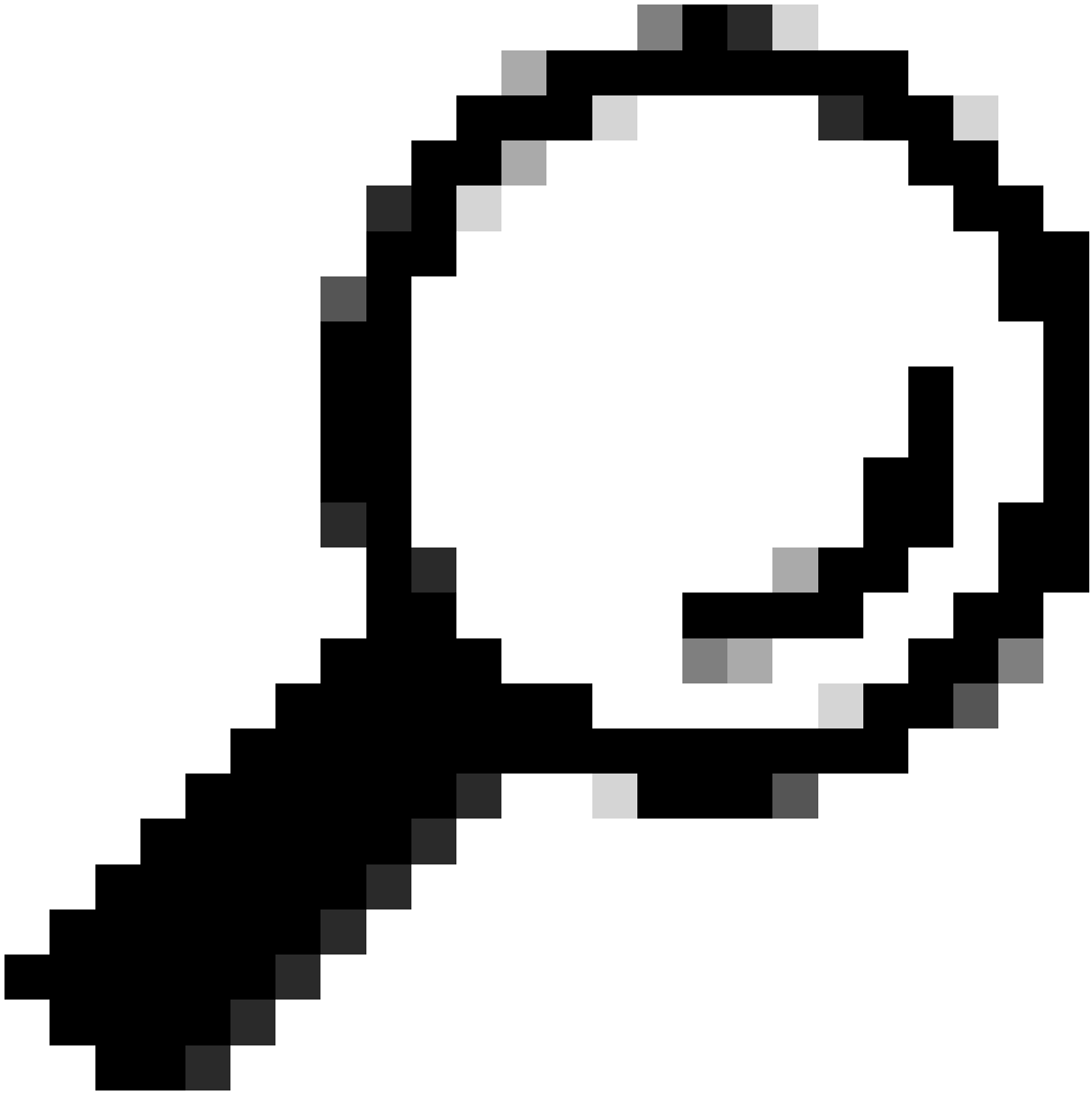
Tipp: Alle Gerätetypen und alle Standorte sind die von der ISE bereitgestellten Standardhierarchien. Sie können Ihre eigenen Hierarchien hinzufügen und die verschiedenen Komponenten bei der Identifizierung eines Netzwerkgeräts definieren, das später in der Richtlinienbedingung verwendet werden kann.

Schritt 2:Fügen Sie jetzt ein Cisco IOS XE-Gerät als Netzwerkgerät hinzu. Navigieren Sie zu Work Centers > Device Administration > Network Resources > Network Devices. Klicken Sie auf Hinzufügen, um ein neues Netzwerkgerät hinzuzufügen. Für diesen Test wäre dies SVS_BRPASR1K.



Schritt 3:Geben Sie die IP-Adresse des Geräts ein, und stellen Sie sicher, dass Standort und Gerätetyp (IOS XE) für das Gerät zugeordnet sind. Aktivieren Sie abschließend die TACACS+ über TLS-Authentifizierungseinstellungen.



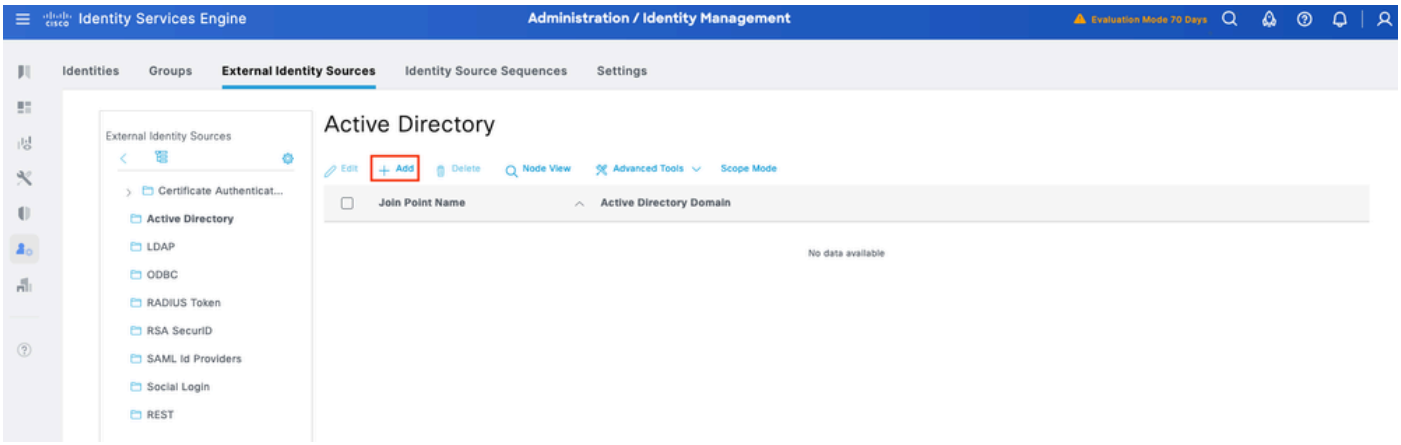


Tipp: Es wird empfohlen, den Single-Connect-Modus zu aktivieren, um zu vermeiden, dass die TCP-Sitzung jedes Mal neu gestartet wird, wenn ein Befehl an das Gerät gesendet wird.

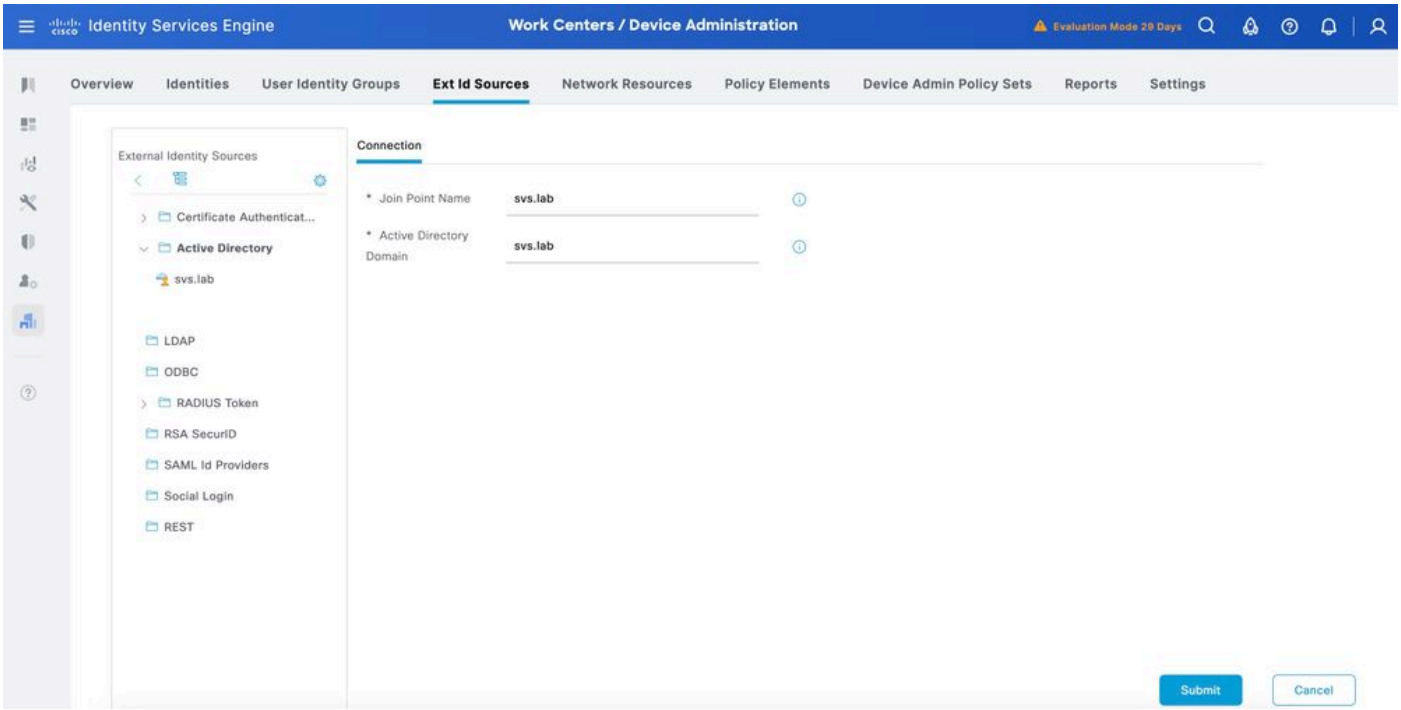
KonfigurierenIdentitätsspeicher

In diesem Abschnitt wird ein Identitätsspeicher für die Geräteadministratoren definiert. Dabei kann es sich um die internen ISE-Benutzer und alle unterstützten externen Identitätsquellen handeln. Verwendet Active Directory (AD), eine externe Identitätsquelle.

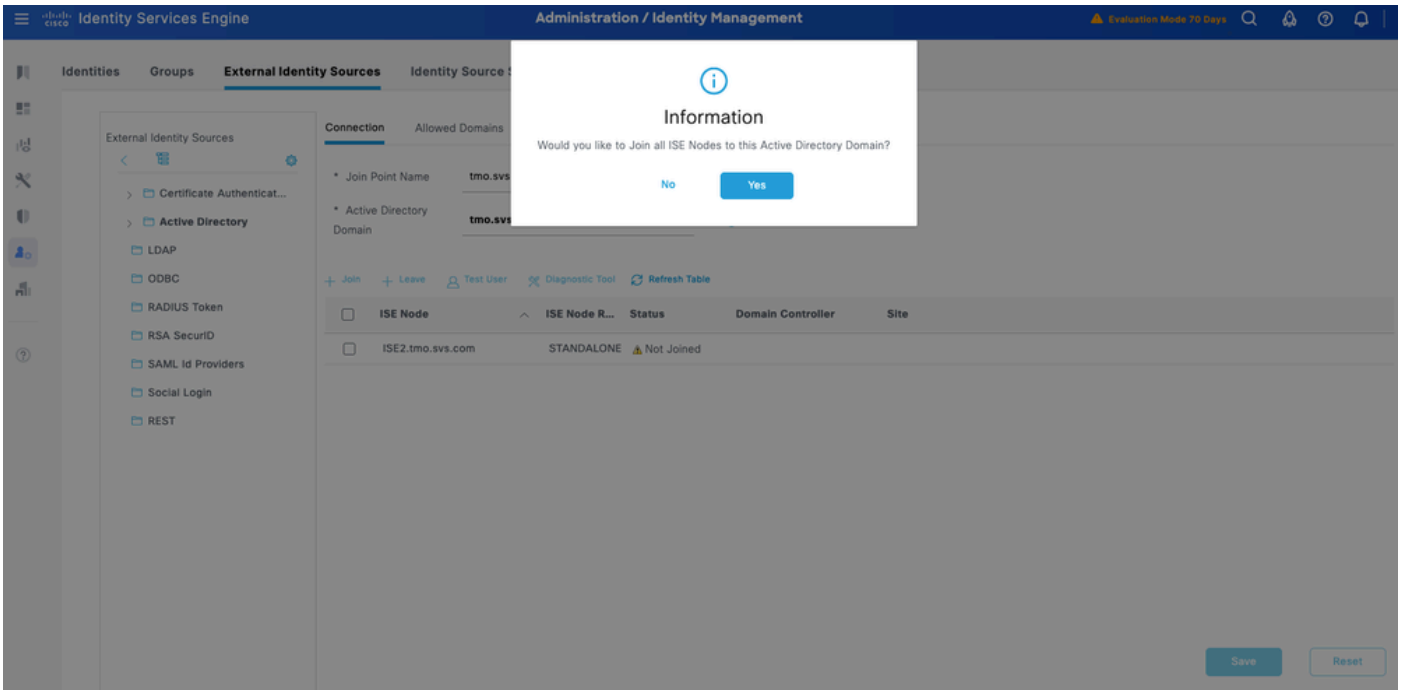
Schritt 1: Navigieren Sie zu Administration > Identity Management > External Identity Stores > Active Directory. Klicken Sie auf Hinzufügen, um einen neuen AD-Gelenkpunkt zu definieren.



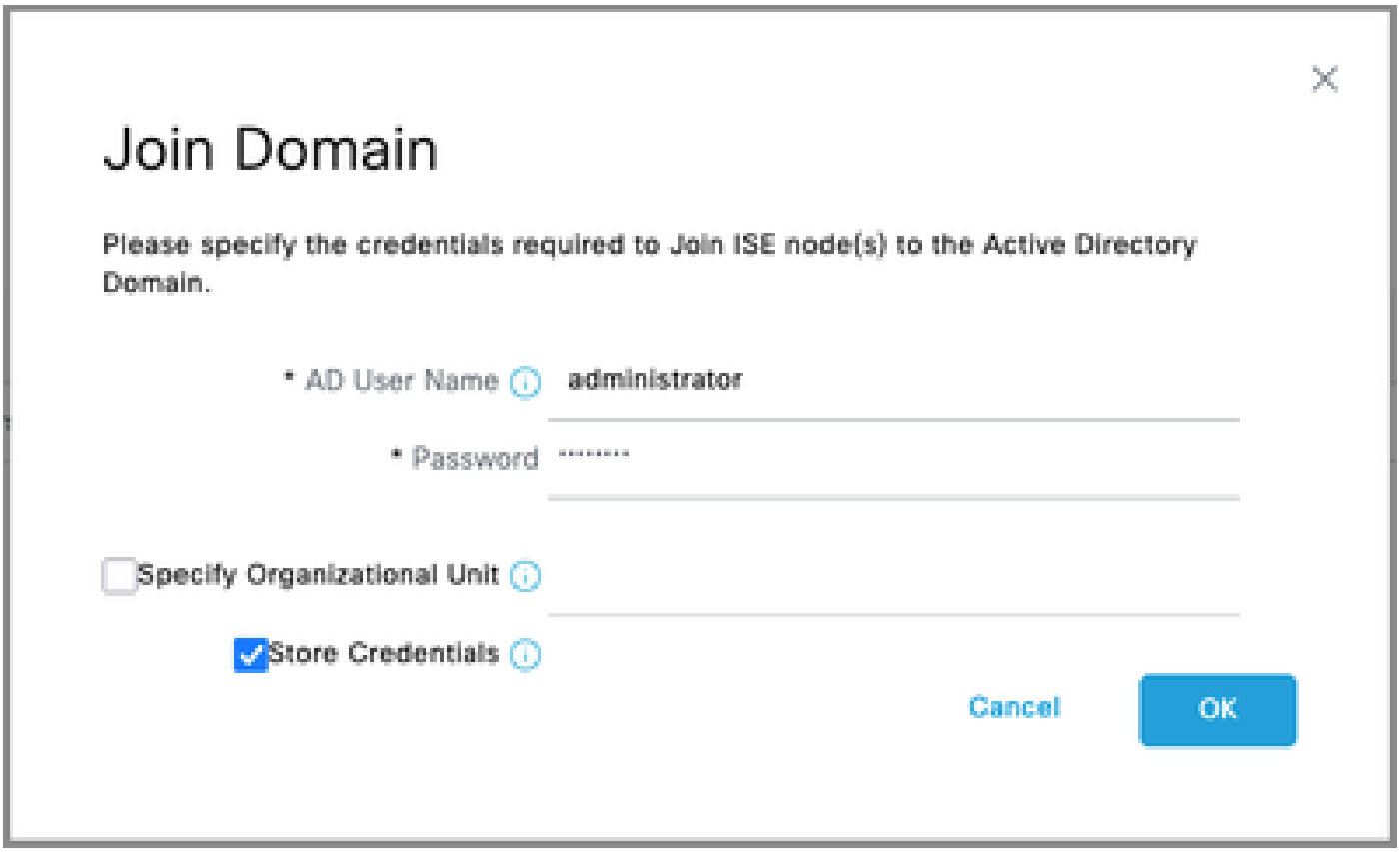
Schritt 2: Geben Sie den Namen des Verbindungspunkts und den AD-Domänennamen an, und klicken Sie auf Senden.

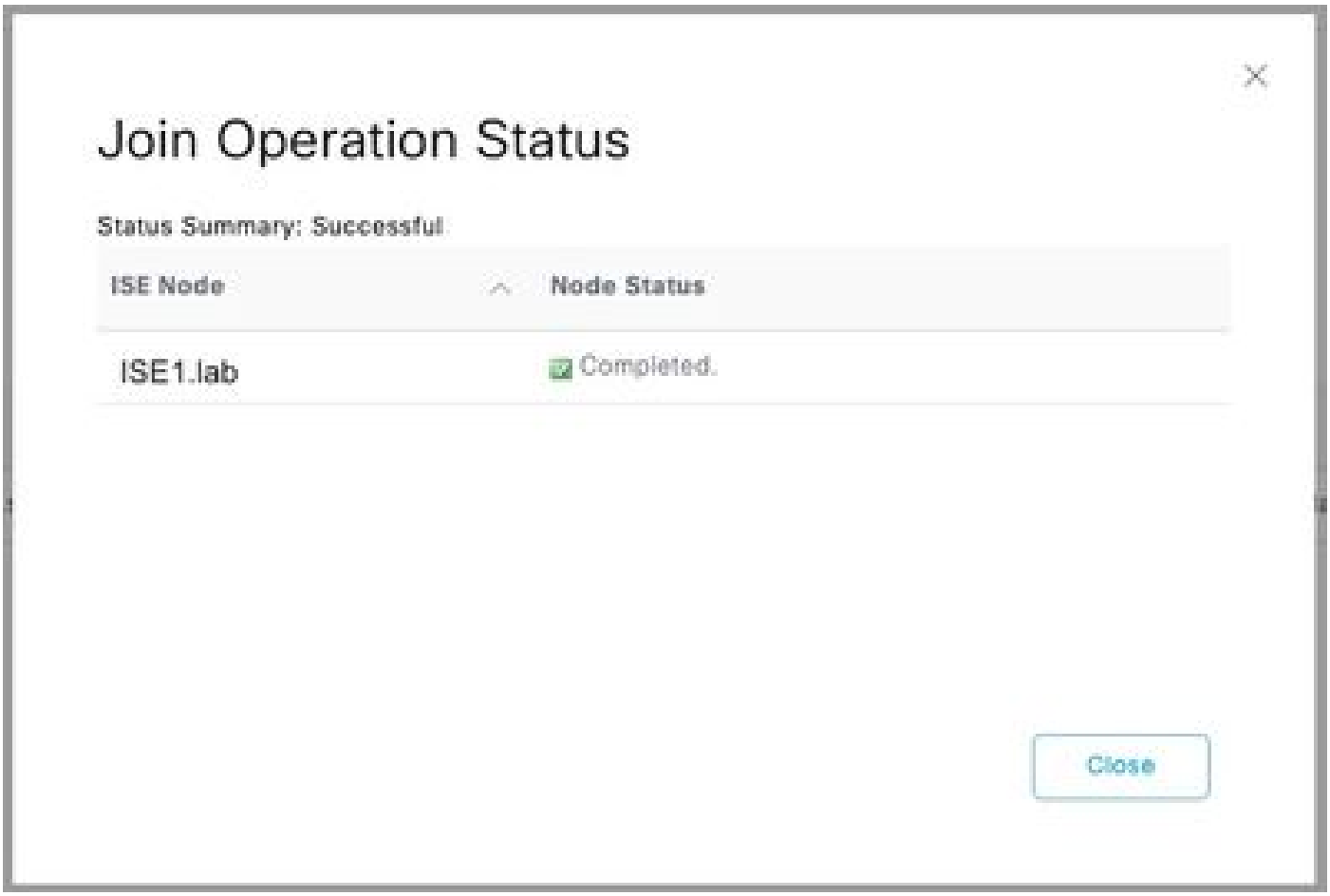


Schritt 3. Klicken Sie auf Ja, wenn Sie dazu aufgefordert werden Möchten Sie allen ISE-Knoten in dieser Active Directory-Domäne beitreten?

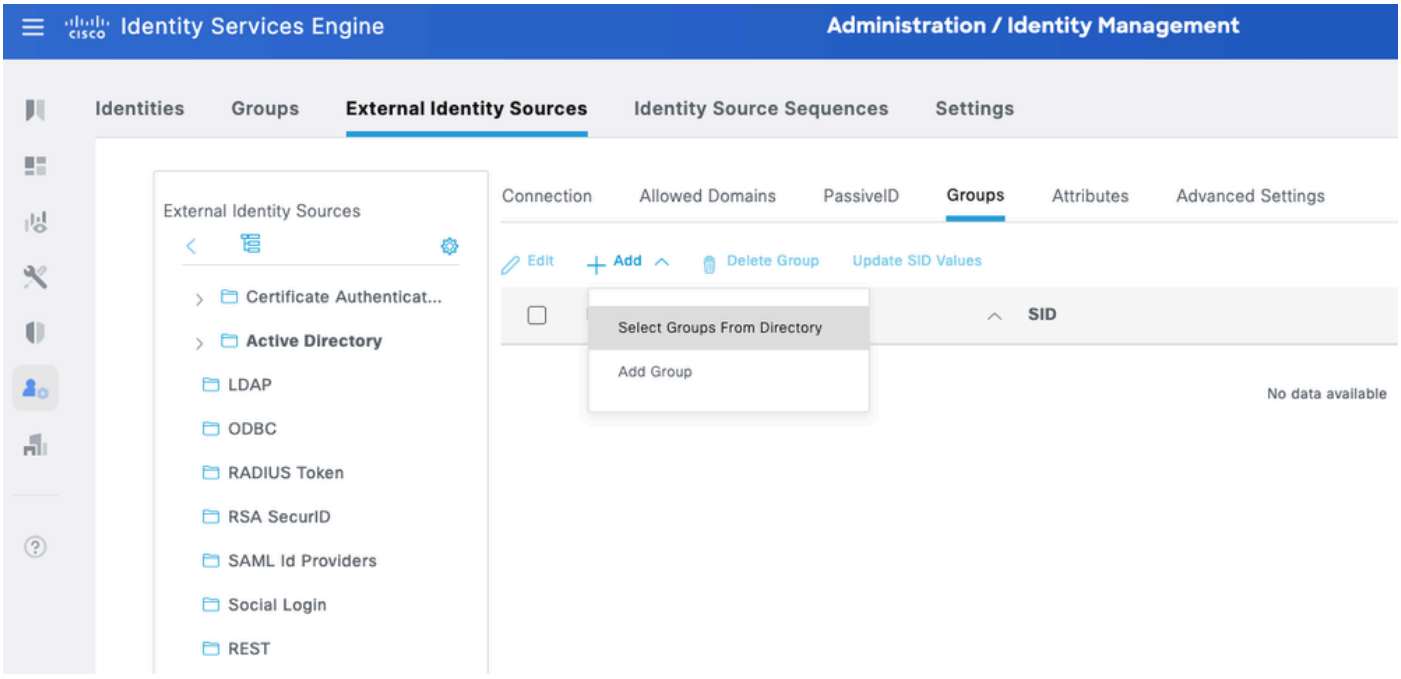


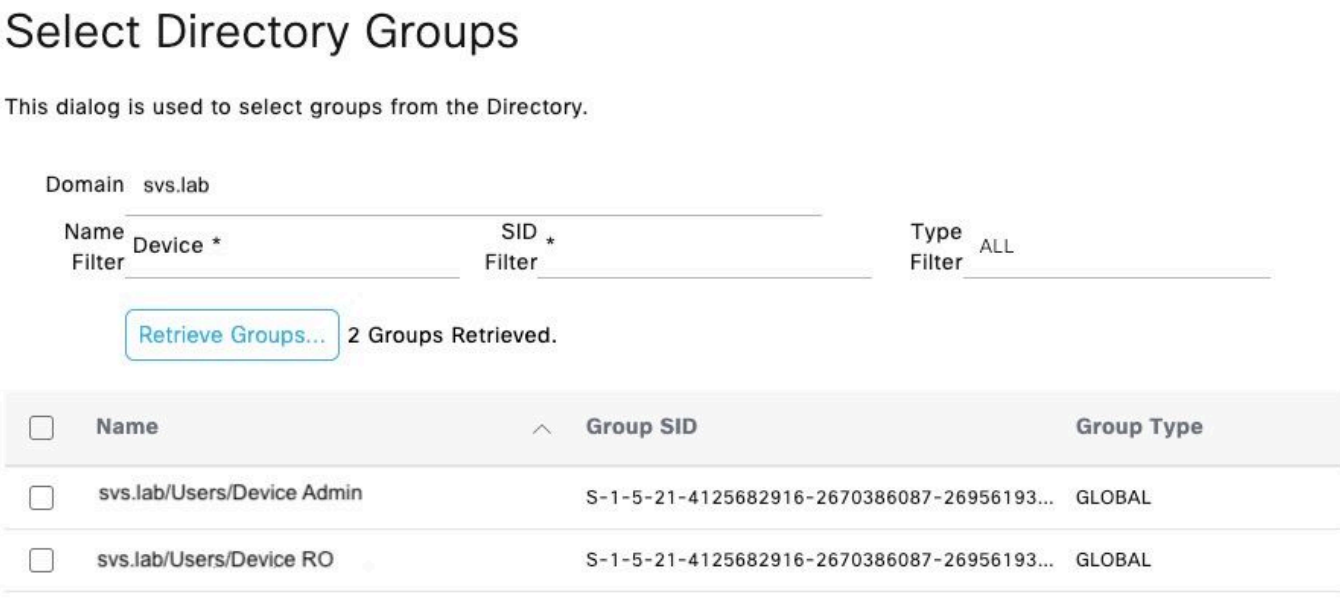
Schritt 4: Geben Sie die Anmeldeinformationen mit AD-Join-Berechtigungen ein, und treten Sie ISE bei AD bei. Überprüfen Sie den Status, um sicherzustellen, dass er betriebsbereit ist.

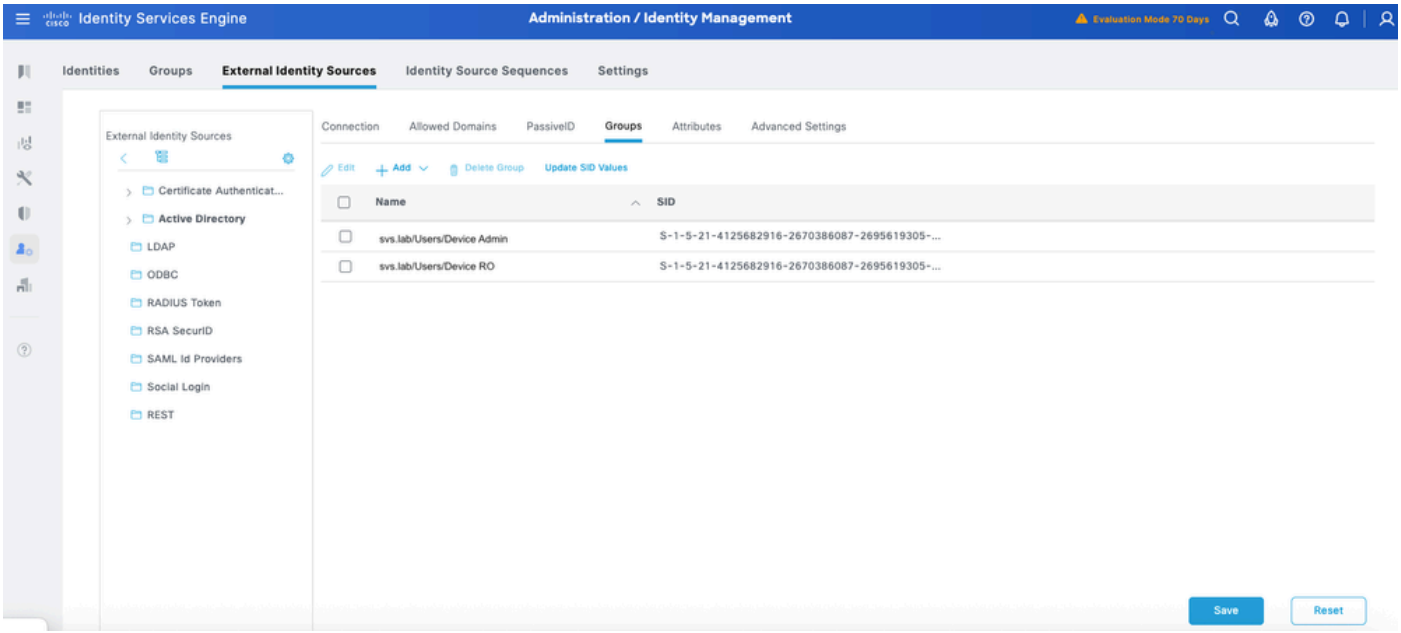




Schritt 5: Navigieren Sie zur Registerkarte Gruppen, und klicken Sie auf Hinzufügen, um alle erforderlichen Gruppen abzurufen, basierend auf denen die Benutzer für den Gerätezugriff autorisiert sind. Dieses Beispiel zeigt die Gruppen, die in der Autorisierungsrichtlinie in diesem Leitfaden verwendet werden.







Konfigurieren von TACACS+-Profilen

Sie ordnen die TACACS+-Profile den beiden Hauptbenutzerrollen auf den Cisco IOS XE-Geräten zu:

- Root-Systemadministrator: Dies ist die Rolle mit den höchsten Berechtigungen auf dem Gerät. Der Benutzer mit der Root-Systemadministratorrolle hat vollständigen Administratorzugriff auf alle Systembefehle und Konfigurationsfunktionen.
- Operator - Diese Rolle ist für Benutzer vorgesehen, die schreibgeschützten Zugriff auf das System benötigen, um das System zu überwachen und Fehler zu beheben.

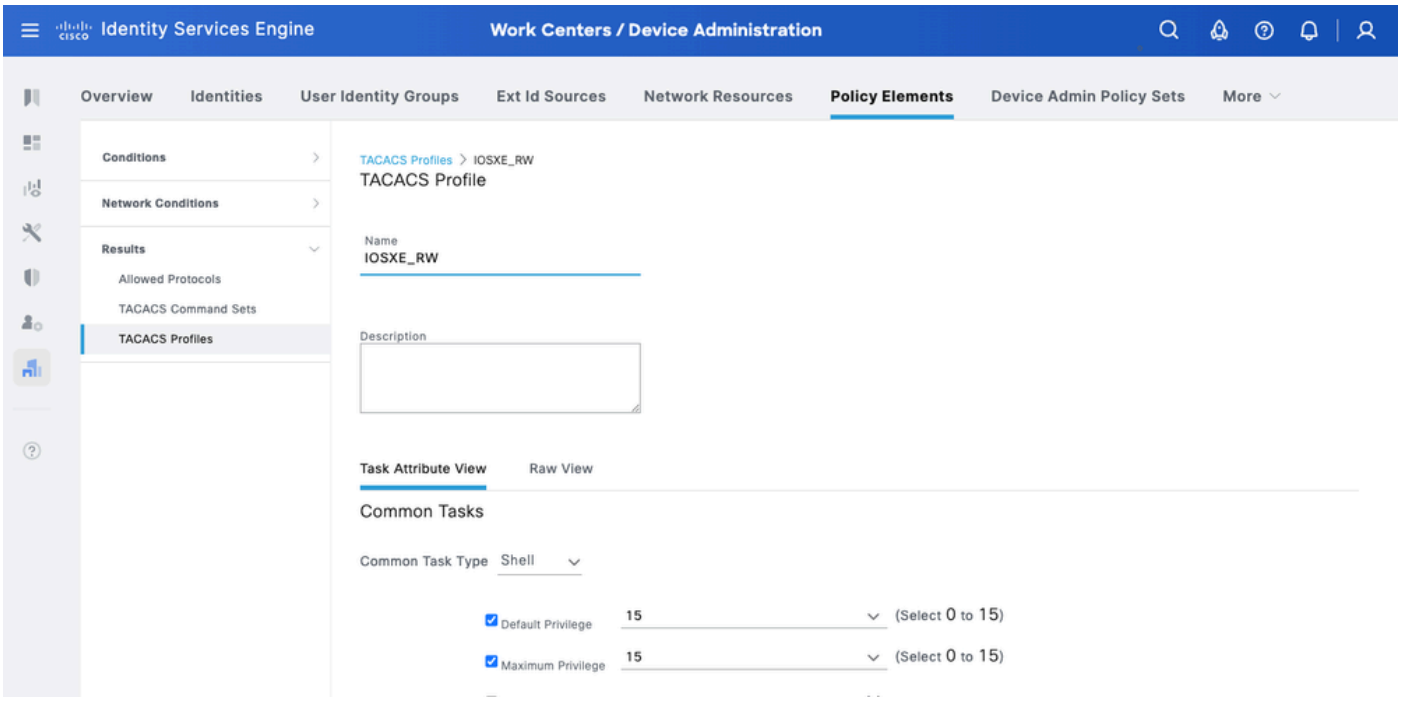
Diese werden als zwei TACACS+-Profile definiert: IOS XE_RW und IOSXR_RO.

IOS XE_RW - Administratorprofil

Schritt 1 Navigieren Sie zu Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles. Fügen Sie ein neues TACACS-Profil hinzu, und nennen Sie es IOS XE_RW.

Schritt 2: Aktivieren Sie das Kontrollkästchen und setzen Sie die Standardberechtigungen und die Höchstberechtigungen auf 15.

Schritt 3:Bestätigen Sie die Konfiguration und speichern Sie.

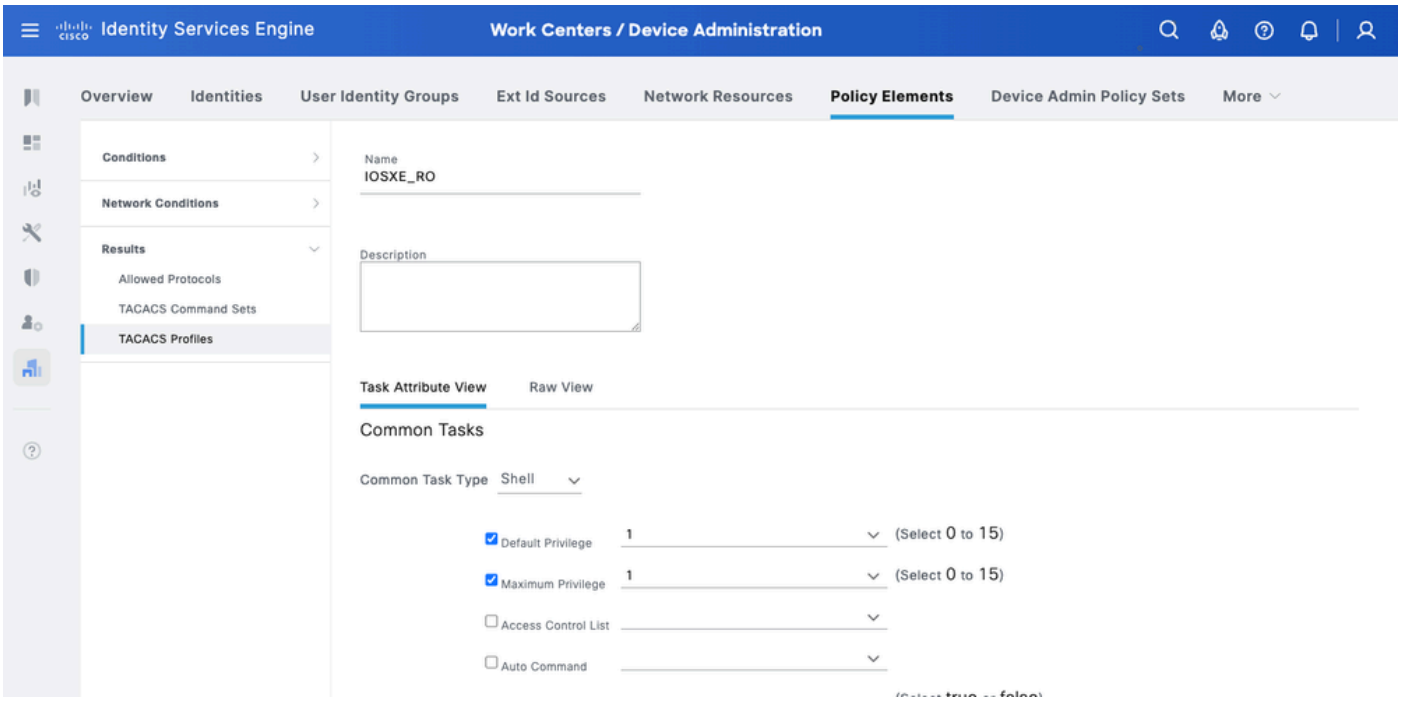


IOS XE_RO - Betreiberprofil

Schritt 1 Navigieren Sie zu Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles. Fügen Sie ein neues TACACS-Profil hinzu, und nennen Sie es IOS XE_RO.

Schritt 2: Aktivieren Sie Default Privilege (Standardberechtigung) und Maximum Privilege (Maximale Berechtigung), und legen Sie als 1 fest.

Schritt 3:Bestätigen Sie die Konfiguration und speichern Sie.



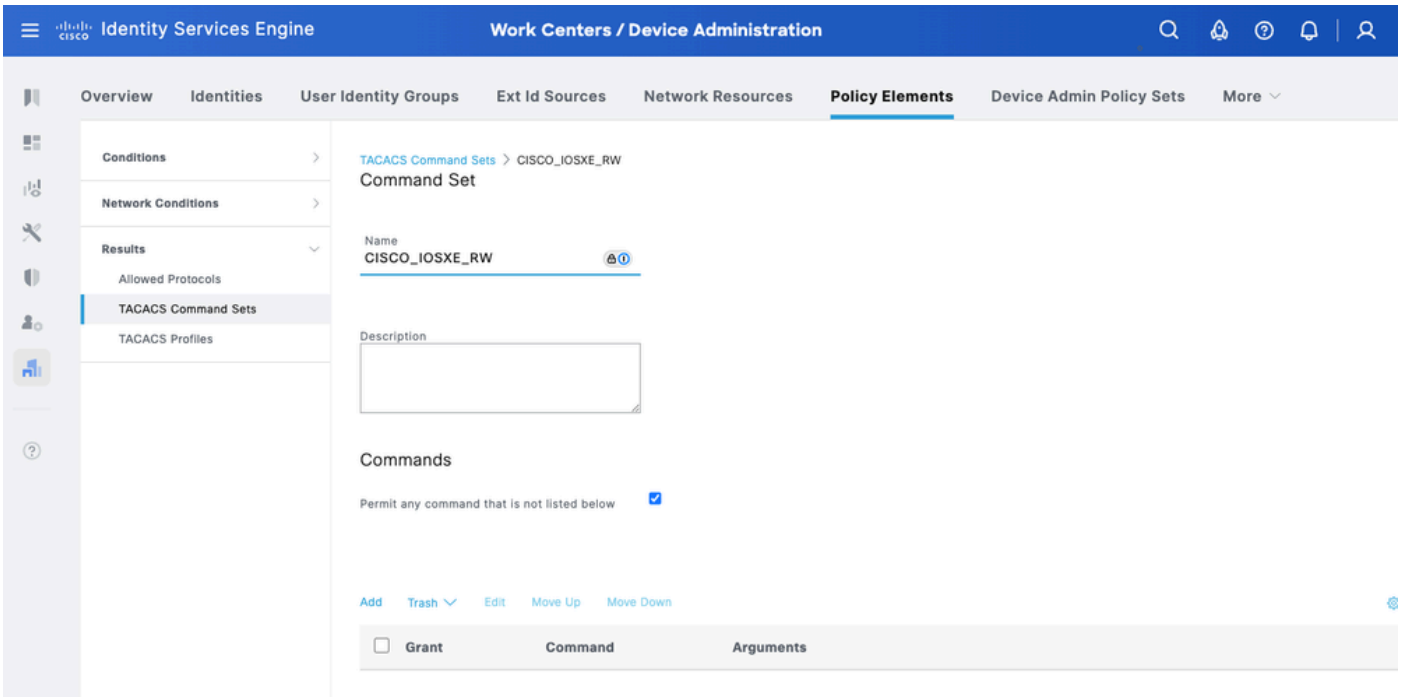
Konfigurieren von TACACS+-Befehlssätzen

Diese werden als zwei TACACS+-Befehlssätze definiert: CISCO_IOS XE_RW und CISCO_IOS XE_RO.

CISCO_IOS XE_RW - Administrator-Befehlssatz

Schritt 1: Navigieren Sie zu Work Centers > Device Administration > Policy Elements > Results > TACACS Command Sets. Fügen Sie einen neuen TACACS Command Set hinzu, und nennen Sie ihn CISCO_IOS XE_RW.

Schritt 2. Aktivieren Sie das Kontrollkästchen Befehle zulassen, die unten nicht aufgeführt sind (dies ermöglicht beliebige Befehle für die Administratorrolle), und klicken Sie auf Speichern.



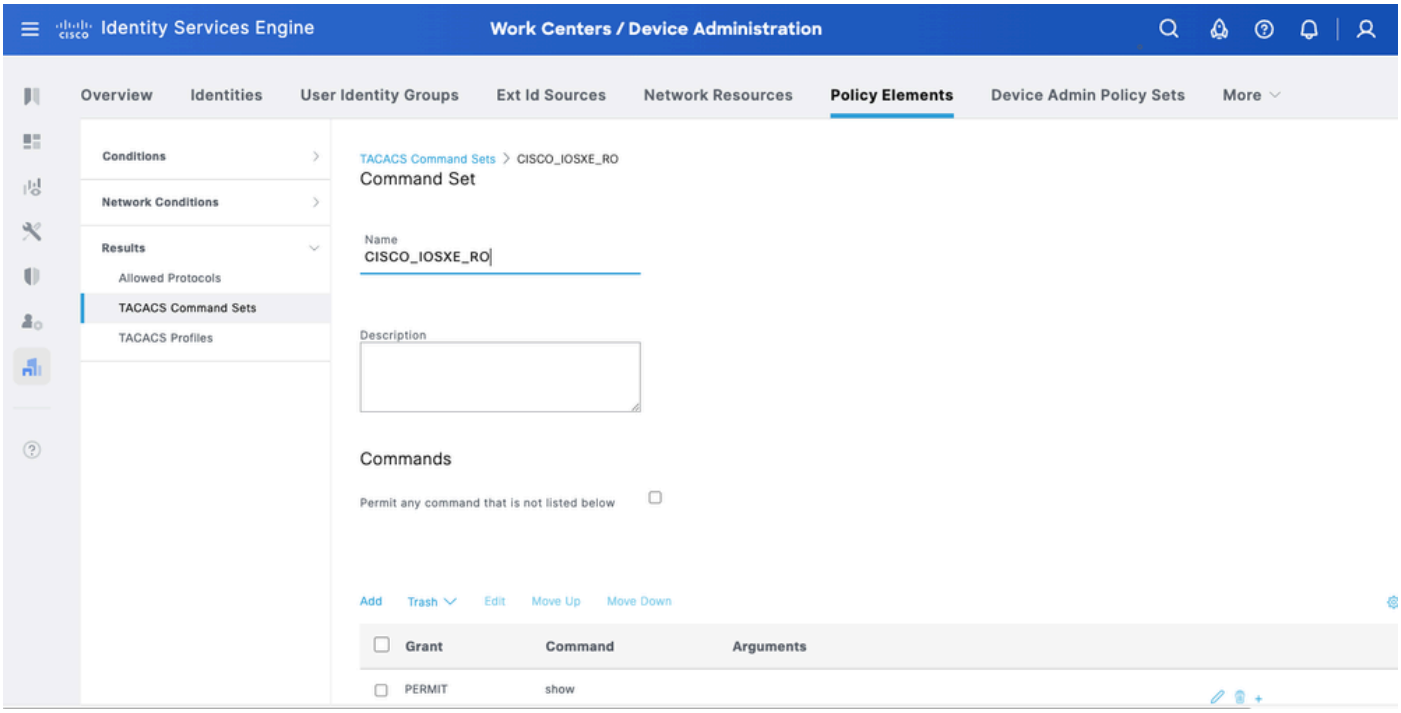
CISCO_IOS XE_RO - Befehlssatz für Bediener

Schritt 1 Navigieren Sie in der ISE-Benutzeroberfläche zu Work Centers > Device Administration > Policy Elements > Results > TACACS Command Sets. Fügen Sie einen neuen TACACS-Befehlssatz hinzu, und nennen Sie ihn CISCO_IOS XE_RO.

Schritt 2. Fügen Sie im Abschnitt "Befehle" einen neuen Befehl hinzu.

Schritt 3. Wählen Sie Zulassen aus der Dropdown-Liste für Grant Spalte und geben show auf der Command Spalte; und klicke auf den Pfeil zum Markieren.

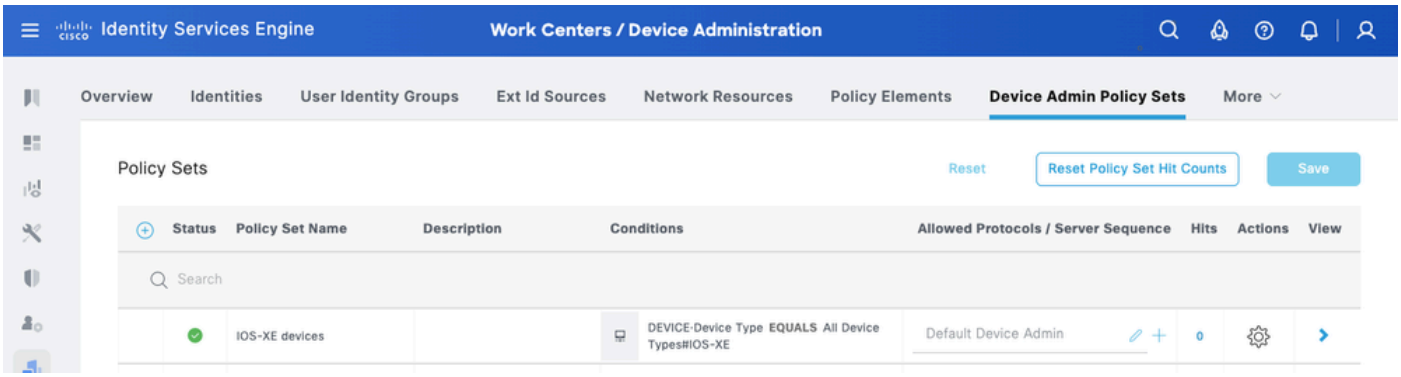
Schritt 4: Bestätigen Sie die Daten, und klicken Sie auf Speichern.



KonfigurierenGeräte-Admin-Richtliniensätze

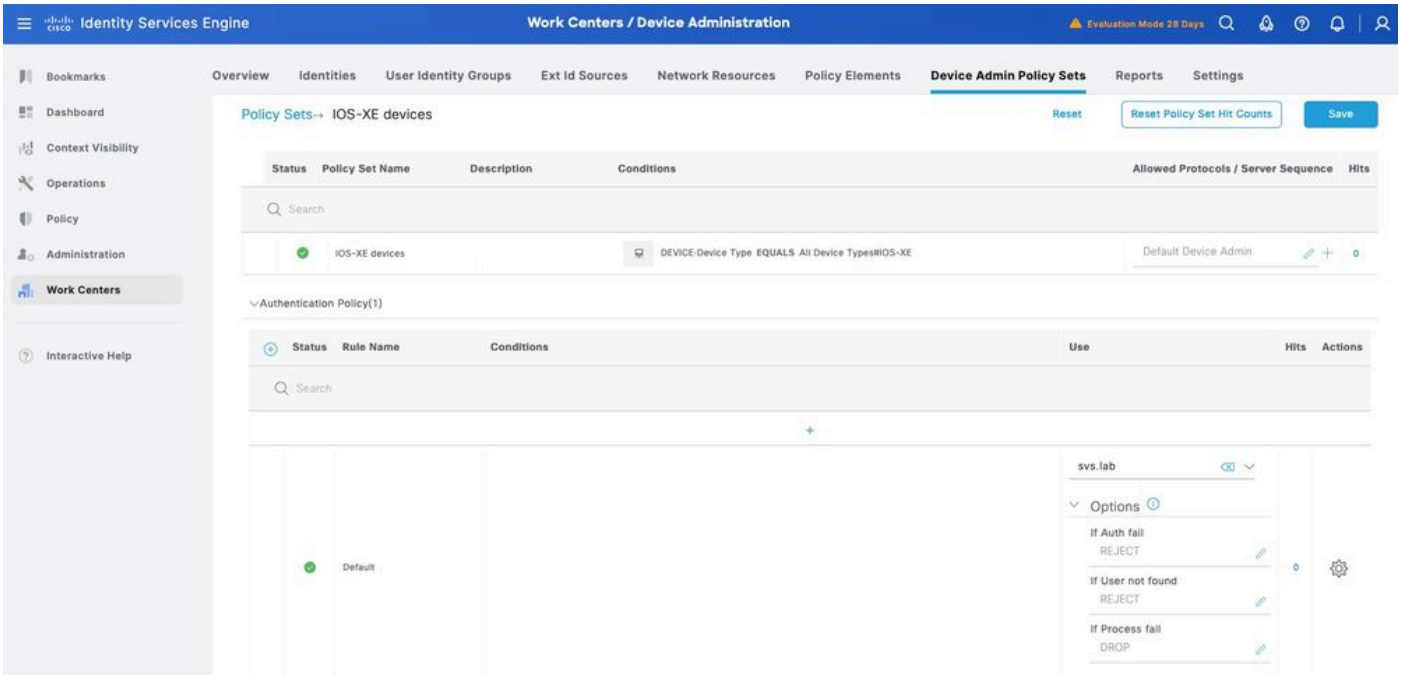
Richtliniensätze sind standardmäßig für die Geräteadministration aktiviert. Richtliniensätze können Richtlinien basierend auf den Gerätetypen aufteilen, um die Anwendung von TACACS-Profilen zu vereinfachen.

Schritt 1:Navigieren Sie zu Work Centers > Device Administration > Device Admin Policy Sets. Hinzufügen eines neuen Richtliniensatzes für IOS XE-Geräte. Geben Sie unter Bedingung DEVICE:Device Type EQUALS All Device Types#IOS XE an. Wählen Sie unter Zugelassene Protokolle die Option Standardgeräteadministrator aus.



Schritt 2: Klicken Sie auf Speichern und dann auf den Pfeil nach rechts, um diesen Richtliniensatz zu konfigurieren.

Schritt 3:Erstellen der Authentifizierungsrichtlinie. Für die Authentifizierung verwenden Sie das AD als ID-Speicher. Behalten Sie die Standardoptionen unter Wenn Auth fehlschlägt, Wenn Benutzer nicht gefunden und Wenn Prozess fehlschlägt bei.



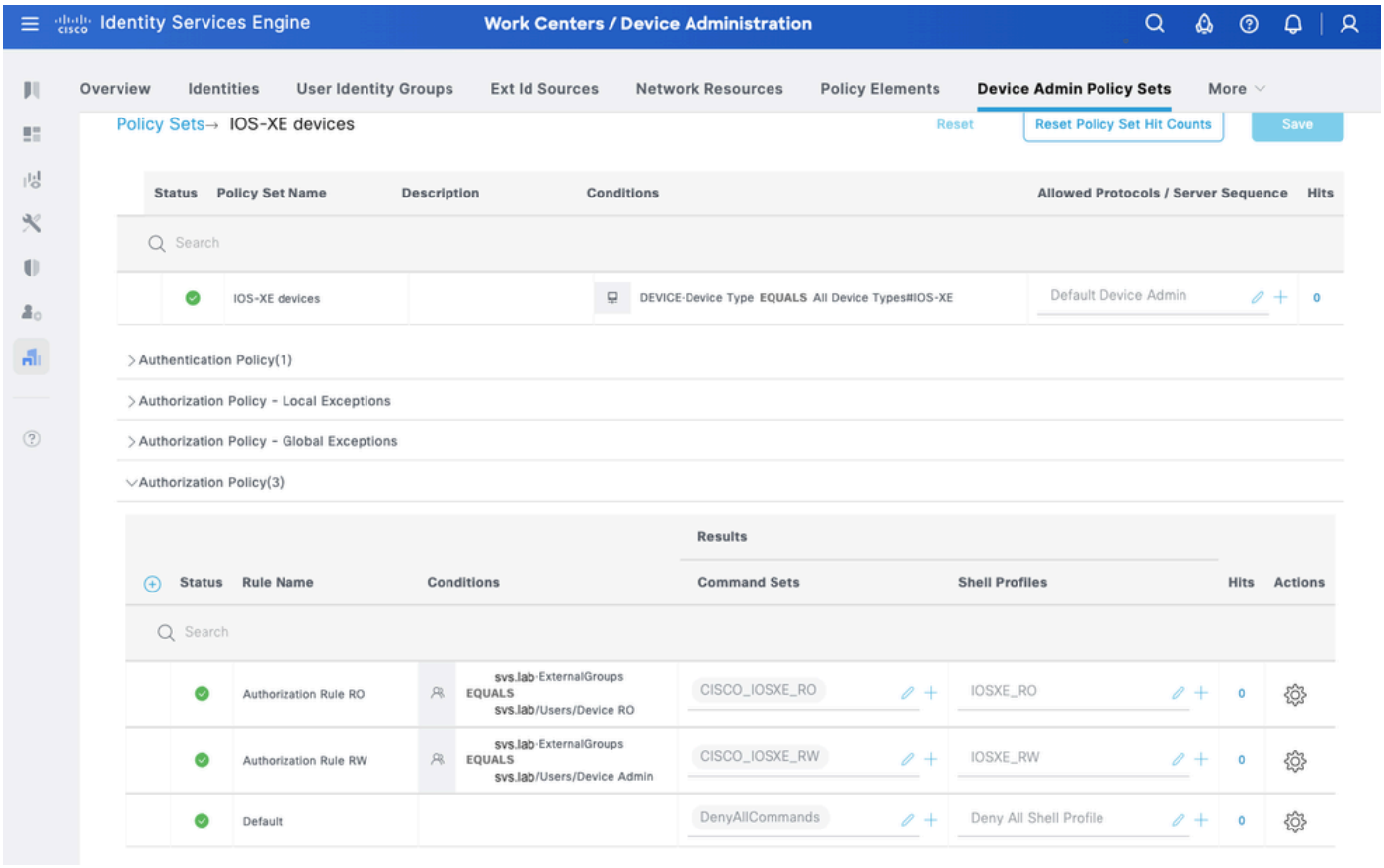
Schritt 4: Definieren der Autorisierungsrichtlinie

Erstellen Sie die Autorisierungsrichtlinie basierend auf Benutzergruppen in Active Directory (AD).

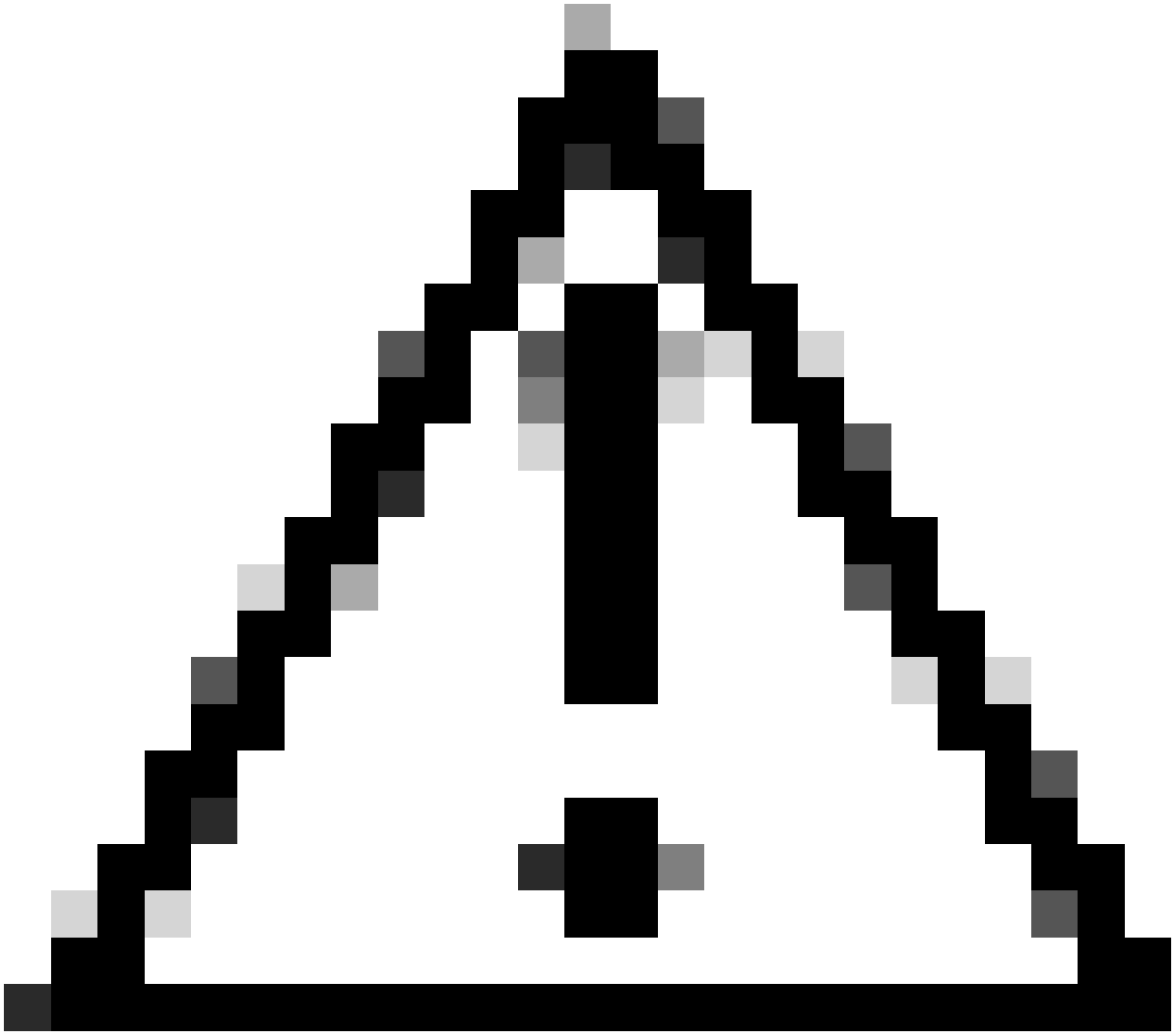
Beispiele:

- Benutzern der AD-Gruppe Device RO werden der CISCO_IOSXR_RO-Befehlssatz und das IOSXR_RO-Shell-Profil zugewiesen.

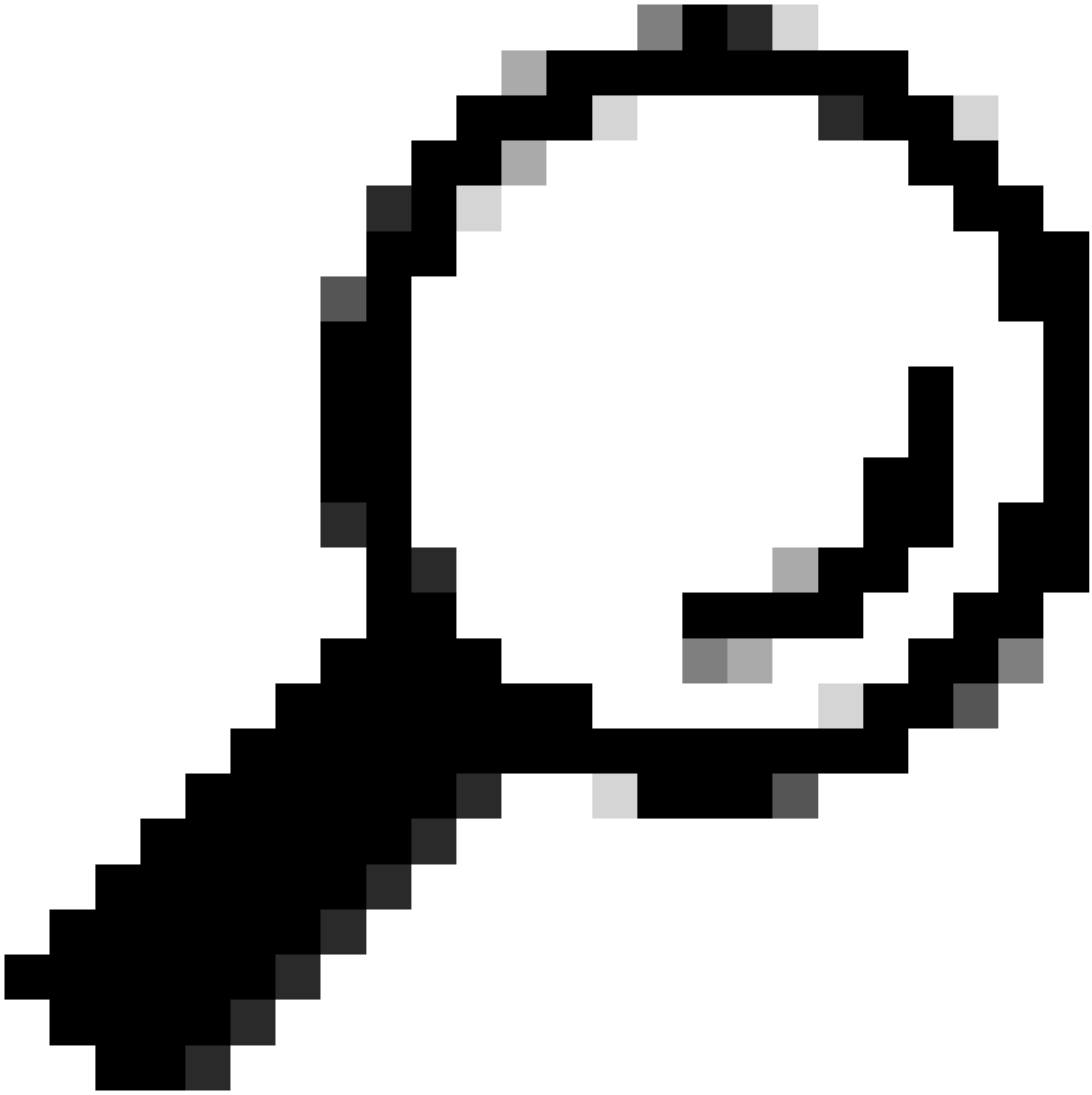
- Benutzern der AD-Gruppe Device Admin werden der CISCO_IOSXR_RW-Befehlssatz und das IOSXR_RW-Shell-Profil zugewiesen.



Teil 2: Konfigurieren von Cisco IOS XE für TACACS+ über TLS 1.3



Vorsicht: Stellen Sie sicher, dass die Konsolenverbindung erreichbar ist und ordnungsgemäß funktioniert.



Tipp: Es wird empfohlen, einen temporären Benutzer zu konfigurieren und die AAA-Authentifizierungs- und Autorisierungsmethoden so zu ändern, dass bei Konfigurationsänderungen lokale Anmeldeinformationen anstelle von TACACS verwendet werden, um ein Sperren des Geräts zu vermeiden.

Konfigurationsmethode 1 - Vom Gerät generiertes Schlüsselpaar

Konfiguration des TACACS+-Servers

Schritt 1Konfigurieren Sie den Domänennamen, und generieren Sie ein Schlüsselpaar für den Router-Vertrauenspunkt.

```
ip domain name svs.lab

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

Konfiguration des Vertrauenspunkts

Schritt 1 Erstellen Sie einen Router-Vertrauenspunkt, und ordnen Sie das Schlüsselpaar zu.

```
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
```

Schritt 2: Authentifizieren Sie den Vertrauenspunkt, indem Sie ein Zertifizierungsstellenzertifikat installieren.

<#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/gC7j8AeP03ir+KZui8
```

```
b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
gJ+kQXe7QtT/u6m1MrtjE3gAEVpL334rTIxy9hpKZIkB86t2ZA3JX8CLsbCa13sA
z1XCoONX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTAO1xh60I4QnK+MNQKpTjt/E4
ydHlOrrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVLl783nTc9wYptQEPi5sw
83g9EMgKVOARIiVUa/qlAgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAYb4
QgEBBAQDAgAHMBkGCWCGSAGG+EIBDQQMFgpTVlMgTGFiIENBMAOGCSqGSIb3DQEB
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/qd2NRSBWffFOXE/AJHQG7STT
HaXLU9r2Ko6O3oecu8ysGTwLlIt/9T1/FOb0xZRugWcpJrVoTgDGuA==

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

Certificate has the following attributes:
   Fingerprint MD5: D9C4O4B2 EC08A26O 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)#
```

Schritt 3: Erstellen einer Zertifikatsanforderung (Certificate Signing Request, 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
Ak5DMQswCQYDVQQGEwJVUzEgMB4GCSqGSIb3DQEJAhYRY2FOOWsudG1vLnN2cy5j
b2OwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATpYE7atscrtl4ddevCh3UgxjYi
4N4oBGWrpJBctKy4so8V5i6RXDt7kHgPzp14Qnf2ObcXVODE1wtTAHHBrIXqoDww
```

```
OgYJKoZIhvcNAQkOMSOwKzAcBgNVHREEFTATghFjYXQ5ay5ObW8uc3ZzLmNvbTAL
BgNVHQ8EBAMCB4AwCgYIKoZIzj0EAwQDRwAwRAIgZqP2QTwM3ZZrmIphJ7+jSTER
4OkTx2DiVs1c1Xf+vR4CIBcSb18DIYz84DmgMHUaf778/cmpe9cWakvdaxMWseBH
-----END CERTIFICATE REQUEST-----

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

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

no

```
cat9k(config)#
```

Schritt 4: CA-signiertes Zertifikat importieren.

<#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
dGlmaWNhdGUwHAYDVR0RBBUwE4IRY2FOOWsudG1vLnN2cy5jb2OwCwYDVR0PBAQD
AgeAMA0GCSqGSIb3DQEBCwUAA4ICAQBObgKVykeyVC9UsvuuOAUsGaZHGwy2H9Yd
m5vIaui6PJczkCzIoAIghHPGQhIgpEcRqtGyXPZ2r8TCJP11WXNN/G73sFyWAhzY
RtmIM5KIojiDHLtifPayxv9juDuOZRx+wYR2PIQ5eLv1bafg7K8E82sqOCfOtcPr
OcONU8UCxqObdOgu4XsdBN1+wcWFqeQSDLmP7nxvhOOm/LXwCWUHwgVioOAuU2Fe
k5NthtvdxNAhRAImQdTyq6u/yB7vwTwJHcRiJc5USsyzCsTBb6RvL+HsXqBgXGc5
lxCSoLtYOdUxFIpJyK2MOZBY2zq2cNSc8Xbso5/OEQmnHtpWPvij4rSPUhQSY+4m
Qq2Sn3iqf4mGh/AO8T4iXfWDWfNezh7ZxMsCSCK/ZRlELZ2hj6OfzwX1H27Uf8XU
ecrOWx+WzRn7LVRCaGQzFkukfi8S4DLLNtxnNHfsLBVX5yHXCLEL+CQ7n8Z/pxcB
VVrPitwN3ZbO9poZyWiRLTnBsb42xNaWiL9bjQznAOiTDfmfFFourBsaAioz7ouY
2r1Mh+OpE83Uu+4lOTMawDgGiEv7iaiJ6xWc95EC+AdmOx3FvBXMtIM9qr7WwHW6
3C2hVYHJH254elV5+H8iiz7rovEPm8ZDsnvYpJn4Km3iDvBNqp/vvAHOFcyXrvG6
3i/1b9erGQ==
-----END CERTIFICATE-----

% Router Certificate successfully imported

cat9k(config)#
```

TACACS und AAA mit TLS-Konfiguration

Schritt 1: Erstellen Sie TACACSS-Server und AAA-Gruppen, und ordnen Sie den Client (Router)-Vertrauenspunkt zu.

```
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
```

Schritt 2: Konfigurieren von AAA-Methoden

```
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
```

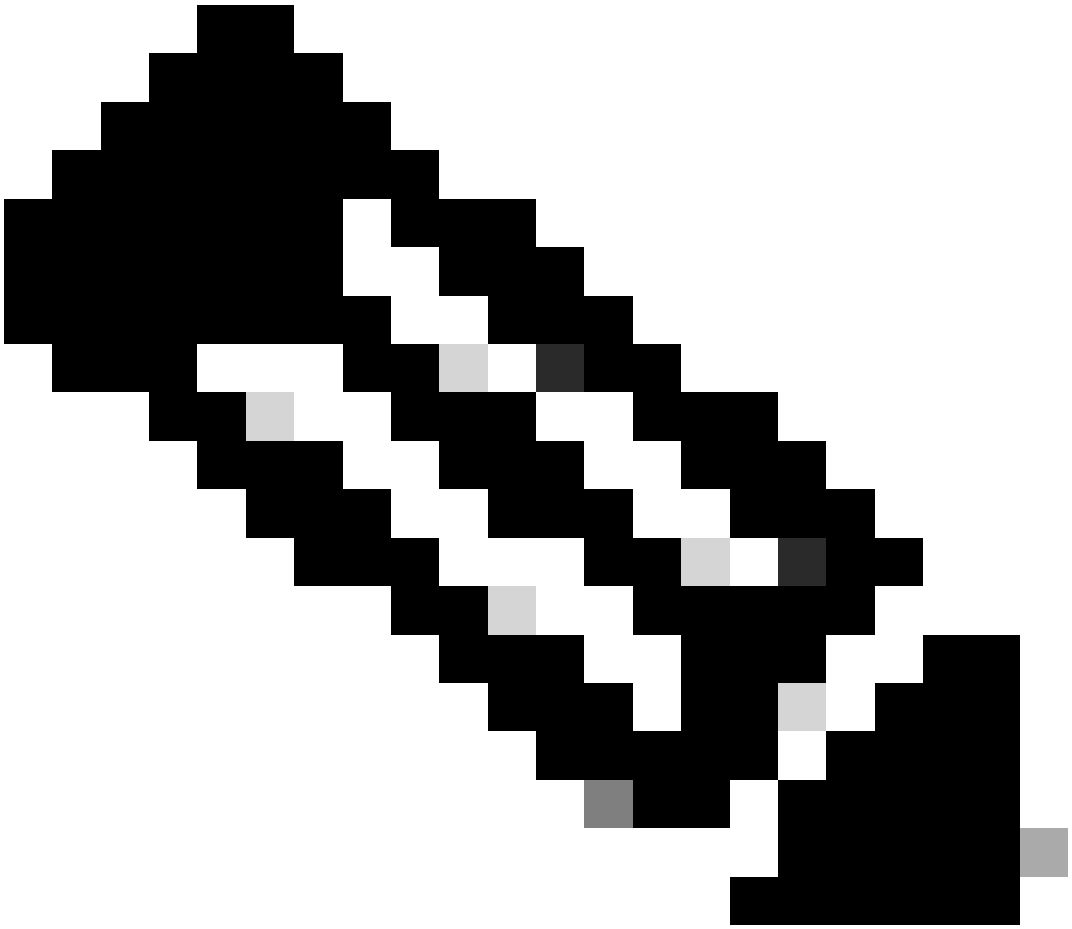
Konfigurationsmethode 2 - Von CA generiertes Schlüsselpaar

Wenn Sie die Schlüssel sowie Geräte- und Zertifizierungsstellenzertifikate direkt im PKCS#12-Format anstelle der CSR-Methode importieren, können Sie diese Methode verwenden.

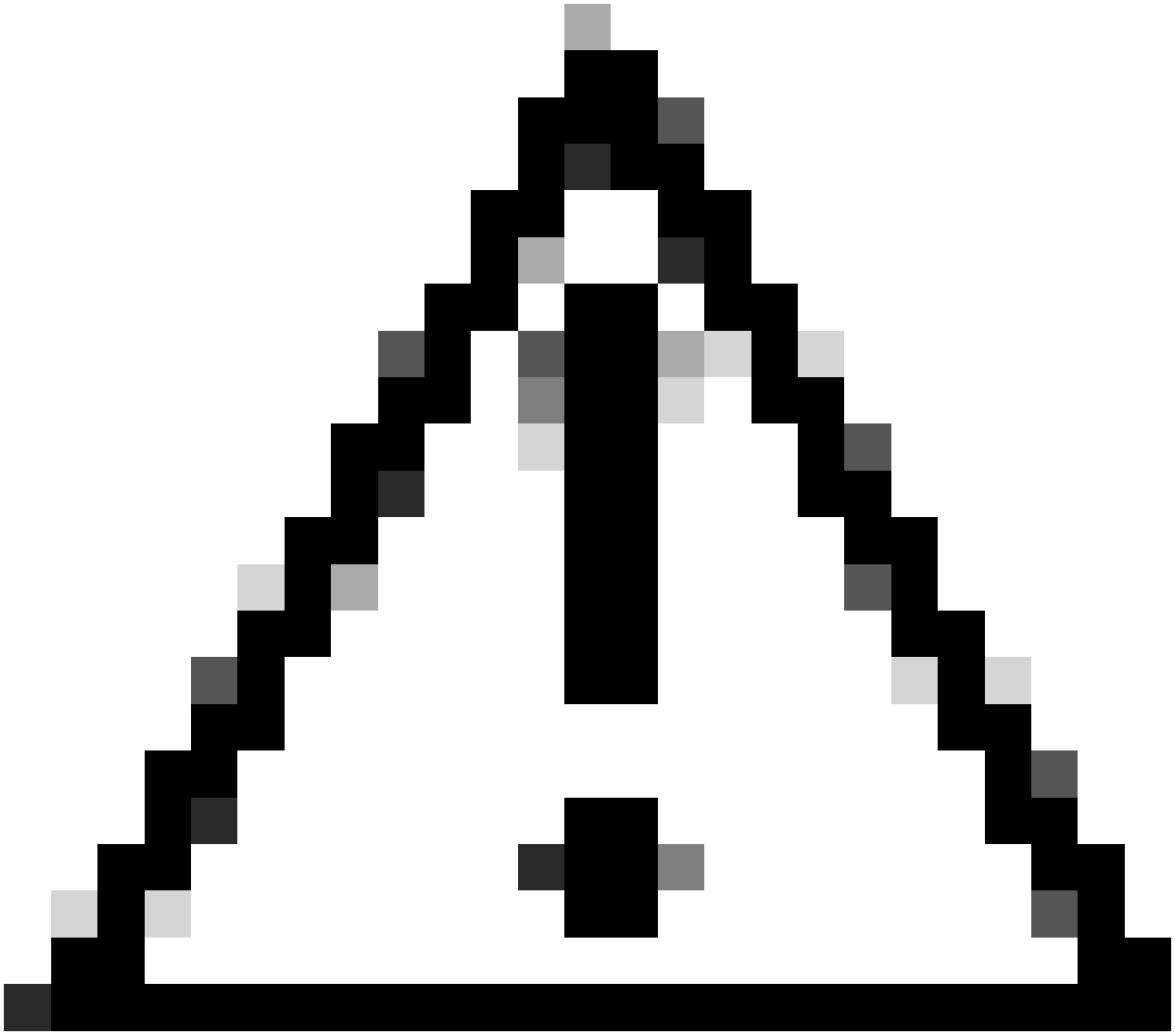
Schritt 1: Erstellen eines Client-Vertrauenspunkts.

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

Schritt 2: Kopieren Sie die Datei PKCS#12 in bootflash.



Anmerkung: Stellen Sie sicher, dass die PKCS#12-Datei die vollständige Zertifikatkette und den privaten Schlüssel als verschlüsselte Datei enthält.



Vorsicht: Die Schlüssel im importierten PKCS#12 müssen RSAs aufweisen (z. B.: RSA 2048), nicht 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)
```

Schritt 3: Importieren Sie die Datei PKCS#12 mit dem Befehl 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 und AAA mit TLS-Konfiguration

Schritt 1: Erstellen Sie TACACS-Server und AAA-Gruppen, ordnen Sie den Client (Router) Trustpoint zu.

```
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
```

Schritt 2: Konfigurieren von AAA-Methoden

```
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
```

Verifizierung

Überprüfen der Konfiguration.

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

Debuggen Sie AAA und 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
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.