

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

Inhalt

[Einleitung](#)

[Überblick](#)

[Verwendung dieses Handbuchs](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Lizenzierung](#)

[Teil 1: ISE-Konfiguration 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 XR RW - Administratorprofil](#)

[IOS XR RO - Betreiberprofil](#)

[Konfigurieren von TACACS+-Befehlssätzen](#)

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

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

[Konfigurieren Geräte-Admin-Richtliniensätze](#)

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

[Startkonfigurationen](#)

[Vertrauenspunkt konfigurieren](#)

[Konfigurieren von TACACS und AAA mit TLS](#)

[Erneuerung des Zertifikats](#)

[Verifizierung](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird ein Beispiel für TACACS+ über TLS mit Cisco Identity Services Engine (ISE) als Server und einem Cisco IOS® XR-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 XR-basierte Netzwerkgeräte verwalten kann.

- Teil 1: Konfigurieren der ISE für den Geräteadministrator
- Teil 2: Konfigurieren von Cisco IOS XR 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 8201 Router, Version 25.3.1

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.

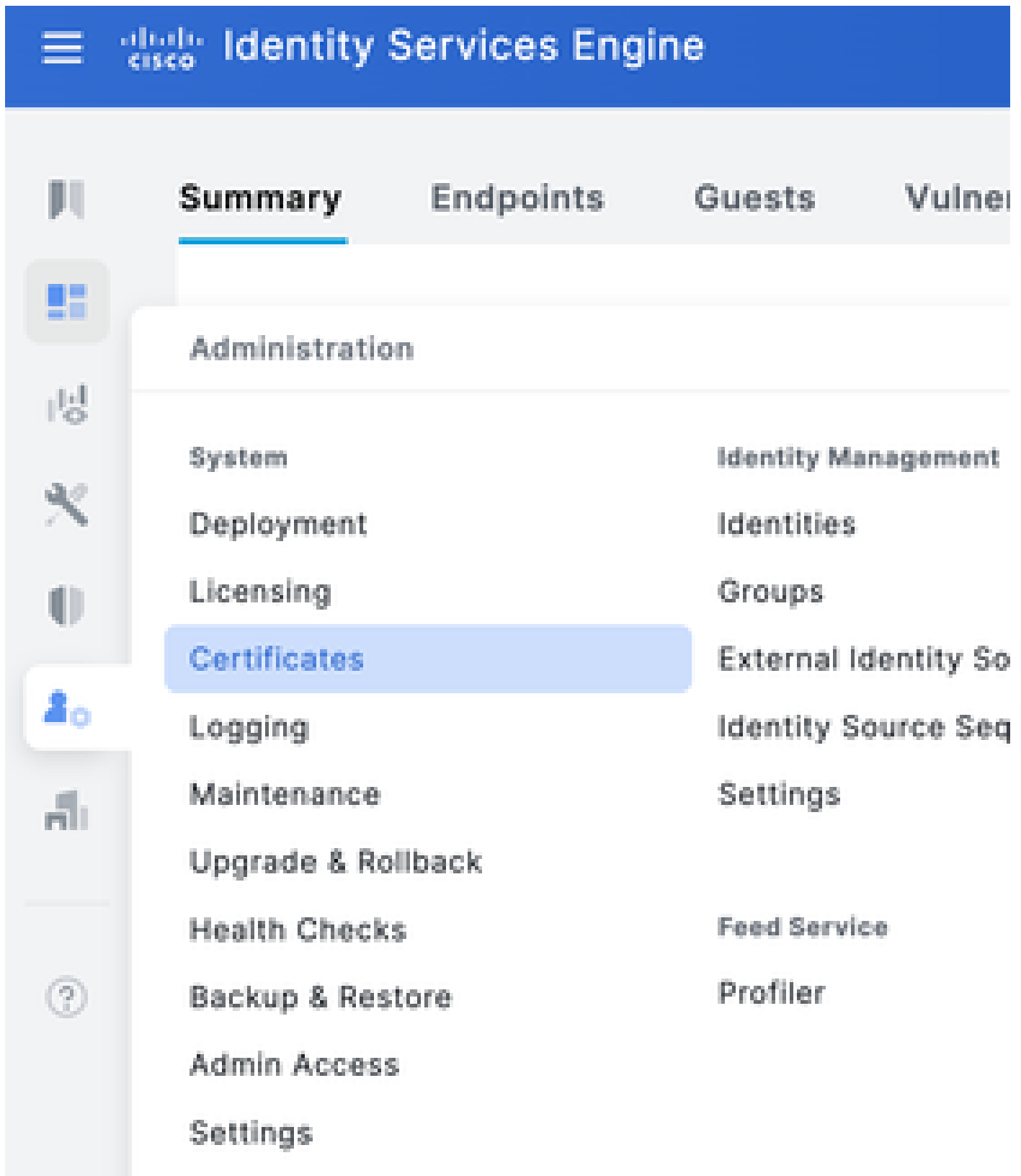
Teil 1: ISE-Konfiguration für die Geräteverwaltung

Zertifikatsignierungsanforderung für TACACS+-Serverauthentifizierung generieren

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

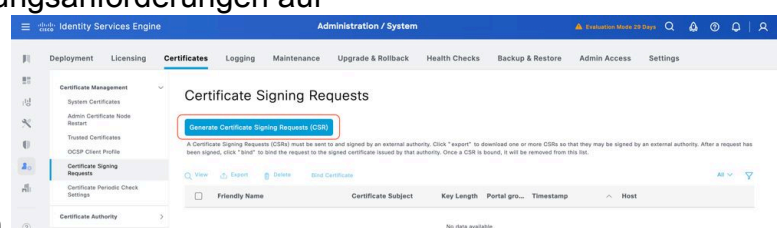
Standardmäßig verwendet die ISE ein selbstsigniertes Zertifikat für alle Dienste. Der erste Schritt besteht darin, eine CSR-Anfrage (Certificate Signing Request) zu erstellen, damit sie von unserer Zertifizierungsstelle (Certificate Authority, CA) signiert wird.

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



Schritt 3: Klicken Sie unter Zertifikatsignierungsanforderungen auf

Zertifikatsignierungsanforderung generieren.



Schritt 4: Wählen Sie TACACS inUsage aus.

Usage

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

Allow Wildcard Certificates ☐ 

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

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☒ 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

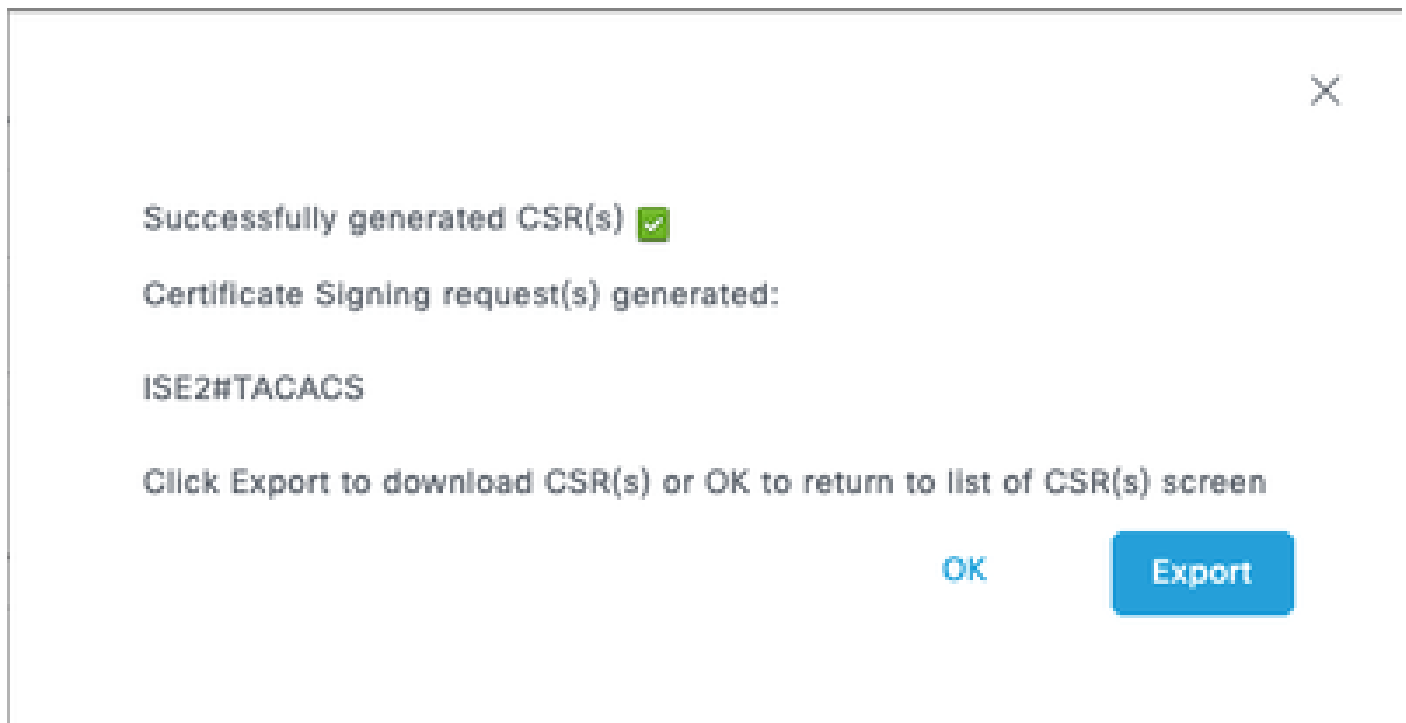
Country (C)
US

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

Subject Alternative Name (SAN)

⋮	DNS Name	✓	ISE1.lab	−	+	
⋮	IP Address	✓	10.225.253.209	−	+	?

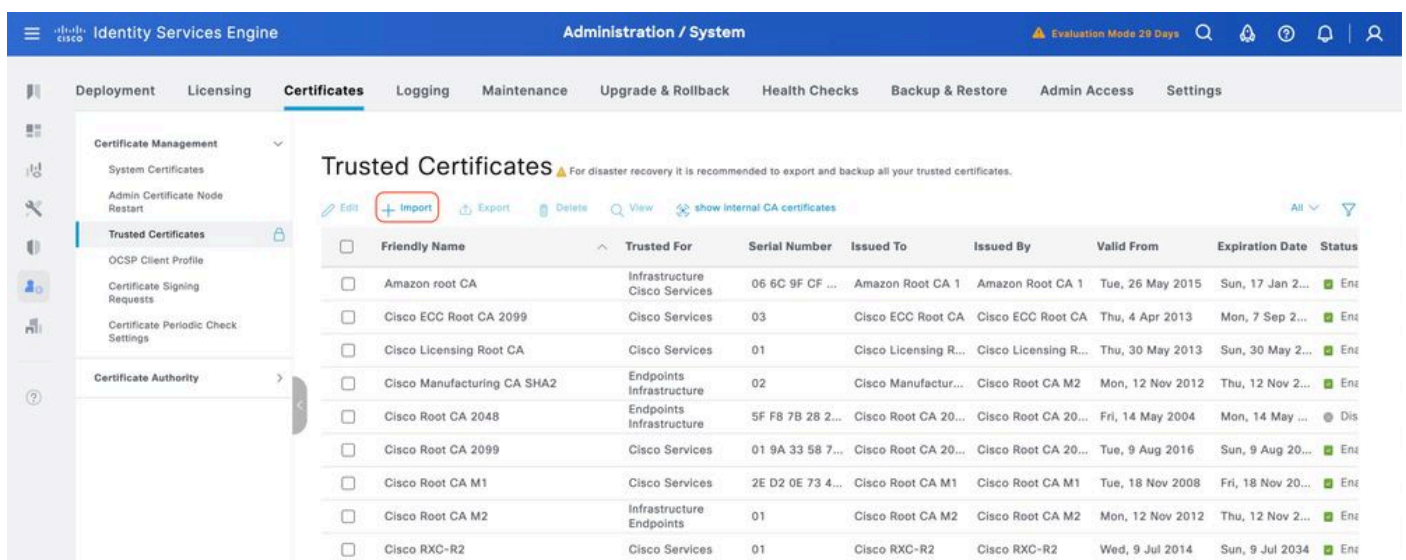
Schritt 8: Klicken Sie auf Generieren und dann auf Exportieren.



Nun können Sie das Zertifikat (CRT) von Ihrer Zertifizierungsstelle (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

Submit

Cancel

Klicken Sie auf Senden. Das Zertifikat muss nun unter Vertrauenswürdige Zertifikate angezeigt werden.

Identity Services Engine Administration / System Evaluation Mode 27 Days

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Admin Certificate Node Restart
- Trusted Certificates**
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check

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

⚙️ Edit + Import 📄 Export 🗑️ Delete 🔍 View 🔗 show internal CA certificates

☐	Friendly Name	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Sta
☐	CN=SVS LabCA, OU=SVS, O=Cisco, L=...	Infrastructure Cisco Services Endpoints AdminAuth	20 CD 74 02 ...	SVS LabCA	SVS LabCA	Mon, 28 Apr 2025	Sat, 28 Apr 2...	

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 Zertifikatsignaturanforderungen die im vorherigen Schritt generierte TACACS-CSR aus, und klicken Sie auf Zertifikat binden.

Identity Services Engine Administration / System Evaluation Mode 29 Days

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Admin Certificate Node Restart
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests**
- Certificate Periodic Check

Certificate Signing Requests

Generate Certificate Signing Requests (CSR)

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

🔍 View 📄 Export 🗑️ Delete **Bind Certificate**

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

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

Identity Services Engine Administration / System Evaluation Mode 29 Days

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Admin Certificate Node Restart
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests**
- Certificate Periodic Check Settings
- Certificate Authority

Bind CA Signed Certificate

* Certificate File

Friendly Name

Validate Certificate Extensions ☐

Usage

☒ TACACS: Use certificate for TACACS Server

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



Warning

The certificate you are importing or generating matches an existing certificate. (Both certificates have the same subject.) If you proceed, the existing certificate will be replaced, and the new certificate will be given the same roles and Portal tag, if applicable, as the existing certificate.

Do you wish to replace the existing certificate?

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

Identity Services Engine Administration / System Evaluation Mode 29 Days

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates**
- Admin Certificate Node Restart
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Settings
- Certificate Authority

System Certificates

For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

[Edit](#) [Generate Self Signed Certificate](#) [Import](#) [Export](#) [Delete](#) [View](#)

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
ISE1							
C=US, ST=NC, L=Raleigh, O=Cisco, OU=SVS, CN=I SE1.lab#ISE1.lab#00010	TACACS		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. Es 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 header is blue with the Cisco logo and the text "Identity Services Engine". The left sidebar contains a navigation menu with the following items: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (highlighted with a blue bar), Work Centers, and Interactive Help. The main content area shows the "System" menu expanded, listing the following 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 blue bar and a checkmark).

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

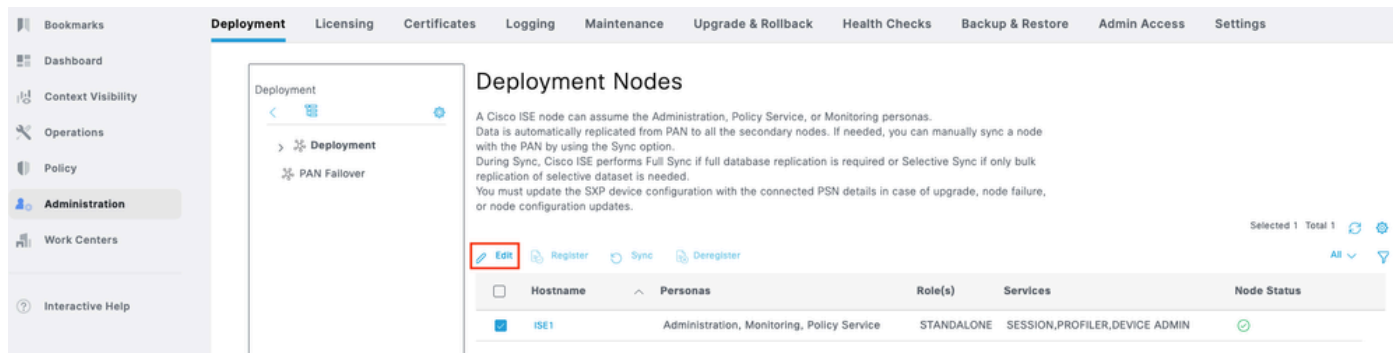


Warnung: Wenn Sie die TLS-Version ändern, wird der Cisco ISE-Anwendungsserver auf allen Cisco ISE-Bereitstellungssystemen neu gestartet.

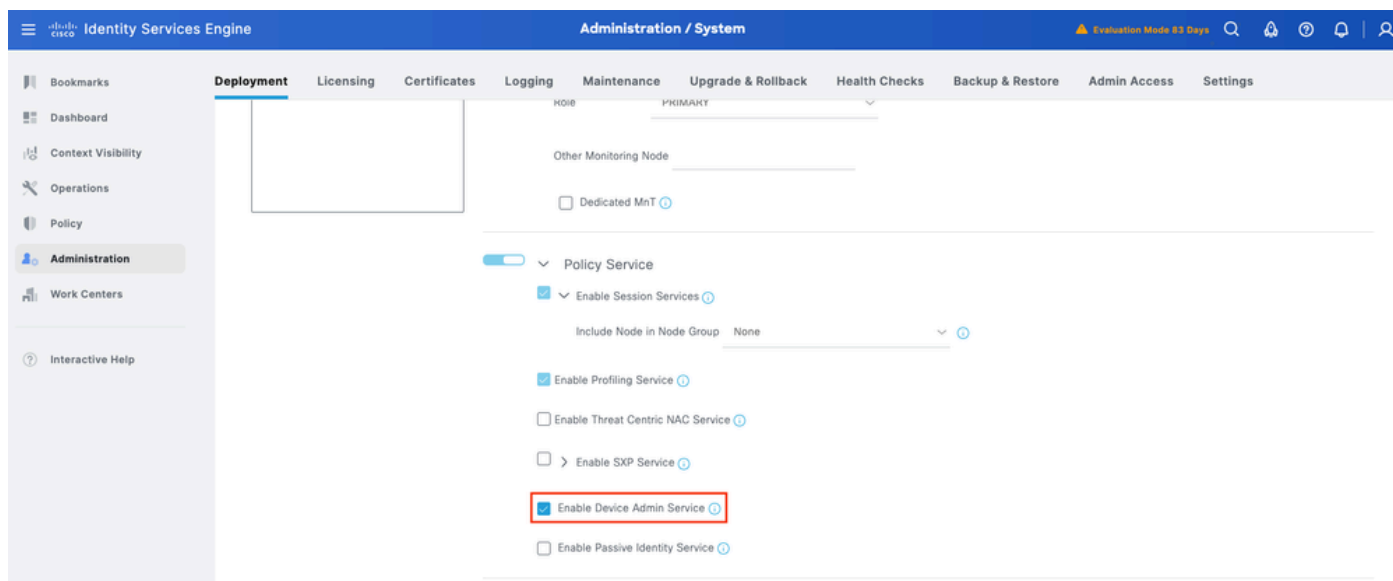
Geräteadministration auf ISE aktivieren

Der Device Administration Service (TACACS+) ist auf einem ISE-Knoten nicht standardmäßig aktiviert. So 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 Bearbeiten.



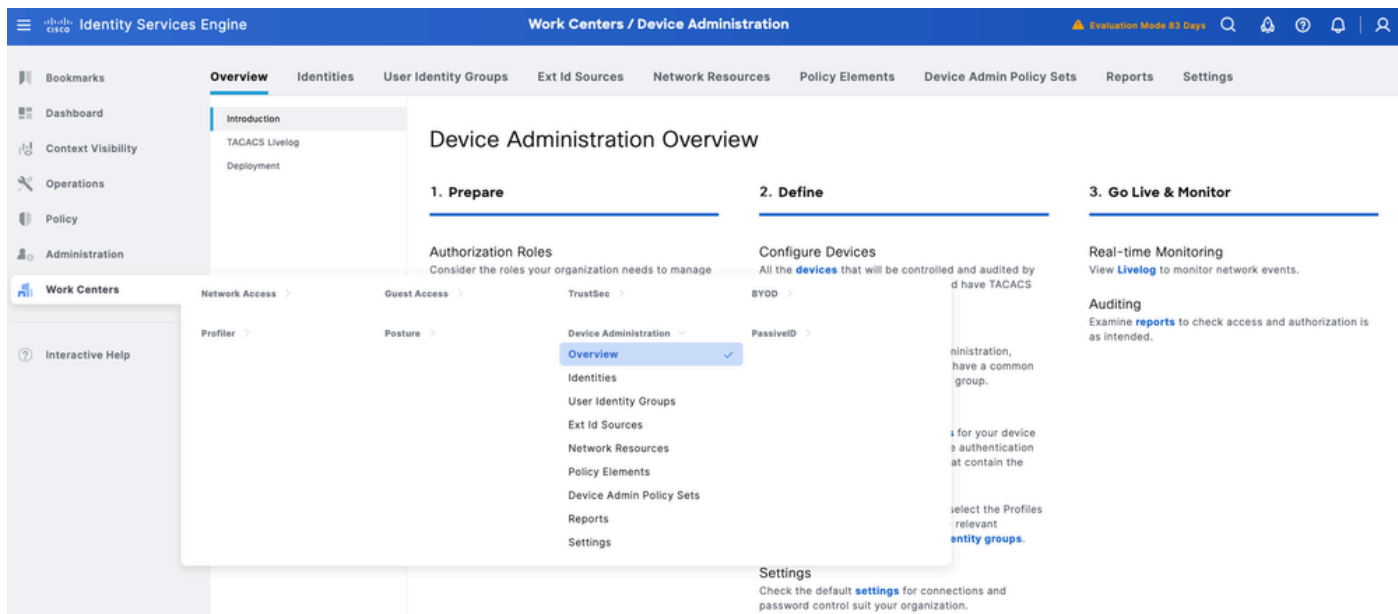
Schritt 2: Blättern Sie unter General Settings nach unten, und aktivieren Sie das Kontrollkästchen neben Enable Device Admin Service (Geräteverwaltungsdienst aktivieren).



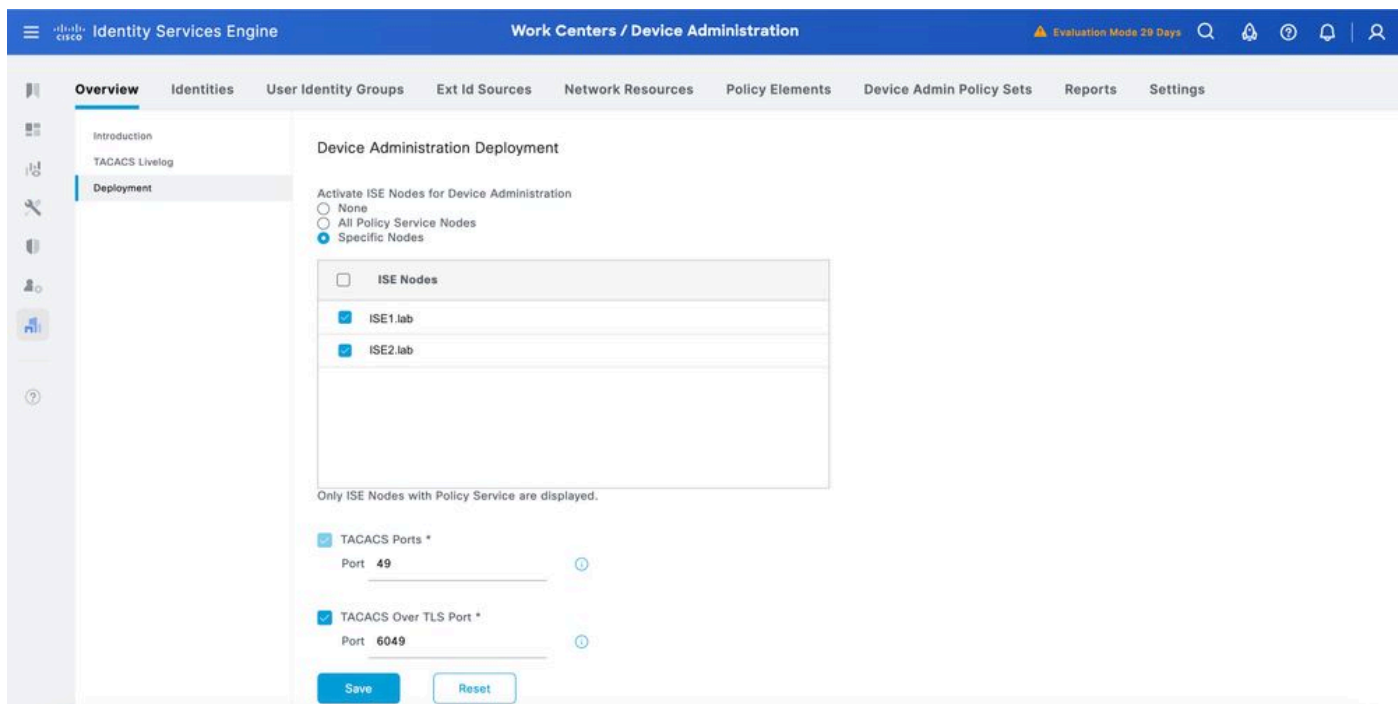
Schritt 3: Speichern der Konfiguration Der Geräteverwaltungsdienst ist jetzt auf der ISE aktiviert.

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 XR.

Identity Services Engine

Work Centers / Device Administration

Subscription Mode 63 Days

OverviewIdentitiesUser

Network Devices

Network Device Groups

Default Devices

TACACS External Servers

TACACS Server Sequence

✕

Edit Group

Name*

IOS-XR

Description

Group Hierarchy

Device Type > All Device Types > IOS-XR

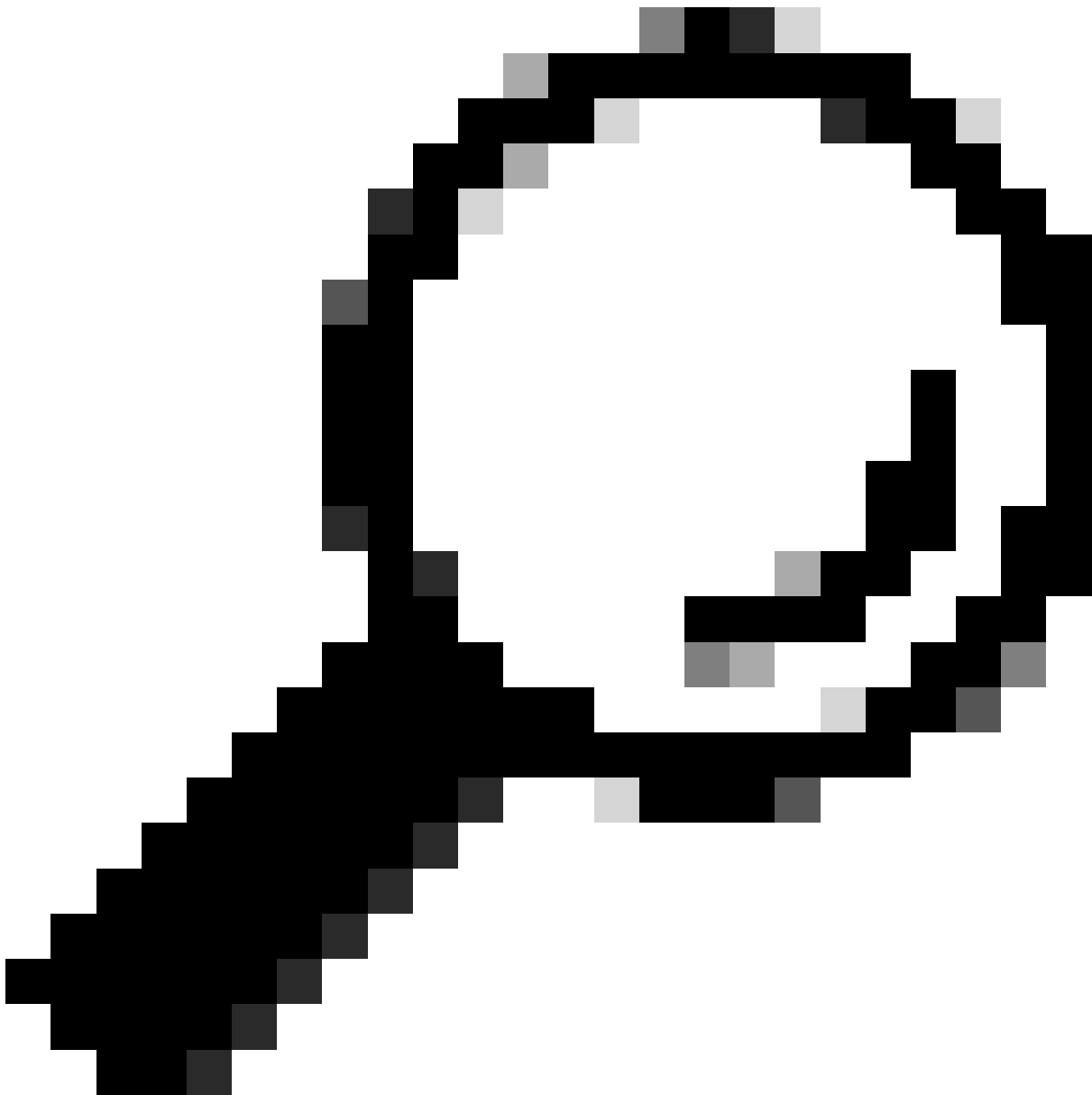
Cancel

Save

☐ ADVA

ADVA SyncDirector Network Time Monitoring

	No. of Network Devices
	--
	702
	0
	11
	243



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 nun ein Cisco IOS XR-Gerät als Netzwerkgerät hinzu. Navigieren Sie zu Work Centers > Device Administration > Network Resources > Network Devices. Klicken Sie auf Hinzufügen, um ein neues Netzwerkgerät hinzuzufügen.

Identity Services Engine Administration / Network Resources Evaluation Mode 11 Days

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences External MDM pxGrid Direct Connectors

Network Devices List > BRC-8201-1

Network Devices

Name

Description

IP Address * IP: 32

IP Address * IP:

Device Profile

Model Name

Software Version

Network Device Group

Location [Set To Default](#)

IPSEC [Set To Default](#)

Device Type [Set To Default](#)

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

Identity Services Engine Work Centers / Device Administration Evaluation Mode 67 Days

Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Help

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements More

Network Devices

Network Device Groups

Default Devices

TACACS External Servers

TACACS Server Sequence

☐ RADIUS Authentication Settings

☐ TACACS Authentication Settings

☒ TACACS over TLS Authentication Settings

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

Subject Alternative Name (SAN)*

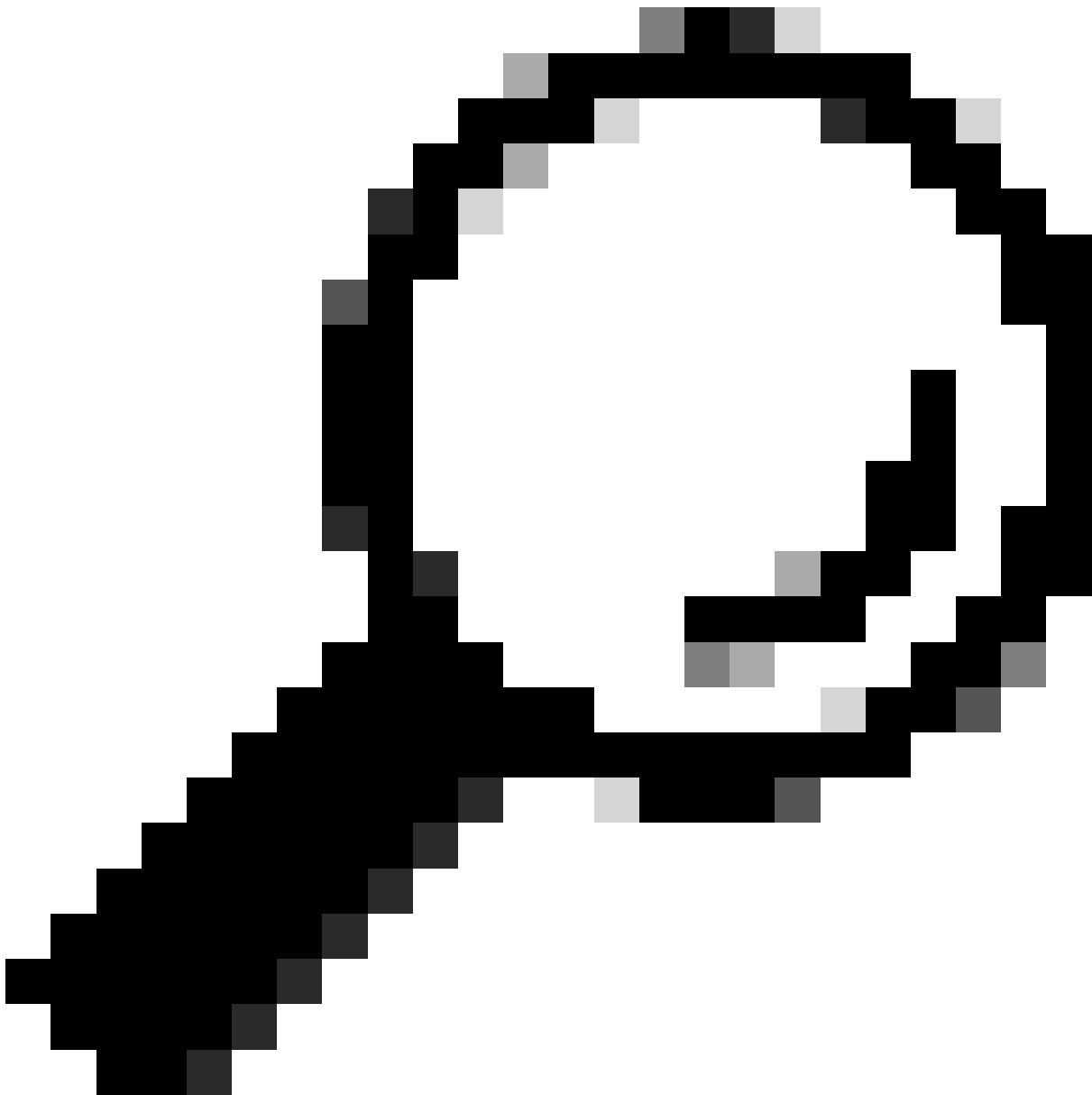
Additional security can be enforced by validating SAN certificate attributes. Cisco ISE supports validating the IP address (IPAddress), DNS Name (dNSName), and Directory Name (directoryName) attributes. The attributes chosen below are evaluated in this order: IP address, DNS Name, Directory Name. When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

☐ IP Address

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

Additional SAN attribute details [Show](#)

Additional SAN Attributes

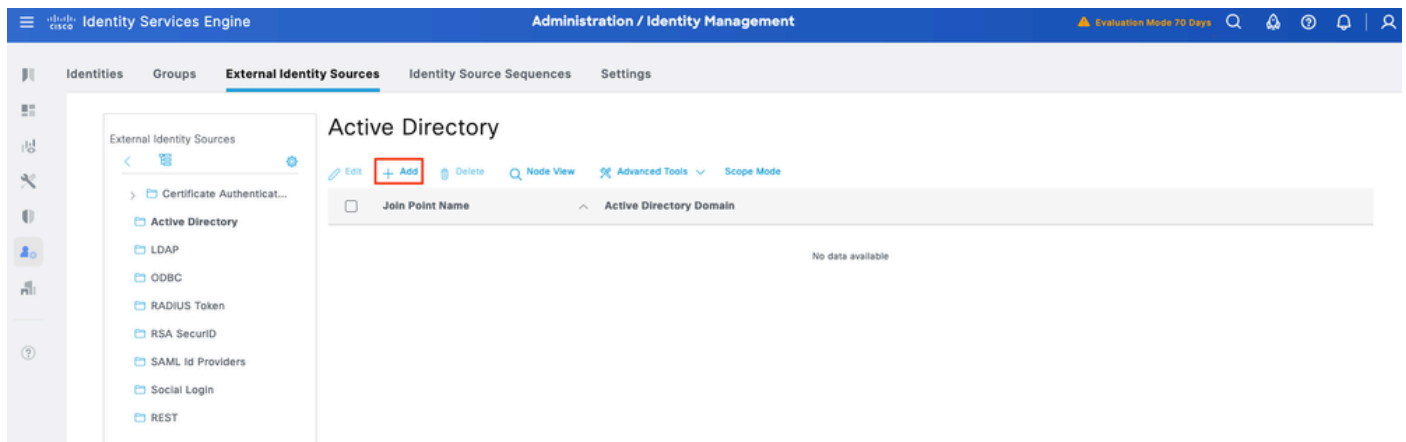


Tipp: Es wird empfohlen, den Single-Connect-Modus zu aktivieren, um zu vermeiden, dass die TCP-Sitzung jedes Mal neu gestartet wird, wenn ein Befehl an das Gerät gesendet wird.

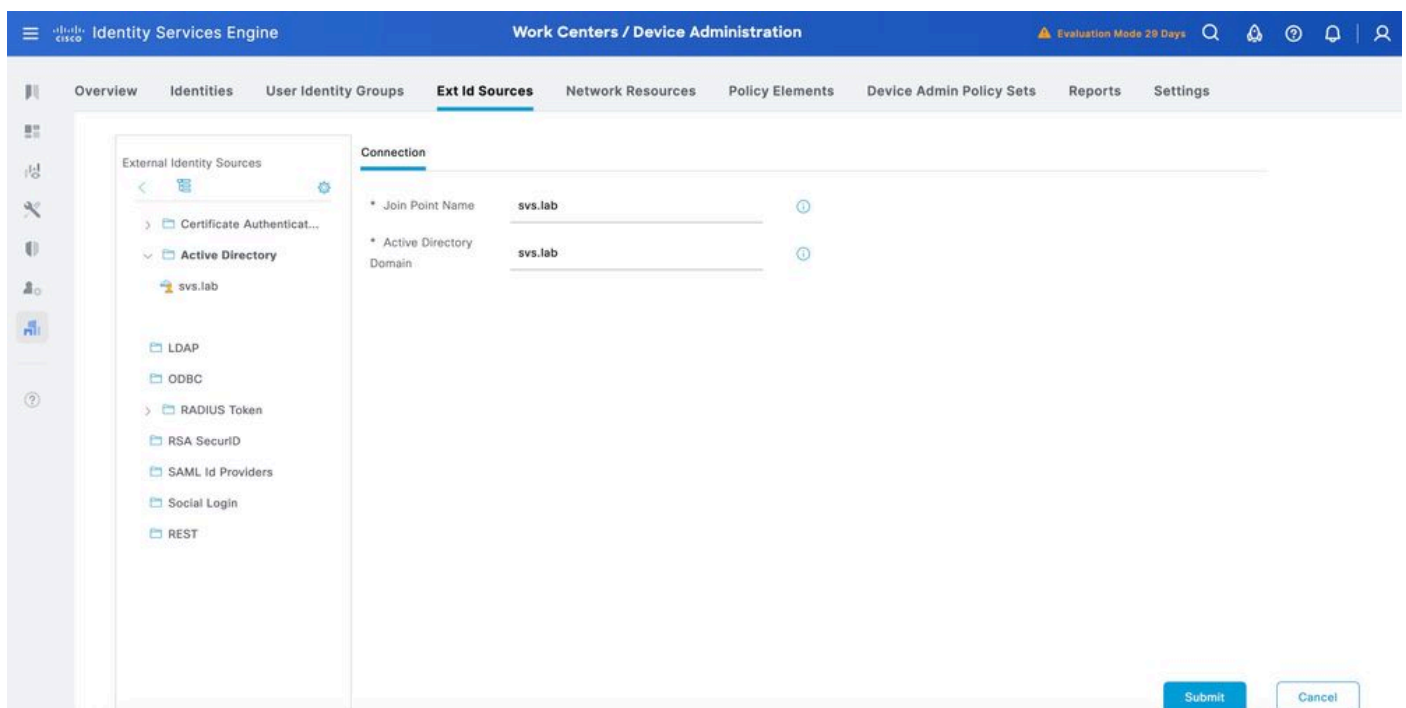
Konfigurieren Identitätsspeicher

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.

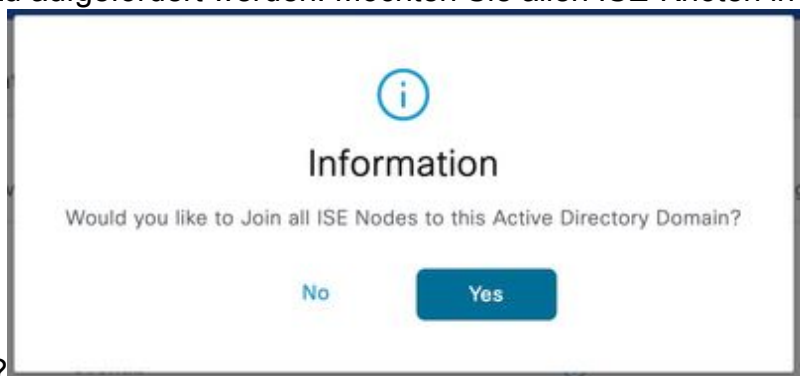


Schritt 2: Geben Sie den Namen des Verbindungspunkts und den AD-Domännennamen an, und klicken Sie auf Senden.



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.

×

Join Domain

Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

* AD User Name ⓘ

administrator

* Password

.....

☐ Specify Organizational Unit ⓘ

☒ Store Credentials ⓘ

Cancel

OK

×

Join Operation Status

Status Summary: Successful.

ISE Node	Node Status
ISE1.lab	✔ Completed.

Close

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. In diesem Beispiel werden die Gruppen dargestellt, die in der

Autorisierungsrichtlinie verwendet werden.

Identity Services Engine

Administration / Identity Management

IdentitiesGroupsExternal Identity SourcesIdentity Source SequencesSettings

External Identity Sources

<+⚙

>Certificate Authenticat...>Active DirectoryLDAPODBCRADIUS TokenRSA SecurIDSAML Id ProvidersSocial LoginREST

ConnectionAllowed DomainsPassiveIDGroupsAttributesAdvanced Settings

Edit+ Add ^Delete GroupUpdate SID Values

Select Groups From Directory

Add Group

SID

No data available

Select Directory Groups

This dialog is used to select groups from the Directory.

Domain

svs.lab

Name

Device *

SID *

Type

ALL

Filter

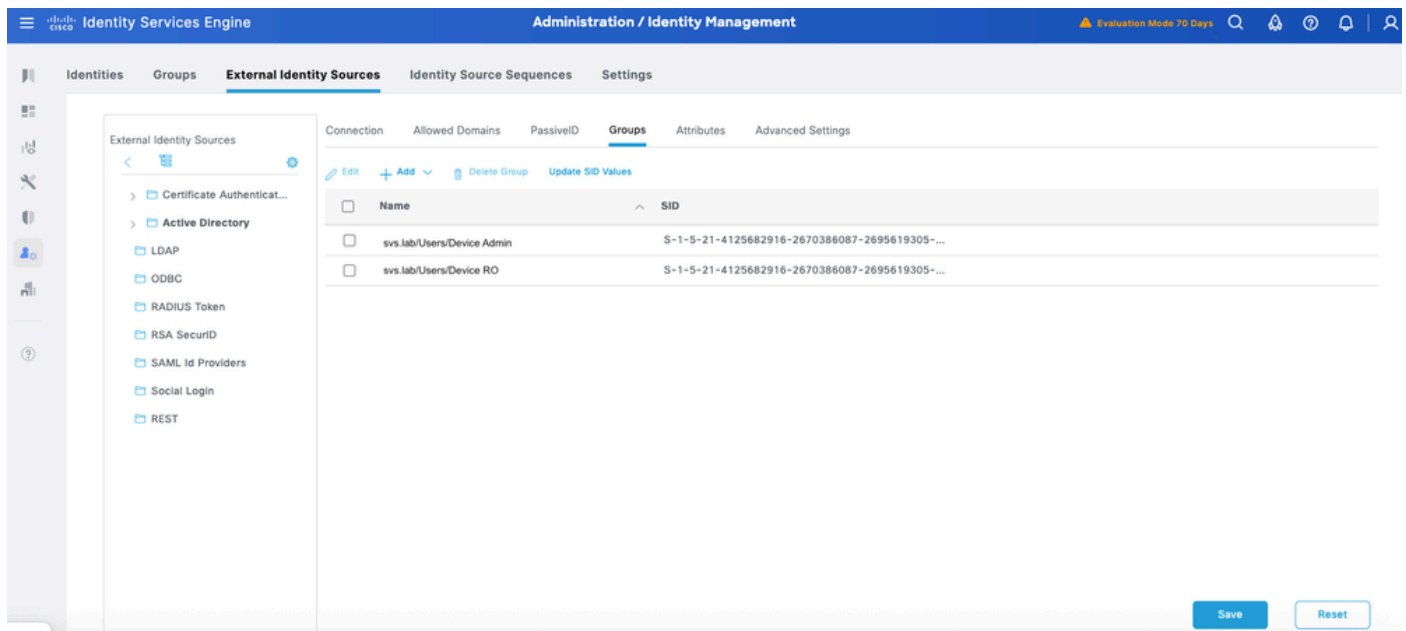
Filter

Filter

Retrieve Groups...

2 Groups Retrieved.

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



Konfigurieren von TACACS+-Profilen

Ordnen Sie die TACACS+-Profile den Benutzerrollen auf den Cisco IOS XR-Geräten zu. In diesem Beispiel sind diese definiert:

- 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.

Definieren von zwei TACACS+-Profilen: IOSXR_RW und IOSXR_RO.

IOS XR_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 IOSXR_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.

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

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

Conditions > Network Conditions > Results > Allowed Protocols > TACACS Command Sets > **TACACS Profiles**

TACACS Profiles > IOSXR_RW
TACACS Profile

Name: IOSXR_RW

Description:

Task Attribute View Raw View

Common Tasks

Common Task Type: Shell

☒ Default Privilege 15 (Select 0 to 15)

☒ Maximum Privilege 15 (Select 0 to 15)

☐ Access Control List

☐ Auto Command

☐ No Escape (Select true or false)

IOS XR_RO - 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 IOSXR_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.

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

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

Conditions > Network Conditions > Results > Allowed Protocols > TACACS Command Sets > **TACACS Profiles**

TACACS Profiles > New
TACACS Profile

Name: IOSXR_RO

Description:

Task Attribute View Raw View

Common Tasks

Common Task Type: Shell

☒ Default Privilege 1 (Select 0 to 15)

☒ Maximum Privilege 1 (Select 0 to 15)

Konfigurieren von TACACS+-Befehlssätzen

Definieren der TACACS+-Befehlssätze: In diesem Beispiel sind dies CISCO_IOSXR_RW und CISCO_IOSXR_RO.

CISCO IOS XR 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_IOSXR_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.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes the Cisco logo, 'Identity Services Engine', 'Work Centers / Device Administration', and a status indicator 'Evaluation Mode 63 Days'. The main navigation menu on the left includes Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements (selected), Device Admin Policy Sets, Reports, and Settings. The 'Policy Elements' section is expanded, showing 'TACACS Command Sets' and 'CISCO_IOSXR_RW'. The 'Command Set' configuration page is displayed, with the 'Name' field set to 'CISCO_IOSXR_RW'. The 'Description' field is empty. The 'Commands' section has a checkbox 'Permit any command that is not listed below' which is checked. Below this, there are buttons for 'Add', 'Trash', 'Edit', 'Move Up', and 'Move Down'. A table with columns 'Grant', 'Command', and 'Arguments' is shown, but it is empty with the message 'No data found.' at the bottom. At the bottom right, there are 'Cancel' and 'Save' buttons.

CISCO IOS XR 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 Command Set hinzu, und nennen Sie ihn CISCO_IOSXR_RO.

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

Schritt 3: Wählen Sie Zulassen aus der Dropdown-Liste für die Spalte Erteilen aus, und geben Sie show in die Spalte Befehl ein. und klicke auf den Pfeil zum Aktivieren.

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

The screenshot shows the 'Policy Elements' configuration page in the Cisco ISE 'Work Centers / Device Administration' section. The left sidebar contains navigation links: Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements (selected), Device Admin Policy Sets, Reports, and Settings. The main content area is titled 'TACACS Command Sets > CISCO_IOSXR_RO Command Set'. It includes fields for 'Name' (CISCO_IOSXR_RO) and 'Description'. Below these is a 'Commands' section with a checkbox for 'Permit any command that is not listed below'. At the bottom, there is a table with columns 'Grant', 'Command', and 'Arguments'. The table contains one entry: 'PERMIT' for the command 'show'. Action buttons 'Add', 'Trash', 'Edit', 'Move Up', and 'Move Down' are located above the table. At the bottom right, there are 'Cancel' and 'Save' buttons.

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 XR-Geräte. Geben Sie unter Bedingung `DEVICE:Device Type EQUALS All Device Types#IOS XR` an. Wählen Sie unter Zugelassene Protokolle die Option Standardgeräteadministrator aus.

The screenshot shows the 'Device Admin Policy Sets' configuration page in the Cisco ISE 'Work Centers / Device Administration' section. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Policy Sets'. It includes a 'Reset' button, a 'Reset Policy Set Hit Counts' button, and a 'Save' button. Below these is a table with columns: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, Hits, Actions, and View. The table contains one entry: 'IOS-XR devices' with a status of 'On'. The 'Conditions' column shows the condition 'DEVICE:Device Type EQUALS All Device Types#IOS-XR'. The 'Allowed Protocols / Server Sequence' column shows 'Default Device Admin'. The 'Hits' column shows '73'. The 'Actions' column has a gear icon for configuration. The 'View' column has a right-pointing arrow.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
On	IOS-XR devices		DEVICE:Device Type EQUALS All Device Types#IOS-XR	Default Device Admin	73		

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

Schritt 3: Erstellen Sie die 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.

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

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

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

Authentication Policy(1)

Status	Rule Name	Conditions	Use	Hits	Actions
	Default				

svs.iab

Options ⓘ

If Auth fail
REJECT

If User not found
REJECT

If Process fail
DROP

85

Schritt 4: Definieren der Autorisierungsrichtlinie

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

Beispiele:

- Benutzern in der AD-Gruppe Gerät RO wird 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.

Identity Services Engine

Work Centers / Device Administration

Evaluation Mode 62 Days

Overview

Identities

User Identity Groups

Ext Id Sources

Network Resources

Policy Elements

Device Admin Policy Sets

Reports

Settings

Policy Sets → IOS-XR devices

Reset

Reset Policy Set Hit Counts

Save

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

> Authentication Policy(1)

> Authorization Policy - Local Exceptions

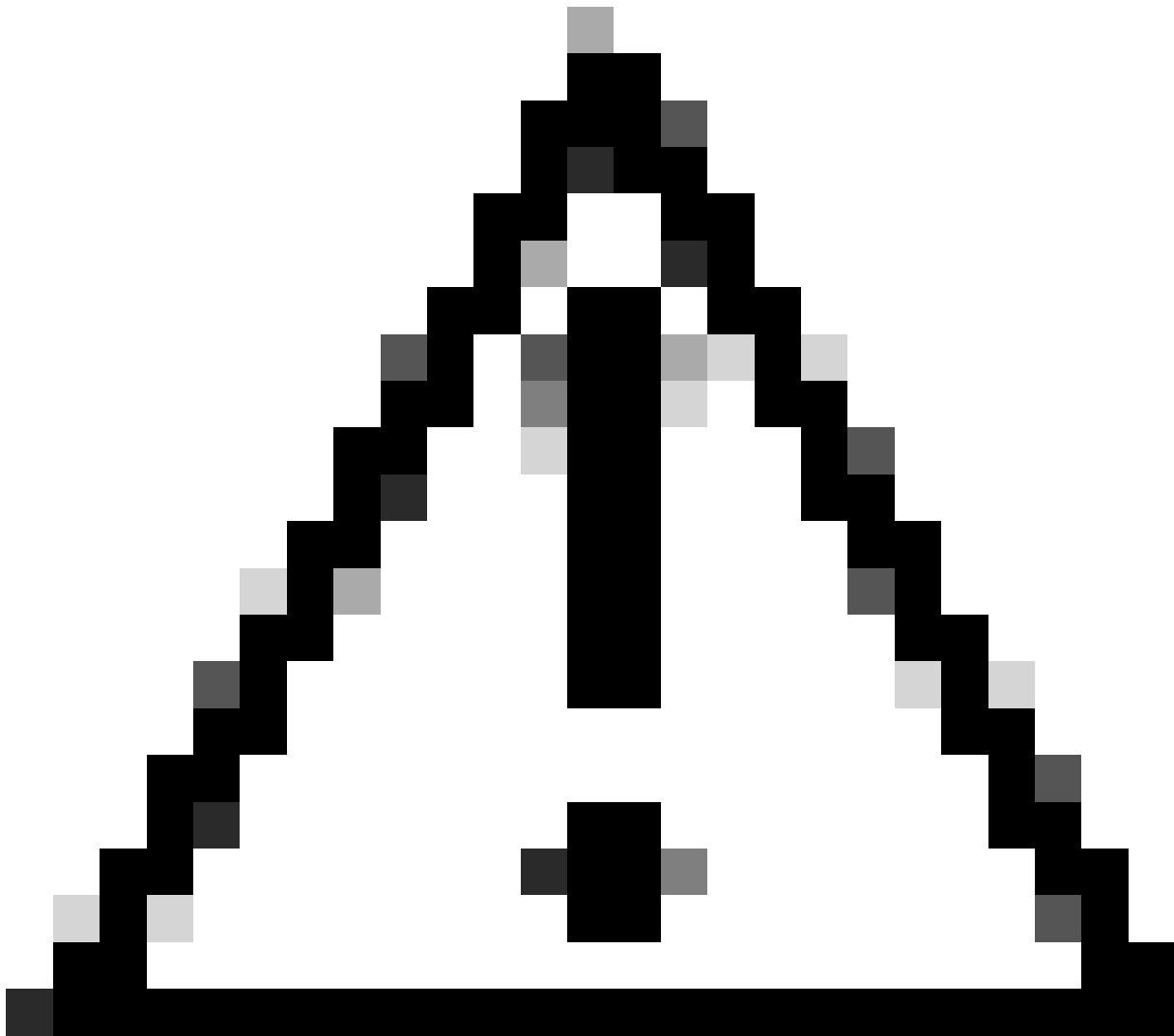
> Authorization Policy - Global Exceptions

> Authorization Policy(3)

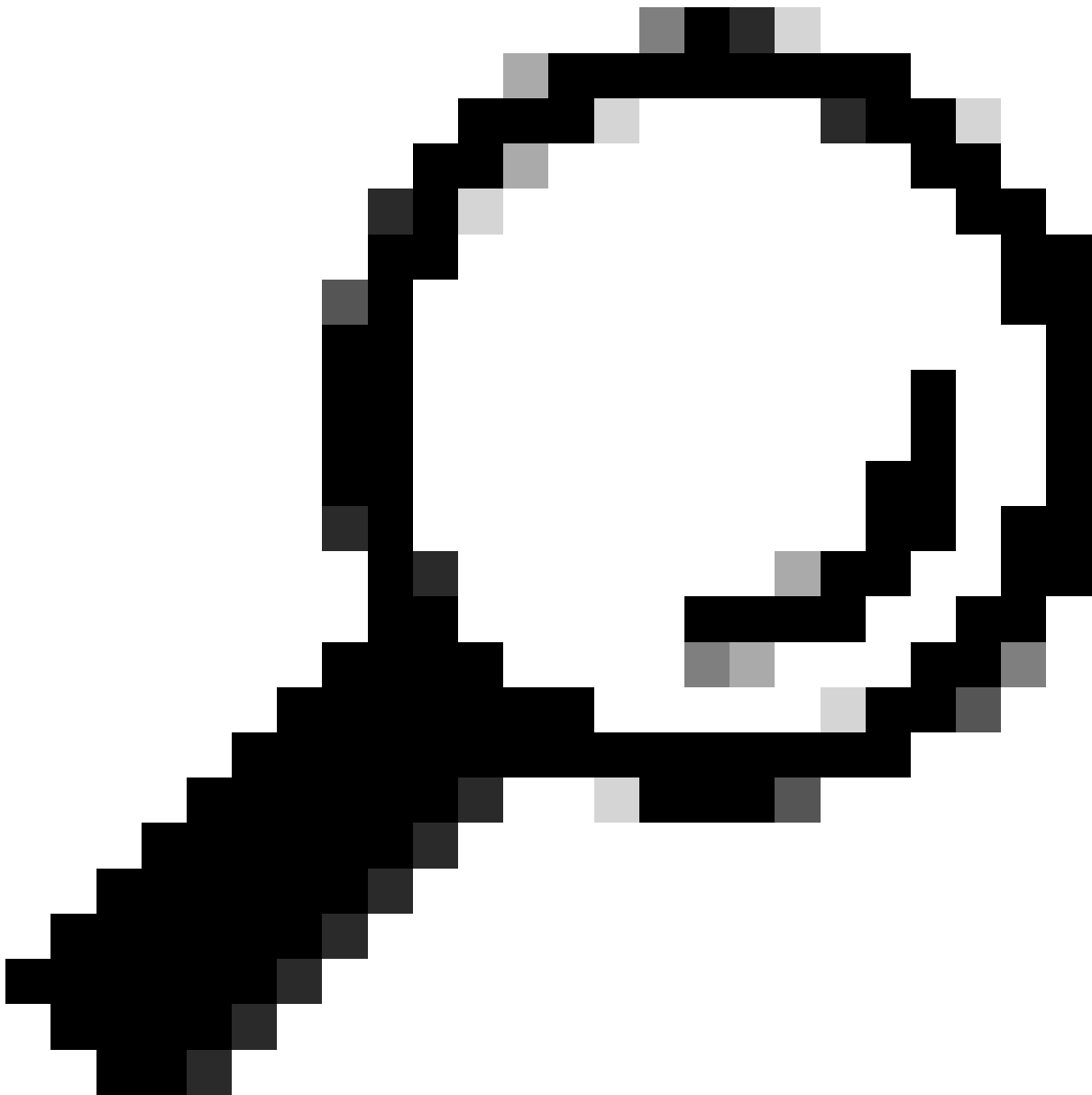
		Results							
	Status	Rule Name	Conditions	Command Sets		Shell Profiles		Hits	Actions
Search									
	✓	Authorization Rule RO	svs.lab - ExternalGroups EQUALS svs.lab /Users/Device RO	CISCO_IOSXR_RO		IOSXR_RO		0	
	✓	Authorization Rule RW	svs.lab - ExternalGroups EQUALS svs.lab /Users/Device Admin	CISCO_IOSXR_RW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

Teil 2: Konfigurieren von Cisco IOS XR 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.

Startkonfigurationen

Schritt 1: Stellen Sie sicher, dass der Namensserver (DNS) konfiguriert ist und der Router erfolgreich FQDNs (Frequently Qualified Domain Names) auflösen kann, insbesondere den FQDN des ISE-Servers.

```
domain vrf mgmt name svs.lab
domain vrf mgmt name-server 10.225.253.247
```

```
no domain vrf mgmt lookup disable
```

```
RP/0/RP0/CPU0:BRC-8201-1#ping vrf mgmt ise1.svs.lab
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.225.253.209 timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

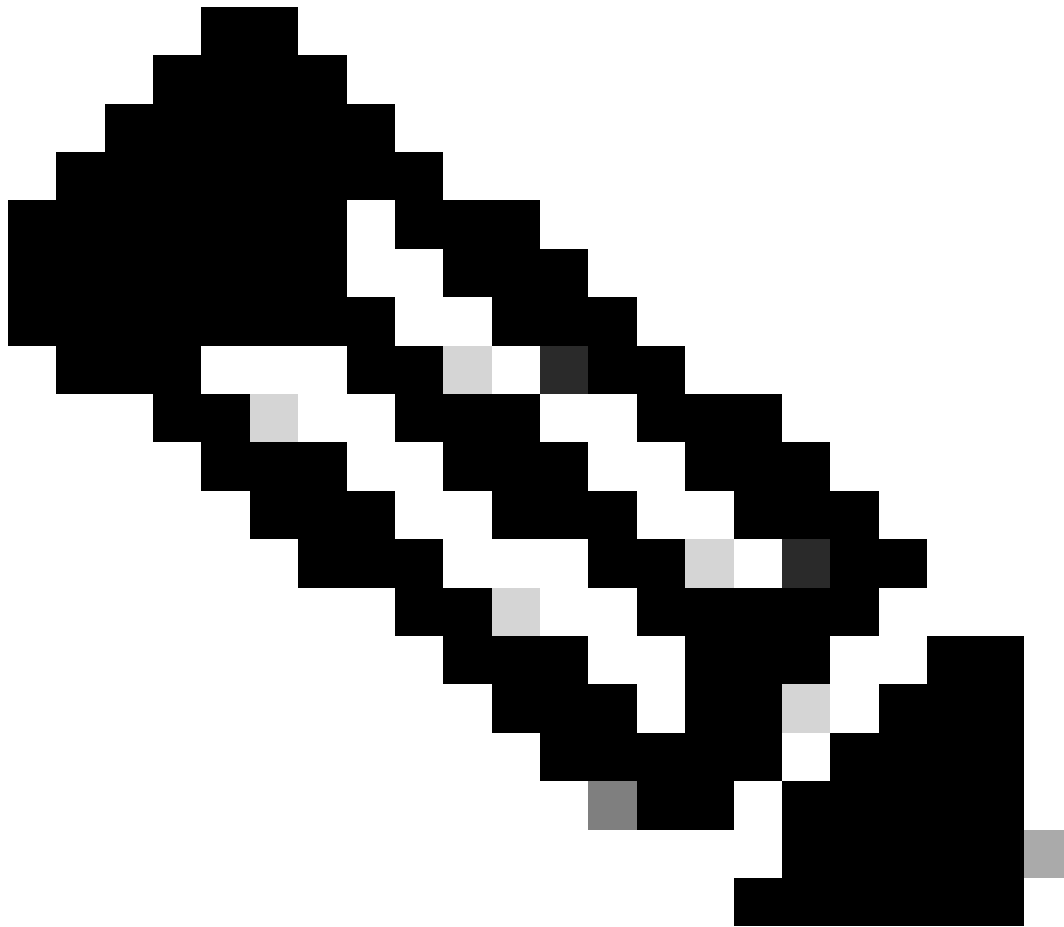
Schritt 2. Löschen Sie alle alten/nicht verwendeten Vertrauenspunkte und Zertifikate. Stellen Sie sicher, dass keine alten Vertrauenspunkte und Zertifikate vorhanden sind. Wenn Sie alte Einträge sehen, entfernen/löschen Sie diese.

```
show crypto ca trustpoint
```

```
show crypto ca certificates
```

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

```
# clear crypto ca certificates <tp-name>
```



Anmerkung: Sie können manuell eine neue RSA-Schlüsselpaarung erstellen und diese unter Vertrauenswürdigkeit anfügen. Wenn Sie keine erstellen, wird das Standard-Tastenpaar verwendet. Das Definieren von ECC-Keypair unter Trustpoint wird derzeit nicht unterstützt.

Vertrauenspunkt konfigurieren

Schritt 1: Konfiguration der Tastatur (optional).

<#root>

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

crypto key generate rsa

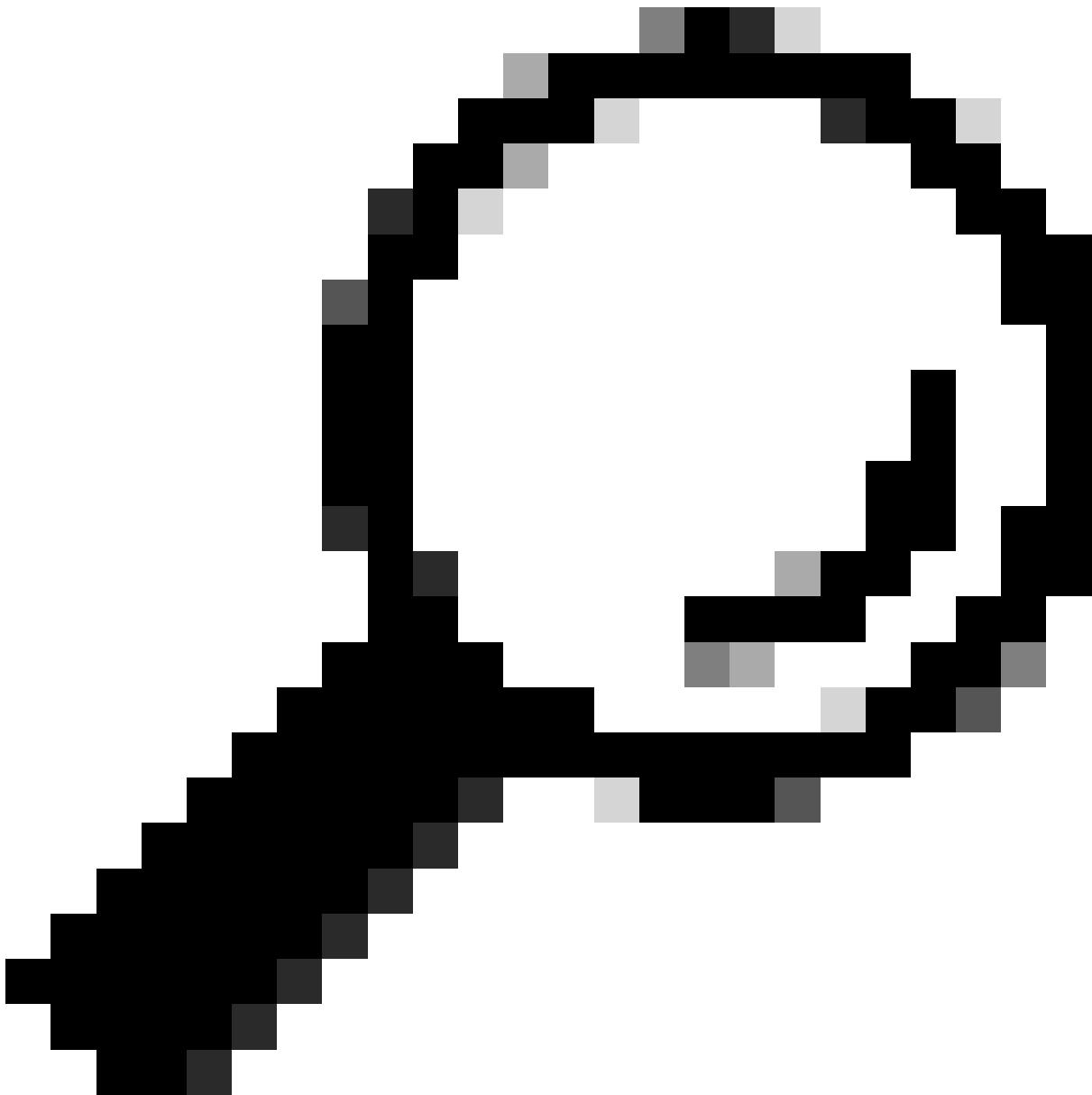
```
RP/0/RP0/CPU0:BRC-8201-1(config)#
```

```
crypto ca trustpoint
```

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

```
rsakeypair
```

Schritt 2: Erstellen eines Vertrauenspunkts.



Tipp: Die DNS-Konfiguration für den alternativen Antragstellernamen ist optional (sofern auf der ISE aktiviert), wird jedoch empfohlen.

```
<#root>
```

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

```
crypto ca trustpoint sv
```

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

```
vrf mgmt
```

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

```
crl optional
```



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

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

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

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

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

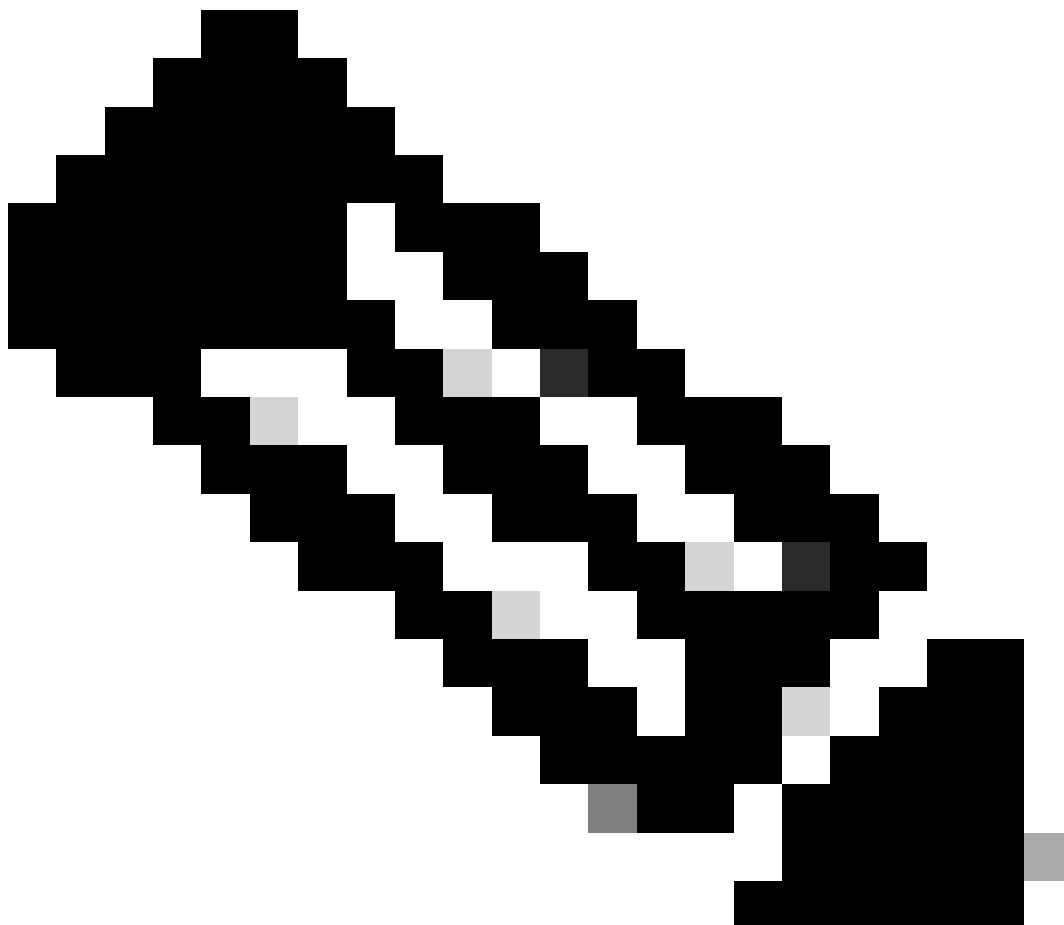
```
enrollment url terminal
```

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

```
rsakeypair svs-4096
```

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

```
commit
```



Anmerkung: Wenn Sie Komma in O oder OU verwenden müssen, können Sie vor dem Komma einen umgekehrten Schrägstrich (\) verwenden. Beispiele: O=Cisco Systems, Inc.

Schritt 3: Authentifizieren Sie den Vertrauenspunkt, indem Sie ein Zertifizierungsstellenzertifikat installieren.

```
<#root>
```

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

```
crypto ca authenticate svcs
```

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

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

```
MIIF1DCCA3ygAwIBAgIIIM10AsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZzFzAVBgNVBAGTDk5vbnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWx1aWdo
MQ4wDAYDVQQKEwVDAhXjBzEMMAoGA1UECjMDU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUGA1UECBMOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBACTB1JhbGVpZ2gxZDZAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTV1MxExAQBgNVBAMTCVNWUyBYWJDDQCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZU0yn2vIn6gKbx3M7vaRq
2YjwZlZSH6EkEvxnJTy+kksFD33GyHQepk7vfp4NFU50tQ4HC7t/A0v9grDa3QW
VwV4MBBjHFM3s0J/ejgDYcMZhIAaPy0Zo5WLboOkXEiKjPLatKXojB8FVrhLF30
jMBSqwa4/Wlniy5S+7s4FFxsCF20COWfBAsnrs0tatIIhmcnx+VLJP7MRm8f0w4m
mutNo7IhbJSrgAFxmjlBjMmgspObULo/wxMhdTbtPBf11HRHTkNI03qy04UADL2
WpoGhgT/FaxxBo2UBcnYVaP+jjRE0NYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7B0e8oDNKU6gXlojKyLP/gC7j8AeP03ir+KZui8
b8X4iYn/67SbzZFhwn3chkw4JYhQ4AImw1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
gJ+kQXe7QtT/u6m1MrtjE3gAEVpL334rTIxy9hpKZIKB86t2ZA3JX8CLsbCa13sA
z1XCoONX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTA01xh60I4QnK+MNQKpTjt/E4
ydH10rrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVL1783nTc9wYptQEPi5sw
83g9EMgKV0ARIiVUa/q1AgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAyb4
QgEBBAQDAgAHMBkGCWCGSAGG+EIBDQMMFgpTV1MgTGFiIENBMAOGCSqGSIb3DQEB
CwUAA4ICAQAIT308oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oK0dGayi
iSEkSSX9qyfLFINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXRX67X+v
O+ja6zTqQj06lqJhmrSkyFbYf/ZTpe4d10zJsZjNsN0r8bF9nOA/7qNZLp3Z3cpU
PU0KdbiSvRqnPw3e8TFITVmAzcX8COI2SrYFMSUazo1VBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIEOf5ay1PKURO/8aj/B7a1uJapXkmnj5qPeGhN0pB
Q9r14reov4so2EspkXS7CrH9yGfpIyTprokz1UvZBZ8v1oI7YZmjFmem+5rT6Gnk
eU/1X7nV61SYG5W5K+I8uaKuyBHOMn7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggz1P0dsS/i6Lo7ypYX0eB9HgVDCkzQsLXQuHGj/2WsgPgDRcjkvnyURk4Jx+Ib
xDrmo7e0XPPSW4172a6K18CR3U2Cr4wsuvndPEq/qd2NRSBWffFOXEX/AJHQG7STT
HaXLU9r2Ko603oeuc8ysGTwL1It/9T1/F0b0xZRugWcpJrVoTgDGUA==
```

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

```
quit
```

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

Subject:

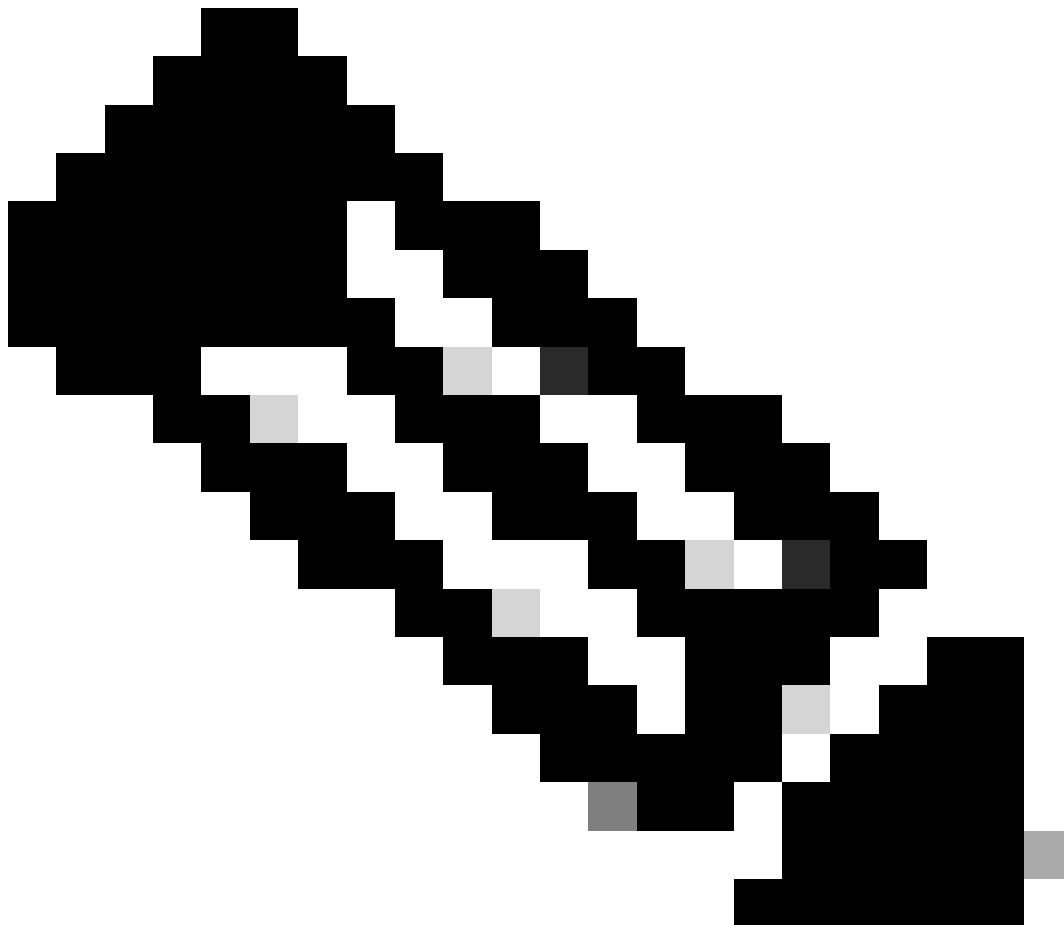
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US

Issued By :

```
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
Validity Start : 17:05:00 UTC Mon Apr 28 2025
Validity End : 17:05:00 UTC Sat Apr 28 2035
RP/0/RP0/CPU0:May 9 14:52:20.961 UTC: pki_cmd[66362]: %SECURITY-PKI-6-LOG_INFO_DETAIL : Fingerprint: 2A
SHA1 Fingerprint:
0EB181E95A3ED7803BC5A8059A854A95C83AC737
Do you accept this certificate? [yes/no]:
```

yes

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



Anmerkung: Wenn Sie über ein untergeordnetes Zertifizierungsstellensystem verfügen, müssen Sie sowohl Stammzertifizierungsstellen- als auch untergeordnete Zertifizierungsstellenzertifikate importieren. Verwenden Sie denselben Befehl mit Sub-CA oben und Root-CA unten.

Schritt 4: Erstellen einer Zertifikatsanforderung (Certificate Signing Request, CSR).

<#root>

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

crypto ca enroll svcs

Fri May 9 14:52:44.030 UTC

% Start certificate enrollment ...

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

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

% Please make a note of it.

Password:

Re-enter Password:

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

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

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

yes

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

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

yes

Enter IP Address[]

10.225.253.167

Fingerprint: 36354532 38324335 43434136 42333545

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

yes

Certificate Request follows:

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

MIIDQTCCAikCAQAwcjELMAkGA1UEBhMCVVMxCzAJBgNVBAGMAK5DMQwwCgYDVQQH
DANSVFAXDjAMBGNVBAoMBUNpc2NvMQwwCgYDVQQLDANTVlMxZzAVBgNVBAMMDjEw
LjIyNS4yNTMuMTY3MREwDwYDVQQFEwg0MDkwODQzYjCCASIwdQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBALwx9w4DnTtrloDH9iOZxPvEDARwN0t4WrPEjaQc1ZUA
6ax6Cxq/0JlQiUf2+eQv+4rKZqAZ1xDhiaIMGqETn00LKpwmtx10IqXL7UYMHwF
9vRII52zomkWA8a63Wx66UkExaXoeXaf5HkLoqDu68X83U7LPvMe1sMwvmq7Rmy2
DAu30HB/Jfy1QCHmTVFz3M5fBt86xx4t1nxTFU/41RWMC73UdL5YdKJLjMpBT2tN
E3piZ+kL4p1c9U4RIBkU8/G4drzFbGvHCikWkWI0cb1X2HgtbVQdCXTAwJDmr2O9
zd2ZCa5enTbOKHbNXuHjpy0k8MewKOV2muwxVcQbej8CAwEAACBiTAYBgkqhkiG
9w0BCCQcxCMJQzFzY28uMTIzMG0GCSqGSIb3DQEJJDjFgMF4wDgYDVR0PAQH/BAQD
AgWgMCAGA1UdJQEB/wQWMBQGCSsGAQUFBwMBBggrBgEFBQcDAjAJBgNVHRMEAjAA
MB8GA1UdEQQYMBaCDjEwLjIyNS4yNTMuMTY3hwQK4f2nMAOGCSqGSIb3DQEBBQUA
A4IBAQBbX0eWF5ZUz701GFjuQHBBdgYb+3lhFOxbYm9psIWfv1uwjkKoL297tGHv
Iux7nMyrDVkSJ81i5BSTdd9FE6AbSFswj1Yp0+IxkUM971Ejwg2rj+jABDR7I8SU
06Y06mS9x2ZJYqImeq8xwIr19Hi+7tyaLe6apFTI1jdgVxB+Xyz0FJMckI05US3j

```
T/3aw/115RcXerdrh36oMUHEepUjIx/15u9s1c7e1mxACoQE6f90A+fdg2zYtOME
Z6VAw64cY+YF6iLbYv7c4l1z05Zj2NJbUKpeqijkFAkY/1rIxTHypzH/p2ma4zuS
46a+kLXsVHZ716ZMB3WrUzB2ZN00
-----END CERTIFICATE REQUEST-----
---End - This line not part of the certificate request---
Redisplay enrollment request? [yes/no]:

no
```

Schritt 5: CA-signiertes Zertifikat importieren.

<#root>

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

crypto ca import svcs certificate

Fri May 9 15:00:35.426 UTC

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

```
-----BEGIN CERTIFICATE-----
MIIE3zCCAsegAwIBAgIINL1NAUzx14UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZmZAVBgNVBAGTDk5vcnRoIENhcm9saW5hMRAdBgYDVQQHEwdSYWx1aWdo
MQ4wDAYDVQQKEwVDAxNjBzEMMAoGA1UECXMdU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNTA5MTQ1NzAwWWhcNMjUwNTA5MTQ1NzAwWjByMQswCQYDVQQGEwJV
UzELMAkGA1UECAwCTMxMDDAKBgNVBACMA1JUUEDEOMAwGA1UECgwFQ2l2Y28xDDAK
BgNVBAsMA1NWUzEXMBUGA1UEAwwOMTAuMjUwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
OTA4NDNiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvDH3Dg0d02uW
gMf2I5nE+8QMBHA3S3has8SNpByV1QDprHoLGr/QmVCJR/b55C/7ispmoBnXE0GJ
qIwaoR0c7QsqnCa3HXQipcvtrGwcfAX29EgjnboiARyDxrdbHrpSQTfpeh5dp/k
eQuio07rxzfzdtss+8x7WwzC+artGbLYMC7fQch879iVAIeZNUXPcz18G3zrHHI3W
fFMVT/iVFYwLvdR0v1h0okuMykFPA00TemJn6QvinVz1ThEgGRTz8bh2vMVsa8cI
iRaTAjRxvVfYeC1tVB0JdMDAK0avY73N3Zkjr16dNs4ods1e4eOnLSTwx7Ao5Xaa
7DFVxBt6PwIDAQABo4GAMH4wHgYJYIZIAyb4QgENBBEWD3hjYSBjZXJ0aWZpY2F0
ZTA0BgNVHQ8BAf8EBAMCBAAwIAYDVR01AQH/BBywFAYIKwYBBQUHAWEGCCsGAQUF
BwMCMakGA1UdEwQCMAAwHwYDVR0RBBgwFoIOMTAuMjUwDQYJKoZIhvcNAQELBQADggIBAARpS5bEck+oj012106WxedDQ8Vdu0bBtrn0H+Nt
94EA1co7HEe4USf1FiASAX7rNveLpY3ICmLh+tQZYTZRQ93tb9mMTZg7exqN89ZU
V1XoB2U0Tri5K10/+izEGgyNq42/yTAP8Y007HR/2jf7gfhovwvR5QNOEHv4o61
Zma5Xio1sBbkA7JB2mpzzZg4ZjsyV81RGXxxgyt1mwNmb7EiAc81odRcgyp7FNh3
F/k9cMMMr51M4Ysvo1tx1k9AeLjzb2syv5/fG6Qu0ZdWwTaaQh0Y2h/cVDiV97wg
0D1mEfdsV6QrxQSujZr22RzVyKKH1tuiV2B74pthUuGRBtFHS5XFy7uTTbfGX8M6
ZJw8rX1SADr8tDp1rf1ZIrPmv3ZPP7woTB22yWzyd0use+5Ia1b0w70twN4t/IiW
8CJu6HfnDXLDLPZ0jsC8steffrS1opwGccp3j6aZKPFz+I/Purb44a9WxEwa2TA7H
+r1oynBcGmet0HxVlnptlsC7Q4mN/MDXeGyW+OTNCirNEG/gqcu+dn9EnNkKE2WV
oF5370w+uNHok8Bdt8mqadUT40oUsqY8ArV0Bom05tzbemreVPmQAZ/IahZ7TqKo
3dGNontAFTTESM1iujQ81iRKsikdHysnwcCM2ni1CKZrhVq5IB8NK6jKRJZ0eQAX
vMt1
-----END CERTIFICATE-----
```

quit

Serial Number : C2:F4:AB:34:02:D2:76:74:65:34:FE:D5
Subject:

```
serialNumber=4090843b,CN=10.225.253.167,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
Issued By :
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
Validity Start : 14:57:00 UTC Fri May 09 2025
Validity End : 14:57:00 UTC Sat May 09 2026
SHA1 Fingerprint:
21E4DA0B02181D08B6E51F0CC754BCE5B815C792
```

Überprüfen Sie, ob das Router-Identitätszertifikat registriert ist.

<#root>

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

show crypto ca trustpoint svs detail

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

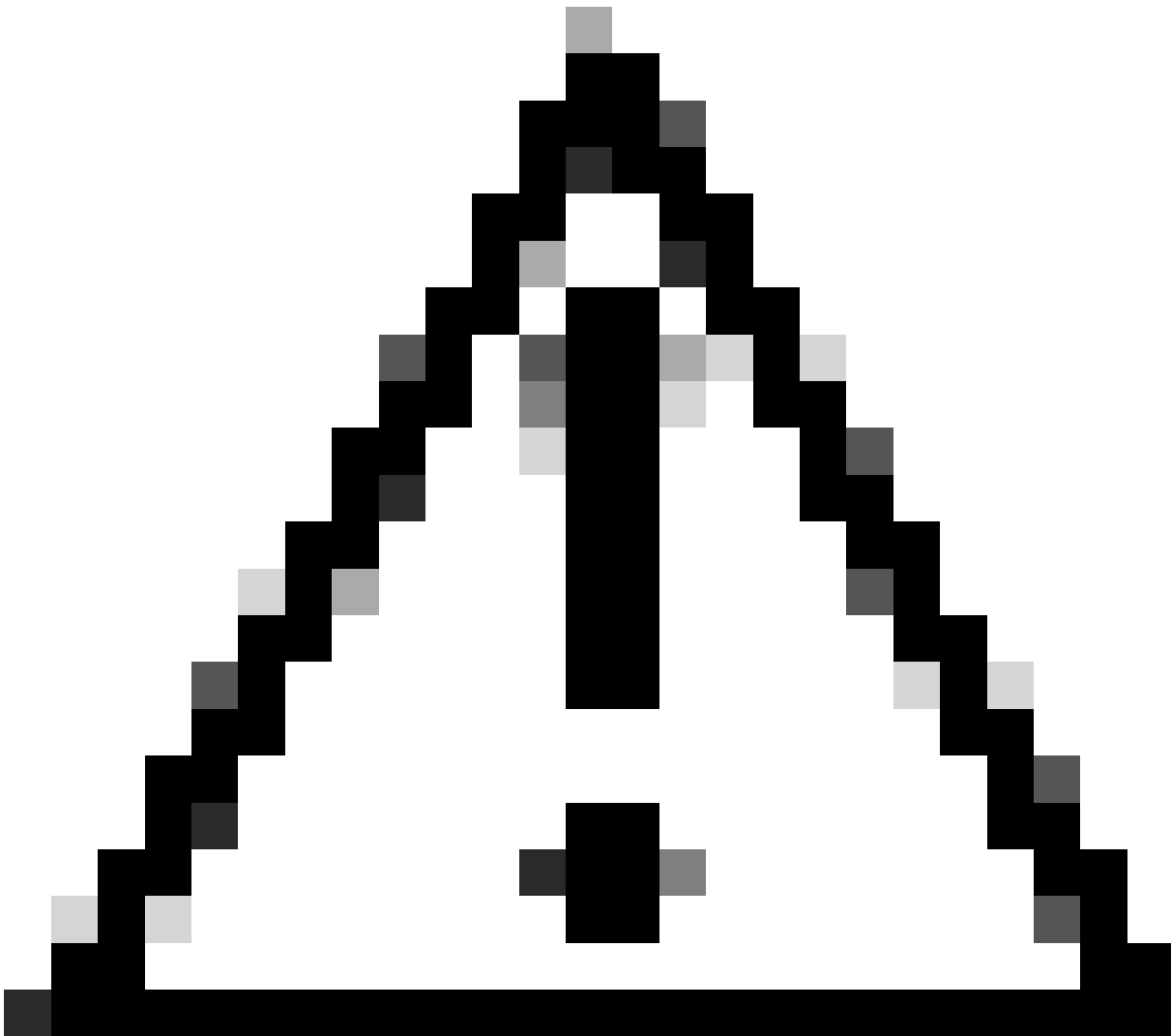
RP/0/RP0/CPU0:BRC-8201-1#

show crypto ca certificates svs

Wed May 14 14:55:58.173 UTC

```
Trustpoint          : svs-new
=====
CA certificate
  Serial Number   : 20:01:20:1F:B6:9D:C3:FE:43:78:FF:64
  Subject:
    CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
  Issued By      :
    CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
  Validity Start : 17:05:00 UTC Mon Apr 28 2025
  Validity End   : 17:05:00 UTC Sat Apr 28 2035
  SHA1 Fingerprint:
    0EB181E95A3ED7803BC5A8059A854A95C83AC737
Router certificate
  Key usage       : General Purpose
  Status          : Available
  Serial Number   : FD:AC:20:1F:B6:9D:C3:FE:98:43:ED
  Subject:
    serialNumber=4090843b,CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
  Issued By      :
    CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
  Validity Start : 19:59:00 UTC Fri May 09 2025
  Validity End   : 19:59:00 UTC Sat May 09 2026
  SHA1 Fingerprint:
    AC17E4772D909470F753BDBFA463F2DF522CC2A6
Associated Trustpoint: svs
```

Konfigurieren von TACACS und AAA mit TLS



Vorsicht: Führen Sie die Konfigurationsänderungen über die Konsole mit lokalen Anmeldeinformationen aus.

Schritt 1: Konfigurieren des TACACS+-Servers.

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

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

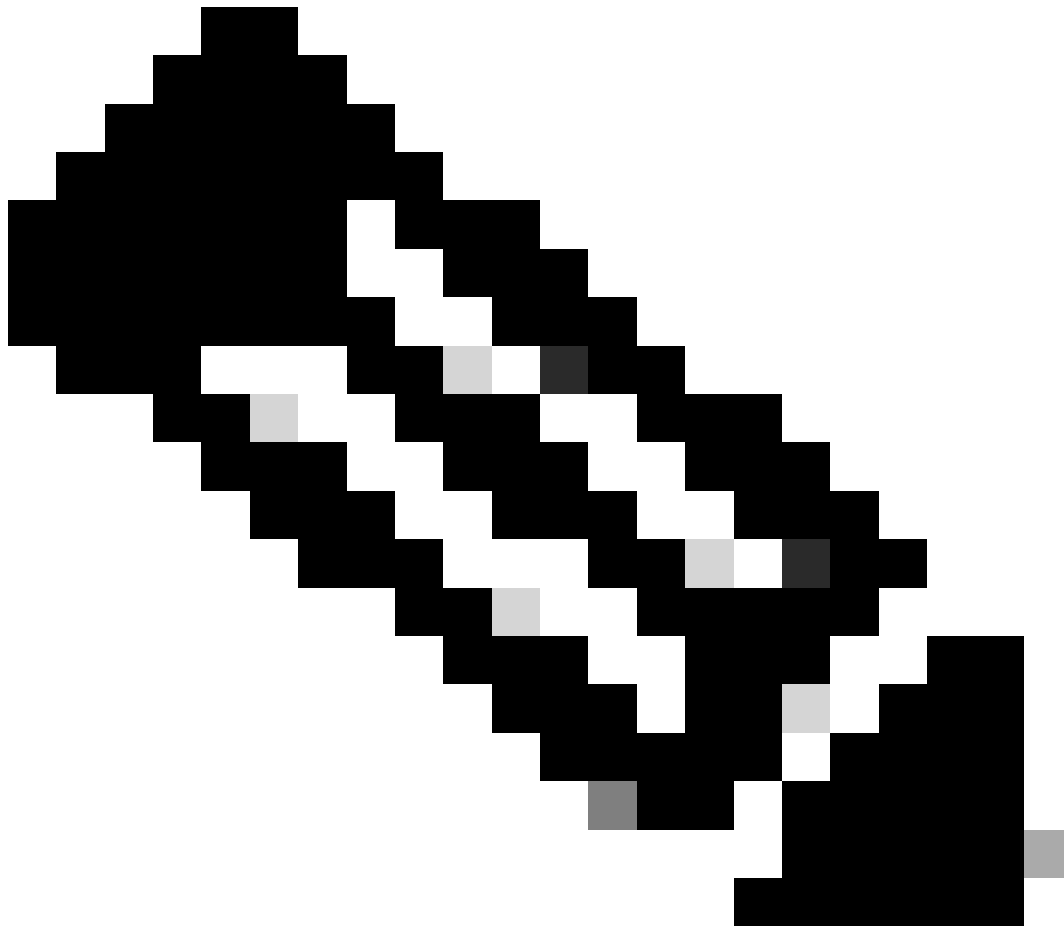
Schritt 2: Konfigurieren der AAA-Gruppe.

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

Schritt 2: Konfigurieren von AAA.

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

Erneuerung des Zertifikats



Anmerkung: Der Vertrauenspunkt muss während der Verlängerung nicht aus der TACACS+-Konfiguration entfernt werden.

Schritt 1: Überprüfen der aktuellen Gültigkeitsdaten des Zertifikats

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

```
Trustpoint : svcs-new
```

```
=====
```

```
CA certificate
```

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

```
Subject:
```

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

```
Issued By :
```

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

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

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

CRL Distribution Point

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

SHA1 Fingerprint:

EA8FB276563B927FCAF0174D9FD1C58F3E8B5FF2

Trusted Certificate Chain

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

Subject:

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

Issued By :

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

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

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

SHA1 Fingerprint:

E225647FF9BDA176D2998D5A3A9770270F37D2A7

Router certificate

Key usage : General Purpose

Status : Available

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

Subject:

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

Issued By :

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

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

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

CRL Distribution Point

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

SHA1 Fingerprint:

B562F3CF507CE7F97893F28BC896794CFF6995C1

Associated Trustpoint: svb-new

Schritt 2: Löschen eines vorhandenen Vertrauenspunktzertifikats

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

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

```
certificates cleared for trustpoint KF_TP
```

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

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

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

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

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

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

Schritt 3: Authentifizieren Sie den Vertrauenspunkt erneut, und registrieren Sie ihn, wie in den Schritten unter "Vertrauenspunktconfiguration" beschrieben.

Schritt 4: Überprüfen, ob die Gültigkeitsdaten des Zertifikats aktualisiert wurden

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

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

Trustpoint : KF_TP

=====

CA certificate

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

Subject:

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

Issued By :

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

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

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

CRL Distribution Point

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

SHA1 Fingerprint:

EA8FB276563B927FCAF0174D9FD1C58F3E8B5FF2

Trusted Certificate Chain

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

Subject:

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

Issued By :

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

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

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

SHA1 Fingerprint:

E225647FF9BDA176D2998D5A3A9770270F37D2A7

Router certificate

Key usage : General Purpose

Status : Available

Serial Number : 1F:B0:AE:44:CF:8E:24:62:83:42:2F:34:BF:D0:82:07:DF:E4:49:0B

Subject:

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

Issued By :

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

Validity Start : 15:17:29 UTC Thu Aug 14 2025

Validity End : 15:17:28 UTC Fri Aug 14 2026

CRL Distribution Point

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

SHA1 Fingerprint:

D3CE0AEB51C5E8009F626A1A9FD633FB9AFA96DE

Associated Trustpoint: KF_TP

Verifizierung

Überprüfen der Konfiguration.

```
show crypto ca certificates [detail]
```

```
show crypto ca trustpoint detail
```

```
show tacacs details
```

Debuggen für TACACS+

```
debug tacacs tls
```

TLS debuggen

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

Testen Sie den Remote-Benutzer, bevor Sie die AAA-Authentifizierung konfigurieren.

```
<#root>
```

```
test aaa group tacacs2
```

```
user has been authenticated
```

Fehlerbehebung

Löschen der Zertifikate (löscht alle Zertifikate, die einem Vertrauenspunkt zugeordnet sind).

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

Neustart des TACACS-Prozesses (falls erforderlich)

```
process restart tacacsd
```

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.