

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

Inhalt

[Einleitung](#)

[Überblick](#)

[Verwendung dieses Handbuchs](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Lizenzierung](#)

[Teil 1: Konfigurieren der ISE für die Geräteverwaltung](#)

[Zertifikatsignierungsanforderung für TACACS+-Serverauthentifizierung generieren](#)

[Hochladen des Zertifikats der Stammzertifizierungsstelle für die TACACS+-Serverauthentifizierung](#)

[Signierte Zertifikatsanforderung \(CSR\) an ISE binden](#)

[TLS 1.3 aktivieren](#)

[Geräteadministration auf ISE aktivieren](#)

[Aktivieren von TACACS über TLS](#)

[Netzwerkgeräte- und Netzwerkgerätegruppen erstellen](#)

[Konfigurieren Identitätsspeicher](#)

[Konfigurieren von TACACS+-Profilen](#)

[IOS XE RW - Administratorprofil](#)

[IOS XE RO - Betreiberprofil](#)

[Konfigurieren von TACACS+-Befehlssätzen](#)

[CISCO IOS XE RW - Administrator-Befehlssatz](#)

[CISCO IOS XE RO - Befehlssatz für Bediener](#)

[Konfigurieren Geräte-Admin-Richtliniensätze](#)

[Teil 2: Konfigurieren von Cisco IOS XE für TACACS+ gegenüber TLS 1.3](#)

[Konfigurationsmethode 1 - Vom Gerät generiertes Schlüsselpaar](#)

[Konfiguration des TACACS+-Servers](#)

[Konfiguration des Vertrauenspunkts](#)

[TACACS und AAA mit TLS-Konfiguration](#)

[Konfigurationsmethode 2 - Von CA generiertes Schlüsselpaar](#)

[TACACS und AAA mit TLS-Konfiguration](#)

[Verifizierung](#)

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.



Summary

Endpoints

Guests

Vulner



Administration

System

Identity Management

Deployment

Identities

Licensing

Groups

Certificates

External Identity So

Logging

Identity Source Seq

Maintenance

Settings

Upgrade & Rollback

Health Checks

Feed Service

Backup & Restore

Profiler

Admin Access

Settings

Schritt 3: Klicken Sie unter Zertifikatsignierungsanforderungen auf Zertifikatsignierungsanforderung generieren.



Schritt 4: Wählen Sie TACACS in Usage.

Usage

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

Allow Wildcard Certificates i

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

Node(s)

Generate CSR's for these Nodes:

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

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

Subject

Common Name (CN)
\$FQDN\$



Organizational Unit (OU)
CX



Organization (O)
Cisco



City (L)
Raleigh

State (ST)
North Carolina

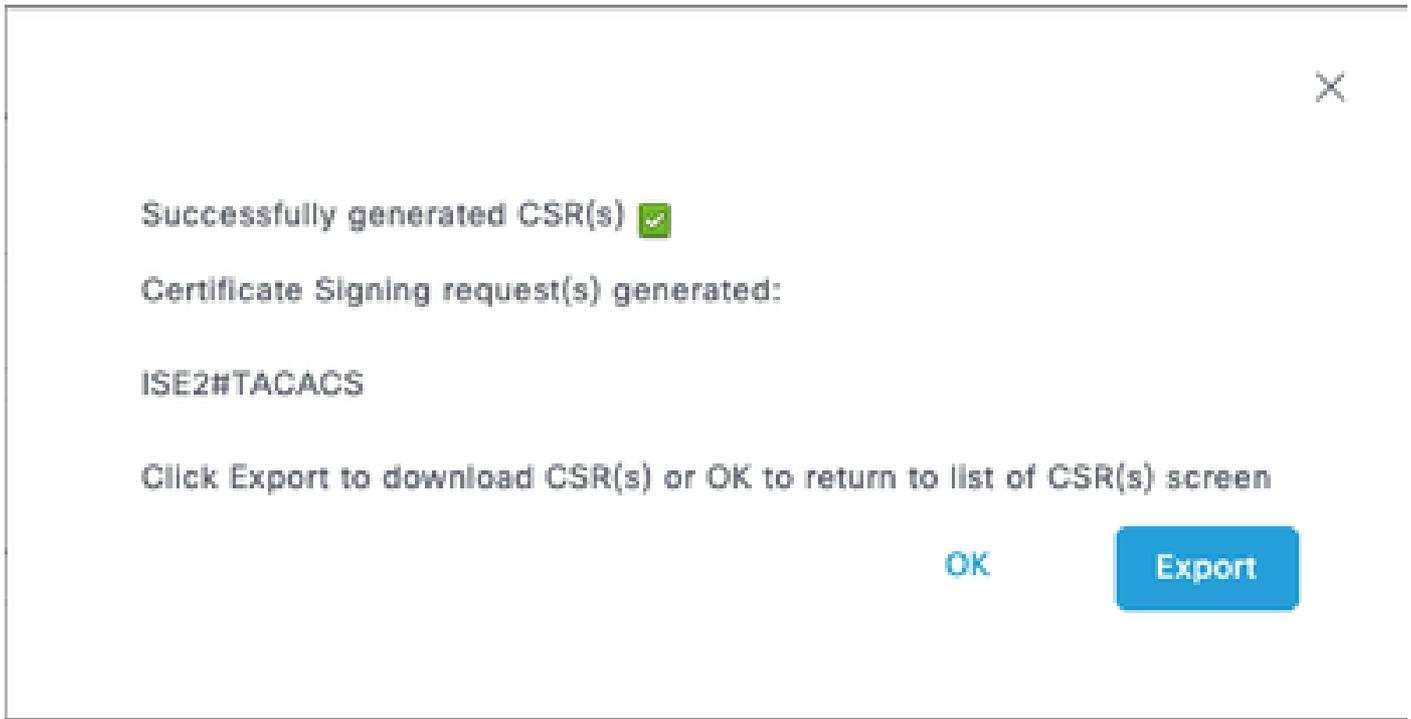
Country (C)
US

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

Subject Alternative Name (SAN)

⋮	DNS Name	ISE1.lab	-	+	
⋮	IP Address	10.225.253.209	-	+	?

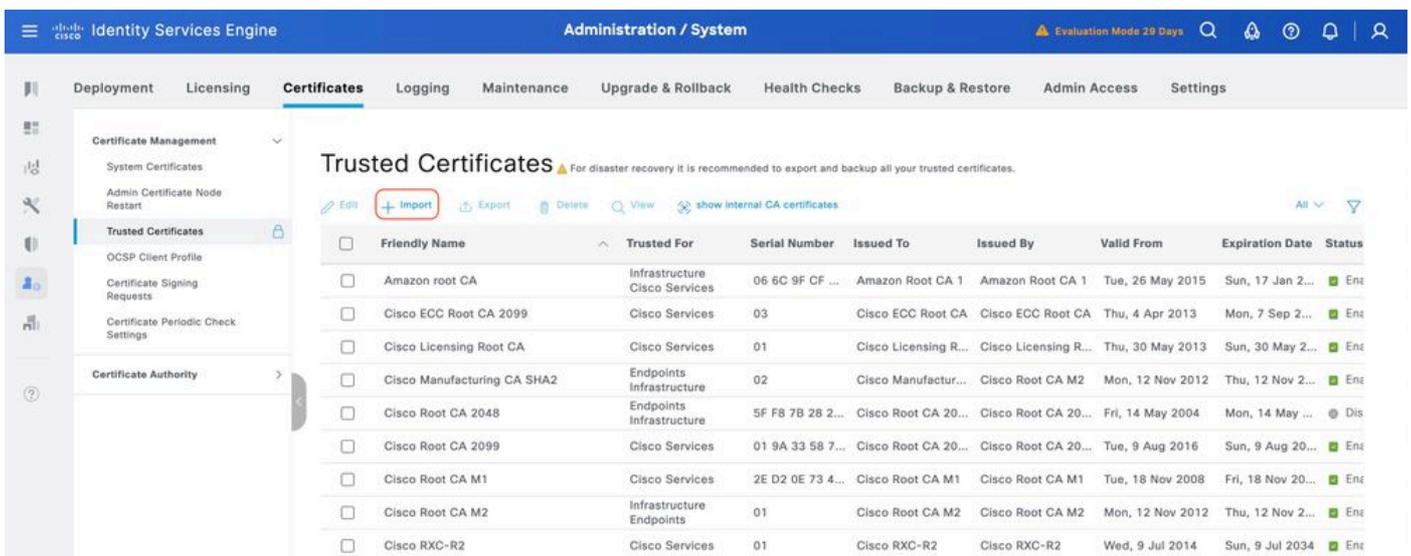
Schritt 8: Klicken Sie auf Generieren und dann auf Exportieren.



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, dass Authentifizierung innerhalb der ISE vertrauenswürdigt ist aktiviert.

Import a new Certificate into the Certificate Store

* Certificate File ISE SVSLab CA.crt

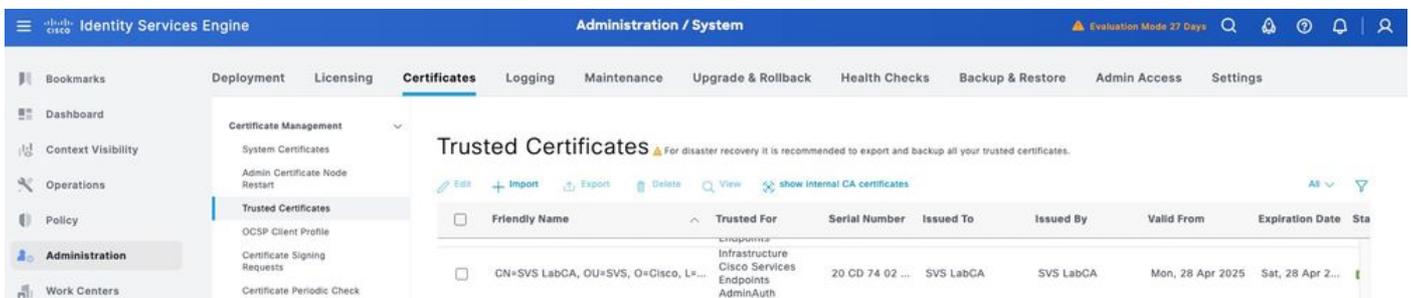
Friendly Name

Trusted For: ⓘ

- Trust for authentication within ISE
- Trust for client authentication and Syslog
 - Trust for certificate based admin authentication
- Trust for authentication of Cisco Services
- Trust for Native IPSec certificate based authentication
- Validate Certificate Extensions

Description

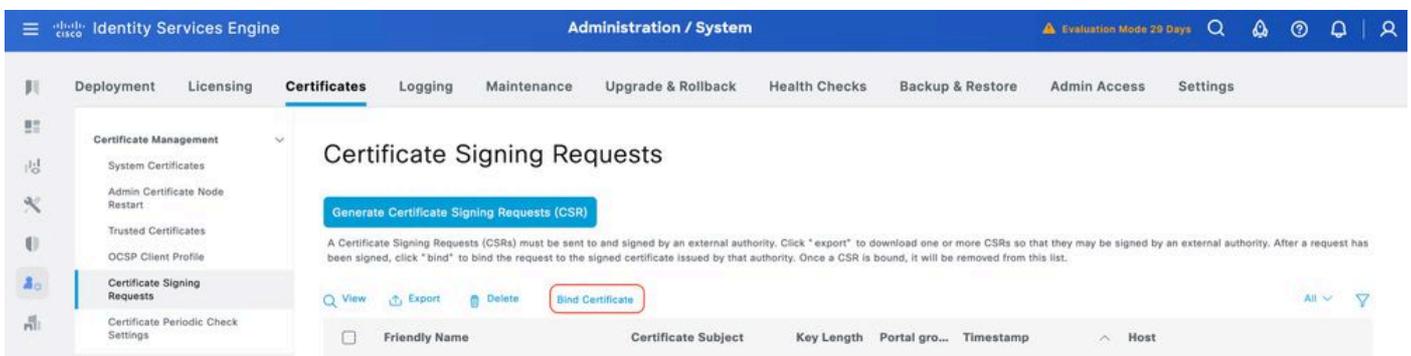
Schritt 3: Klicken Sie auf Senden. Das Zertifikat muss jetzt unter Vertrauenswürdige Zertifikate angezeigt werden.



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.

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
ISE1	C=US, ST=NC, L=Raleigh, TACACS O=Cisco, OU=SVS, CN=I SE1.lab#ISE1.lab#00010		ISE1.lab	ISE1.lab	Wed, 10 Sep 2025	Fri, 10 Sep 2027	Active

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.

The screenshot displays the Cisco Identity Services Engine (ISE) administration interface. The top navigation bar is blue with the Cisco logo and "Identity Services Engine" text. A left sidebar contains menu items: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (highlighted), Work Centers, and Interactive Help. A "Deployment" dropdown menu is open, showing options: Client Provisioning, FIPS Mode, Security Settings, Alarm Settings, System, Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade & Rollback, Health Checks, Backup & Restore, Admin Access, and Settings (highlighted with a checkmark). A "Licensing" dropdown menu is also visible, showing Client Provisioning, FIPS Mode, Security Settings, and Alarm Settings.

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

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

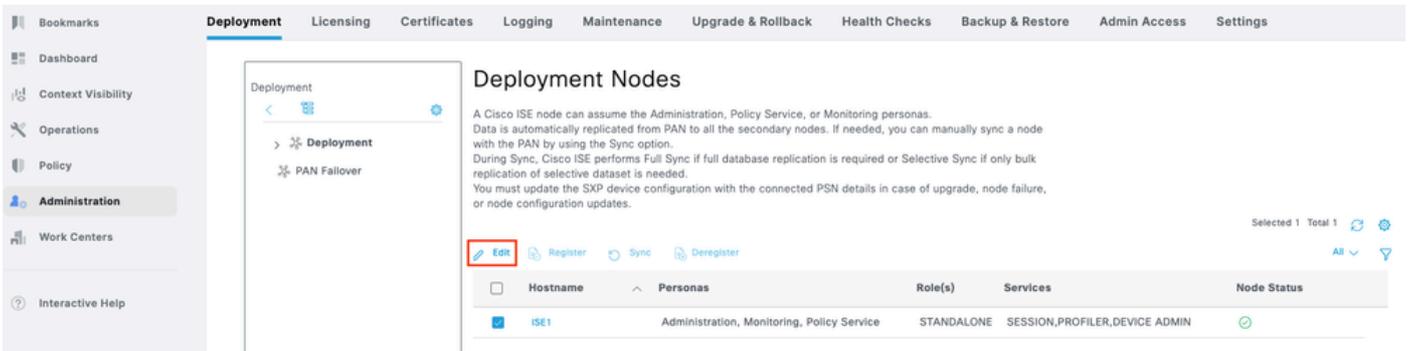


Warnung: Wenn Sie die TLS-Version ändern, wird der Cisco ISE-Anwendungsserver auf allen Cisco ISE-Bereitstellungssystemen neu gestartet.

Geräteadministration auf ISE aktivieren

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

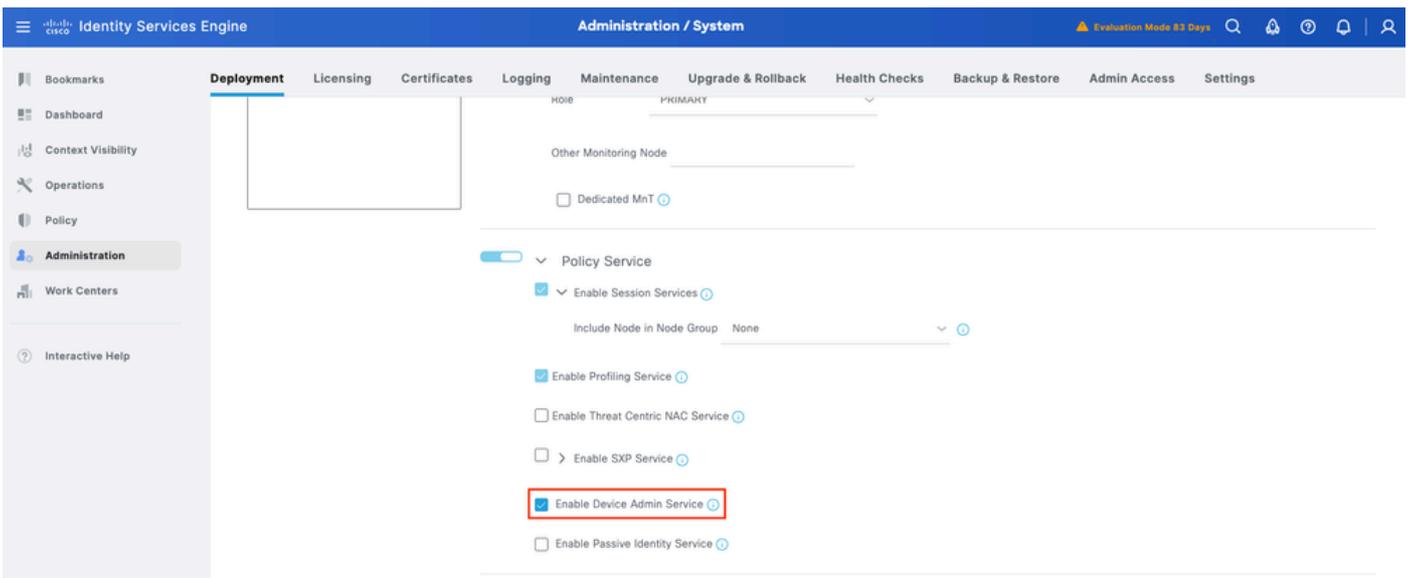
Schritt 1: Navigieren Sie zu Administration > System > Deployment. Aktivieren Sie das Kontrollkästchen neben dem ISE-Knoten, und klicken Sie auf Edit.



The screenshot shows the Cisco ISE Administration console. The left sidebar contains navigation options: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (selected), Work Centers, and Interactive Help. The main content area is titled 'Deployment Nodes' and includes a 'Deployment' breadcrumb. Below the breadcrumb is a 'PAN Failover' section. The main content area contains a table of deployment nodes. The 'Edit' button for the 'ISE1' node is highlighted with a red box.

Hostname	Personas	Role(s)	Services	Node Status
ISE1	Administration, Monitoring, Policy Service	STANDALONE	SESSION, PROFILER, DEVICE ADMIN	🟢

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



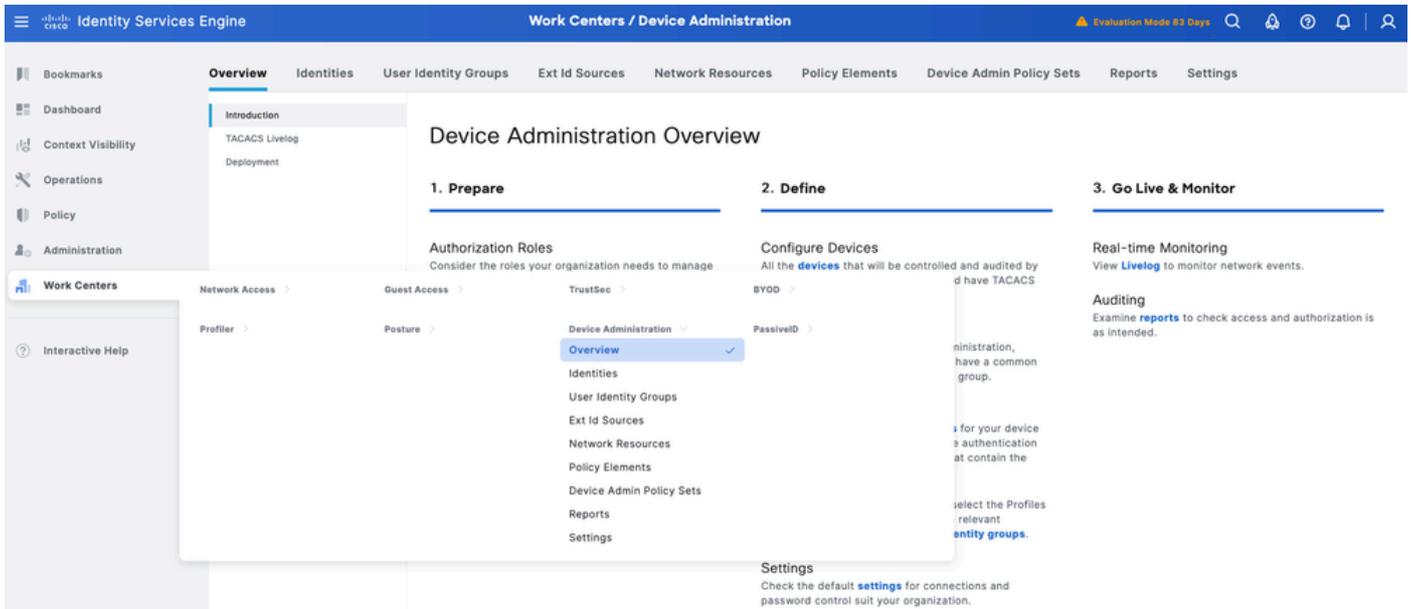
The screenshot shows the Cisco ISE Administration console. The left sidebar contains navigation options: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (selected), Work Centers, and Interactive Help. The main content area is titled 'Administration / System' and includes a 'Deployment' breadcrumb. Below the breadcrumb is a 'General Settings' section. The 'Enable Device Admin Service' checkbox is highlighted with a red box.

Enable Device Admin Service

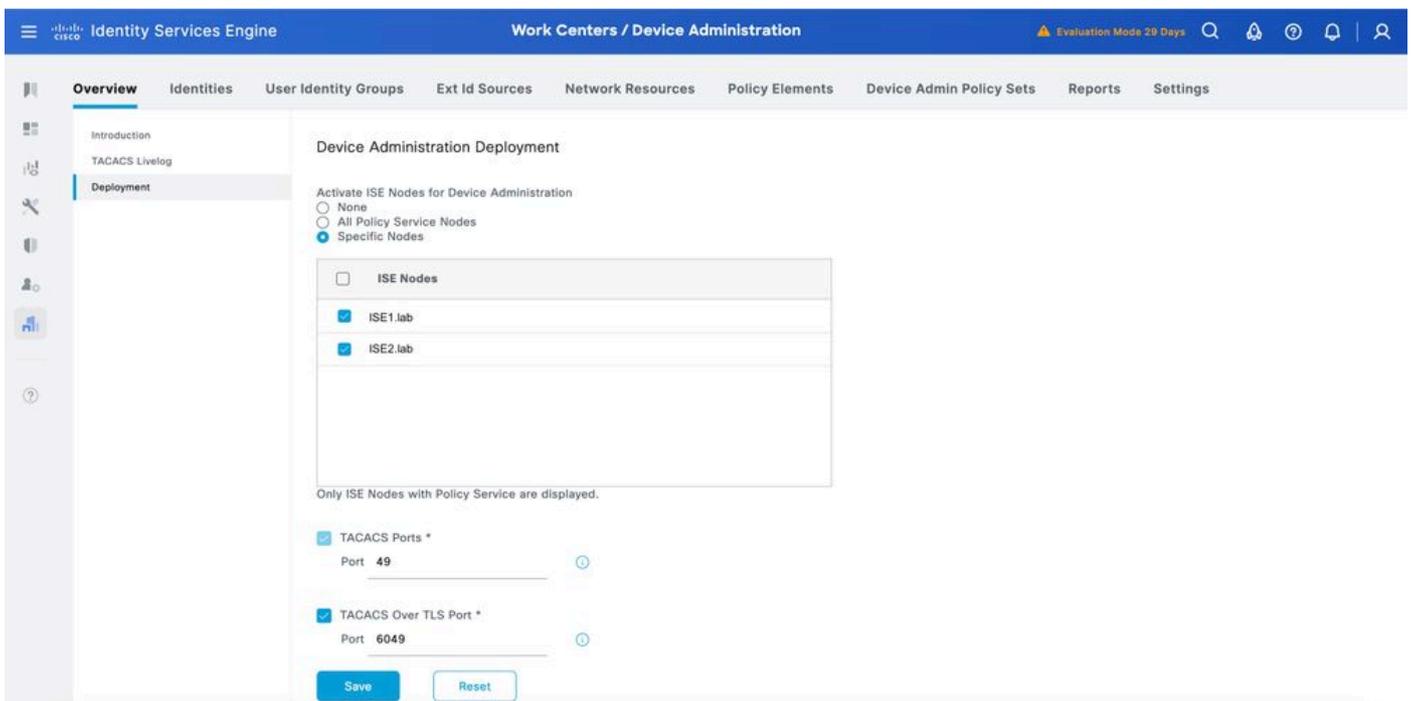
Schritt 3: Speichern der Konfiguration Der Geräteverwaltungsdienst ist jetzt auf der ISE aktiviert.

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.

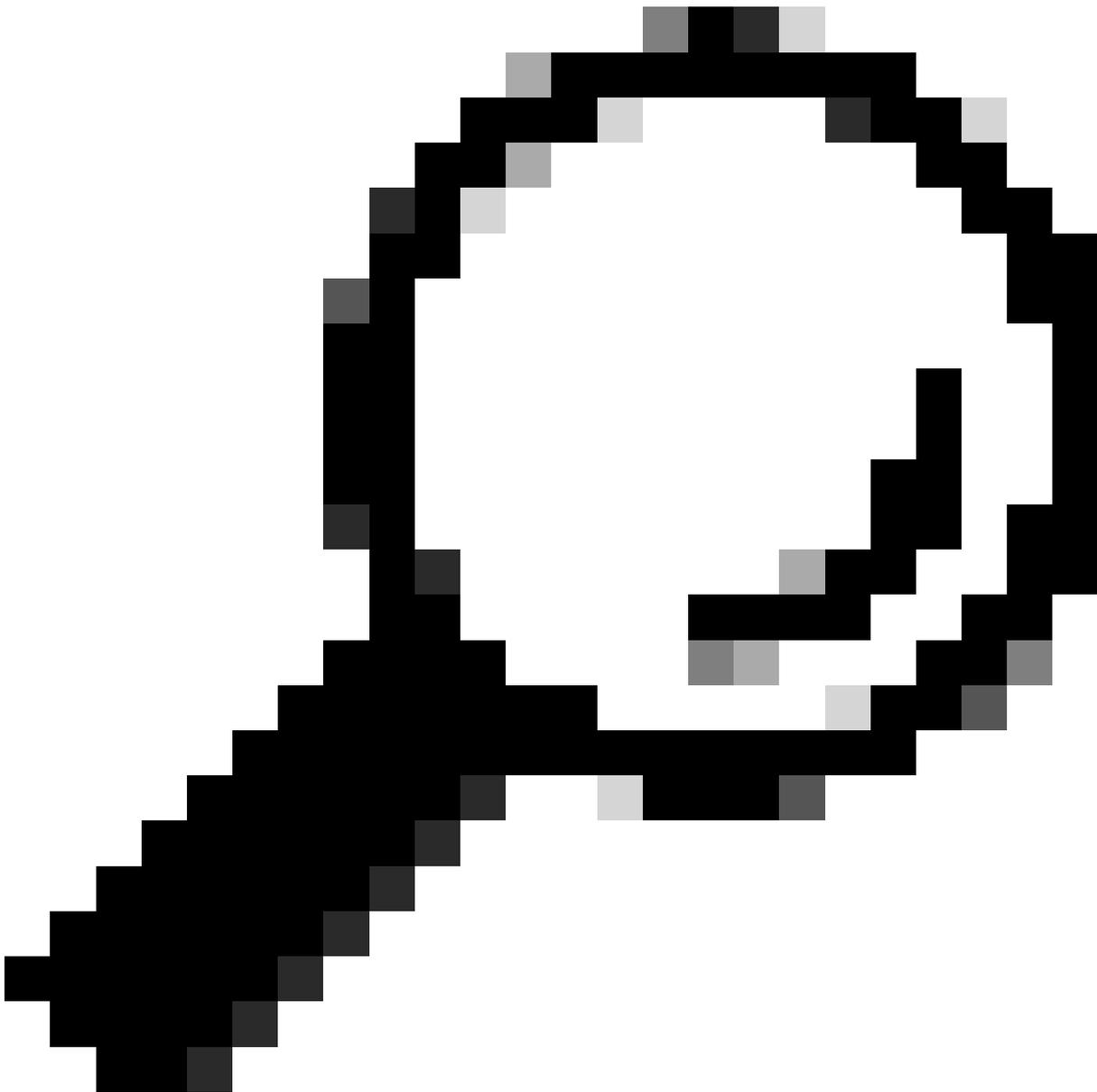
Add Group

Name*
IOSXE 6/10

Description

Parent Group*
Select Group or Add as root group

Cancel Save



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.

The screenshot shows the Cisco ISE interface for configuring a network device. The breadcrumb trail is "Network Devices List > SVS_BRPASR1K". The main heading is "Network Devices".

Fields visible include:

- Name: SVS_BRPASR1K
- Description: (empty)
- IP Address: 10.225.253.180 (with a subnet of /32)
- Device Profile: Cisco
- Model Name: (empty)
- Software Version: (empty)
- Network Device Group: (empty)
- Location: All Locations (with a "Set To Default" link)

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.

The screenshot shows the "TACACS over TLS Authentication Settings" configuration page in Cisco ISE. The breadcrumb trail is "Network Resources > TACACS over TLS Authentication Settings".

Configuration options include:

- RADIUS Authentication Settings
- TACACS Authentication Settings
- TACACS over TLS Authentication Settings

Text description: "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."

Section: Subject Alternative Name (SAN)*

Text description: "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."

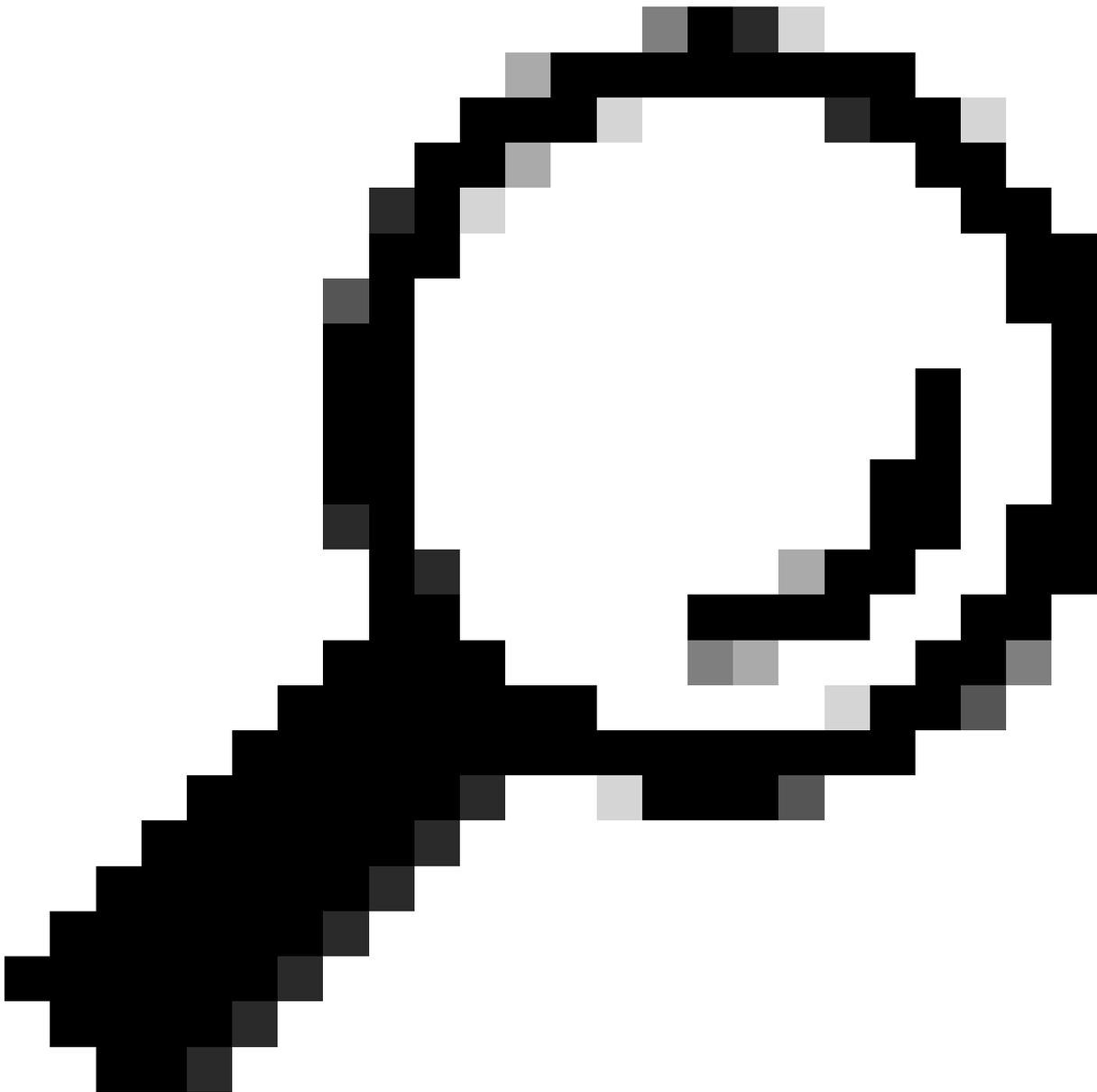
IP Address

Text description: "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

(Empty text input field)

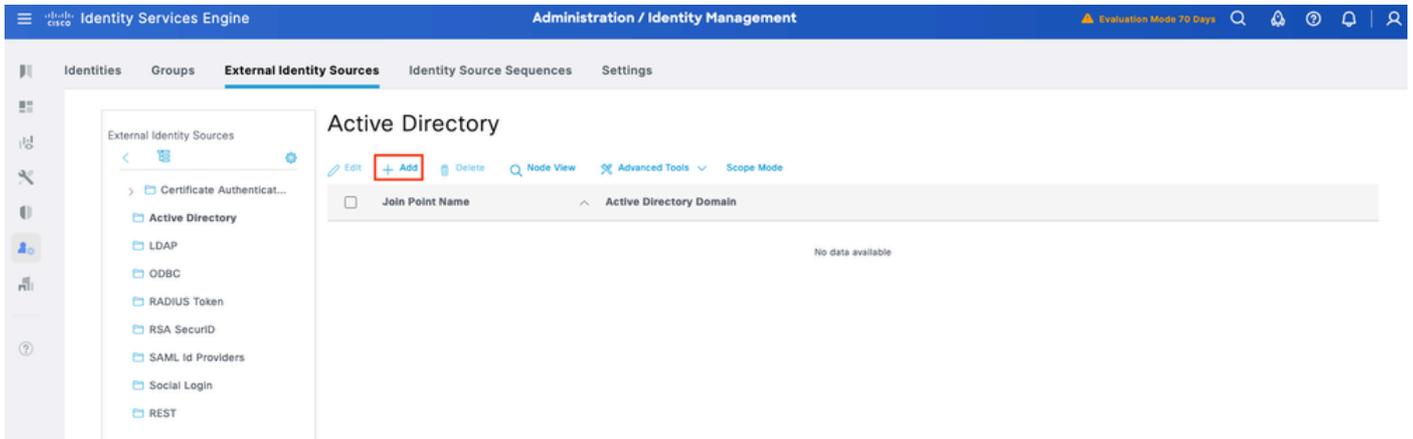


Tipp: Es wird empfohlen, den Single-Connect-Modus zu aktivieren, um zu vermeiden, dass die TCP-Sitzung jedes Mal neu gestartet wird, wenn ein Befehl an das Gerät gesendet wird.

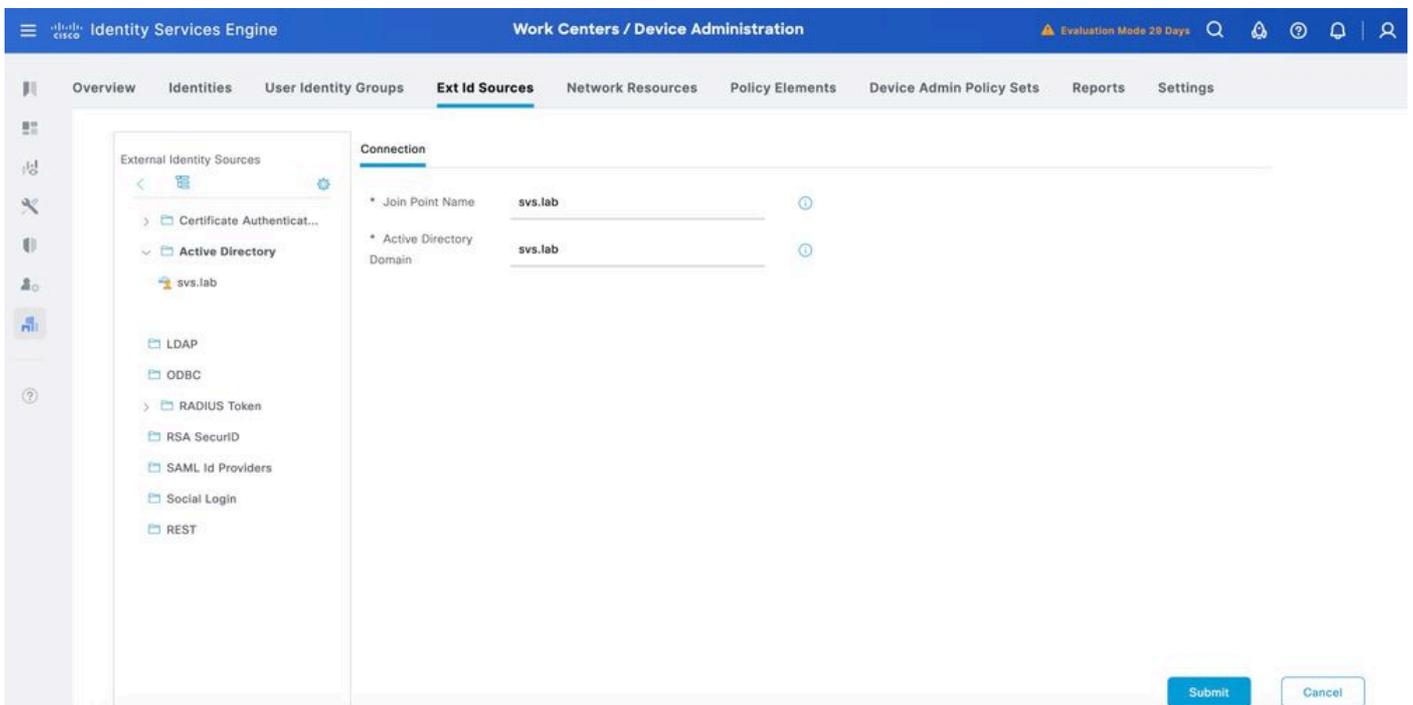
Konfigurieren Identitätsspeicher

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.

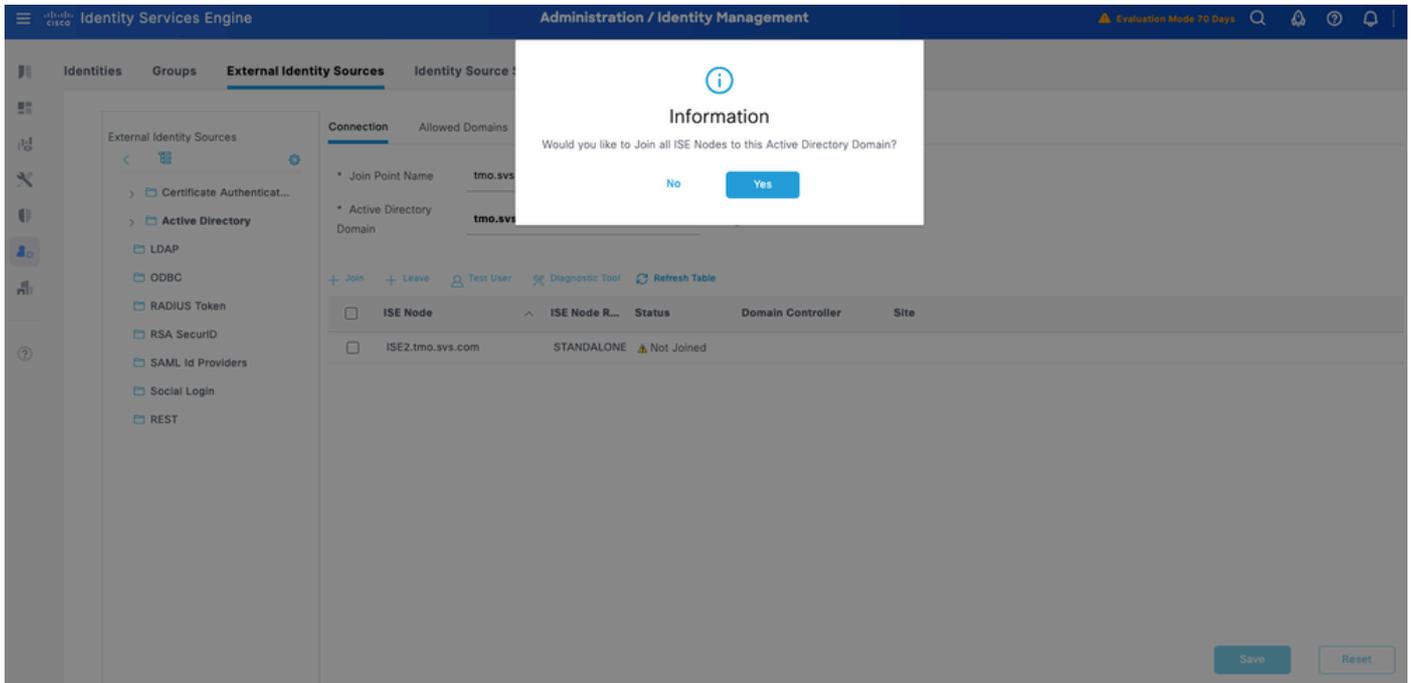
Schritt 1: Navigieren Sie zu Administration > Identity Management > External Identity Stores > Active Directory. Klicken Sie auf Hinzufügen, um einen neuen AD-Gelenkpunkt zu definieren.



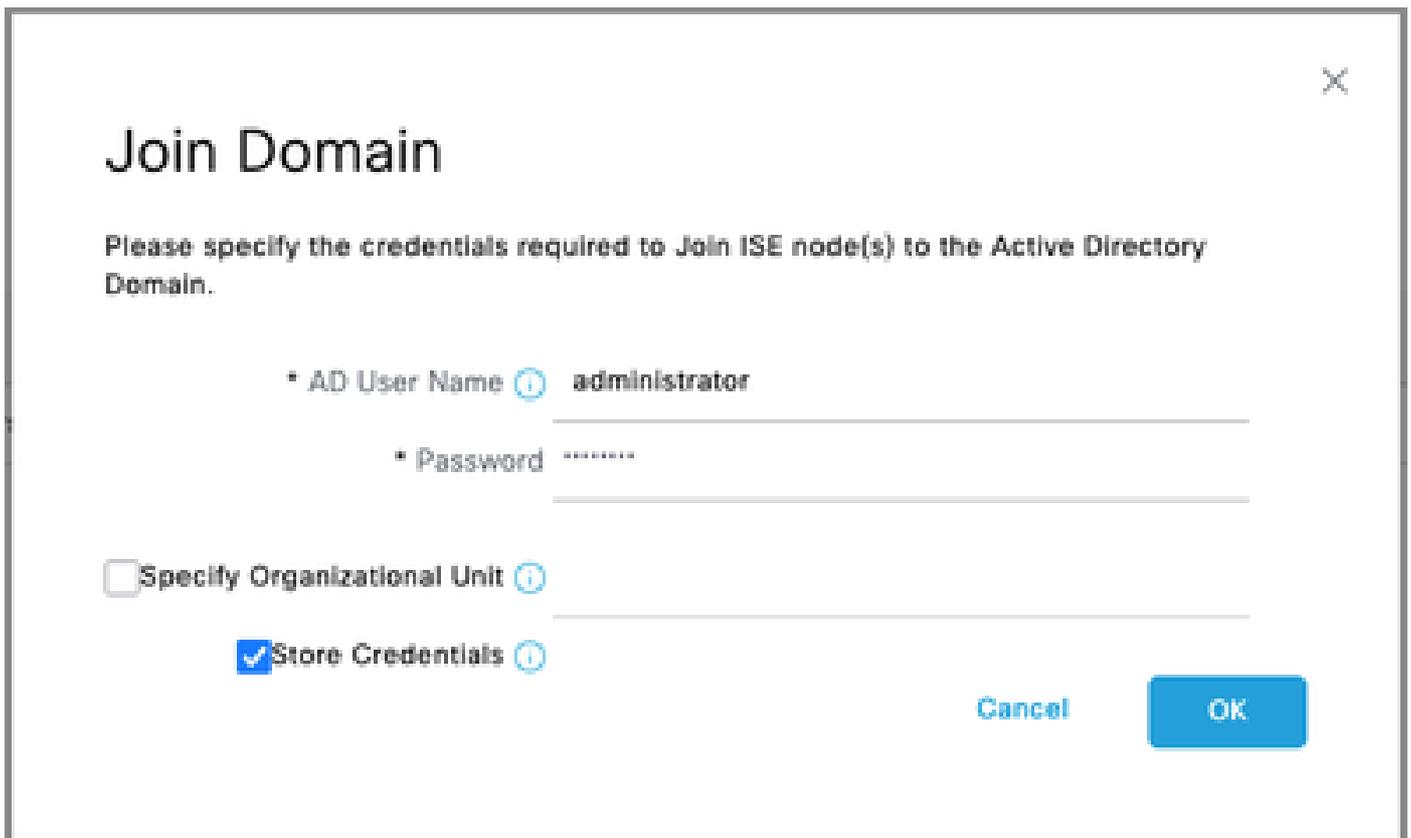
Schritt 2: Geben Sie den Namen des Verbindungspunkts und den AD-Domännennamen an, und klicken Sie auf Senden.

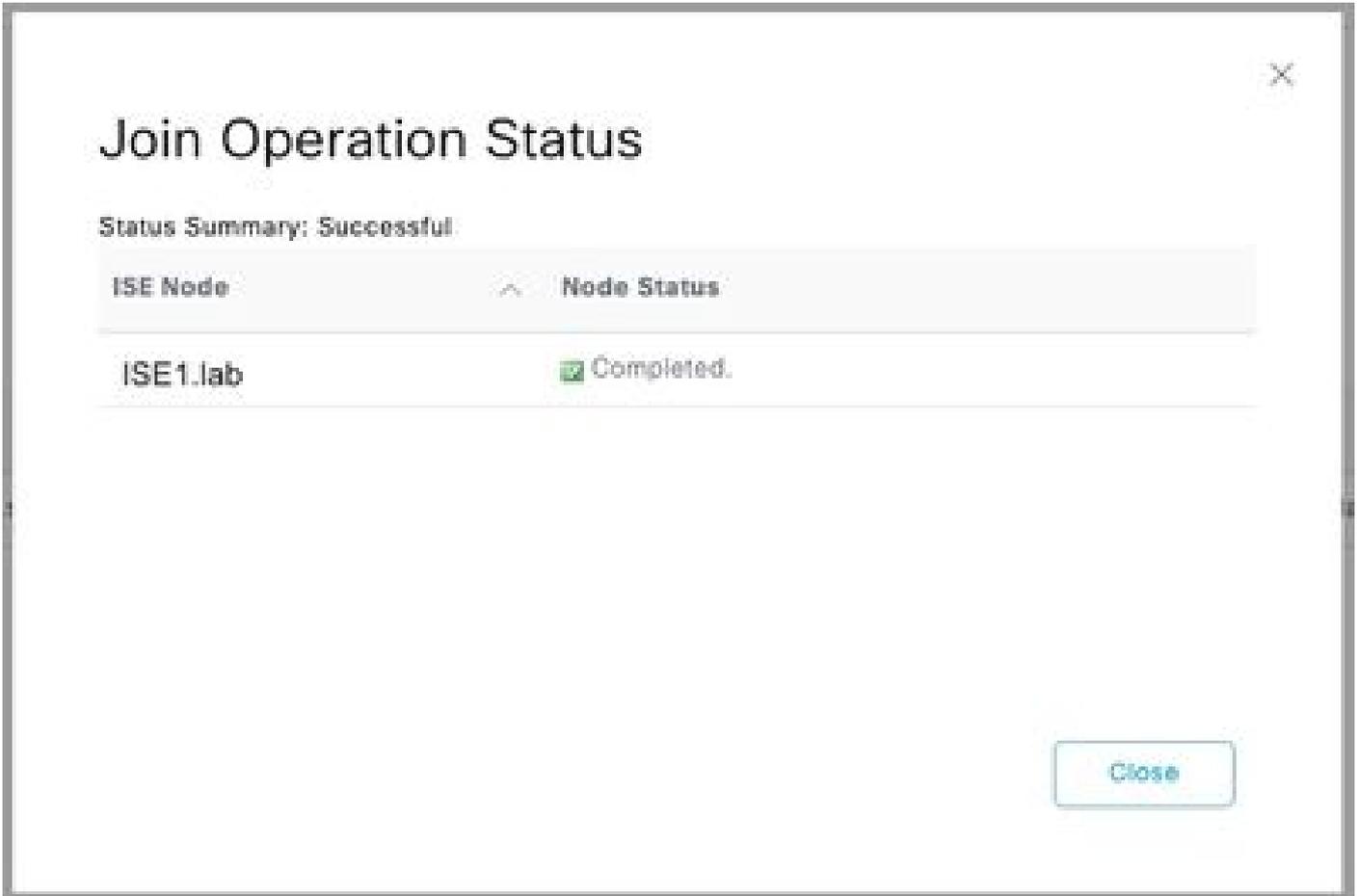


Schritt 3. Klicken Sie auf Ja, wenn Sie dazu aufgefordert werden Möchten Sie allen ISE-Knoten in dieser Active Directory-Domäne beitreten?

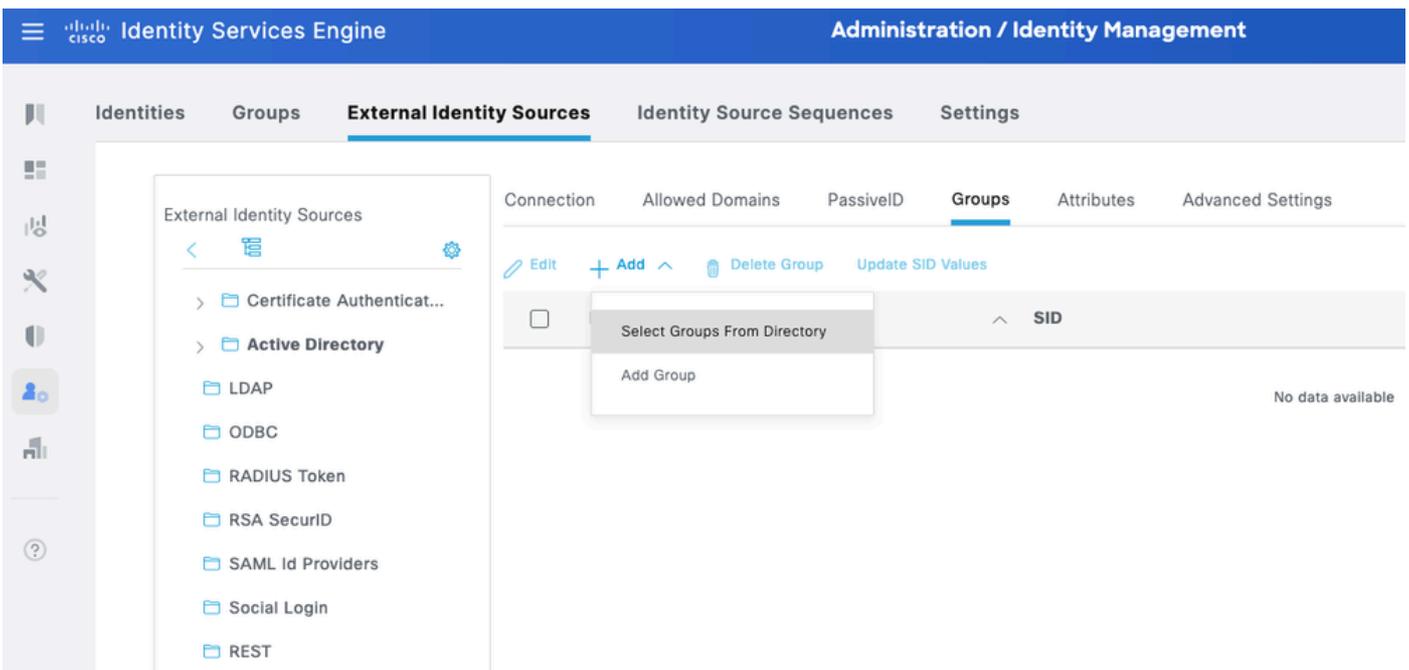


Schritt 4: Geben Sie die Anmeldeinformationen mit AD-Join-Berechtigungen ein, und treten Sie ISE bei AD bei. Überprüfen Sie den Status, um sicherzustellen, dass er betriebsbereit ist.





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.



Select Directory Groups

This dialog is used to select groups from the Directory.

Domain

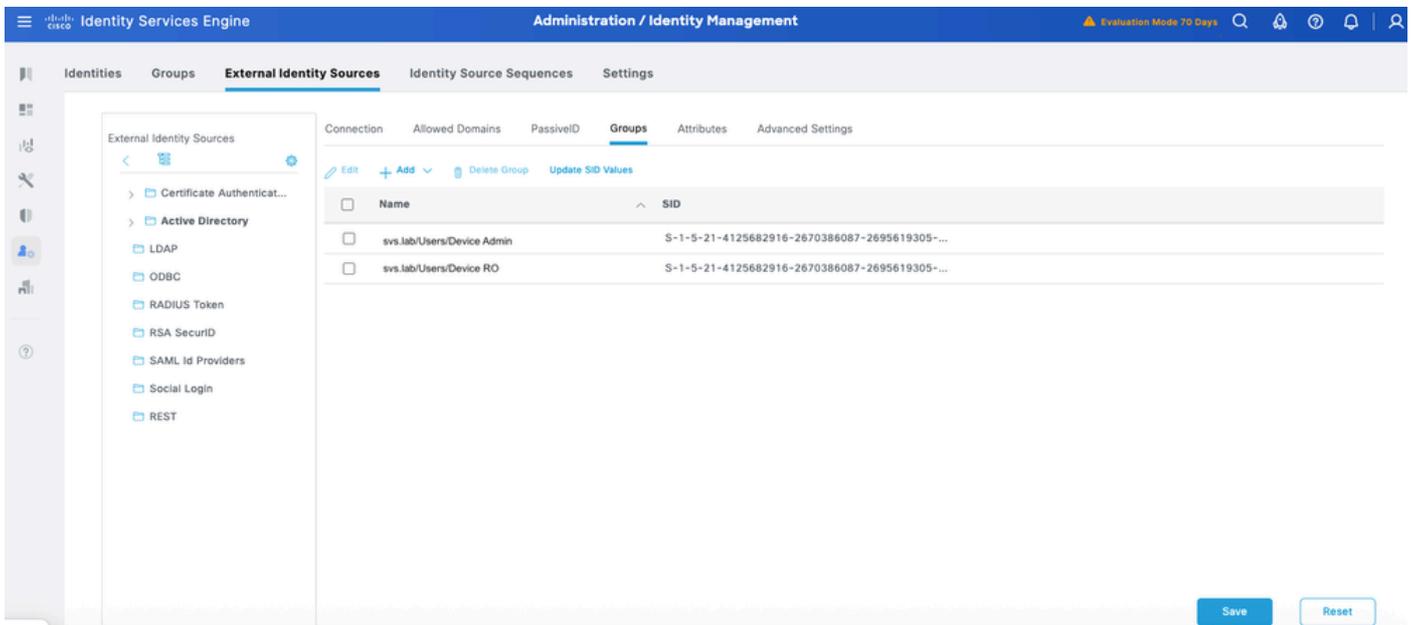
Name
Filter

SID *
Filter

Type
Filter

2 Groups Retrieved.

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



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.

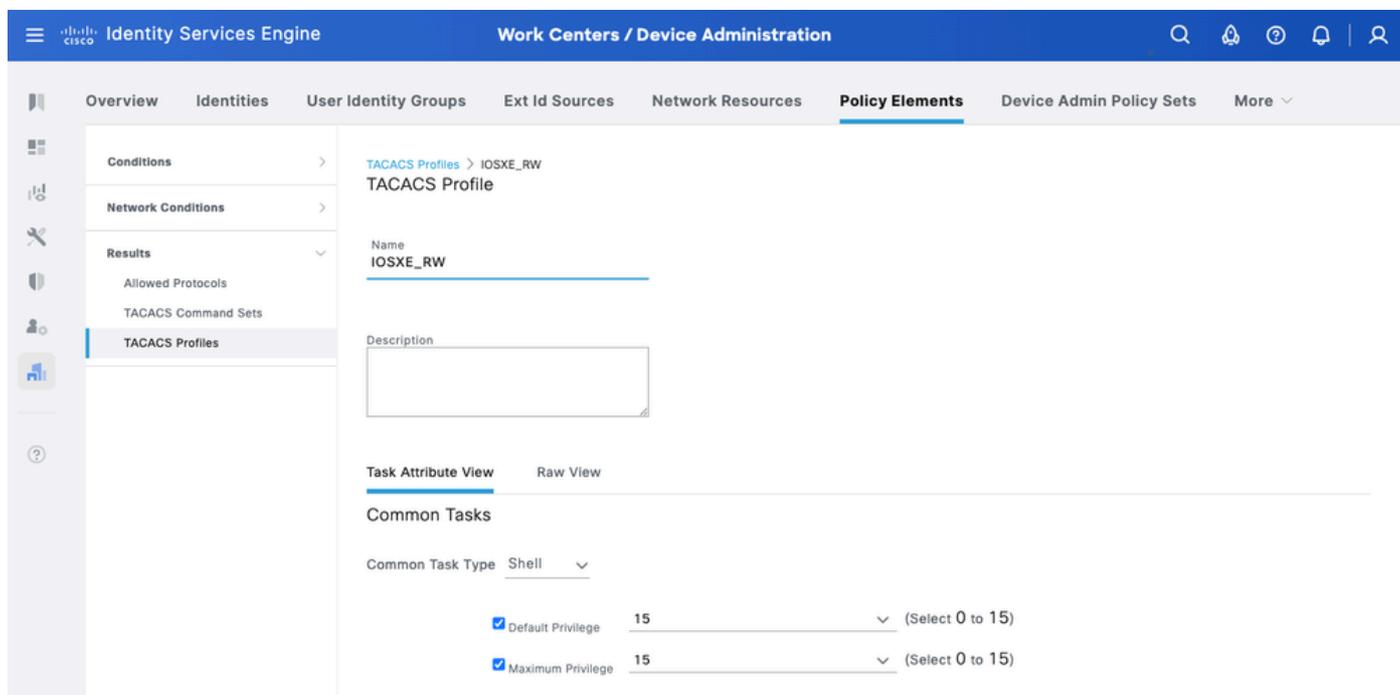
Diese werden als zwei TACACS+-Profile definiert: IOS_XE_RW und IOSXR_RO.

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.

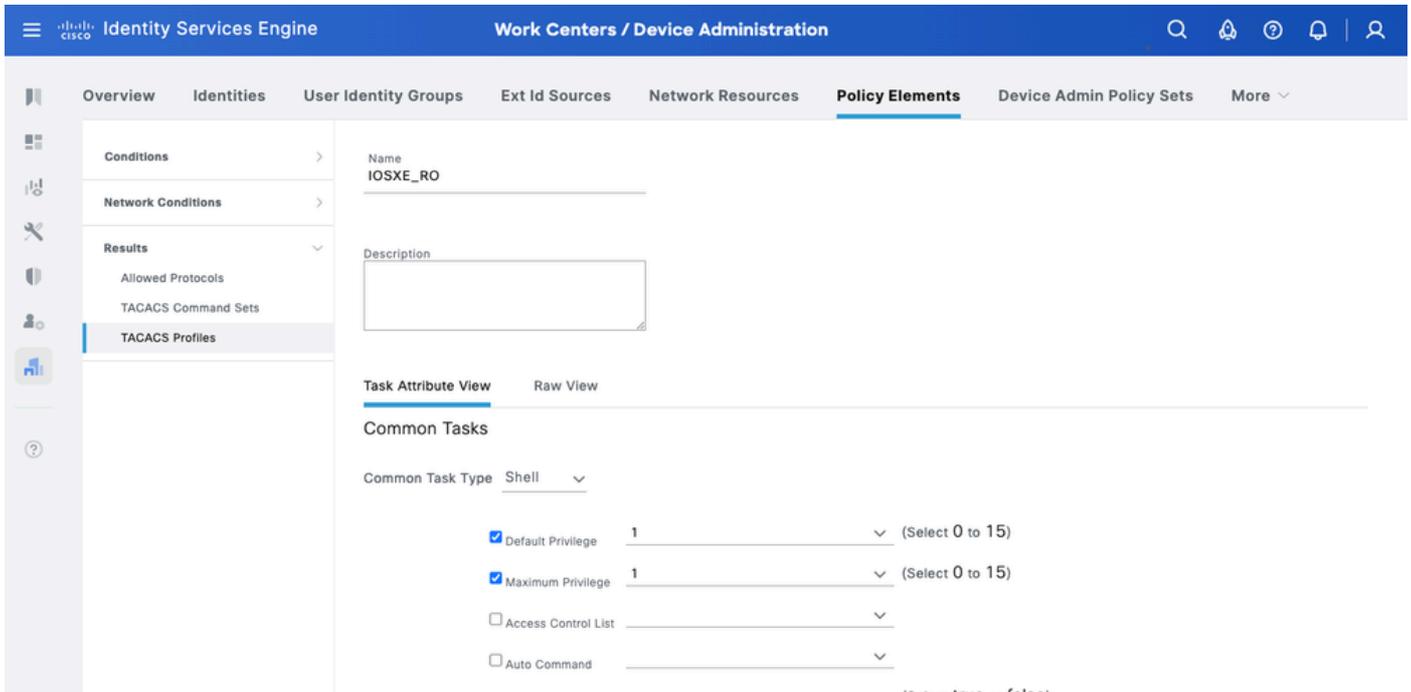


IOS_XE_RO - Betreiberprofil

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.



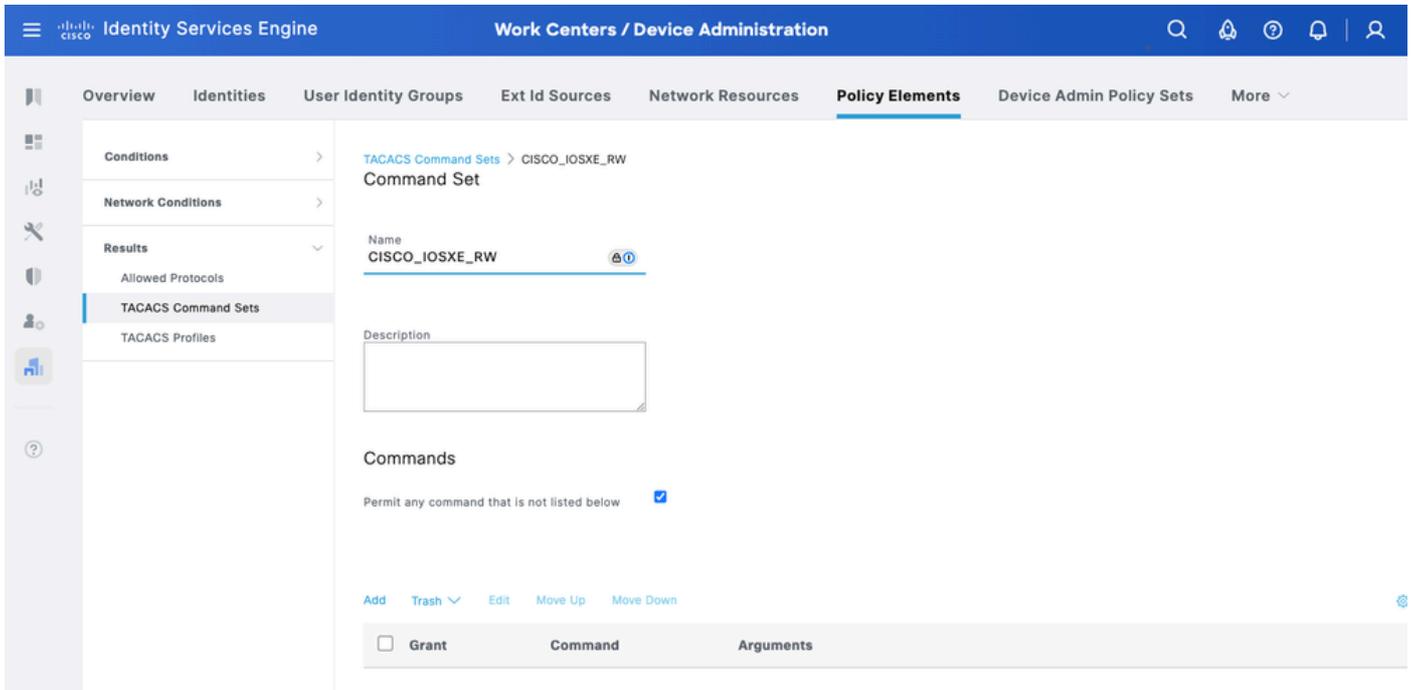
Konfigurieren von TACACS+-Befehlssätzen

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.



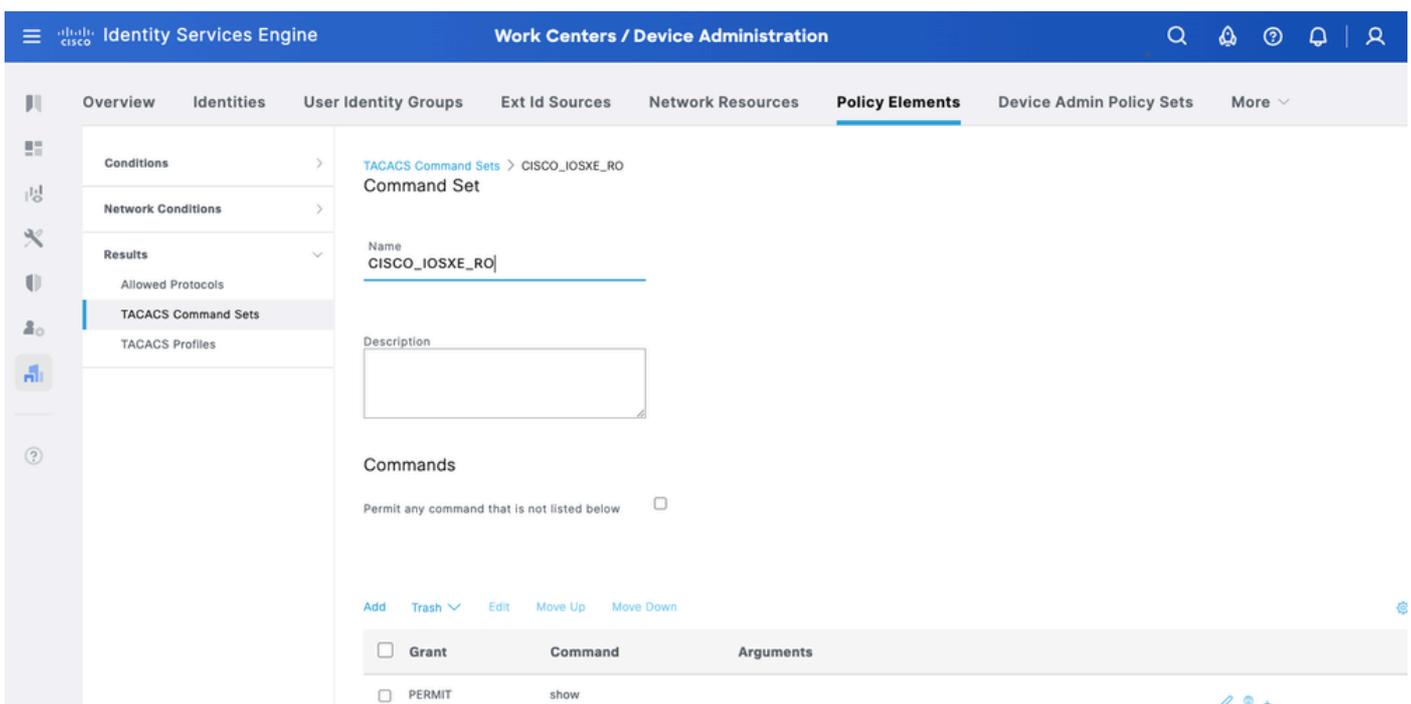
CISCO_IOS XE_RO - Befehlssatz für Bediener

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.



Konfigurieren Geräte-Admin-Richtliniensätze

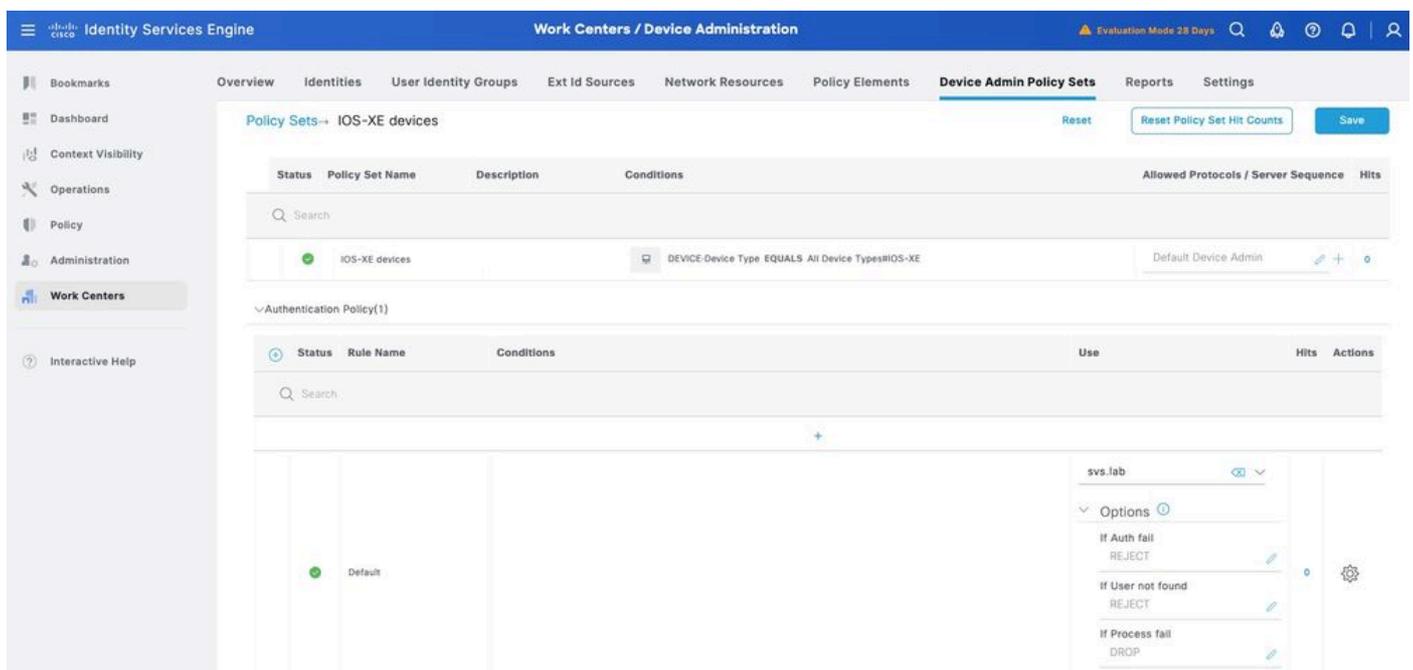
Richtliniensätze sind standardmäßig für die Geräteadministration aktiviert. Richtliniensätze können Richtlinien basierend auf den Gerätetypen aufteilen, um die Anwendung von TACACS-Profilen zu vereinfachen.

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.

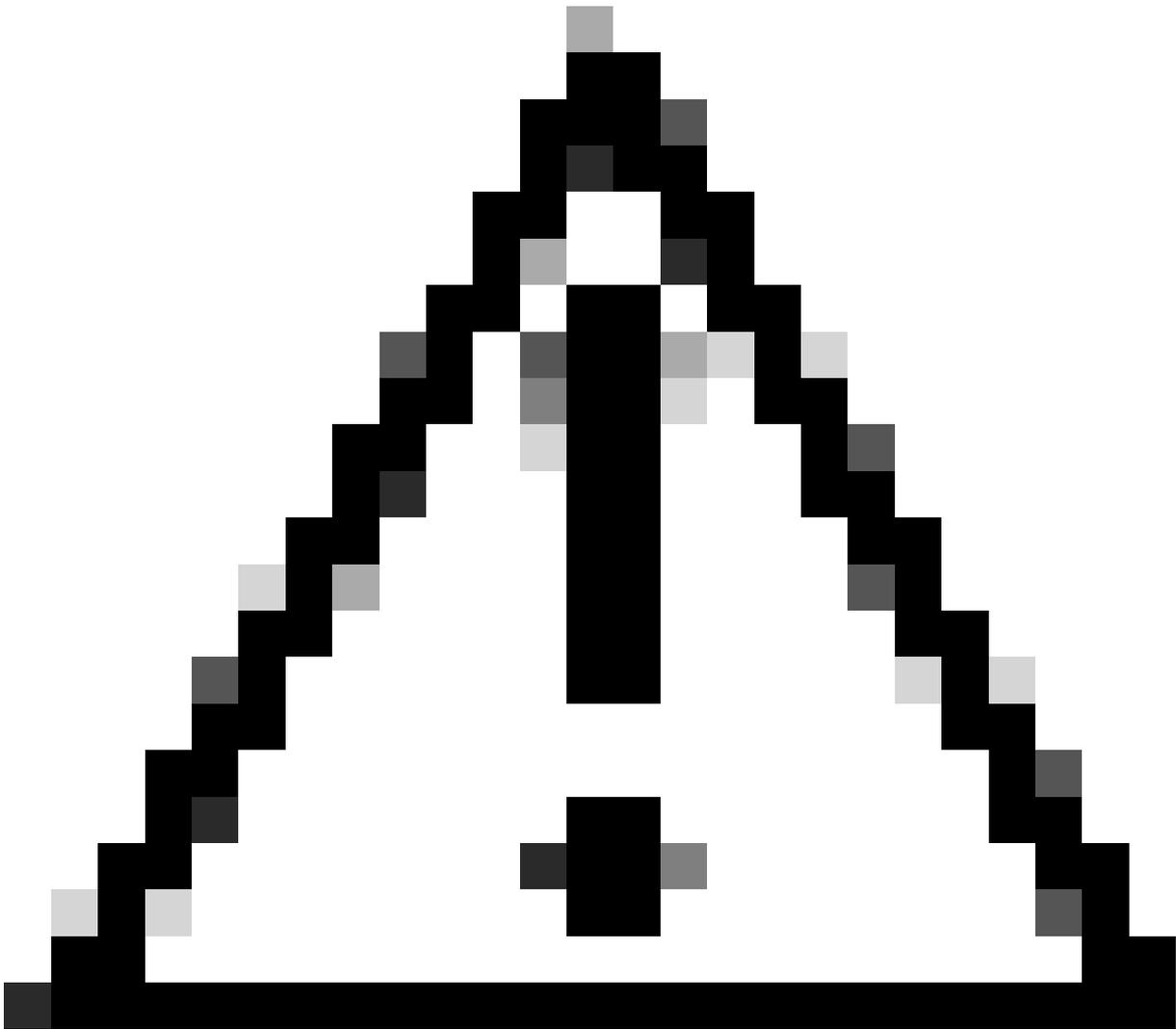
The screenshot displays the Cisco Identity Services Engine (ISE) Work Centers / Device Administration interface. The main navigation bar includes 'Overview', 'Identities', 'User Identity Groups', 'Ext Id Sources', 'Network Resources', 'Policy Elements', and 'Device Admin Policy Sets'. The current view is 'Policy Sets -> IOS-XE devices'. A table lists the policy sets:

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

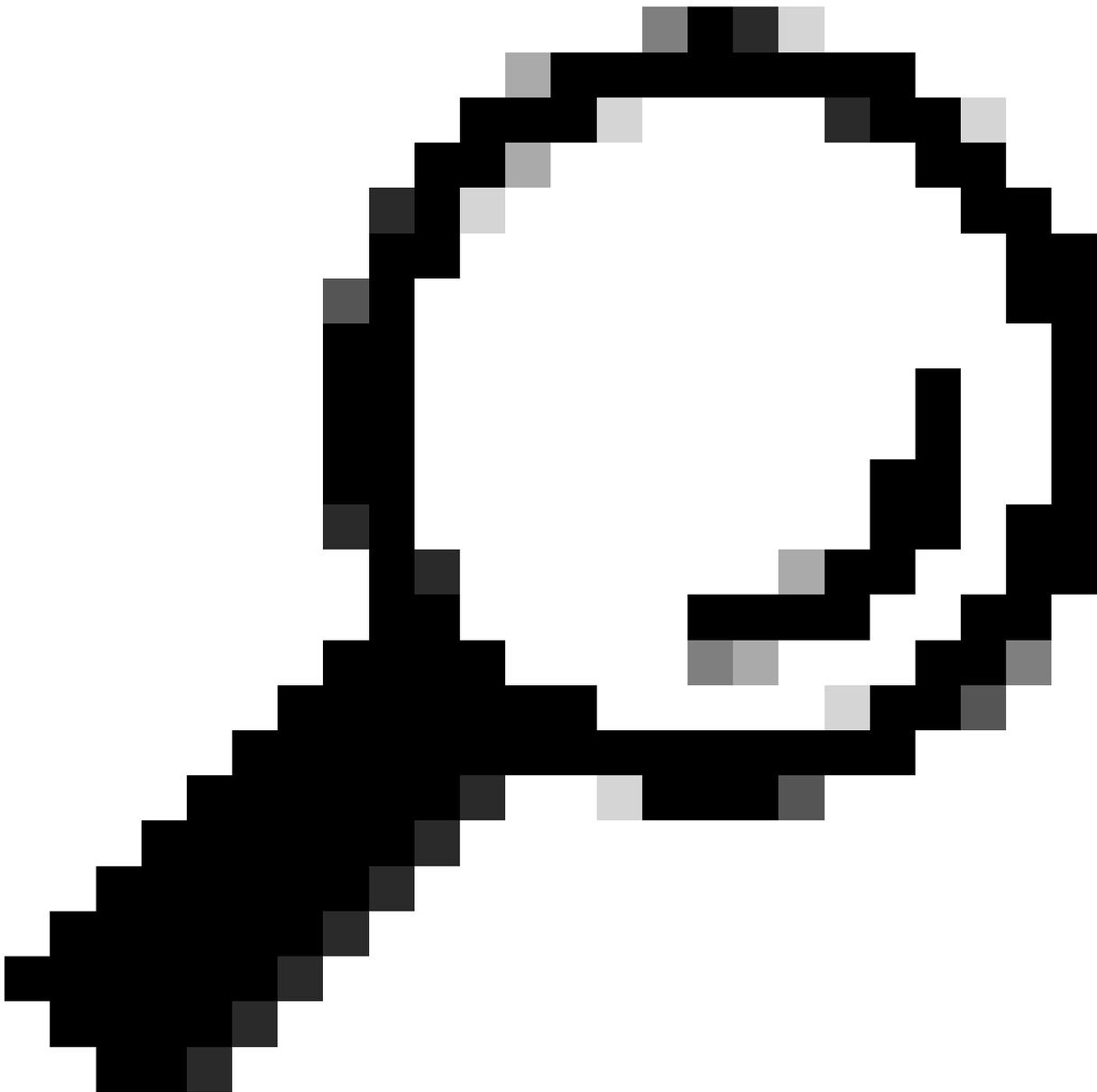
Below this, there are sections for 'Authentication Policy(1)', 'Authorization Policy - Local Exceptions', 'Authorization Policy - Global Exceptions', and 'Authorization Policy(3)'. The 'Authorization Policy(3)' section is expanded to show a detailed table of rules:

Status	Rule Name	Conditions	Results			Hits	Actions
			Command Sets	Shell Profiles	Hits		
✓	Authorization Rule RO	svs.lab-ExternalGroups EQUALS svs.lab/Users/Device RO	CISCO_IOSXE_RO	IOSXE_RO	0	⚙️	
✓	Authorization Rule RW	svs.lab-ExternalGroups EQUALS svs.lab/Users/Device Admin	CISCO_IOSXE_RW	IOSXE_RW	0	⚙️	
✓	Default		DenyAllCommands	Deny All Shell Profile	0	⚙️	

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

ip domain name sv.s.lab

crypto key generate ec keysize 256 label sv.s-256ec-key

Konfiguration des Vertrauenspunkts

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

```
crypto pki trustpoint sv.s_cat9k
  enrollment terminal pem
  subject-name C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=cat9k.sv.s.lab
  serial-number none
  ip-address none
  revocation-check none
  eckeypair sv.s-256ec-key
```

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

<#root>

cat9k(config)#

```
crypto pki authenticate sv.s_cat9k
```

Enter the base 64 encoded CA certificate.

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

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

```
MIIF1DCCA3ygAwIBAgIIIM10AsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZmZAVBgNVBAGTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECXMdU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUGA1UECBMOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBACTB1JhbGVpZ2gxDjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNNTV1MxEjAQBgNVBAMTCVNWUyBYWJDQTCC
AiiwDQYJKoZIhvcNAQEBBQADgGIPADCCAgogCggIBAJvZU0yn2vIn6gKbx3M7vaRq
2YjwZ1zSH6EkEvxnJT+y+kksiFD33GyHQepk7vfp4NFU50tQ4HC7t/A0v9grDa3QW
Vwv4MBBjHfM3s0J/ejgDYcMZhIAaPy0Zo5WLbo0kXEiKjPLatkXojB8FVrhLF30
jMBSqwa4/Wlniy5S+7s4FFxsCf20COWfBAsnrs0tatIIhmcnx+VLJP7MRm8f0w4m
mutNo7IhbJSrgAFXmj1bBjMmgsp0bULo/wxMHdTbtPBf11HRHTkNIo3qy04UADL2
WpoGhgT/FaxxBo2UBcnYVaP+jjREONYT973MCbVAAXtNVU6bEBR0z+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7B0e8oDNKU6gX1ojKyLP/gC7j8AeP03ir+kZui8
```

```
b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
gJ+kQXe7QtT/u6m1MrtjE3gAEVpL334rTIxy9hpKZIKB86t2ZA3JX8CLsbCa13sA
z1XCoONX+6a1ekmXuAOI+t3c1sNbn2AtFi4cJovTA01xh60I4QnK+MNQKpTjt/E4
ydH10rrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVL1783nTc9wYptQEPi5sw
83g9EMgKV0ARIiVUa/q1AgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAyb4
QgEBBAQDAgAHMBkGCWCSAGG+EIBDQMFgpTV1MgTGFIEENBMAOGCSqGSIB3DQEB
CwUAA4ICAQAIT308oL2L6j/7Kk9VdcouaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qjo54HTpxRLgo5oK0dGayi
iSEkSSX9qyflFINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXRX67X+v
O+ja6zTQqj06lqJhmrSkyFbYf/ZTpe4d10zJsZjNsN0r8bF9n0A/7qNZLp3Z3cpU
PU0KdbiSvRqnPw3e8TfITVmAzcx8COI2SrYFMSUazo1VBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIE0f5ay1PKURO/8aj/B7a1uJapXkmnj5qPeGhN0pB
Q9r14reov4so2EspkXS7CrH9yGfpIyTprokz1UvZBZ8v1oI7YZmjFmem+5rT6Gnk
eU/1X7nV61SYG5W5K+I8uaKuyBHOMn7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgrU8
8ggz1P0dsS/i6Lo7ypYX0eB9HgVDCkzQsLXQuHGj/2WsgPgdRcjkvnyURk4Jx+Ib
xDrmo7e0XPPSW4172a6K18CR3U2Cr4wsuvndPEq/qd2NRSBWffFOXe/AJHQG7STT
HaXLU9r2Ko603oecu8ysGTwL1It/9T1/F0b0xZRugWcpJrVoTgDGuA==
```

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

Certificate has the following attributes:

Fingerprint MD5: D9C404B2 EC08A260 EC3539E7 F54ED17D

Fingerprint SHA1: 0EB181E9 5A3ED780 3BC5A805 9A854A95 C83AC737

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

yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

cat9k(config)#

Schritt 3: Erstellen einer Zertifikatsanforderung (Certificate Signing Request, CSR).

```
<#root>
```

cat9k(config)#

```
crypto pki enroll svcs_cat9k
```

% Start certificate enrollment ..

% The subject name in the certificate will include: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=cat9k.svs.lab

% The subject name in the certificate will include: cat9k.svs.lab

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

yes

Certificate Request follows:

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

```
MIIBfDCCASMAQAwYQxGjAYBgNVBAMTEWdhD1rLnRtby5zdnMuY29tMQwwCgYD
VQQLEwNTV1MxDjAMBGAoTBUNpc2NvMQwwCgYDVQQHEwNSVFAXCzAJBgNVBAGT
Ak5DMQswCQYDVQQGEwJVUzEgMB4GCSpqGSIB3DQEJAHYRY2F00wsudG1vLnN2cy5j
b20wWTATBgcqhkiOPQIBggqhkjOPQMBBwNCAATpYE7atscrt14ddevCh3UgxjYi
4N4oBGWrpJBctKy4so8V5i6RXDt7kHgPzp14Qnf20bcXVODE1wtTAHhBrIXqoDww
```

```
OgYJKoZIhvcNAQkOMSOwKzAcBgNVHREEFTATghFjYXQ5ay50bW8uc3ZzLmNvbTAL
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)#

Schritt 4: CA-signiertes Zertifikat importieren.

<#root>

cat9k(config)#

```
crypto pki import svcs_cat9k certificate
```

Enter the base 64 encoded certificate.

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

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

```
MIID8zCCAadugAwIBAgIiKfdYwg5WpskwDQYJKoZIhvcNAQELBQAwaJELMAkGA1UE
BhMCVVMxZmFzAVBgNVBAGTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWx1aWdo
MQ4wDAYDVQQKEwVDAxNjBzEMMAoGA1UECXMU1ZTMRIwEAYDVQQDEw1TV1MgTGF-i
Q0EwHhcNMjUwNTE0MTUxMjAwWhcNMjUwNTE0MTUxMjAwWjCBhDEaMBGGA1UEAxMR
Y2F0OWsudG1vLnN2cy5jb20xDDAKBgNVBAsTA1NWUzE0MAwGA1UEChMFQ21zY28x
DDAKBgNVBAcTA1JUUEDELMkGA1UECBMCTkMxCzAJBgNVBAYTA1VTMSAwHgYJKoZI
hvcNAQkCFhFjYXQ5ay50bW8uc3ZzLmNvbTBZMBMGByqGSM49AgEGCCqGSM49AwEH
A0IAB01gtTq2xyu2Xh1168KHdSDGNiLg3igEZaukkFy0rLiYjXmLpFc03uQeA/O
nXhCd/bRtxdU4MTXC1MAccGsheqjTTBLMB4GCWCGSAGG+EIBDQRRFg94Y2EgY2Vy
dG1maWNhdGUwHAYDVRORBBUwE4IRY2F0OWsudG1vLnN2cy5jb20wCwYDVR0PBAQD
AgeAMAOGCSqGSIb3DQEBCwUAA4ICAQB0bgKVykeyVC9Usvuu0AUsGaZHGwy2H9Yd
m5vIauI6PJczkCzIoAIghHPGQhIgpEcRqtGyXPZ2r8TCJP11WXNN/G73sFyWAHzY
RtmIM5KIojiDHLtiFpayxv9juDuZRx+wYR2PIQ5eLv1bafg7K8E82sq0Cf0tcPr
Oc0NU8UCxq0bd0gu4XsdBN1+wcWFqeQSDLmP7nxvh00m/LXwCWUhwgVio0AuU2Fe
k5NthtvdXNAhRAImQdTyq6u/yB7vwTwJHcRiJc5USsyzCsTBb6RvL+HsXqBgXGc5
1xCSoltYodUxFIpJyK2MOZBY2zq2cNSc8Xbso5/OEQmnHtpWPvij4rSPUHQSY+4m
Qq2Sn3iqf4mGh/A08T4iXfWdWfNezh7ZxMsCSCK/ZR1ELZ2hj60fzwX1H27Uf8XU
ecr0Wx+WzRn7LVRCaGQzFkukfi8S4DLLNtxNHFSLBVX5yHXCLEL+CQ7n8Z/pxcB
VVRpitwN3Zb09poZywiRLTnBsb42xNaWiL9bjQznA0iTDfmfFFourBsaAioz7ouY
2r1Mh+OpE83Uu+41OTMawDgGiEv7iaij6xWc95EC+Adm0x3FvBXmtIM9qr7WwHW6
3C2hVYHJH254e1V5+H8iiz7rovEpm8ZDsnvYpJn4Km3iDvBNqp/vvAHOfcyXrvG6
3i/1b9erGQ==
```

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

% Router Certificate successfully imported

cat9k(config)#

TACACS und AAA mit TLS-Konfiguration

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

```
tacacs server sv_s_tacacs
  address ipv4 10.225.253.209
  single-connection
  tls port 6049
  tls idle-timeout 60
  tls connection-timeout 60
  tls trustpoint client sv_s_cat9k
  tls ip tacacs source-interface GigabitEthernet0/0
  tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ sv_s_tls
  server name sv_s_tacacs
  ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request
```

Schritt 2: Konfigurieren von AAA-Methoden

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

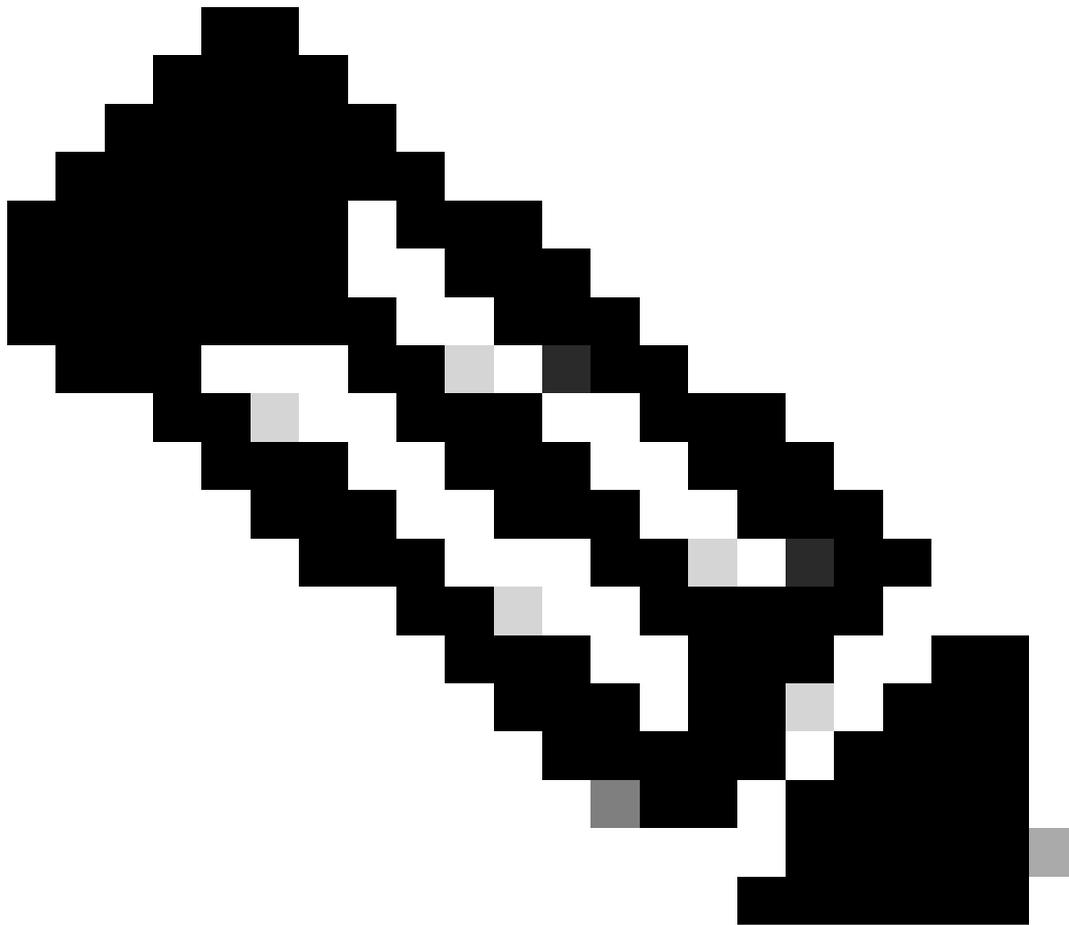
Konfigurationsmethode 2 - Von CA generiertes Schlüsselpaar

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

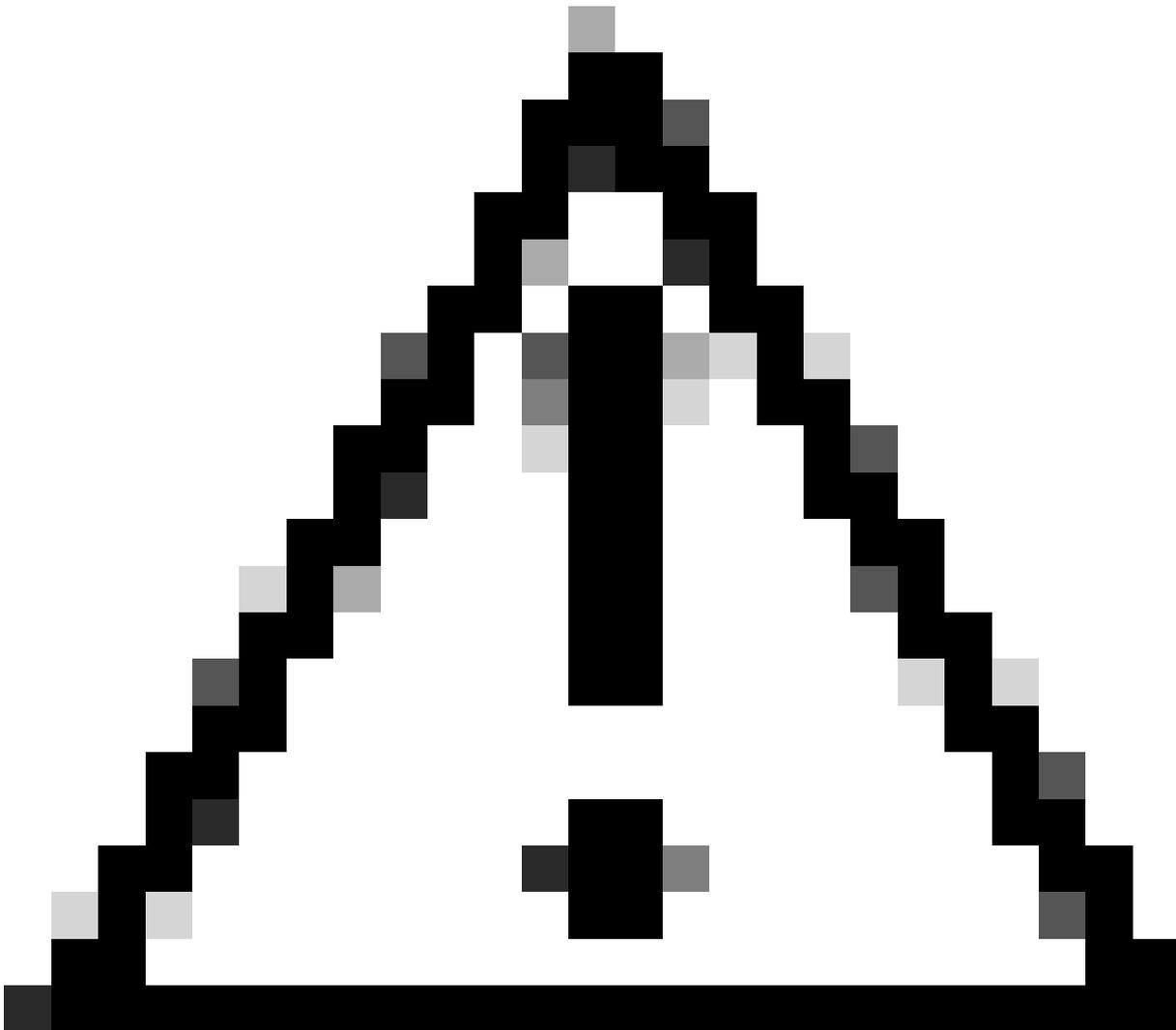
Schritt 1: Erstellen eines Client-Vertrauenspunkts.

```
cat9k(config)#crypto pki trustpoint sv_s_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 svc_cat9k_25jun17 pkcs12 bootflash:cat9k-25jun17.pfx
```

```
password Cisco.123
```

```
% Importing pkcs12...Reading file from bootflash:cat9k-25jun17.pfx
```

```
CRYPTO_PKI: Imported PKCS12 file successfully.
```

cat9k#

cat9k#

```
show crypto pki certificates svc_cat9k_25jun17
```

Certificate

Status: Available

Certificate Serial Number (hex): 5860BF33A2033365

Certificate Usage: General Purpose

Issuer:

cn=SVS LabCA

ou=SVS

o=Cisco

l=Raleigh

st=North Carolina

c=US

Subject:

Name: cat9k.svs.lab

e=pkalkur@cisco.com

cn=cat9k.svs.lab

ou=svs

o=cisco

l=rtp

st=nc

c=us

Validity Date:

start date: 17:56:00 UTC Jun 17 2025

end date: 17:56:00 UTC Jun 17 2026

Associated Trustpoints: svc_cat9k_25jun17

CA Certificate

Status: Available

Certificate Serial Number (hex): 20CD7402C4DA37F5

Certificate Usage: General Purpose

Issuer:

cn=SVS LabCA

ou=SVS

o=Cisco

l=Raleigh

st=North Carolina

c=US

Subject:

cn=SVS LabCA

ou=SVS

o=Cisco

l=Raleigh

st=North Carolina

c=US

Validity Date:

start date: 17:05:00 UTC Apr 28 2025

end date: 17:05:00 UTC Apr 28 2035

Associated Trustpoints: svc_cat9k_25jun17 svc_cat9k

Storage: nvram:SVSLabCA#37F5CA.cer

TACACS und AAA mit TLS-Konfiguration

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

```
tacacs server sv_s_tacacs
  address ipv4 10.225.253.209
  single-connection
  tls port 6049
  tls idle-timeout 60
  tls connection-timeout 60
  tls trustpoint client sv_s_cat9k
  tls ip tacacs source-interface GigabitEthernet0/0
  tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ sv_s_tls
  server name sv_s_tacacs
  ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request
```

Schritt 2: Konfigurieren von AAA-Methoden

```
aaa authentication login default group sv_s_tls local enable
aaa authentication login console local enable
aaa authentication enable default group sv_s_tls enable
aaa authorization config-commands
aaa authorization exec default group sv_s_tls local if-authenticated
aaa authorization commands 1 default group sv_s_tls local if-authenticated
aaa authorization commands 15 default group sv_s_tls
aaa accounting exec default start-stop group sv_s_tls
aaa accounting commands 1 default start-stop group sv_s_tls
aaa accounting commands 15 default start-stop group sv_s_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 subsystem
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.