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

Inhalt

Einleitung

In diesem Dokument wird ein Beispiel für TACACS+ über TLS mit Cisco Identity Services Engine (ISE) als Server und einem Cisco NX-OS-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 NX-OS-basierte Netzwerkgeräte verwalten kann.
- Teil 1: Konfigurieren der ISE für den Geräteadministrator
- Teil 2: Konfigurieren von Cisco NX-OS 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 basieren auf den folgenden Software- und Hardwareversionen:

- ISE VMware Virtual Appliance, Version 3.4 Patch 2.
- Nexus 9000 Switch-Modell C9364D-GX2A, Cisco NX-OS Version 10.5(3t).

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.

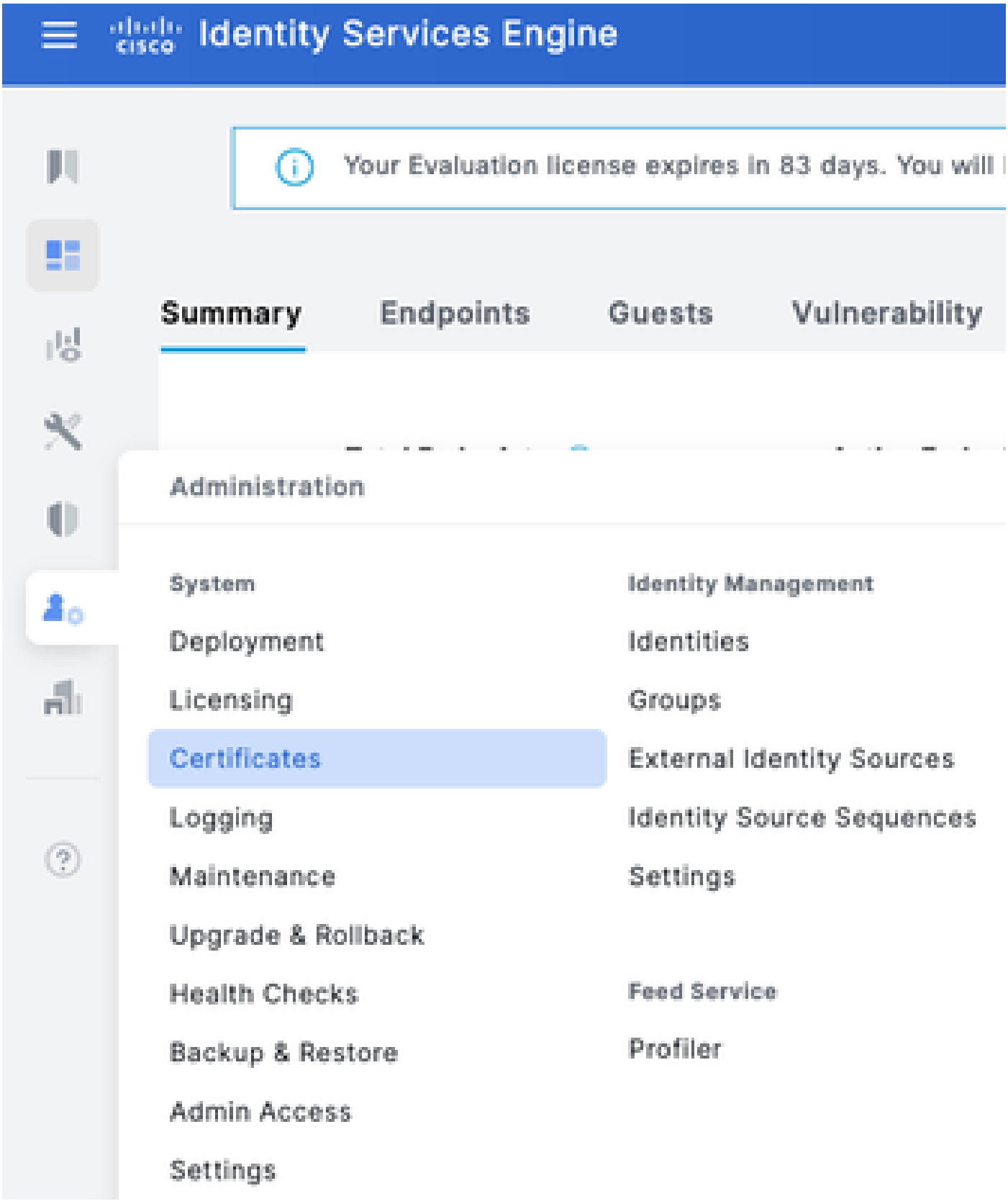
Konfigurieren der ISE für den Geräteadministrator

Zertifikatsignierungsanforderung für TACACS+-Serverauthentifizierung generieren

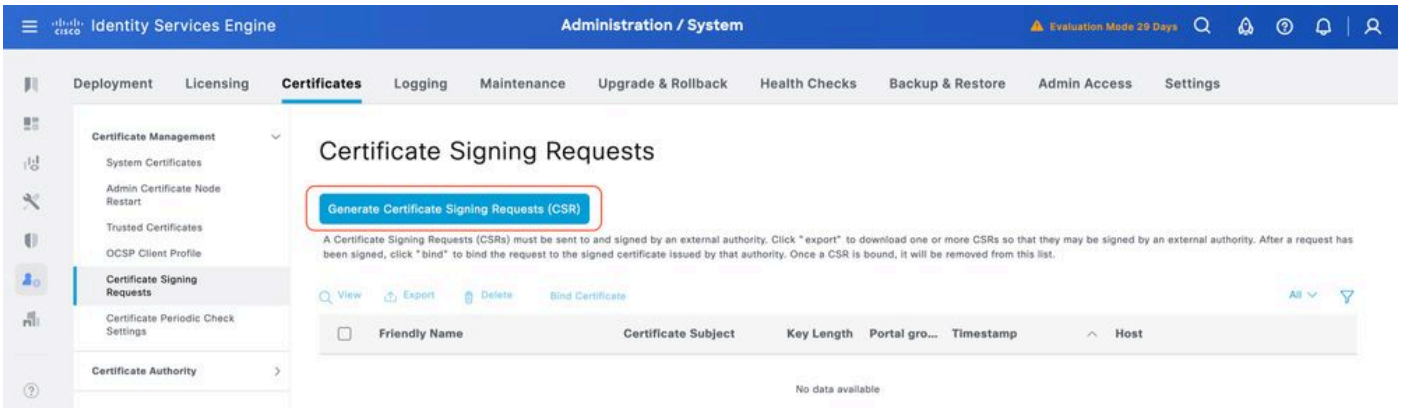
Schritt 1: Melden Sie sich mit einem der unterstützten Browser beim ISE-Admin-Webportal an.

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.

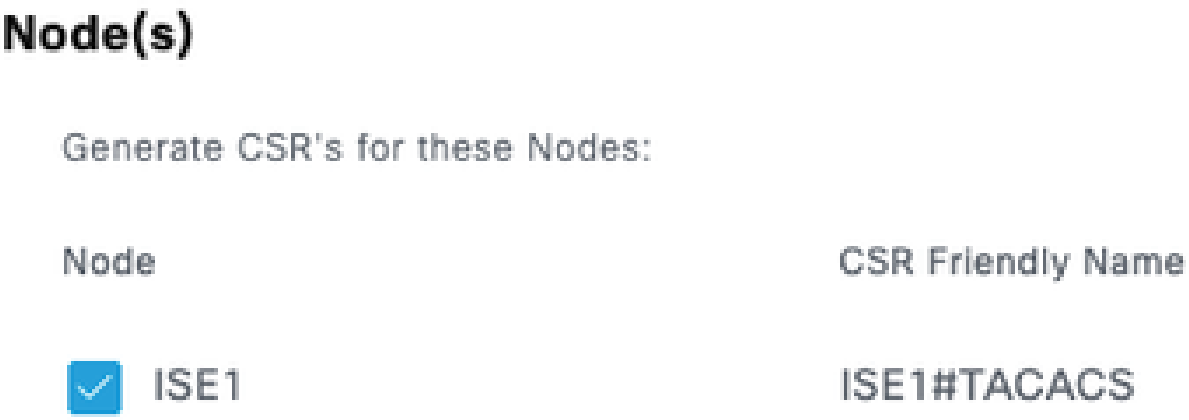


Schritt 3: Klicken Sie unter Zertifikatsignierungsanforderungen auf Zertifikatsignierungsanforderung generieren.

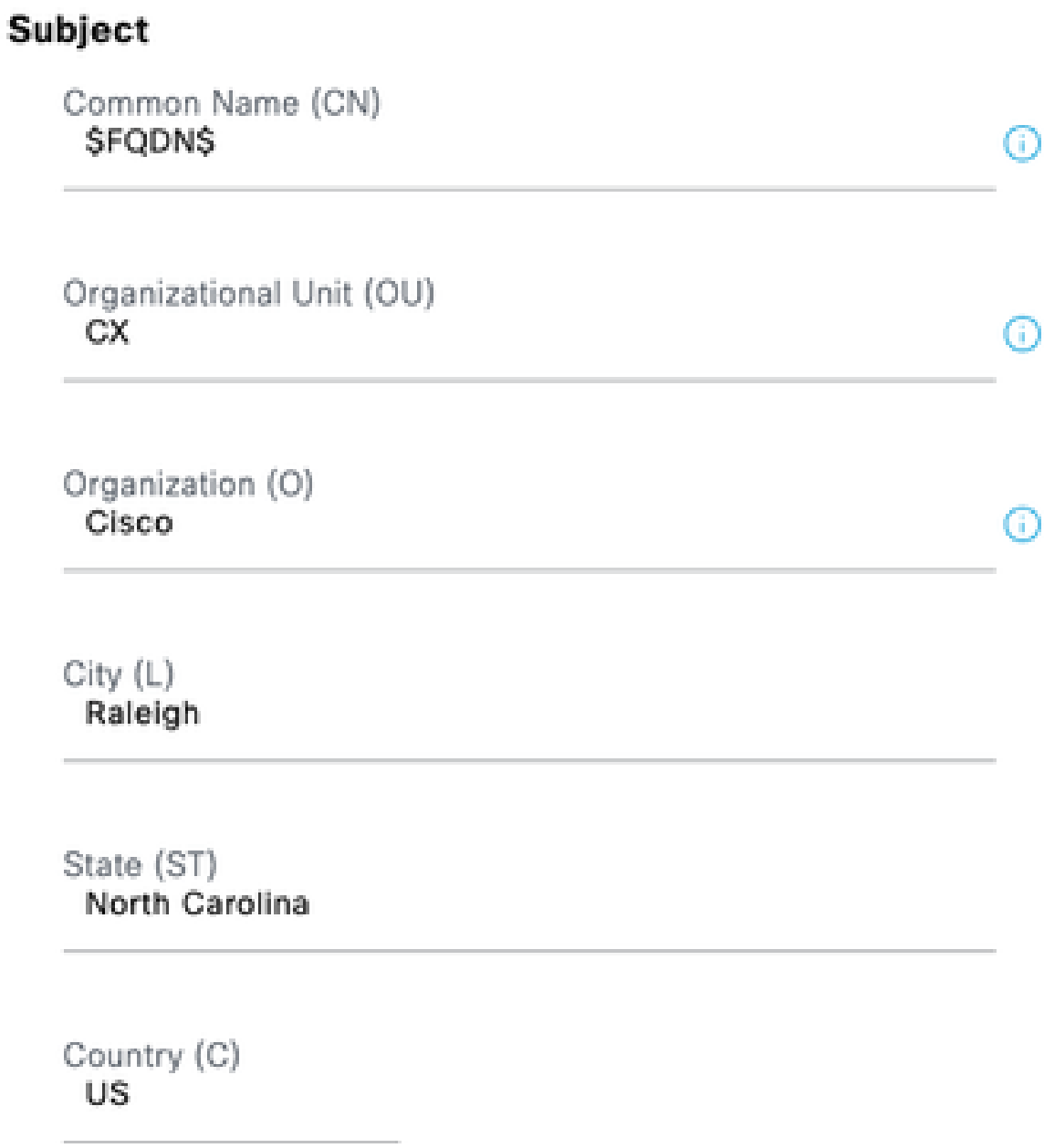


Schritt 4: Wählen Sie TACACS in Usage aus.

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



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



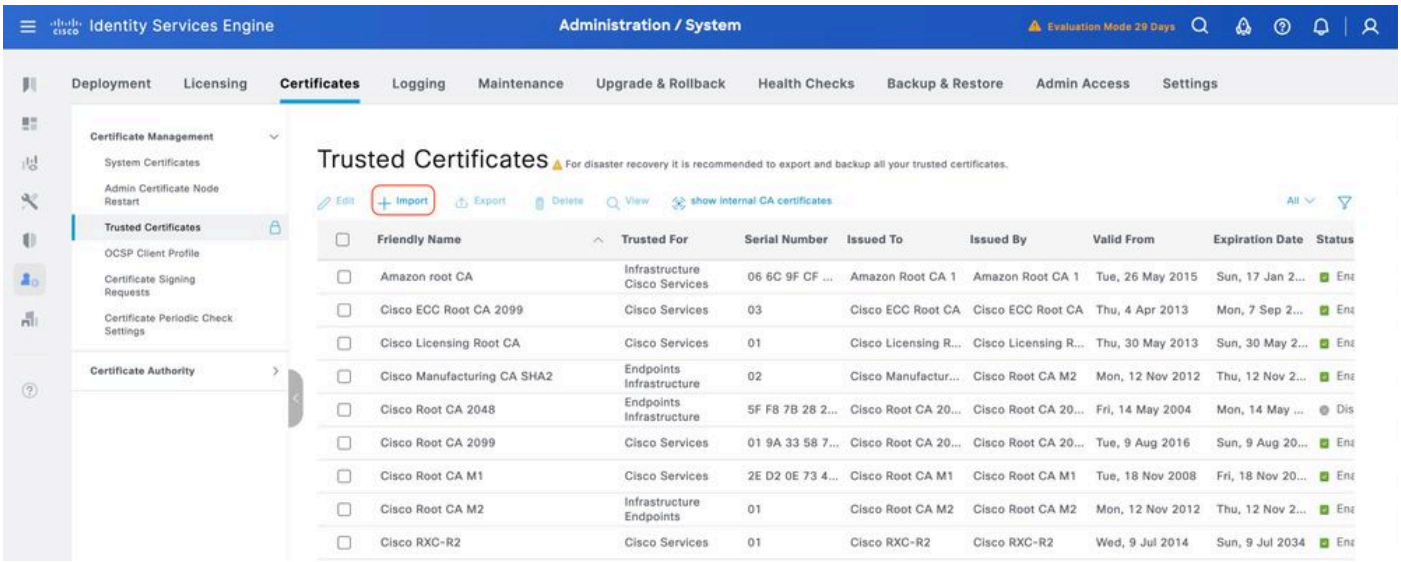
Schritt 7: Fügen Sie den DNS-Namen und die IP-Adresse unter Alternativer Antragstellername (SAN) hinzu.

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

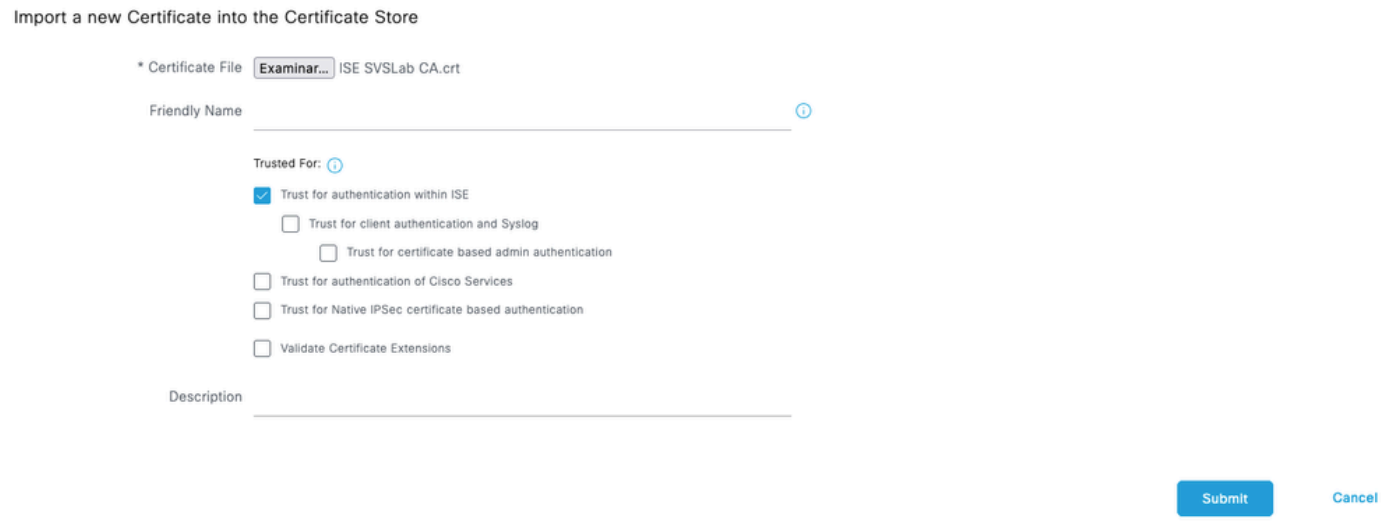
Jetzt können Sie das Zertifikat (CRT) von Ihrer Zertifizierungsstelle (Certificate Authority, CA) signieren lassen.

Hochladen des Zertifikats der Stammzertifizierungsstelle für die TACACS+-Serverauthentifizierung

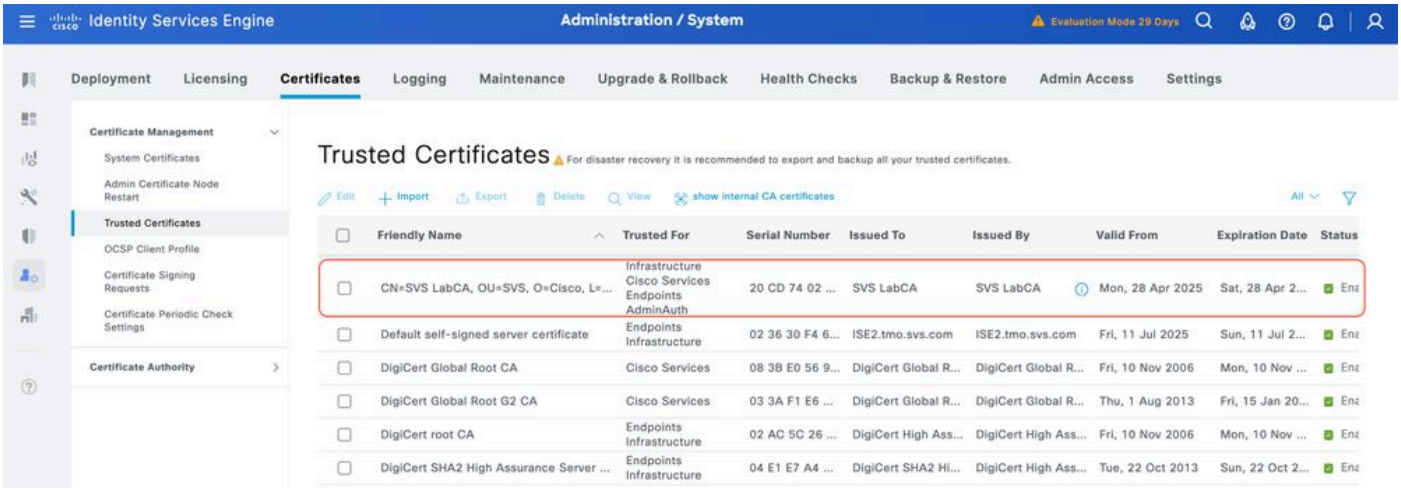
Schritt 1: Navigieren Sie zu Administration > System > Certificates. Klicken Sie unter Vertrauenswürdige Zertifikate auf Importieren.



Schritt 2. Wählen Sie das Zertifikat aus, das von der Zertifizierungsstelle ausgestellt wurde, die die TACACS-Zertifikatsignierungsanforderung (CSR) signiert hat. Stellen Sie sicher, dass die Option Für Authentifizierung in ISE vertrauen aktiviert ist.



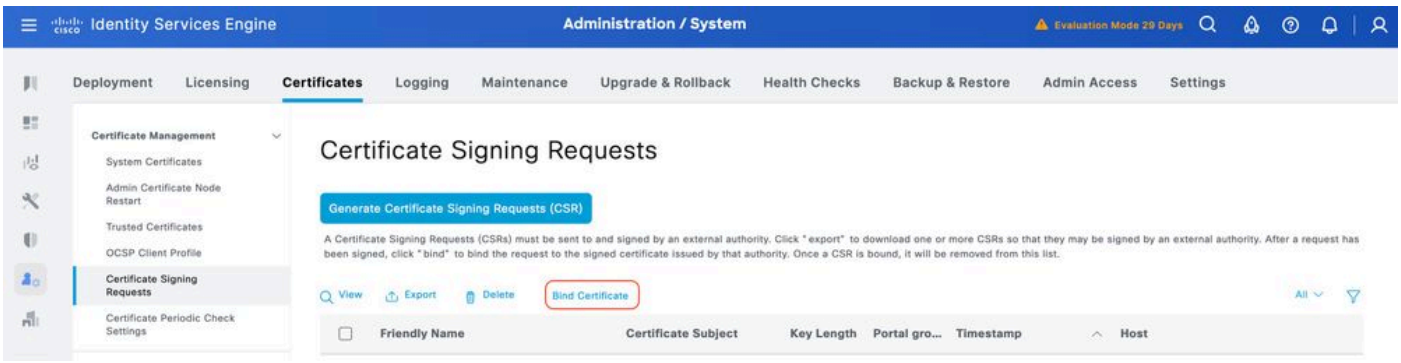
Klicken Sie auf Senden. Das Zertifikat muss jetzt unter Vertrauenswürdige Zertifikate angezeigt werden.



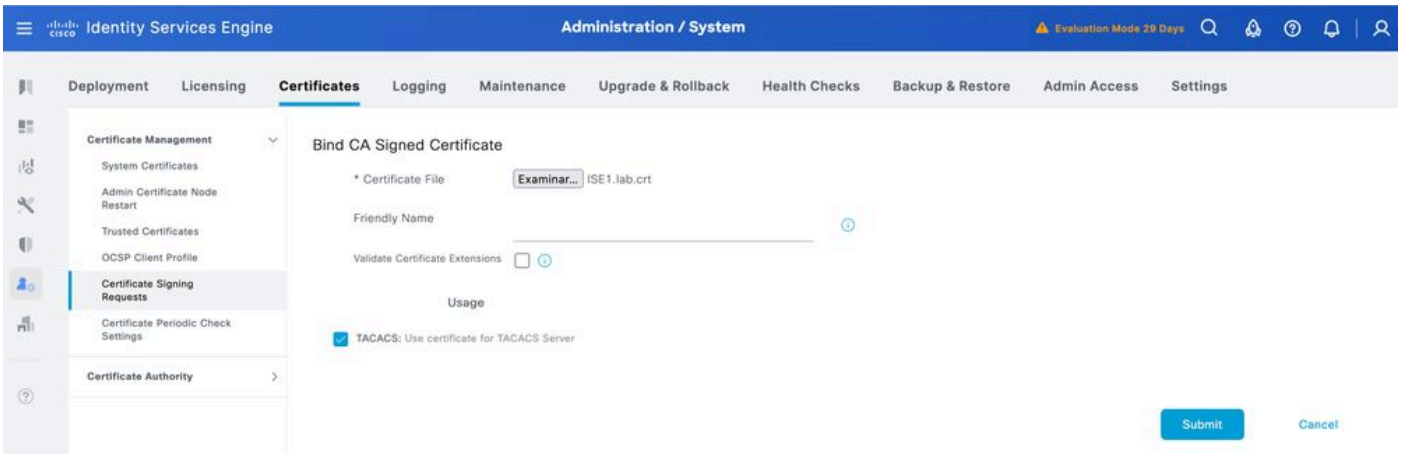
Signierte Zertifikatsanforderung (CSR) an ISE binden

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

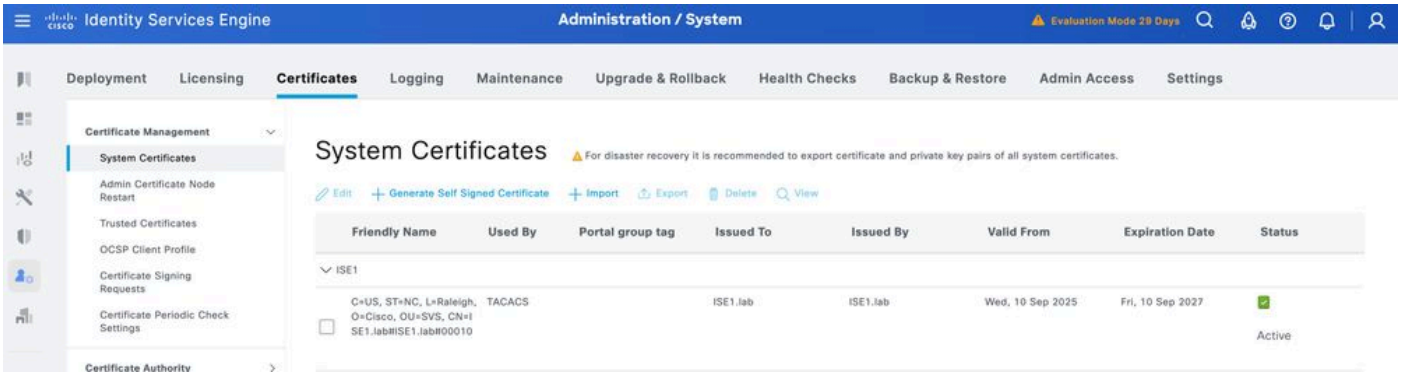


Schritt 2: Wählen Sie das signierte Zertifikat aus, und stellen Sie sicher, dass das Kontrollkästchen TACACS unter Verwendung aktiviert bleibt.



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

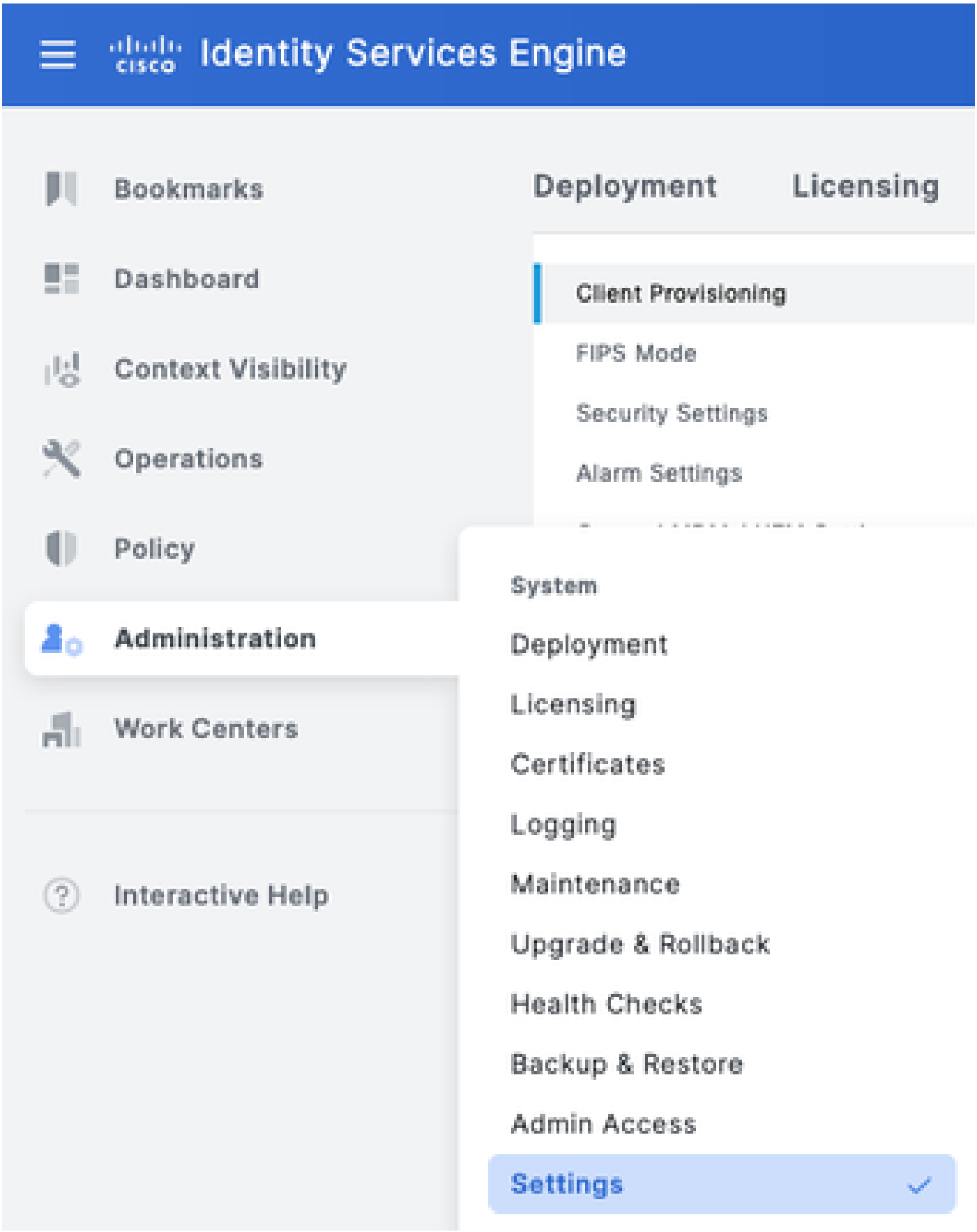
Das Zertifikat muss nun korrekt installiert sein. Sie können dies unter Systemzertifikate überprüfen.



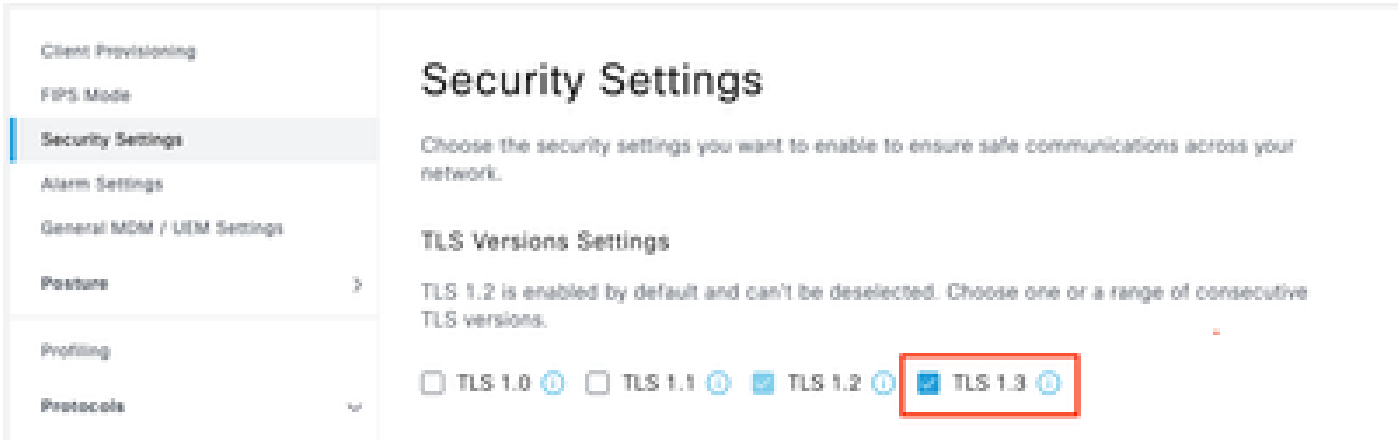
TLS 1.3 aktivieren

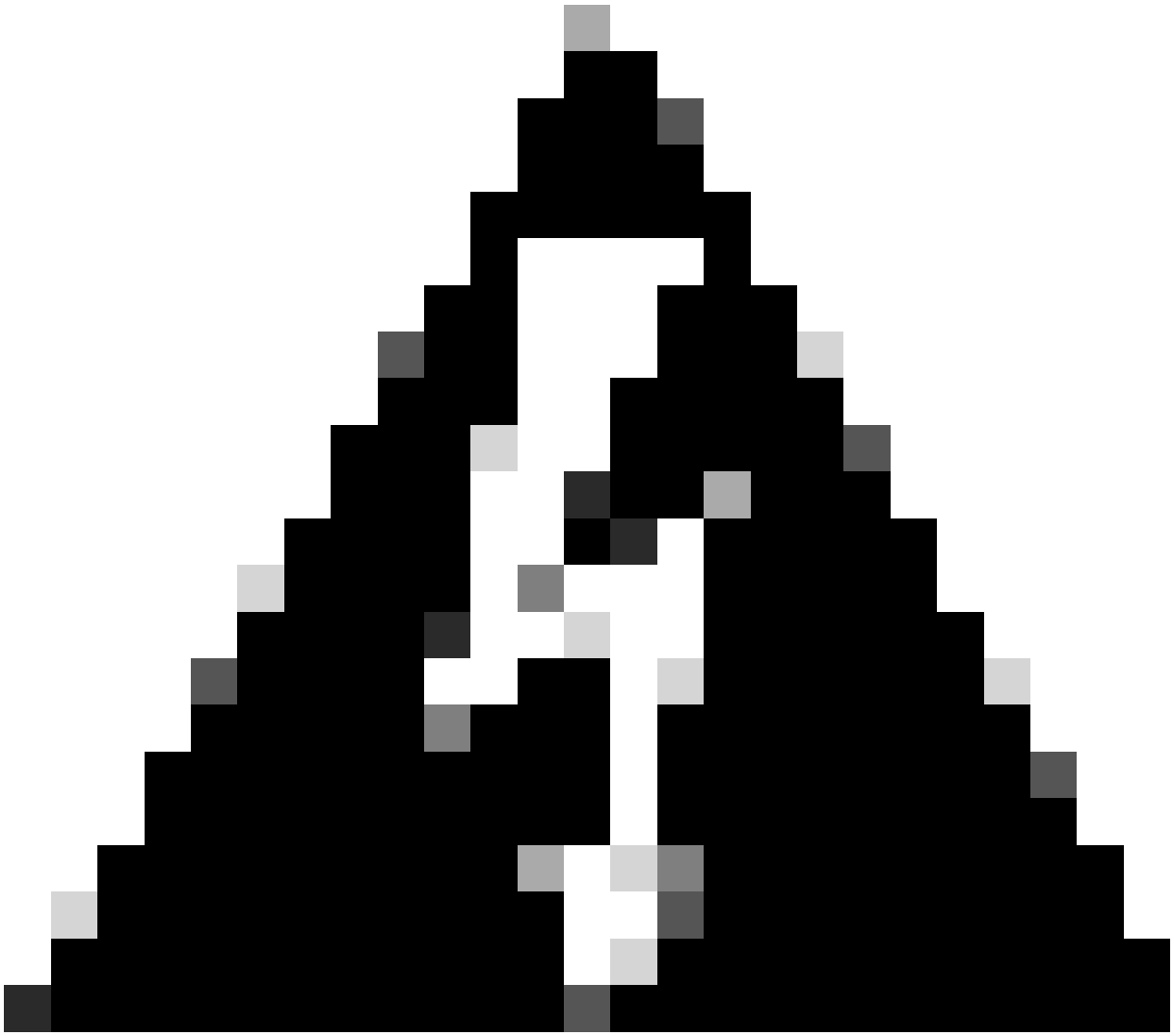
TLS 1.3 ist in ISE 3.4.x nicht standardmäßig aktiviert. Sie muss manuell aktiviert werden.

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



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



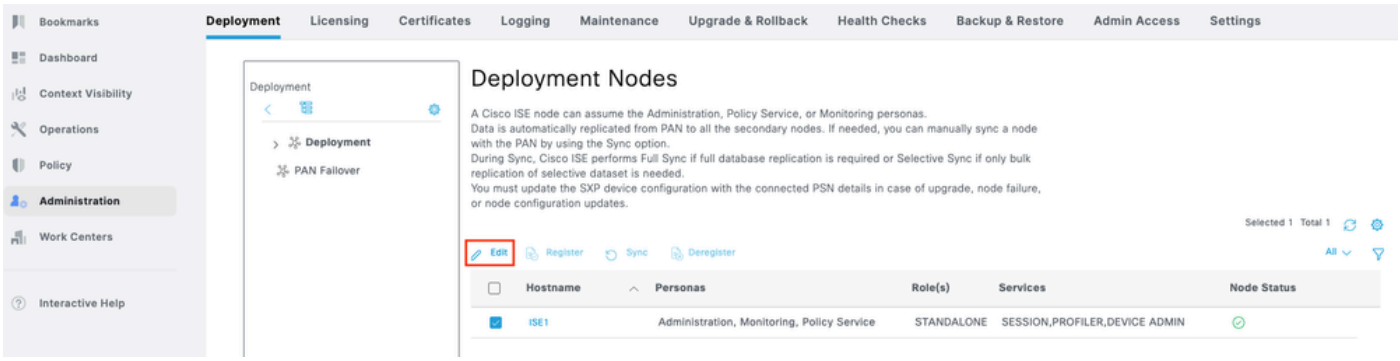


Warnung: Wenn Sie die TLS-Version ändern, wird der Cisco ISE-Anwendungsserver auf allen Cisco ISE-Bereitstellungssystemen neu gestartet.

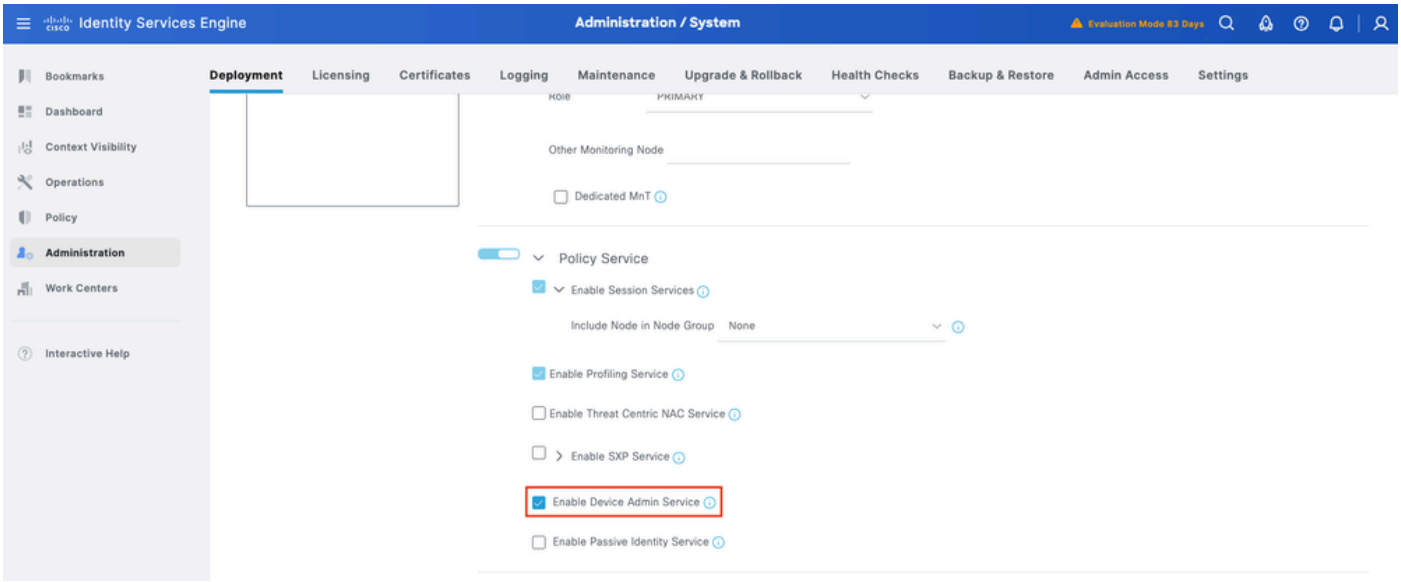
Geräteadministration auf ISE aktivieren

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

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



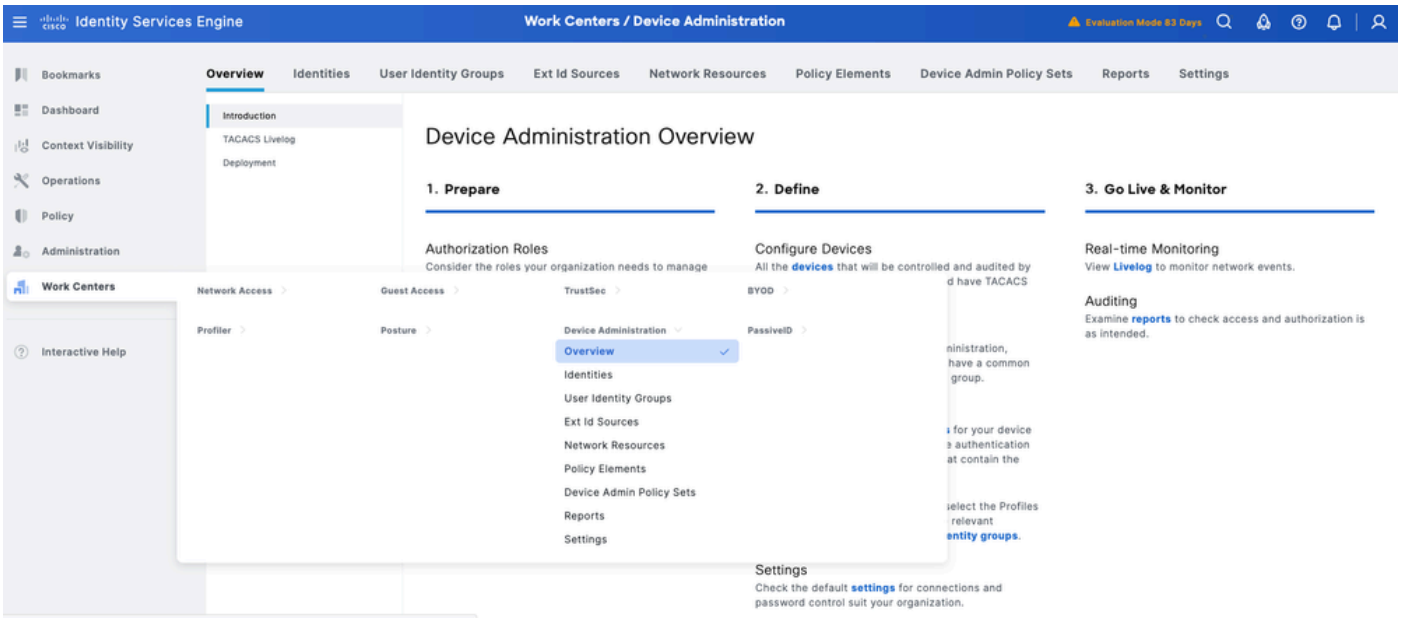
Schritt 2: Führen Sie unter Allgemeine Einstellungen einen Bildlauf nach unten durch, und aktivieren Sie das Kontrollkästchen neben Geräteverwaltungsdienst aktivieren.



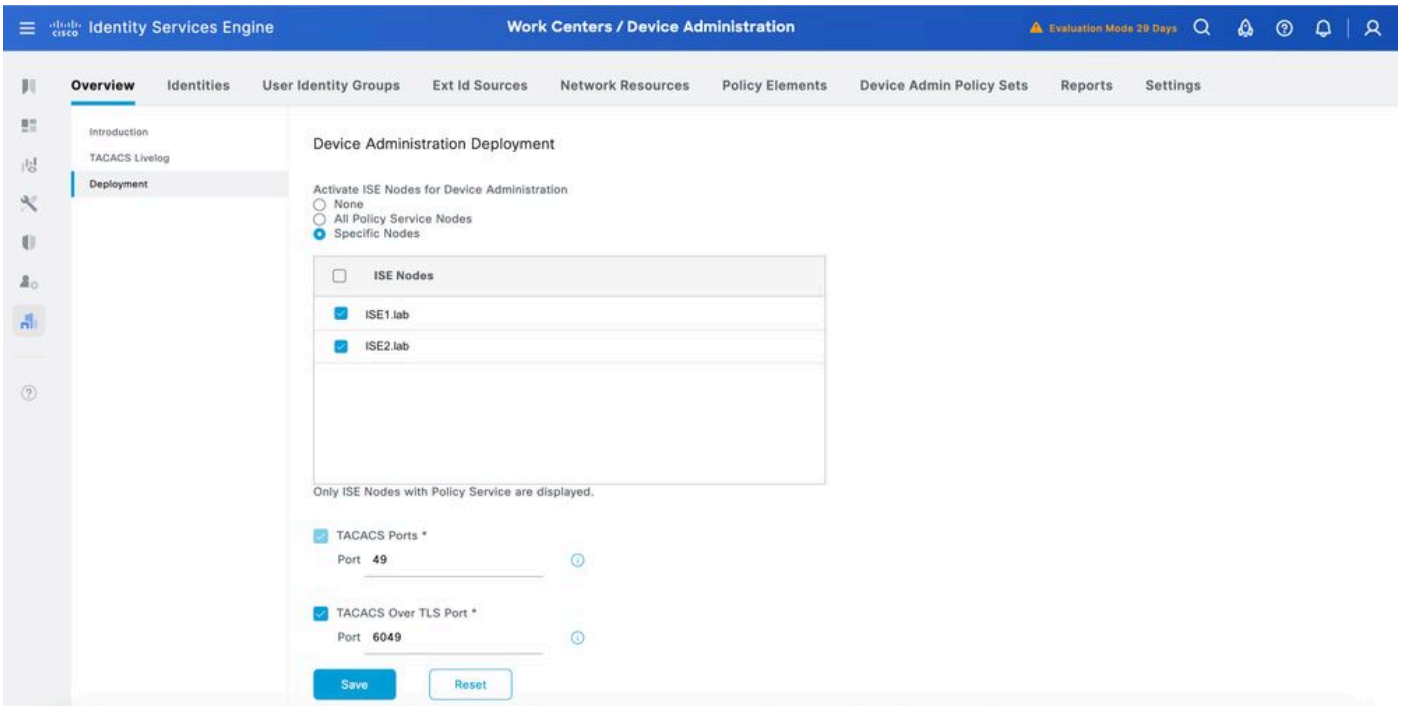
Schritt 3: Speichern der Konfiguration Der Geräteverwaltungsdienst ist jetzt auf der ISE aktiviert.

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.

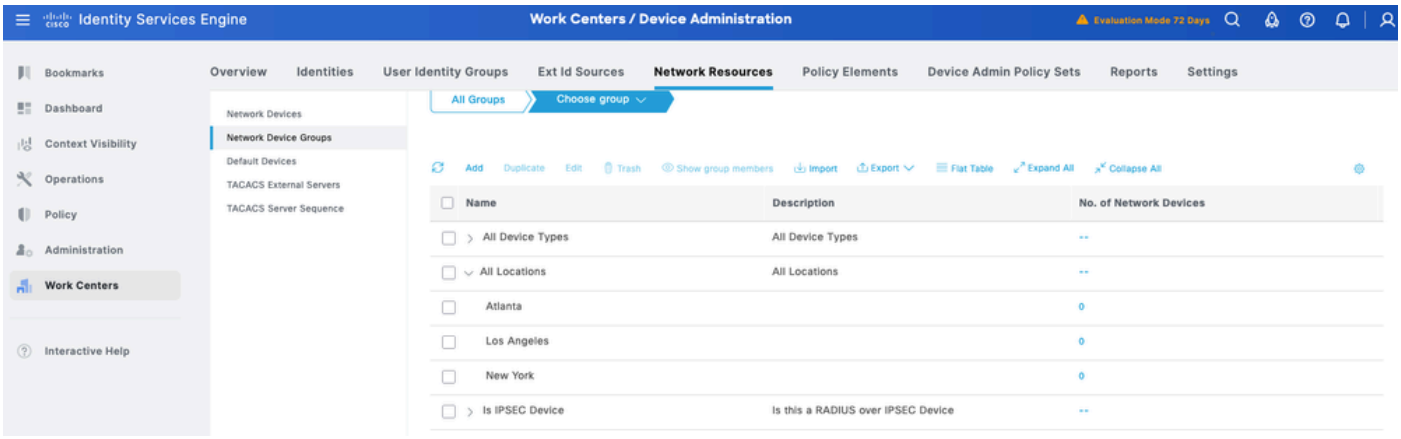


Schritt 3: Behalten Sie den Standardport 6049 bei, oder geben Sie einen anderen TCP-Port für TACACS über TLS an. Klicken Sie dann auf Speichern.

Netzwerkgeräte- und Netzwerkgerätegruppen

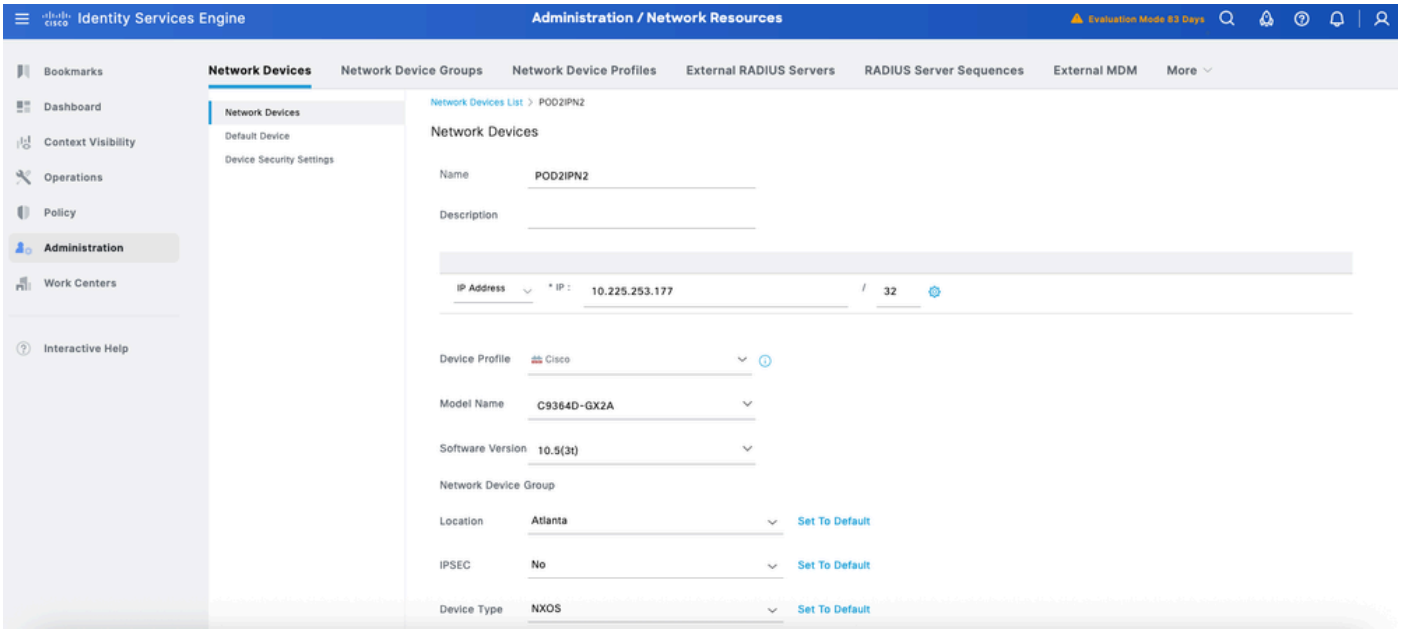
Die ISE ermöglicht eine leistungsstarke Gruppierung von Geräten mit mehreren Hierarchien von Gerätegruppen. Jede Hierarchie stellt eine eigene und unabhängige Klassifizierung von Netzwerkgeräten dar.

Schritt 1: Navigieren Sie zu Work Centers > Device Administration > Network Resource. Klicken Sie auf Netzwerkgerätegruppen.

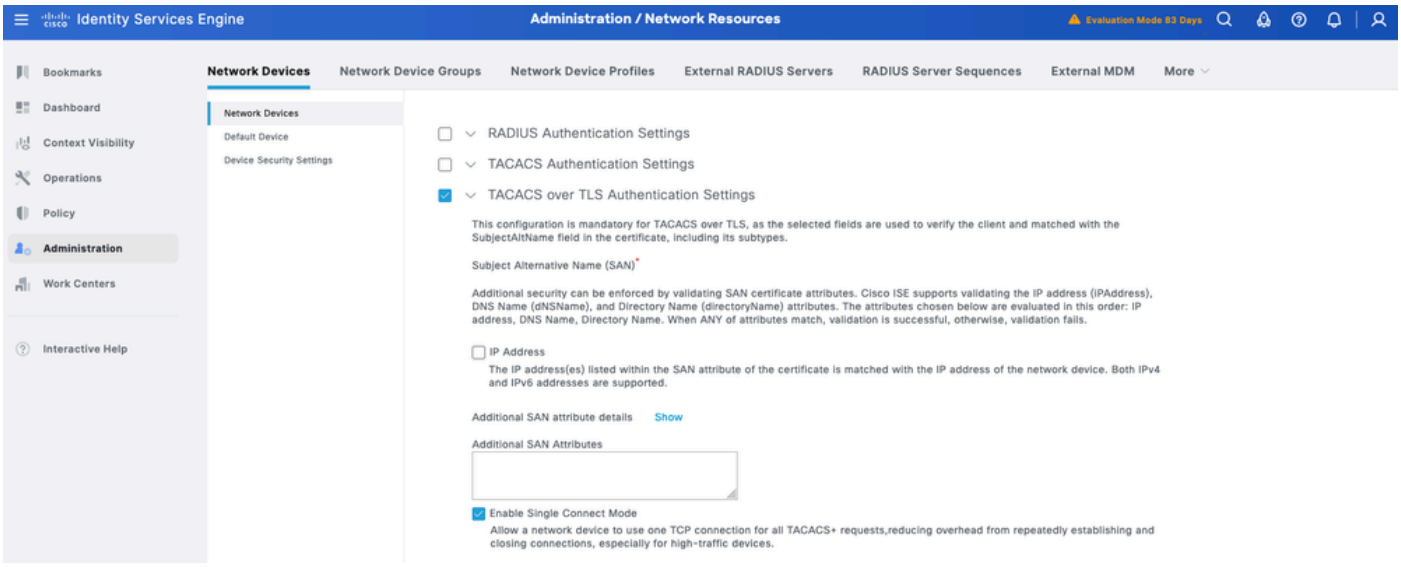


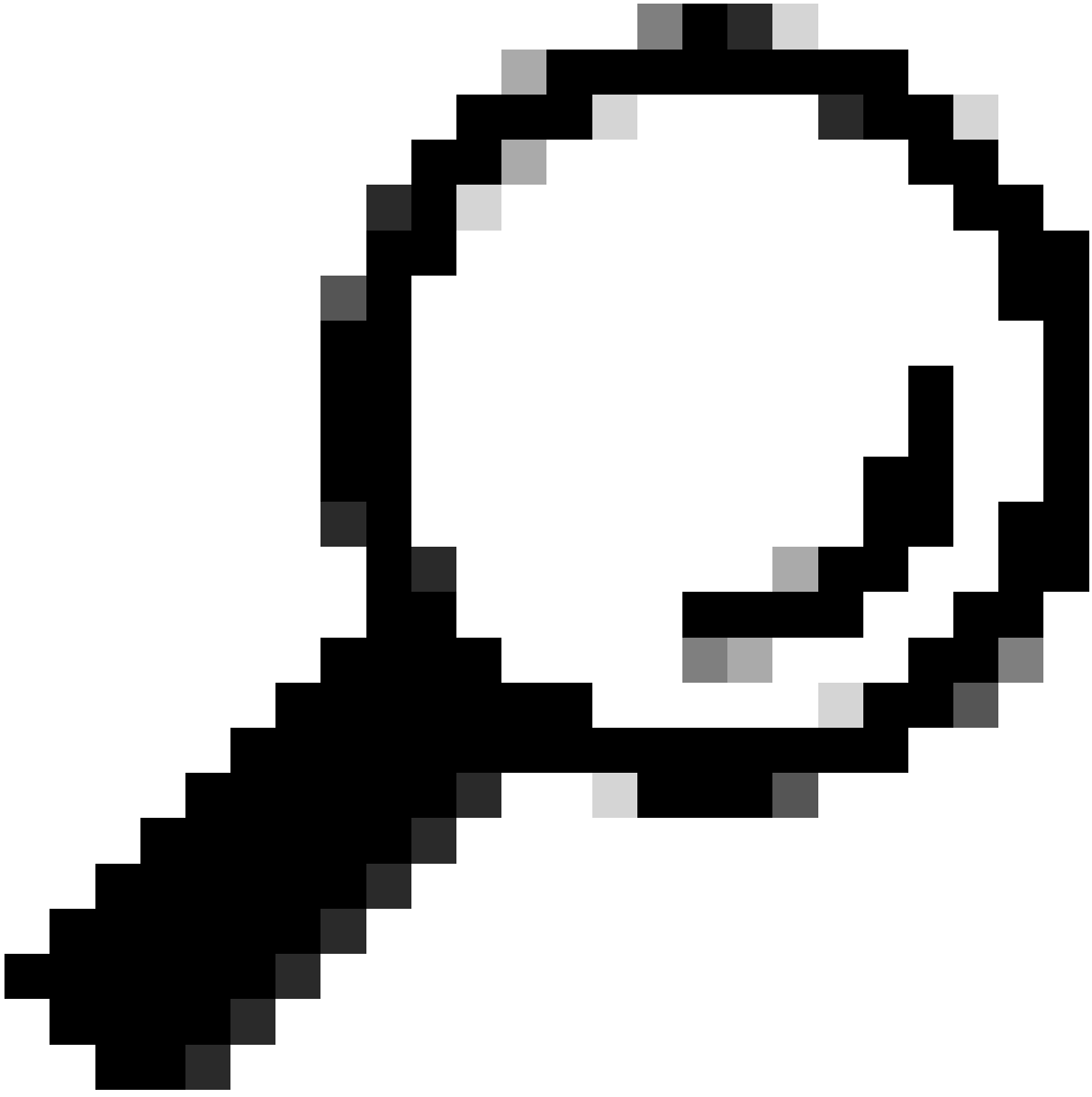
Alle Gerätetypen und alle Standorte sind die von der ISE bereitgestellten Standardhierarchien. Sie fügen eigene Hierarchien hinzu und definieren die verschiedenen Komponenten bei der Identifizierung eines Netzwerkgeräts, das später in der Richtlinienbedingung verwendet werden kann.

Schritt 2: Fügen Sie nun ein NS-OX-Gerät als Netzwerkgerät hinzu. Navigieren Sie zu Work Centers > Device Administration > Network Resources. Klicken Sie auf Hinzufügen, um ein neues Netzwerkgerät POD2IPN2 hinzuzufügen.



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


Identity Services Engine
Administration / Network Resources
Evaluation Mode 83 Days
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Help
Network Devices
Network Device Groups
Network Device Profiles
External RADIUS Servers
RADIUS Server Sequences
External MDM
More
Network Devices
Default Device
Device Security Settings
RADIUS Authentication Settings
TACACS Authentication Settings
TACACS over TLS Authentication Settings
This configuration is mandatory for TACACS over TLS, as the selected fields are used to verify the client and matched with the SubjectAltName field in the certificate, including its subtypes.
Subject Alternative Name (SAN)*
Additional security can be enforced by validating SAN certificate attributes. Cisco ISE supports validating the IP address (IPAddress), DNS Name (dNSName), and Directory Name (directoryName) attributes. The attributes chosen below are evaluated in this order: IP address, DNS Name, Directory Name. When ANY of attributes match, validation is successful, otherwise, validation fails.
IP Address
The IP address(es) listed within the SAN attribute of the certificate is matched with the IP address of the network device. Both IPv4 and IPv6 addresses are supported.
Additional SAN attribute details
Show
Additional SAN Attributes
Enable Single Connect Mode
Allow a network device to use one TCP connection for all TACACS+ requests,reducing overhead from repeatedly establishing and closing connections, especially for high-traffic devices.

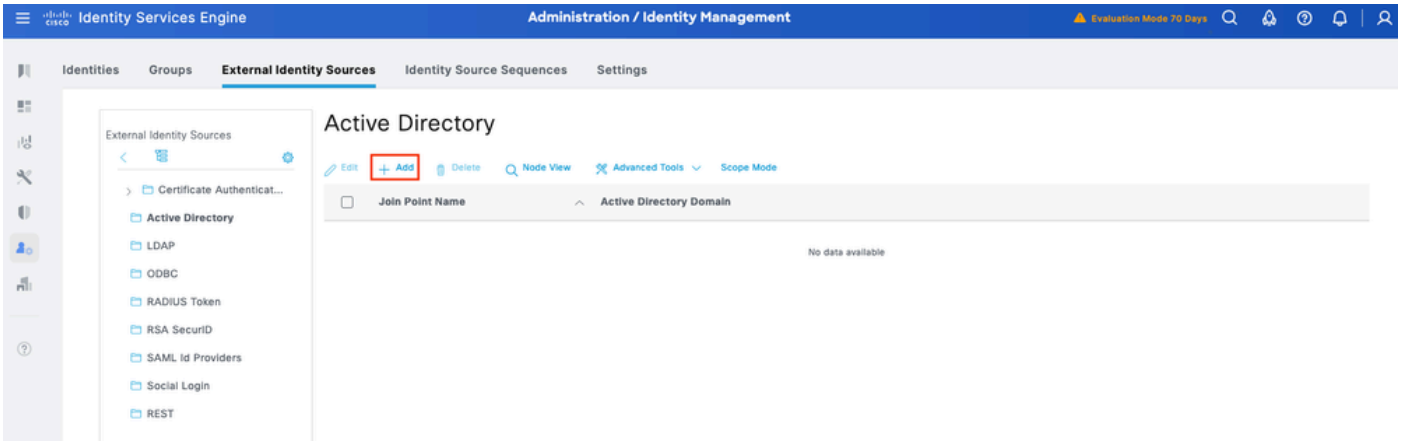


Tipp: Es wird empfohlen, den Single-Connect-Modus zu aktivieren, um zu vermeiden, dass die TCP-Sitzung jedes Mal neu gestartet wird, wenn ein Befehl an das Gerät gesendet wird.

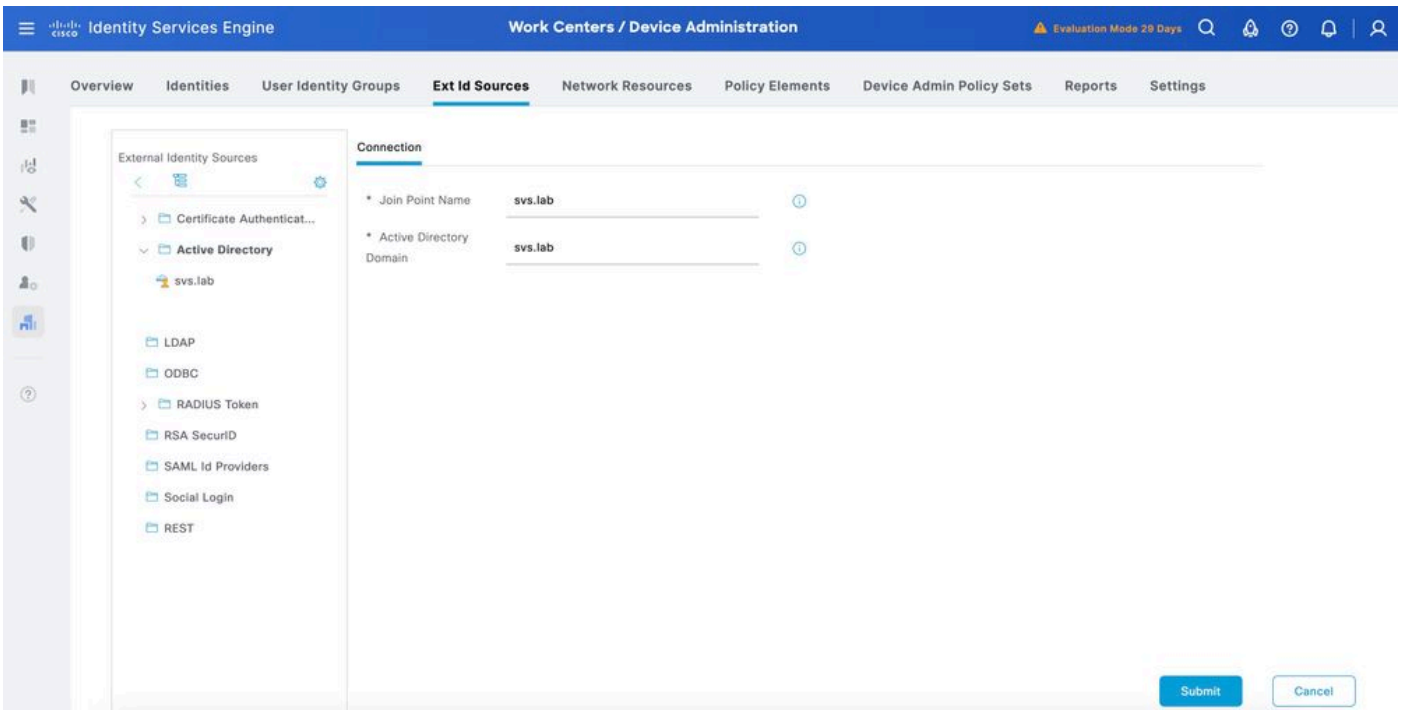
Identitätsspeicher konfigurieren

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

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



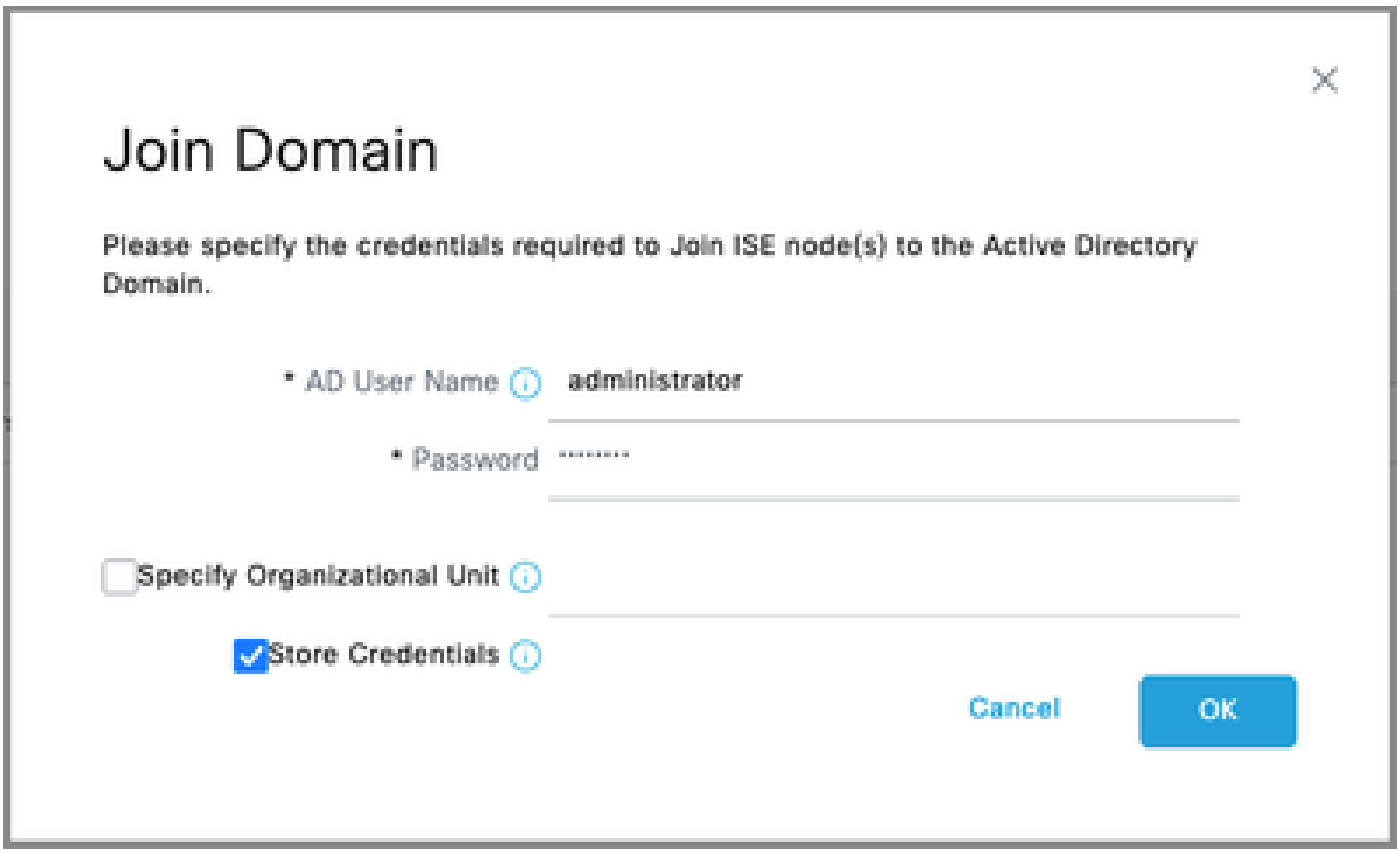
Schritt 2: Geben Sie den Namen des Verbindungspunkts und den AD-Domänennamen an, und klicken Sie auf Senden.

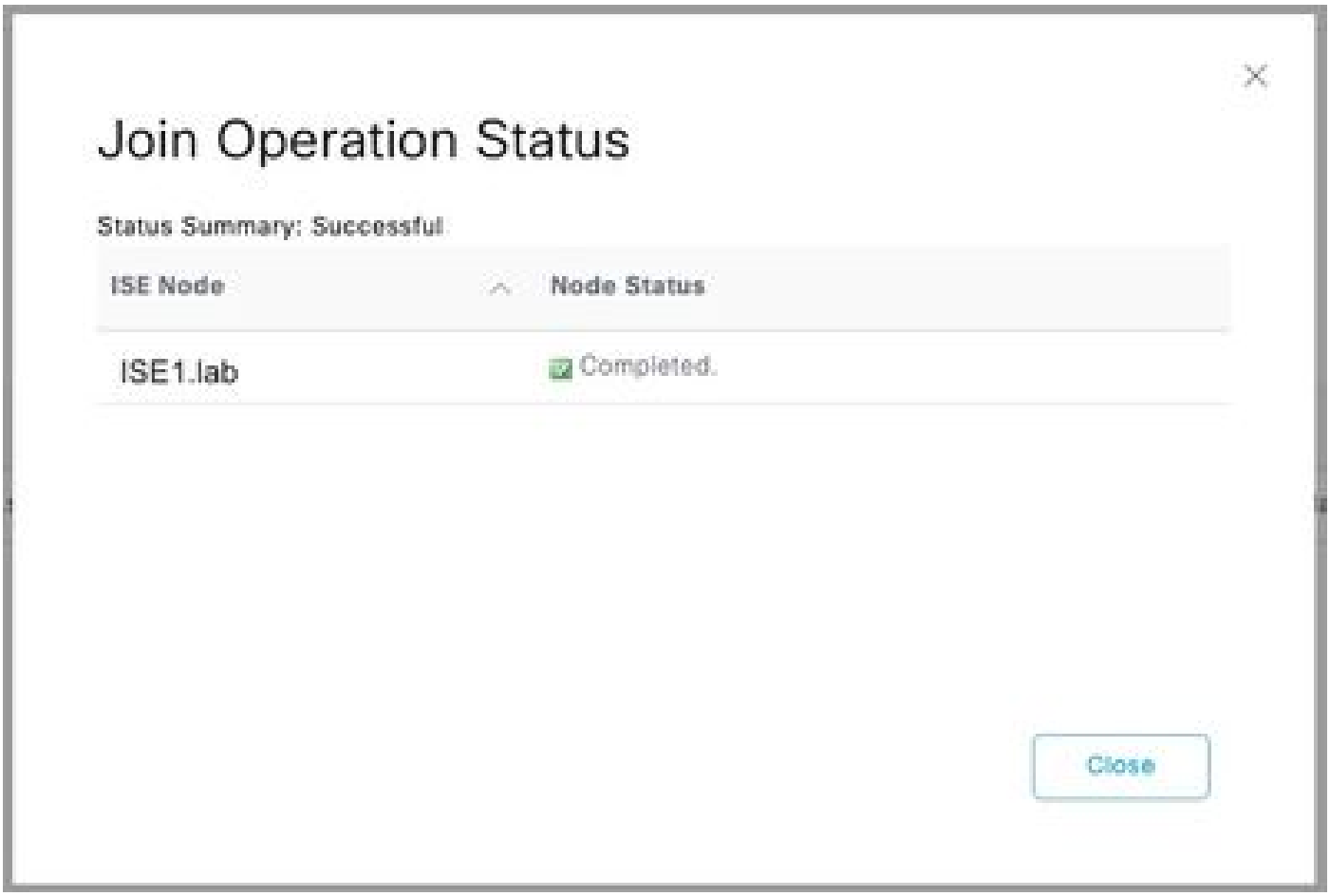


Schritt 3. Klicken Sie auf Ja, wenn Sie gefragt werden "Möchten Sie allen ISE-Knoten in dieser

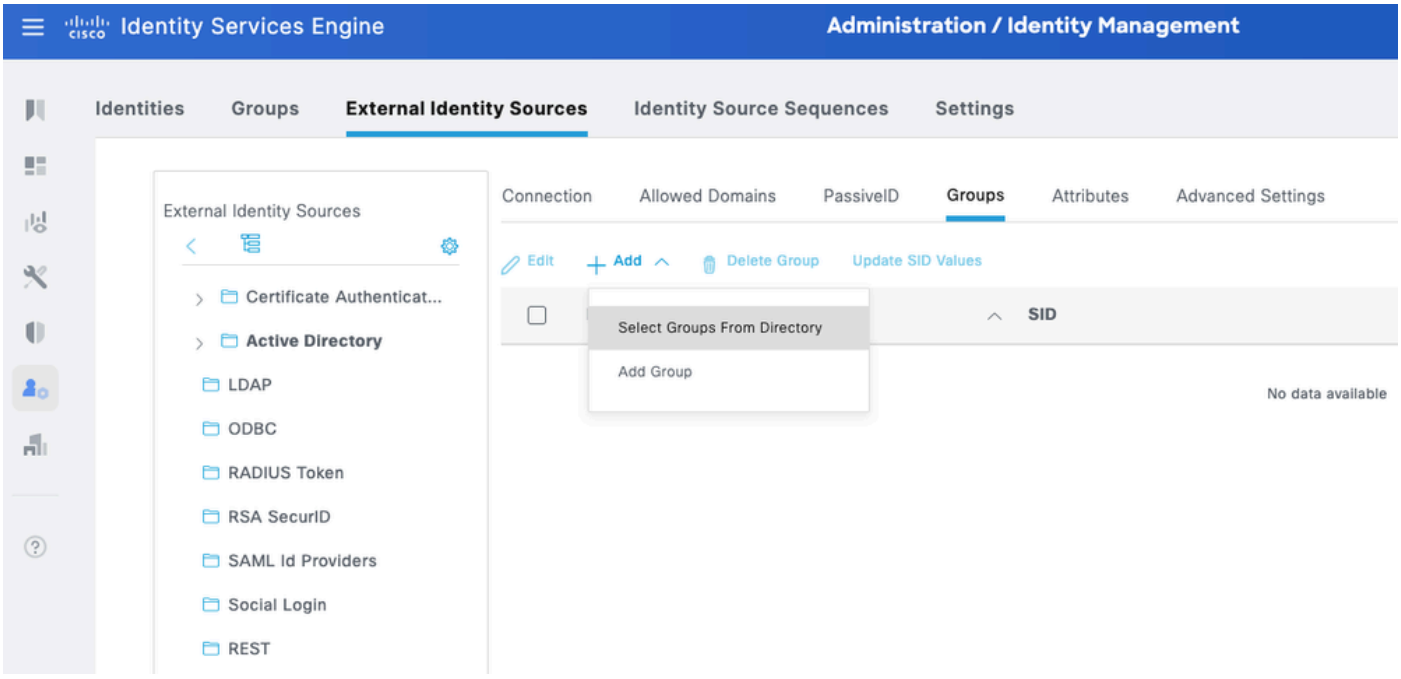
Active Directory-Domäne beitreten?"

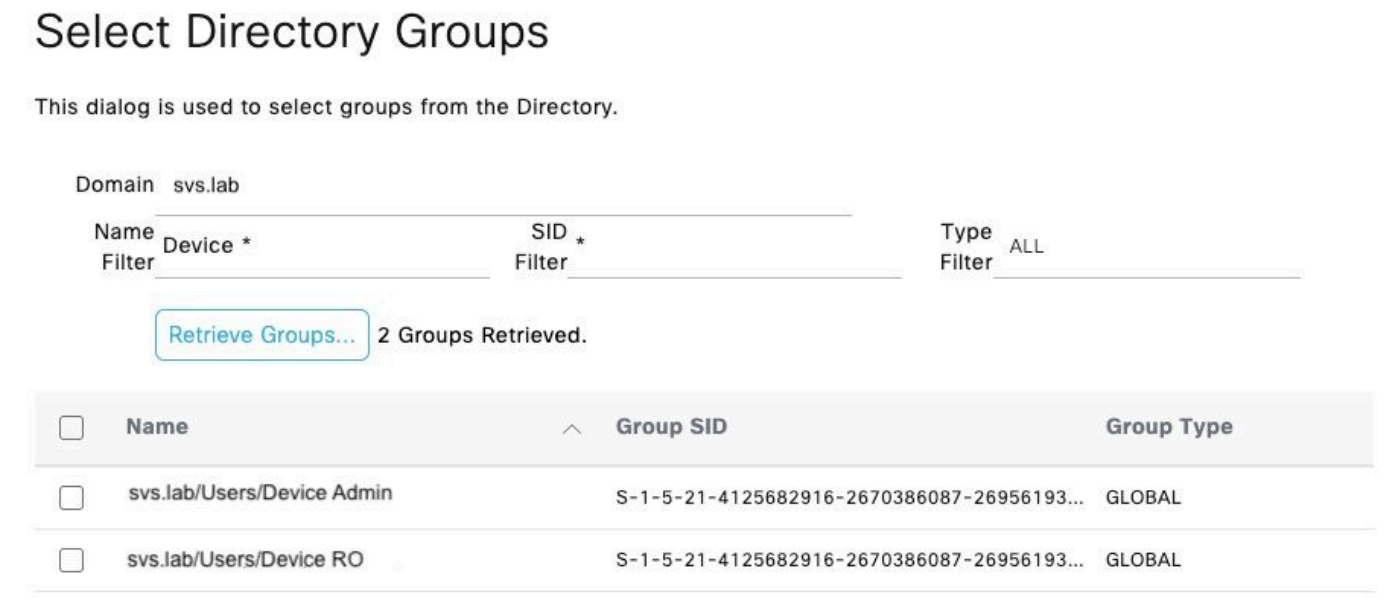
Schritt 4: Geben Sie die Anmeldeinformationen mit AD-Join-Berechtigungen ein, und treten Sie ISE bei AD bei. Überprüfen Sie den Status, um sicherzustellen, dass er betriebsbereit ist.

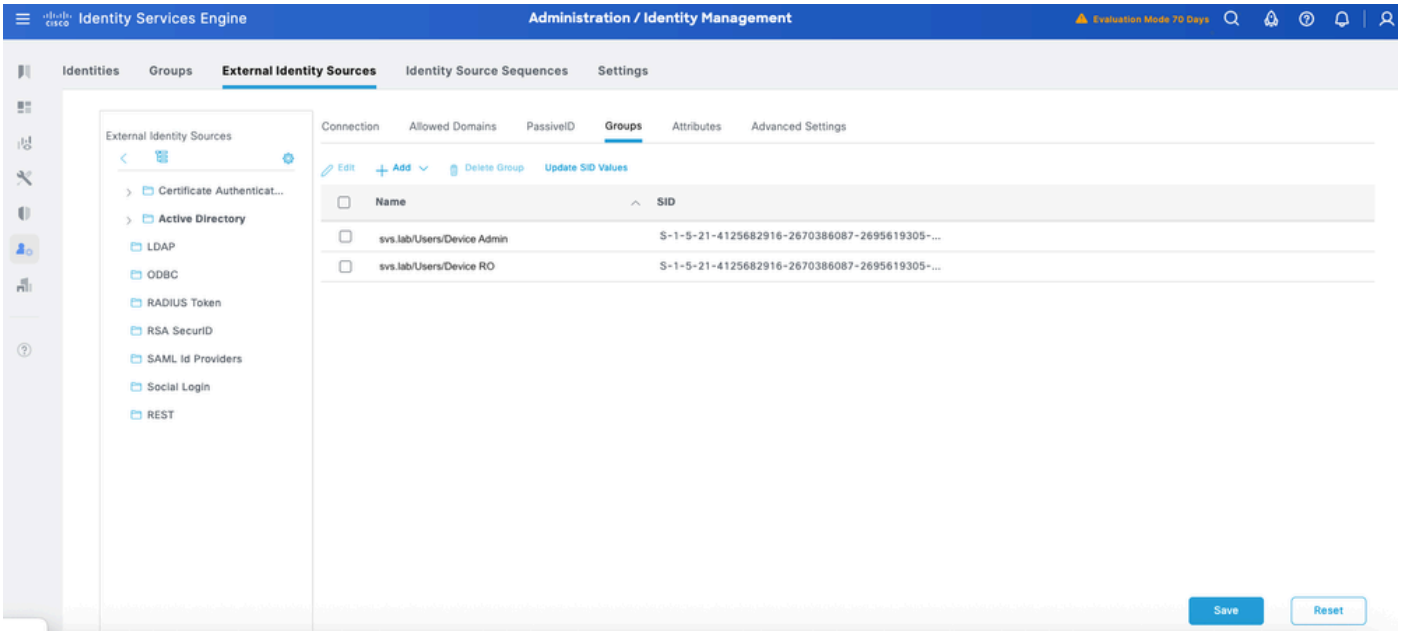




Schritt 5: Navigieren Sie zur Registerkarte Gruppen, und klicken Sie auf Hinzufügen, um alle erforderlichen Gruppen abzurufen, basierend auf denen die Benutzer für den Gerätezugriff autorisiert sind. Dieses Beispiel zeigt die Gruppen, die in der Autorisierungsrichtlinie in diesem Leitfaden verwendet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







Konfigurieren von TACACS+-Shell-Profilen

Im Gegensatz zu Cisco IOS-Geräten, die Berechtigungsebenen für die Autorisierung verwenden, implementieren Cisco NX-OS-Geräte eine rollenbasierte Zugriffskontrolle (RBAC). In der ISE können Sie mithilfe von allgemeinen Aufgaben vom Nexus-Typ TACACS+-Profile Benutzerrollen auf Cisco NX-OS-Geräten zuordnen.

Die vordefinierten Rollen auf NX-OS-Geräten unterscheiden sich von NX-OS-Plattformen. Zwei gebräuchliche sind:

- network-admin - vordefinierte Netzwerkadministratorrolle mit vollständigem Lese- und Schreibzugriff auf alle Befehle am Switch nur verfügbar, wenn die Geräte (z. B. Nexus 7000) über mehrere VDCs verfügen. Verwenden Sie den CLI-Befehl show cli syntax roles network-admin in NX-OS, um die vollständige Befehlsliste anzuzeigen, die für diese Rolle verfügbar

ist.

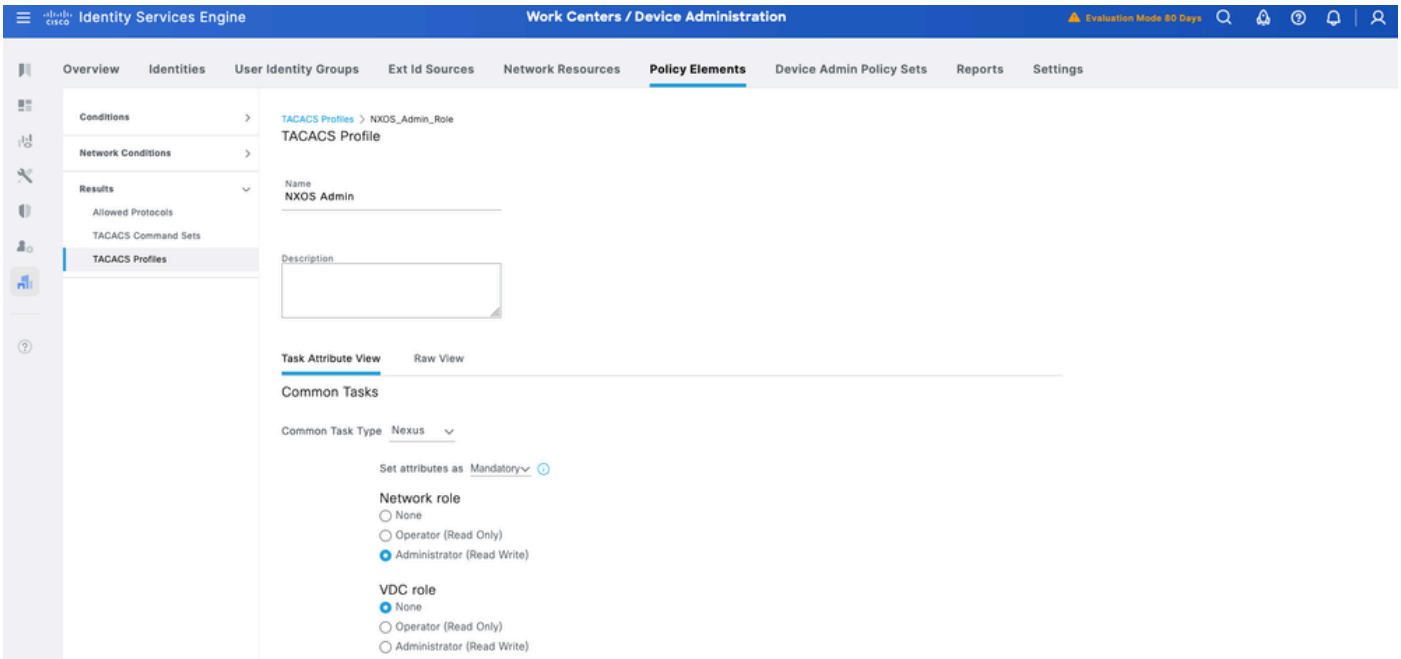
- network-operator - vordefinierte Netzwerk-Administratorrolle mit vollständigem Lesezugriff auf alle Befehle des Switches nur verfügbar, wenn die Geräte (z. B. Nexus 7000) über mehrere VDCs verfügen. Verwenden Sie den CLI-Befehl show cli syntax roles network-operator von NX-OS, um die vollständige für diese Rolle verfügbare Befehlsliste anzuzeigen.

Als Nächstes werden zwei TACACS-Profile definiert: NXOS Admin und NXOS HelpDesk.

NX-OS-Administrator

Schritt 1: Fügen Sie ein weiteres Profil hinzu, und nennen Sie es NX-OS-Admin.

Schritt 2. Wählen Sie Obligatorisch aus dem Dropdown-Menü Attribute festlegen als. Wählen Sie unter Allgemeine Aufgaben die Option Administrator aus.



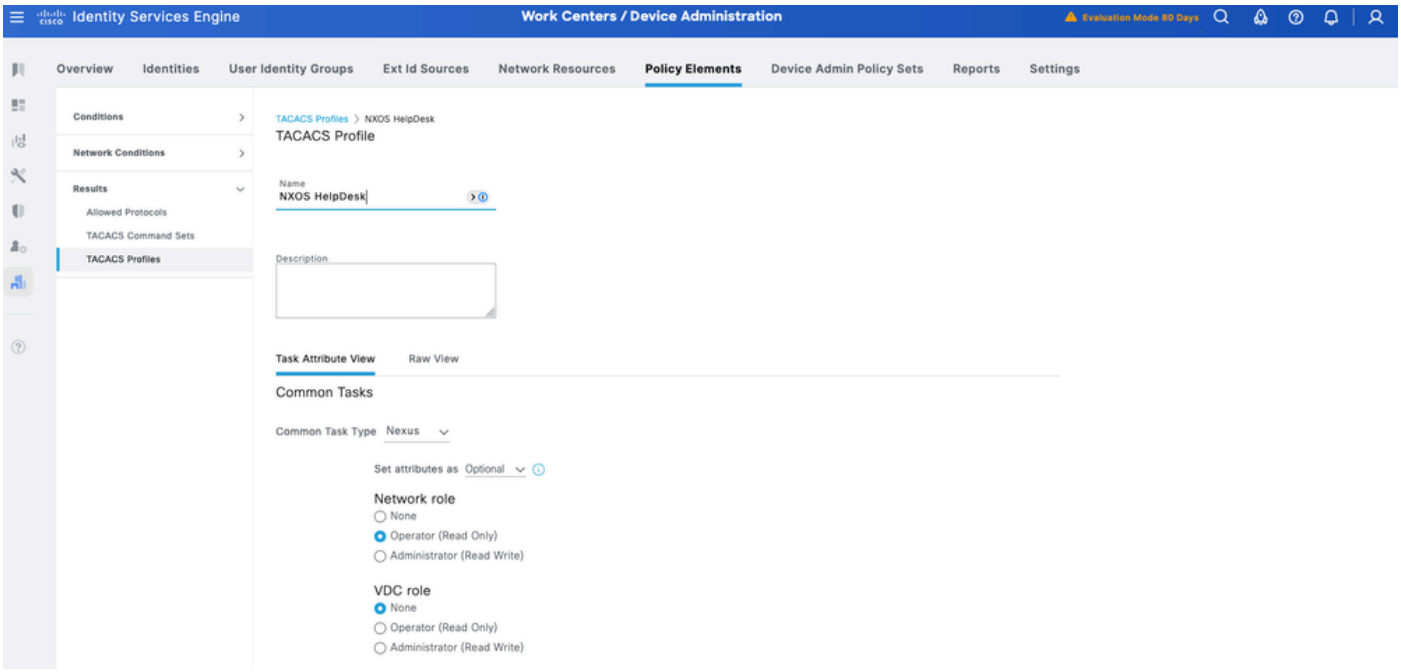
Schritt 3: Klicken Sie auf Senden, um das Profil zu speichern.

NX-OS-Helpdesk

Schritt 1: Navigieren Sie in der ISE-Benutzeroberfläche zu Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles. Fügen Sie ein neues TACACS-Profil hinzu, und nennen Sie es NXOS HelpDesk. Wechseln Sie zum Dropdown-Menü Allgemeiner Aufgabentyp, und wählen Sie Nexus

Sie können die Vorlagenänderungen für die Benutzerrolle sehen. Sie können diese Optionen für die Benutzerrolle auswählen, die Sie konfigurieren möchten.

Schritt 2. Wählen Sie Obligatorisch aus dem Dropdown-Menü Attribute festlegen als. Wählen Sie unter Allgemeine Aufgaben die Option Operator aus Network-role.

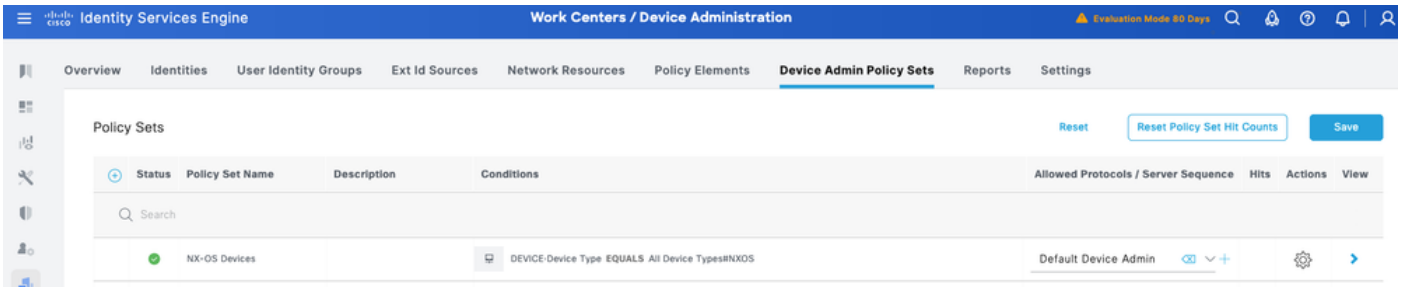


Schritt 3: Klicken Sie auf Speichern, um das Profil zu speichern.

Admin-Richtliniensätze für Geräte konfigurieren

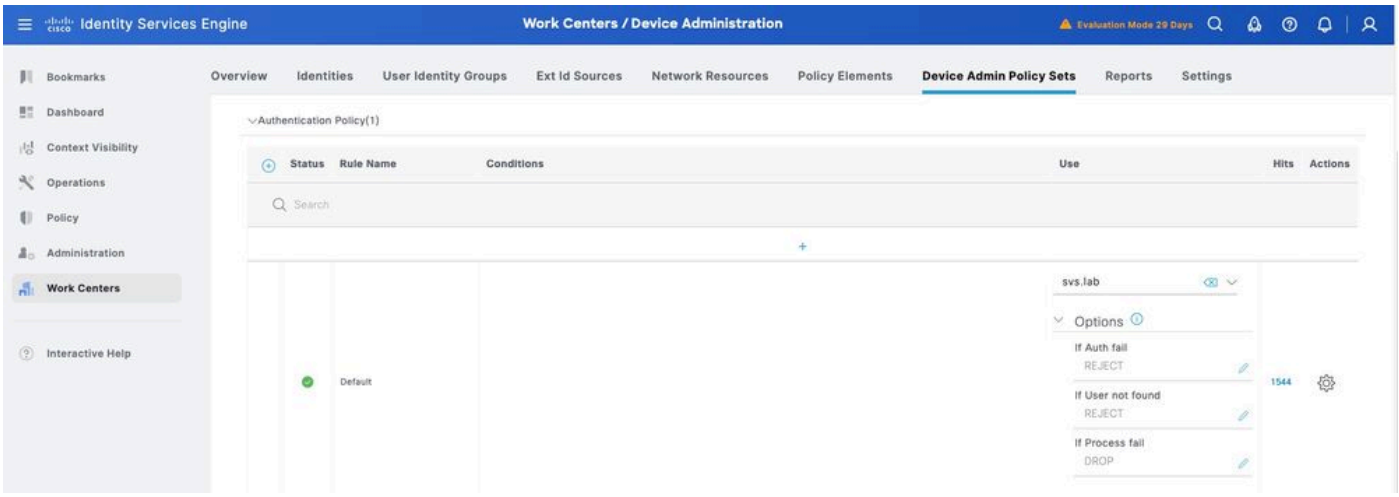
Richtliniensätze sind standardmäßig für die Geräteadministration aktiviert. Richtliniensätze können Richtlinien basierend auf den Gerätetypen aufteilen, um die Anwendung von TACACS-Profilen zu vereinfachen. Beispielsweise verwenden Cisco IOS-Geräte Privilegstufen und/oder Befehlssätze, während Cisco NX-OS-Geräte benutzerdefinierte Attribute verwenden.

Schritt 1: Navigieren Sie zu Work Centers > Device Administration > Device Admin Policy Sets. Fügen Sie einen neuen Richtliniensatz für NX-OS-Geräte hinzu. Geben Sie unter condition (Bedingung) DEVICE:Device Type EQUALS All Device Types#NXOS (GERÄTETYP ENTSPRICHT ALLEN GERÄTETYPEN) an. Wählen Sie unter Zugelassene Protokolle die Option Standardgeräteadministrator aus.



Schritt 2: Klicken Sie auf Speichern, und klicken Sie auf den rechten Pfeil, 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.

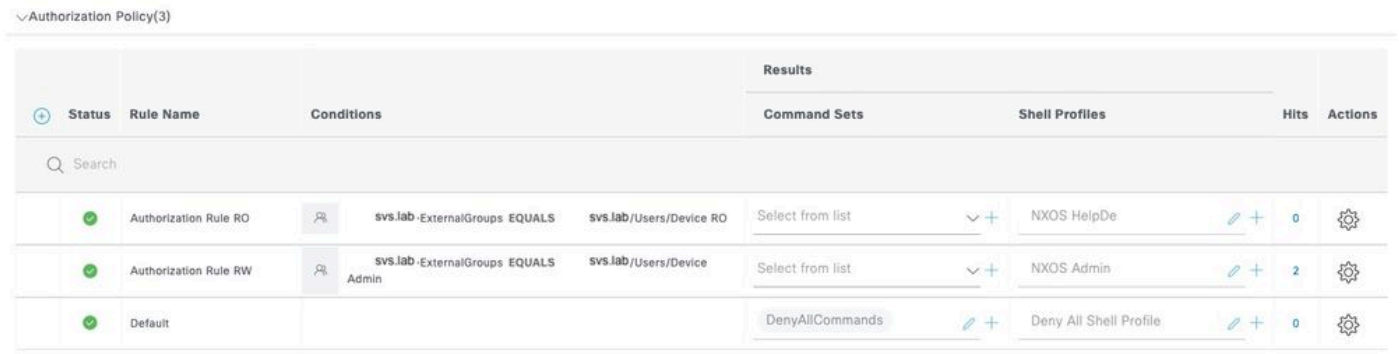


Schritt 4: Definieren der Autorisierungsrichtlinie

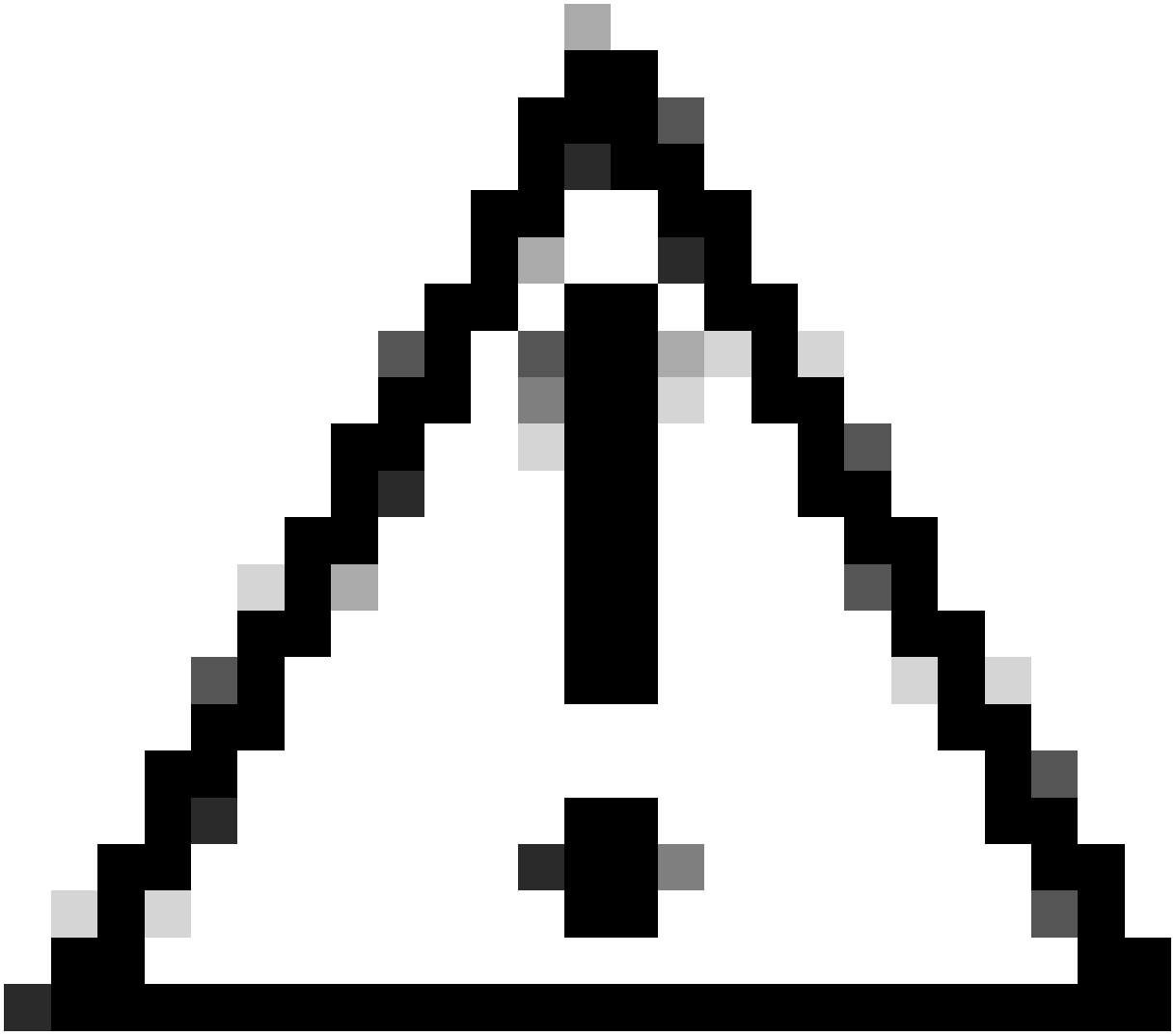
Erstellen Sie die Autorisierungsrichtlinie auf Basis von Benutzergruppen in Active Directory (AD).

Beispiele:

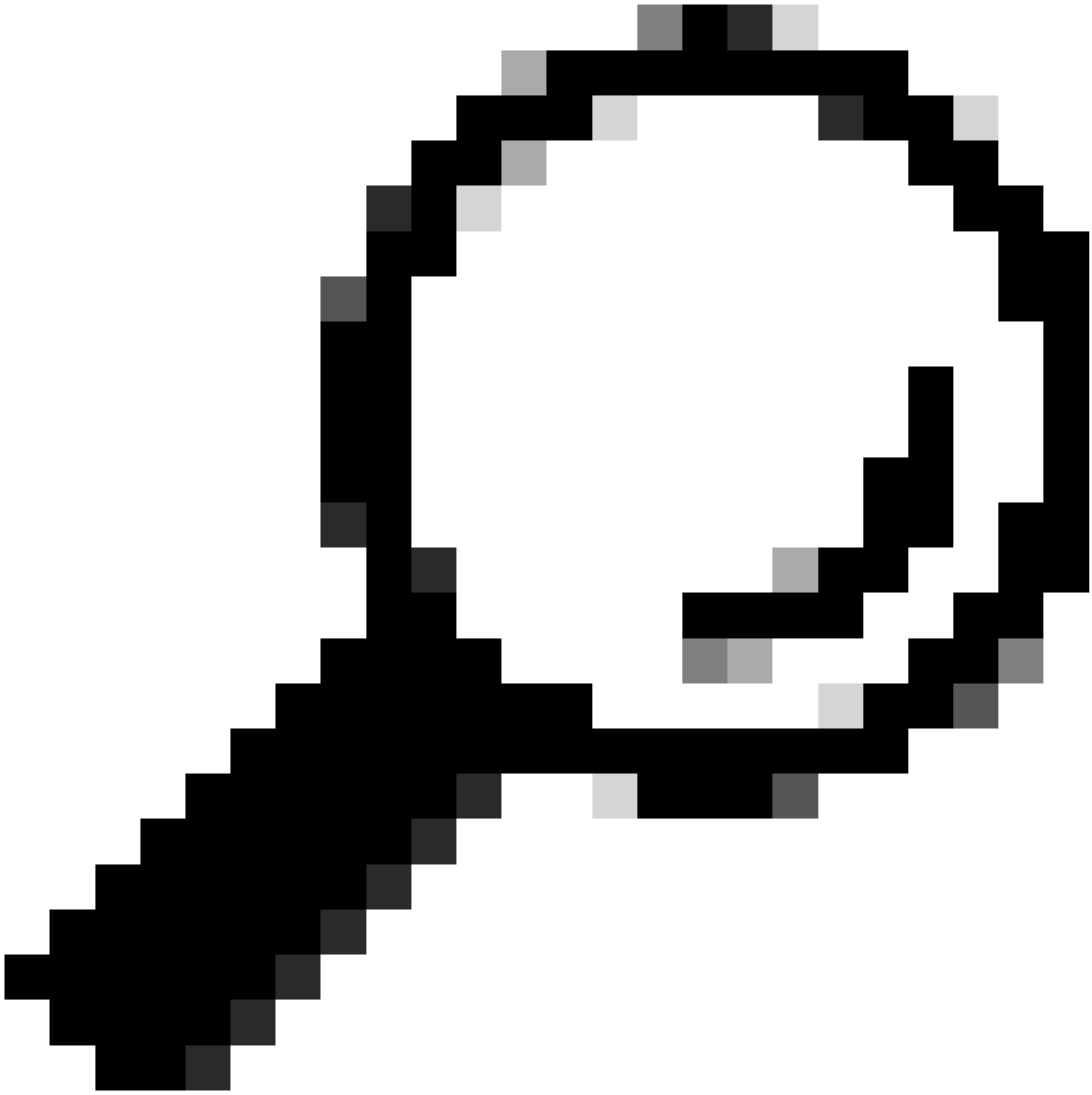
- Benutzern der AD-Gruppe "Device Admin" (Geräteadministrator) wird das NXOS-Admin-TACACS-Profil zugewiesen.
- Benutzern in der AD-Gruppe Device RO wird das NXOS HelpDesk TACACS-Profil zugewiesen.



Konfigurieren von Cisco NX-OS für TACACS+ über TLS



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.

Konfiguration des TACACS+-Servers

Schritt 1: Erstkonfiguration.

```
POD2IPN2# sho run tacacs

feature tacacs+

tacacs-server host 10.225.253.209 key 7 "F1whg.123"
```

```
aaa group server tacacs+ tacacs2
  server 10.225.253.209
  use-vrf management
```

Konfiguration des Vertrauenspunkts

Schritt 1. Erstellen Sie eine Schlüsselbezeichnung, in Ihrem Fall, verwenden Sie ecc Schlüsselpaar.

<#root>

```
POD2IPN2(config)#
```

crypto key generate ecc label ec521-label exportable modulus 521

Schritt 2: Ordnen Sie dies einem Vertrauenspunkt zu.

<#root>

```
POD2IPN2(config)#
```

crypto ca trustpoint ec521-tp

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

ecckeypair ec521-label

Schritt 3: Installieren Sie den öffentlichen CA-Schlüssel.

<#root>

```
POD2IPN2(config)#
```

crypto ca authenticate ec521-tp

```
input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----BEGIN CERTIFICATE-----
MIIFlDCCA3ygAwIBAgIIIM1OAsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
QOEwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUGA1UECBMOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBAcTB1JhbGVpZ2gxDjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTVlMxEjAQBgNVBAMTCVNWUyBMYWJDQTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZUOyn2vIn6gKbx3M7vaRq
2YjwZlzSH6EkEvxnJTy+kksiFD33GyHQepk7vfp4NFU5OtQ4HC7t/AOv9grDa3QW
VwvV4MBbJhFM3sOJ/ejgDYcMZhIAaPyOZo5WLboOkXEiKjPLatkXojB8FVrhLF3O
jMBSqwa4/Wlniy5S+7s4FFxsCf2OCOWfBAsnrsOtatIIhmcnx+VLJP7MRm8fOw4m
mutNo7IhbJSrgAFXmjlbBjMmgspObULo/wxMHdTbtPBf11HRHTkNIo3qyO4UADL2
```

```
WpoGhgT/FaxxBo2UBcnYVaP+jjRE0NYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7BOe8oDNKU6gXlojKyLP/gC7j8AePO3ir+KZui8
b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
gJ+kQXe7QtT/u6m1MrtjE3gAEVpL334rTIxy9hpKZIkB86t2ZA3JX8CLsbCa13sA
z1XCoONX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTA01xh6OI4QnK+MNQKpTjt/E4
ydHlOrrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVLl783nTc9wYptQEPi5sw
83g9EMgKVOARIiVUa/qlAgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAYb4
QgEBBAQDAgAHMBkGCWCGSAGG+EIBDQQMFgpTVlMgTGFiIENBMAOGCSqGSIb3DQEB
CwUAA4ICAQAIT3O8oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oKOdGayi
iSEkSSX9qyfLfINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXRX67X+v
O+ja6zTQqjO6lqJhmrSkyFbYf/ZTpe4d1OzJsZjNsNOr8bF9nOA/7qNZLp3Z3cpU
PUOKdbiSvRqnPw3e8TfITVmAzcx8COI2SrYFMSUazolVBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIEOf5ay1PKURO/8aj/B7aluJapXkmnj5qPeGhNOpB
Q9r14reov4so2EspkXS7CrH9yGfpIyTprokz1UvZBZ8vloI7YZmjFmem+5rT6Gnk
eU/lX7nV61SYG5W5K+I8uaKuyBHOMn7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggzlPOdsS/i6Lo7ypYXOeB9HgVDCkzQsLXQuHGj/2WsgPgdRcjkvnyURk4Jx+Ib
xDrmo7eOXPpSW4l72a6Kl8CR3U2Cr4wsuvndPEq/qd2NRSBWffF0XE/AJHQG7STT
HaXLU9r2Ko6O3oecu8ysGTwLlIt/9T1/FOb0xZRugWcpJrVoTgDGuA==
-----END CERTIFICATE-----
```

END OF INPUT

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

Do you accept this certificate? [yes/no]:yes
POD2IPN2(config)#
POD2IPN2(config)#
```

show crypto ca certificates ec521-tp

```
Trustpoint: ec521-tp
CA certificate 0:
subject=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
issuer=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
serial=20CD7402C4DA37F5
notBefore=Apr 28 17:05:00 2025 GMT
notAfter=Apr 28 17:05:00 2035 GMT
SHA1 Fingerprint=0E:B1:81:E9:5A:3E:D7:80:3B:C5:A8:05:9A:85:4A:95:C8:3A:C7:37
purposes: sslserver sslclient
POD2IPN2(config)#
```

Schritt 4: Generieren der Anforderung für das Switch-Identitätszertifikat.

<#root>

```
POD2IPN2(config)#
```

crypto ca enroll ec521-tp

```
 Create the certificate request ..
 Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.
  Password:C1sco.123
```

```
 The subject name in the certificate will be the name of the switch.
 Include the switch serial number in the subject name? [yes/no]:
```

yes

```
 The serial number in the certificate will be: FDO26490P4T
 Include an IP address in the subject name [yes/no]:
```

yes

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

no

```
 The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
MIIBtjCCARcCAQAwKTERMA8GA1UEAwwIUE9EMklQTjIxFDASBgNVBAUTC0ZETzI2
NDkwUDRUMIGbMBAGByqGSM49AgEGBSuBBAAjA4GGAAQBGYT0iw7OvqIKQ/a22Lkg
Na9IhqWQvetjxKq485gqTSBEo6LzpkOhPAGE4jBveNHxYeIA7PfNWvJ7xTBWjDNX
/IYBm6E7Hd7q42OmCe8Mef+bqJBdJ9wzpyEjhI2lIIoXt4814nBxObkIWWyR5cZN
IiXTLk8P4IMZvPq8jRnELRxd8RGgSTAYBgkqhkiG9w0BCQcxCwwJQzFzY28uMTIz
MC0GCSqGSIb3DQEJDjEgMB4wHAYDVR0RAQH/BBIwEIIIUE9EMklQTjKHBArh/bEw
CgYIKoZIzj0EAwIDgYwAMIGIAkIAtzQ/knrW2ovCVoHAuq1v2cr0n3NenS/44lul
+3H1y52vn4Rm4CGU3wkzXU3qGO3YjhNjCXjhp3+uN2afFf1Wf3ECQgC4bumHVsfj
b5rwPIC5tvXS/A8upqIzqc0yt3OhpaDDOTWzzvZY7qFflCOl5p6pvUpHigqoZNg5
9xhNdM1CQSykOg==
-----END CERTIFICATE REQUEST-----
```

Schritt 5: Importieren Sie das von der Zertifizierungsstelle signierte Switch-Identitätszertifikat.

```
<#root>

POD2IPN2(config)#

crypto ca import ec521-tp certificate


input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIDzTCCAbWgAwIBAgIIC6zS76XYDm8wDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
Q0EwHhcNMjUwNTA3MTkxMDAwWhcNMjYwNTA3MTkxMDAwWjApMREwDwYDVQQDDAhQ
T0QySVBOMjEUMBIGA1UEBRMLRkRPMjY0OTBQNFQwgZswEAYHKoZIzj0CAQYFK4EE
ACMDgYYABAEZhPSLDs6+ogpD9rbYuSA1r0iGpZC962PEqrjzmCpNIESjovOmQ6E8
AYTiMG940fFh4gDs981a8nvFMFaMM1f8hgGboTsd3urjY6YJ7wx5/5uokF0n3DOn
ISOEjaUgihe3jzXicHE5uQhZbJHlxk0iJdMuTw/ggxm8+ryNGcQtHF3xEaNAMD4w
HgYJYIZIAYb4QgENBBEWD3hjYSBjZXJ0aWZpY2F0ZTAcBgNVHREBAf8EEjAQgghQ
T0QySVBOMocECuH9sTANBgkqhkiG9w0BAQsFAAOCAgEANWGb6zm9TDPaM1yhPMx7
8uai/pF7VQC8NSCdOKqr4w4+695ZjJuzqFL3msodOQK0EdgxpQ4+pEa5msRtK0i8
mms2X/Px3/EShxoHrZO1PUXNTyZidXpGd/yTrdQAl5JzpW4pEudrbCJMZEEYtqoP
wD+4OE8vKoYEgyWlDrpRZOZG1usZczuUhLZ8orkjXMhWC26Q5aqiCKkyg1ONt6nb
liToeYy2Q0cTesSZCKvRBv6Ewj5JuSLemURyB4GHY+LT+A9UNmEUM2n+OSVEL329
3hS0qd/YVaEuxjjlg7jNiZb+UsW7IRx3Q8Rouo++ISACpH/PJ61LnlVxhXombiS6
INoa0GvQONrl+lFT8ADIdZ/Ukd5Ubhc9bh/sYzf4MWtkK1wVO16Hv7vGpSMYonD6
a271im+tJPyKnnezQ6OykzlGqsL/Ta6JOdip/fEYp8UmRq9InDh23gDjqrojWL7k
```

```
1R/bZpc+baMYXd/2pohHMSNOsKN3zNrJTlnuk5KCqFx//4P7mAoyZYiTIDp1pkYS
VK65fJKD+pYxIhSP9wN8rnwtzSCWbOZ78sgOO6Y6wIXyTPOUB3FWhD+GxtTkmEce
ZnAQbgxpgrg5lhpAEVabpC/zRU4UzTuBmv/WoY12zwXCr5WLXEOWtIe8CwFjSnch
lfKuuebdZkbwz72r7OyyX/U=
-----END CERTIFICATE-----
POD2IPN2(config)#
```

Überprüfen Sie, ob das Switch-Identitätszertifikat registriert ist.

<#root>

```
POD2IPN2(config)#
```

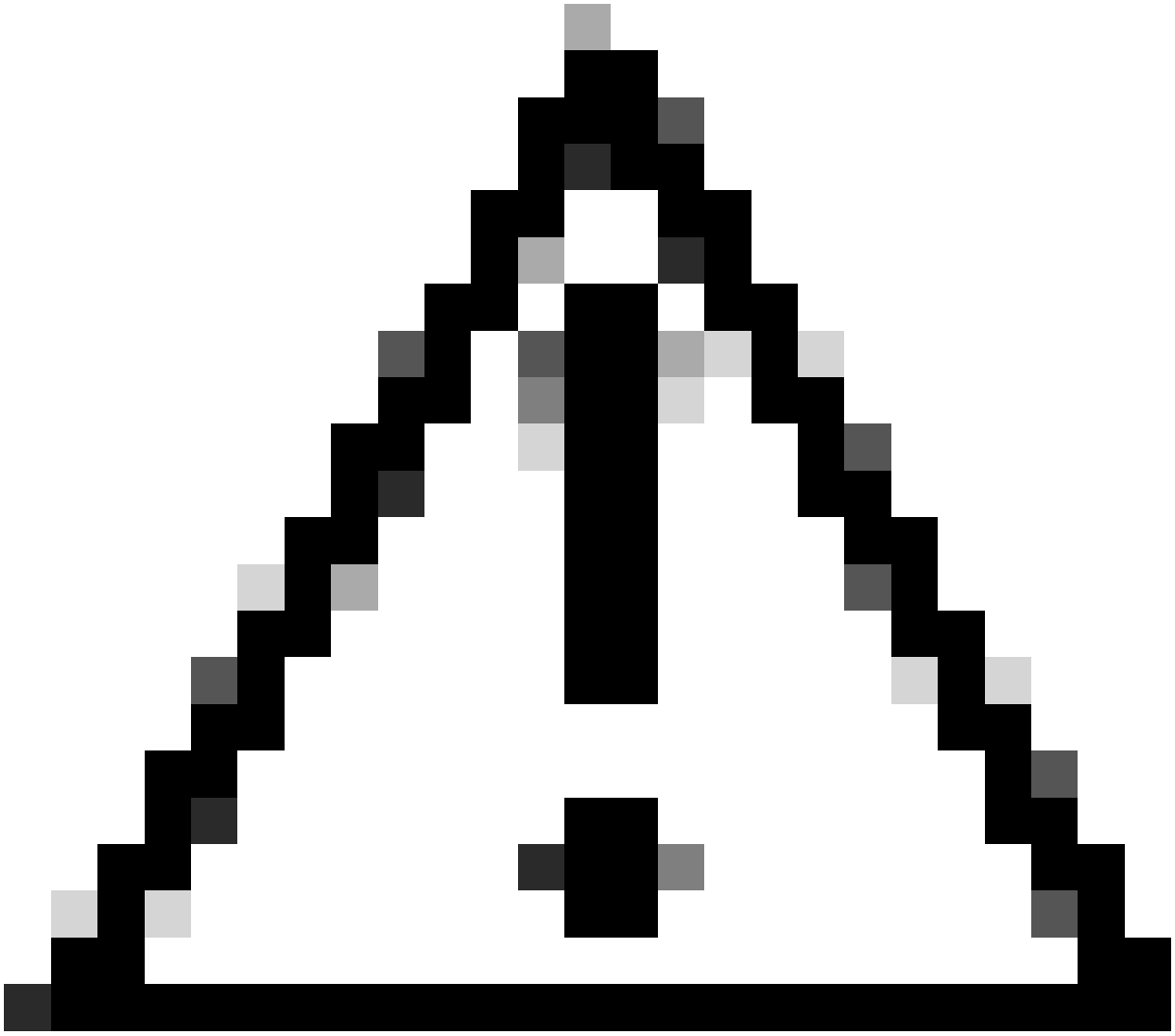
show crypto ca certificates ec521-tp

```
Trustpoint: ec521-tp
certificate:
subject=CN = POD2IPN2, serialNumber = FDO2649OP4T
issuer=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
serial=0BACD2EFA5D8OE6F
notBefore=May  7 19:10:00 2025 GMT
notAfter=May  7 19:10:00 2026 GMT
SHA1 Fingerprint=CA:B2:BF:3F:ED:2F:06:0B:C1:E4:DC:21:9F:9D:54:61:98:32:C5:13
purposes: sslserver sslclient

CA certificate 0:
subject=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
issuer=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
serial=20CD7402C4DA37F5
notBefore=Apr 28 17:05:00 2025 GMT
notAfter=Apr 28 17:05:00 2035 GMT
SHA1 Fingerprint=0E:B1:81:E9:5A:3E:D7:8O:3B:C5:A8:05:9A:85:4A:95:C8:3A:C7:37
purposes: sslserver sslclient

POD2IPN2(config)#
```

TACACS+-TLS-Konfiguration



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

Schritt 1: Konfigurieren Sie globale tacacs tls.

<#root>

```
POD2IPN2(config)#
tacacs-server secure tls
```

Schritt 2: Ändern Sie den ISE-Port in den TLS-Port, mit dem der ISE-Server konfiguriert ist.

<#root>

```
POD2IPN2(config)#
```

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

Schritt 3: Verknüpfen Sie die ISE-Serverkonfiguration auf dem Switch mit dem Vertrauenspunkt für die TLS-Verbindung.

```
<#root>

POD2IPN2(config)#

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

Schritt 4: Erstellen Sie eine TACACS-Servergruppe.

```
<#root>

POD2IPN2(config)#

aaa group server tacacs+ tacacs2


POD2IPN2(config-tacacs+)#

server 10.225.253.209


POD2IPN2(config-tacacs+)#

use-vrf management
```

Schritt 5: Überprüfen der Konfiguration

```
<#root>

POD2IPN2#

sho run tacacs


feature tacacs+

tacacs-server secure tls
tacacs-server host 10.225.253.209 port 6049 timeout 60 single-connection
tacacs-server host 10.225.253.209 tls client-trustpoint ec521-tp
aaa group server tacacs+ tacacs2
    server 10.225.253.209
    use-vrf management
```

Schritt 6: Testen Sie den Remote-Benutzer, bevor Sie die AAA-Authentifizierung konfigurieren.

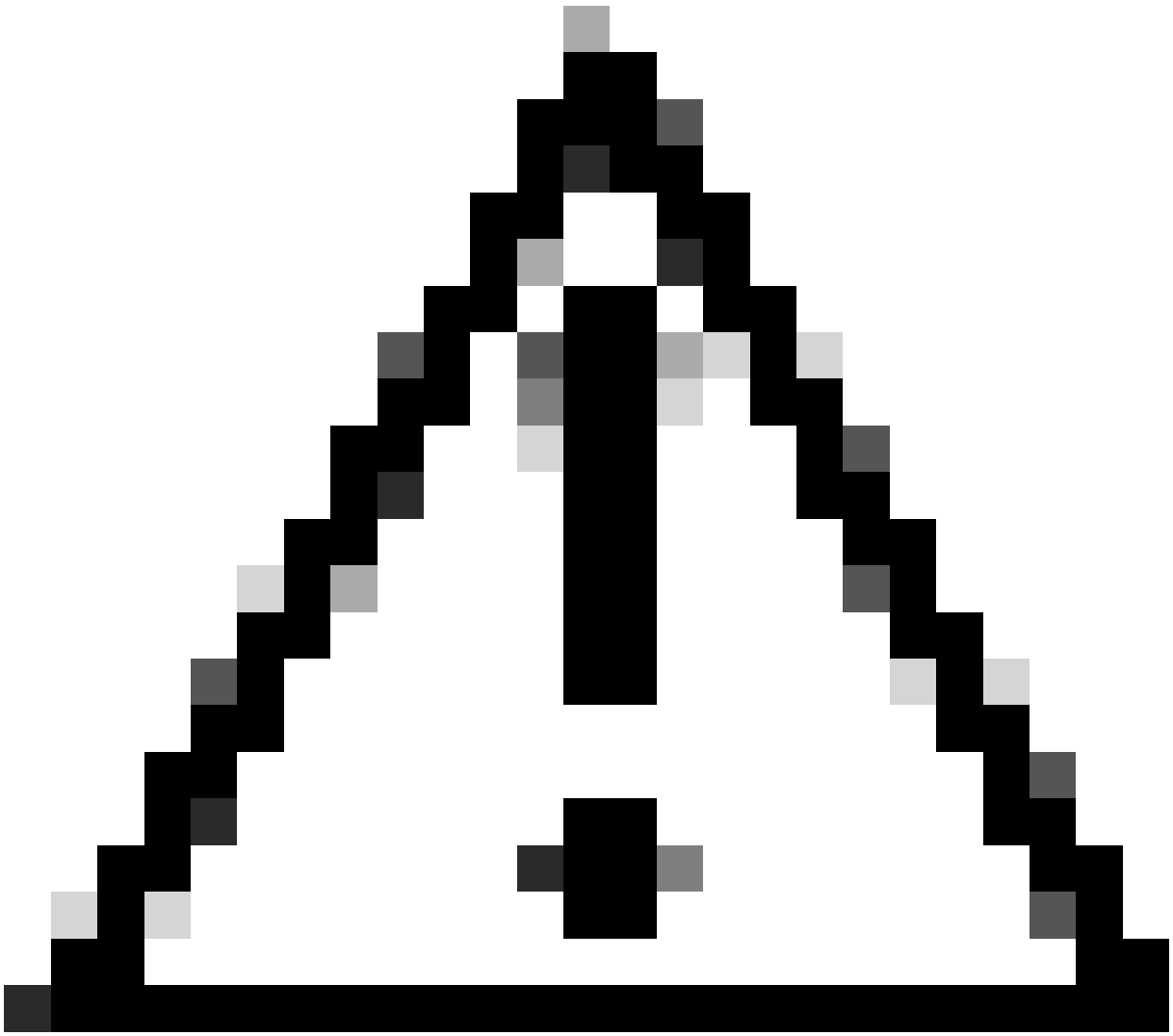
<#root>

POD2IPN2#

test aaa group tacacs2

user has been authenticated
POD2IPN2#

AAA-Konfiguration



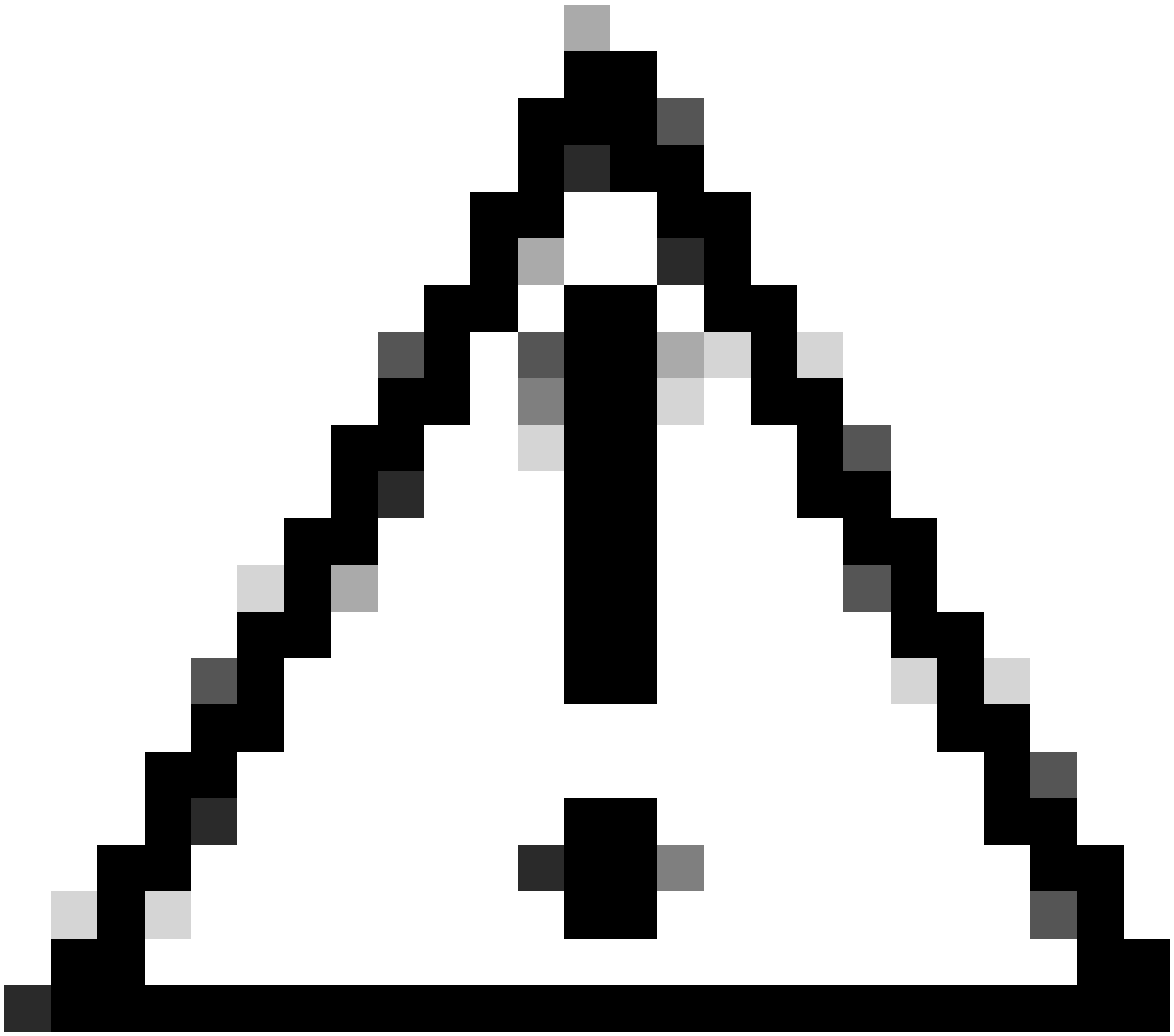
Vorsicht: Stellen Sie sicher, dass die Remote-Benutzerauthentifizierung erfolgreich ist, bevor Sie mit den AAA-Konfigurationen fortfahren.

Schritt 1: Konfigurieren der AAA-Remote-Authentifizierung.

<#root>

```
POD2IPN2(config)#
aaa authentication login default group tacacs2
```

Schritt 2: Konfigurieren Sie die AAA-Remote-Autorisierung nach dem Testen des Befehls.



Vorsicht: Stellen Sie sicher, dass der Autorisierungsstatus "AAA_AUTHOR_STATUS_PASS_ADD" lautet.

<#root>

POD2IPN2#

test aa authorization command-type config-commands default user

command "feature bgp"

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

Schritt 3: Konfigurieren des AAA-Befehls und der Konfigurationsbefehl-Autorisierung

<#root>

POD2IPN2(config)#

aaa authorization config-commands default group tacacs2 local

POD2IPN2(config)#

aaa authorization commands default group tacacs2 local

Testen und Problembehebung für den Benutzerzugriff für NX-OS

Verifizierung

Die Konfiguration der Geräteadministration für Cisco NX-OS ist abgeschlossen. Validieren Sie die Konfiguration.

Schritt 1: SSH und Anmeldung bei den NX-OS-Geräten als verschiedene Rollen

Schritt 2: Überprüfen Sie auf der Befehlszeilenschnittstelle des Geräts, ob der Benutzer Zugriff auf die richtigen Befehle hat. Beispielsweise muss ein Helpdesk-Benutzer in der Lage sein, einen Ping an eine reguläre IP-Adresse zu senden (z. B. 10.225.253.129), ihm jedoch die Anzeige der aktuellen Konfiguration verweigert wird.

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

```
64 bytes from 10.225.253.129: icmp_seq=4 ttl=254 time=0.712 ms

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

Fehlerbehebung

NX-OS-Konfigurationsprüfung

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

Verwenden Sie diese Befehle, um die Benutzerverbindungen und Rollen anzuzeigen.

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

Dies sind nützliche Fehlerbehebungen für TACACS+:

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

```
2016 Jan 11 03:03:08.655054 TACACS[6288]:  num_inet_addrs: 1 first s_addr: -1268514550 10.100.1.10 s6_a
2016 Jan 11 03:03:08.655065 TACACS[6288]:  non_blocking_connect(259):interface ip_type: IPV4
2016 Jan 11 03:03:08.656023 TACACS[6288]:  non_blocking_connect(369): Proceeding with bind
2016 Jan 11 03:03:08.656216 TACACS[6288]:  non_blocking_connect(388): setsockopt success error:22
2016 Jan 11 03:03:08.656694 TACACS[6288]:  non_blocking_connect(489): connect() is in-progress for serv
2016 Jan 11 03:03:08.679815 TACACS[6288]:  tplus_decode_authen_response: copying hostname into context
```

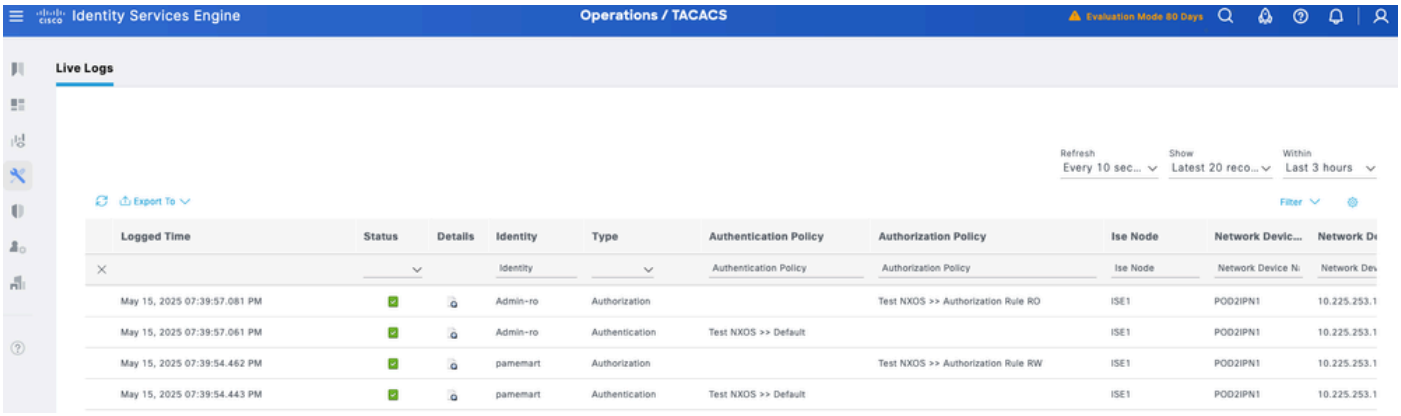
SSL-Debugging aktivieren.

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

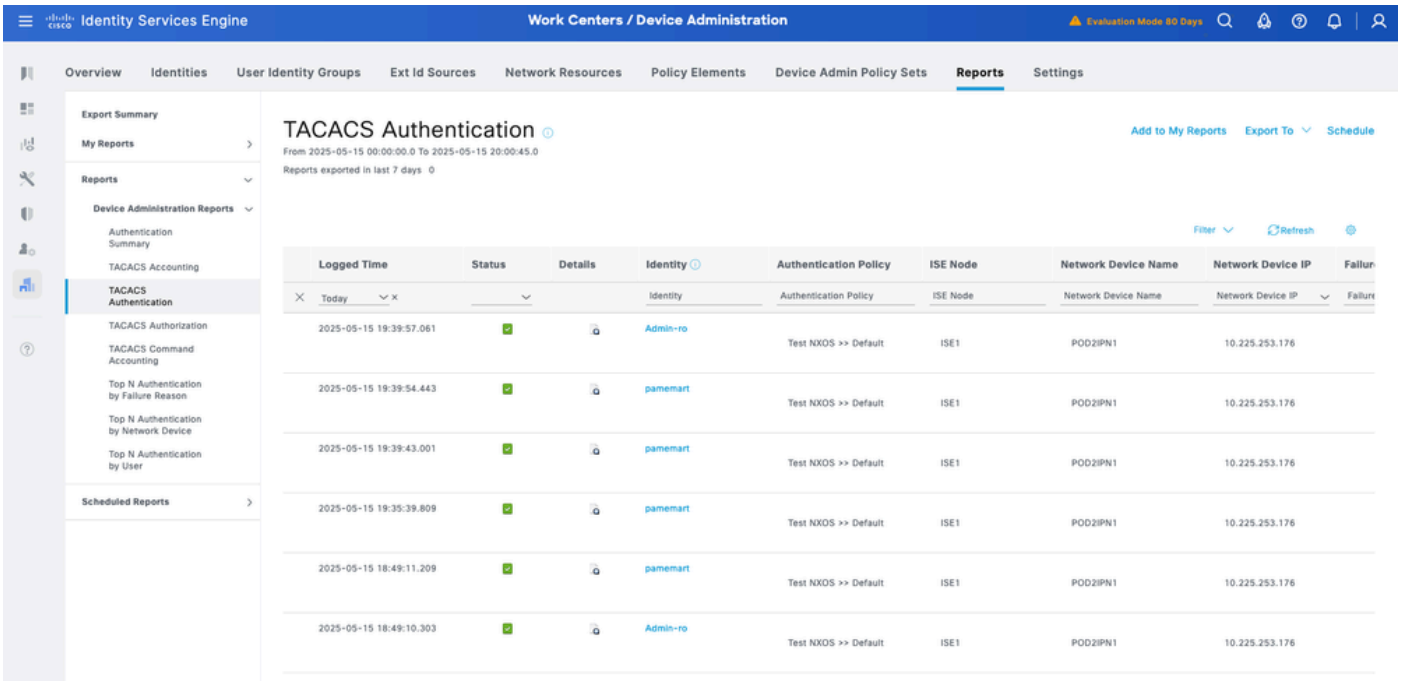
Inhalt der Debugdatei anzeigen.

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

Navigieren Sie in der ISE-GUI zu Operations > TACACS Livelog. Alle TACACS-Authentifizierungs- und Autorisierungsanforderungen werden hier erfasst, und die Schaltfläche mit den Details liefert detaillierte Informationen darüber, warum eine bestimmte Transaktion erfolgreich war bzw. fehlgeschlagen ist.



Für historische Berichte: Navigieren Sie zu Work Centers > Device Administration > Reports > Device Administration, um die Berichte zur Authentifizierung, Autorisierung und Abrechnung abzurufen.


Identity Services Engine
Work Centers / Device Administration
Evaluation Mode 80 Days
Overview
Identities
User Identity Groups
Ext Id Sources
Network Resources
Policy Elements
Device Admin Policy Sets
Reports
Settings
Export Summary
My Reports
Reports
Device Administration Reports
Authentication Summary
TACACS Accounting
TACACS Authentication
TACACS Authorization
TACACS Command Accounting
Top N Authentication by Failure Reason
Top N Authentication by Network Device
Top N Authentication by User
Scheduled Reports
TACACS Authentication
From 2025-05-15 00:00:00.0 To 2025-05-15 20:00:45.0
Reports exported in last 7 days 0
Add to My Reports
Export To
Schedule
Filter
Refresh
Logged Time
Status
Details
Identity
Authentication Policy
ISE Node
Network Device Name
Network Device IP
Today
Identity
Authentication Policy
ISE Node
Network Device Name
Network Device IP
2025-05-15 19:39:57.061
Admin-ro
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176
2025-05-15 19:39:54.443
pamemart
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176
2025-05-15 19:39:43.001
pamemart
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176
2025-05-15 19:35:39.809
pamemart
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176
2025-05-15 18:49:11.209
pamemart
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176
2025-05-15 18:49:10.303
Admin-ro
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176

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.