Konfigurieren von Catalyst Center External Authentication TACACS mit ISE

Inhalt

- Einleitung
- Voraussetzungen
  - Anforderungen
  - Verwendete Komponenten
- Hintergrundinformationen
- Konfigurieren
  - Cisco Identity Services Engine (ISE)
    - Lizenzierung und Aktivierung der TACACS+ Services
    - Administrator-Benutzer erstellen und Netzwerkgerät hinzufügen
    - TACACS+-Profil konfigurieren
    - Konfigurieren von TACACS+-Richtlinien
  - Cisco Catalyst Center
    - Konfigurieren des ISE-/AAA-Servers
    - Aktivieren und Konfigurieren der externen Authentifizierung
- Überprüfung
- Fehlerbehebung
  - 1. Attributfehlkonfiguration
  - 2. Nicht übereinstimmender gemeinsamer geheimer Schlüssel

Einleitung

In diesem Dokument werden die erforderlichen Schritte zur Integration der Cisco Identity Services Engine in Catalyst Center zur Aktivierung der TACACS+-Authentifizierung beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Administratorzugriff auf die Cisco ISE und Cisco Catalyst Center.
- Grundlegendes Verständnis von AAA-Konzepten (Authentifizierung, Autorisierung und Abrechnung)
- Praktische Kenntnisse des TACACS+-Protokolls.
- Netzwerkverbindungen zwischen Catalyst Center und dem ISE-Server.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Hardware- und Softwareversionen:

- Cisco Catalyst Center Version 2.3.7.x
- Cisco Identity Services Engine (ISE) Version 3.x (oder höher)
- TACACS+-Protokoll für die externe Benutzerauthentifizierung

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.

Hintergrundinformationen

Diese Integration ermöglicht externen Benutzern die Anmeldung bei Catalyst Center für Administratorzugriff und -management.

Konfigurieren

Cisco Identity Services Engine (ISE)

Lizenzierung und Aktivierung der TACACS+ Services

Bevor Sie mit der TACACS+-Konfiguration in der ISE beginnen, müssen Sie bestätigen, dass die richtige Lizenz installiert und die Funktion aktiviert ist.

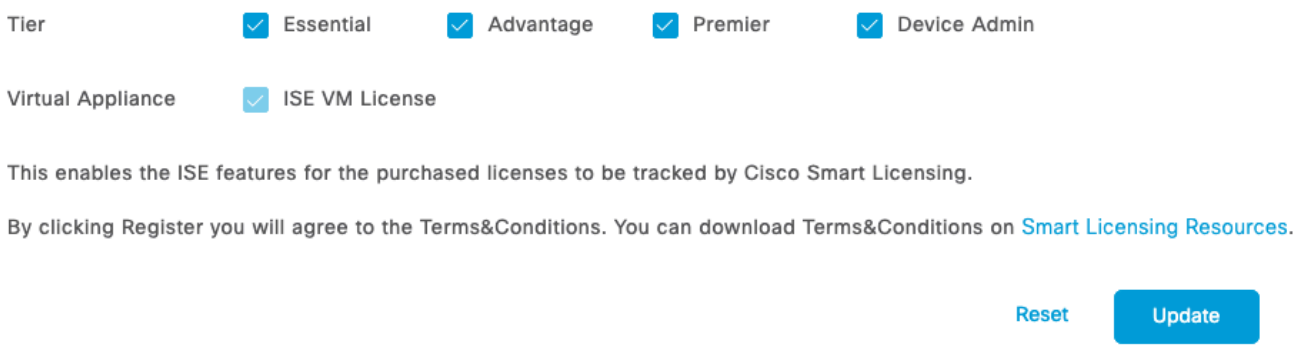
1. Vergewissern Sie sich, dass Sie die PID-Lizenz L-ISE-TACACS-ND= im Portal von Cisco Smart Software Manager oder Cisco License Central haben.

Aktivieren Sie die Geräteadministration im ISE-Lizenzportal.

- Die Geräteadministratorlizenz (PID: L-ISE-TACACS-ND=) aktiviert TACACS+-Dienste auf einem Policy Service Node (PSN).
- Navigieren Sie zu:

  Administration > System > Lizenzierung

- Aktivieren Sie unter den Tier-Optionen das Kontrollkästchen "Device Admin".



Geräte-Administrator

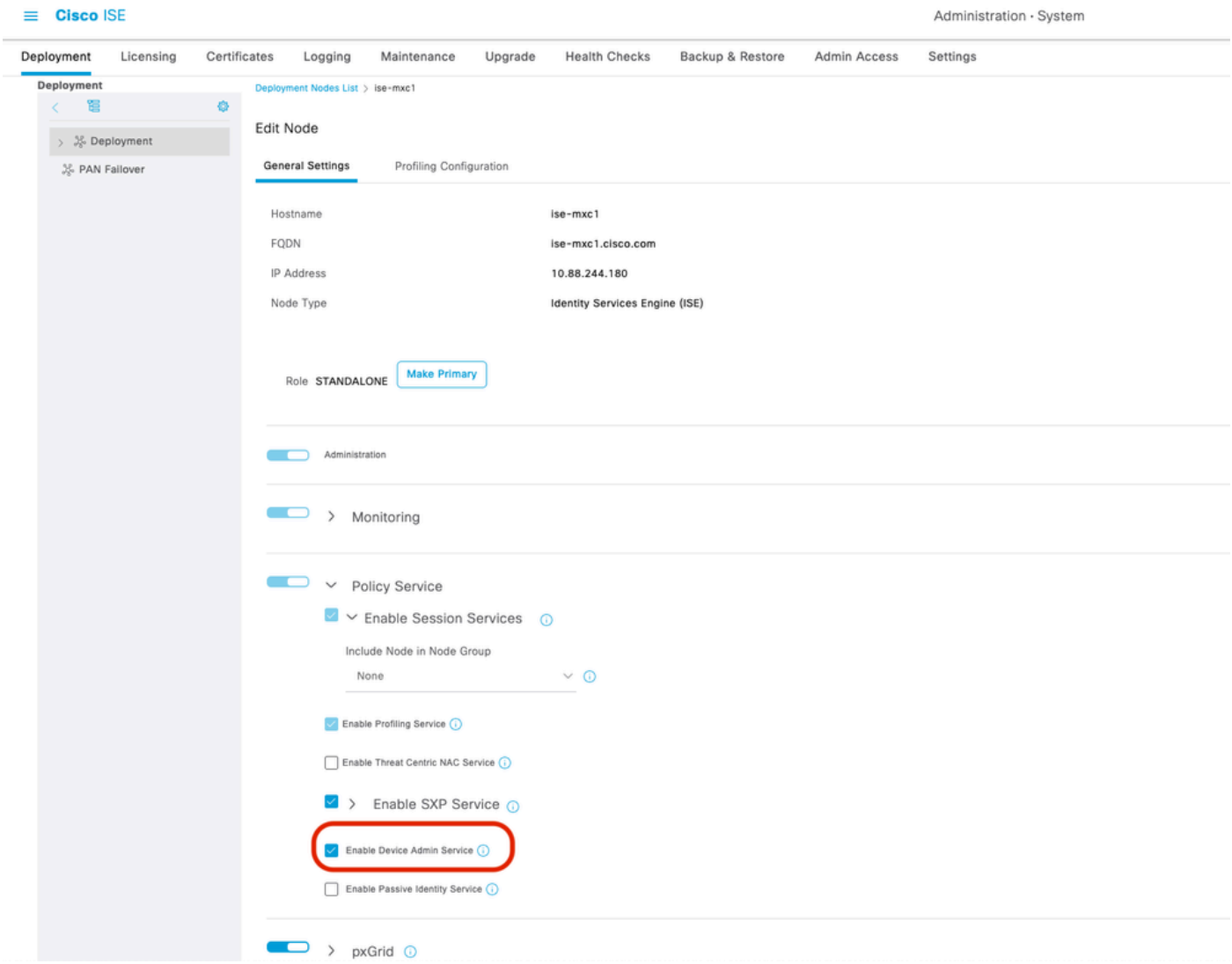
Administrator für Lizenzgerät

3. Aktivieren Sie den Geräteverwaltungsdienst auf dem ISE-Knoten, der den TACACS+-Dienst ausführt.

- Navigieren Sie zu:

  Administration > System > Bereitstellung > Knoten auswählen

- Aktivieren Sie die Option Enable Device Admin Service.



Geräteverwaltungsdienst aktivieren

Administrator-Benutzer erstellen und Netzwerkgerät hinzufügen

1. Erstellen Sie den Administrator-Benutzer.

- Dieses Benutzerkonto wird für die Anmeldung bei der Catalyst Center-Benutzeroberfläche mittels ISE-Authentifizierung verwendet.
- Navigieren Sie zu:

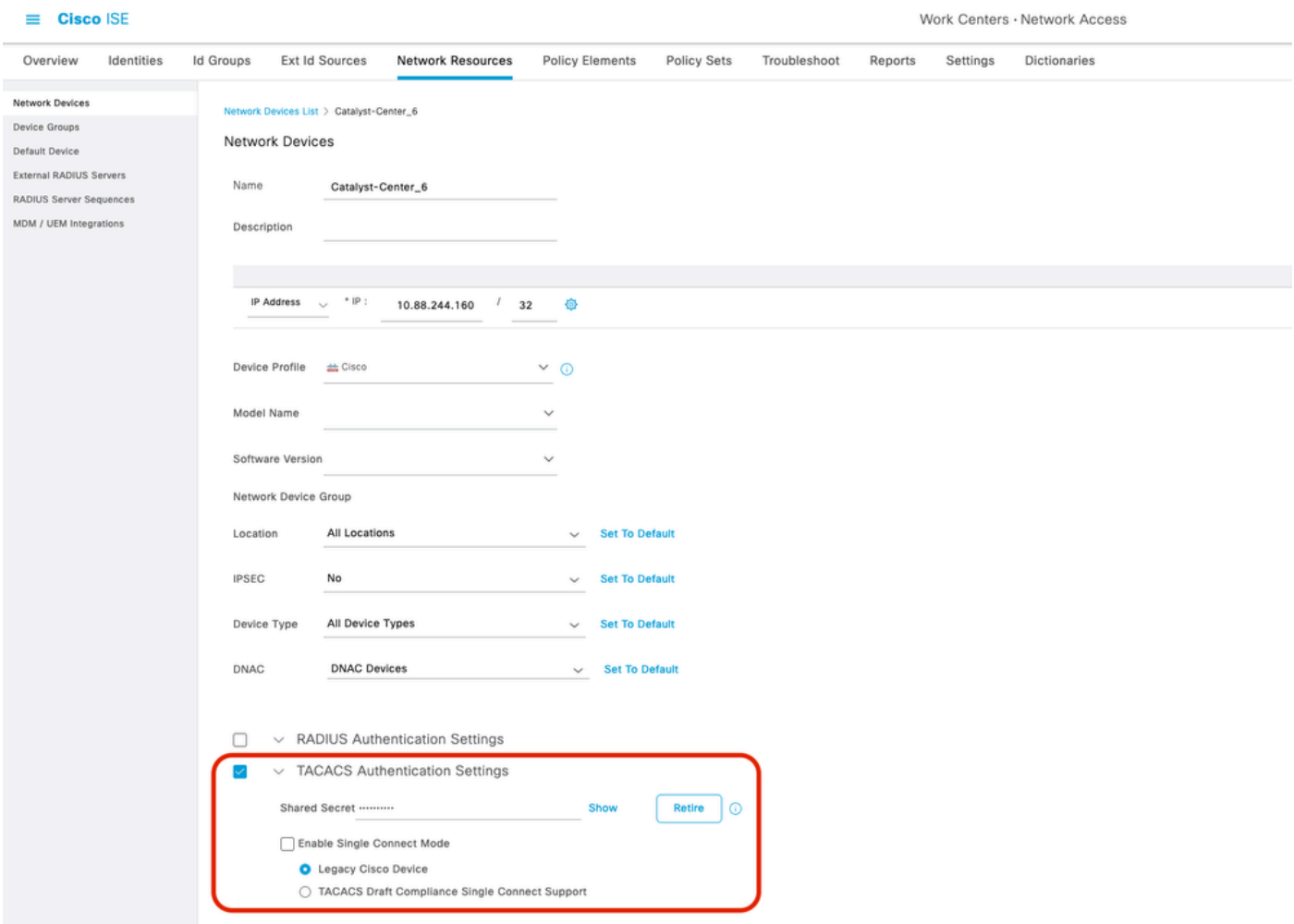
  Work Center > Netzwerkzugriff > Identitäten > Netzwerkzugriffsbenutzer
- Fügen Sie einen neuen Benutzer hinzu (z. B. catc-user).
- Wenn der Benutzer bereits vorhanden ist, fahren Sie mit dem nächsten Schritt fort.

2. Erstellen Sie das Netzwerkgerät.

- Navigieren Sie zu:

  Work Center > Netzwerkzugriff > Identitäten > Netzwerkressource

- Fügen Sie die IP-Adresse von Catalyst Center hinzu, oder definieren Sie das Subnetz, in dem sich die Catalyst Center-IP befindet.
- Wenn das Gerät bereits vorhanden ist, überprüfen Sie, ob die folgenden Parameter vorhanden sind:
    - Die TACACS-Authentifizierungseinstellungen sind aktiviert.
    - Der gemeinsame geheime Schlüssel ist konfiguriert und bekannt (speichern Sie diesen Wert, wie er später in Catalyst Center erforderlich ist).



TACACS-Authentifizierungseinstellungen

TACACS+-Profil konfigurieren

1. Erstellen Sie ein neues TACACS+-Profil.

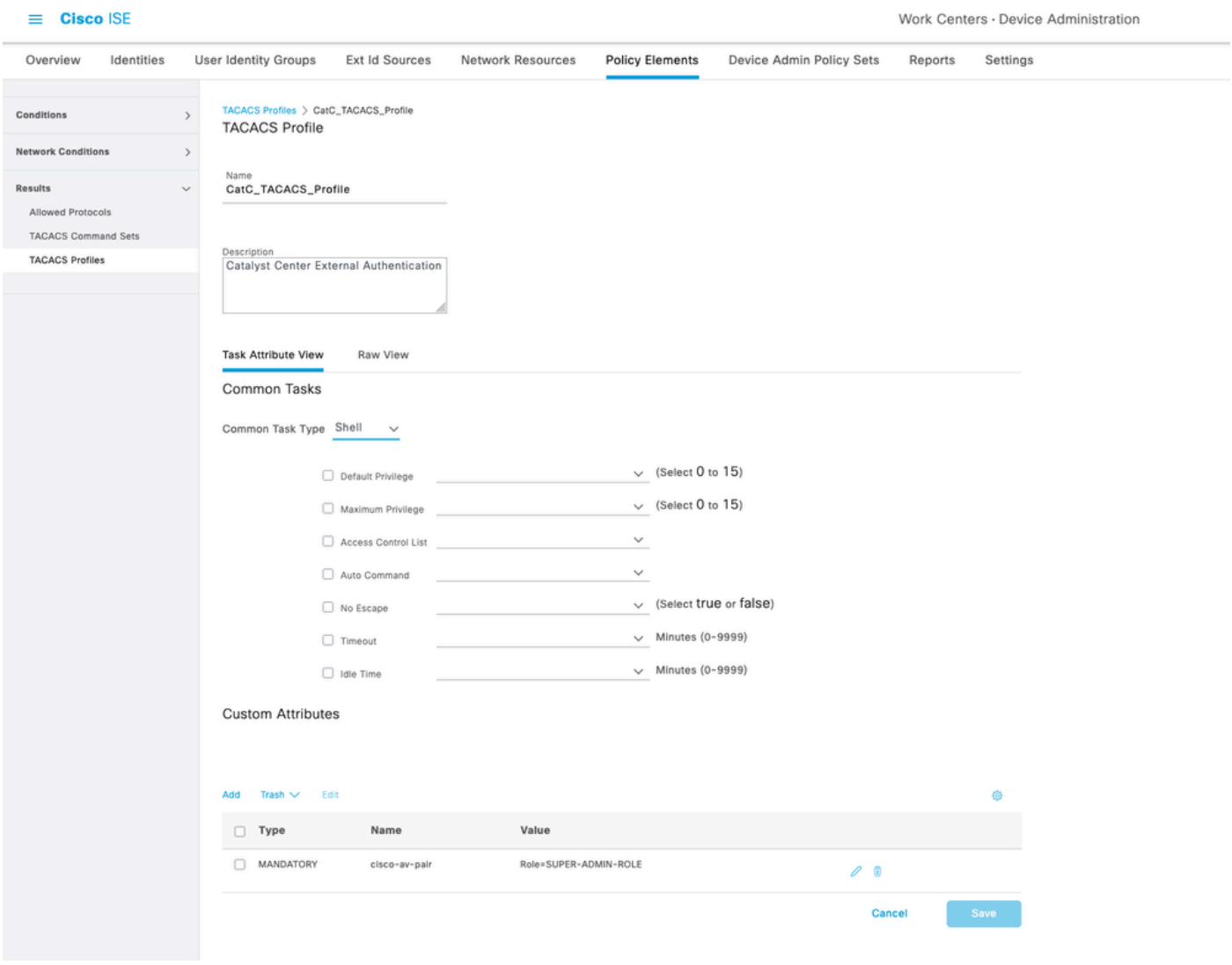
- Navigieren Sie zu:

  Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles

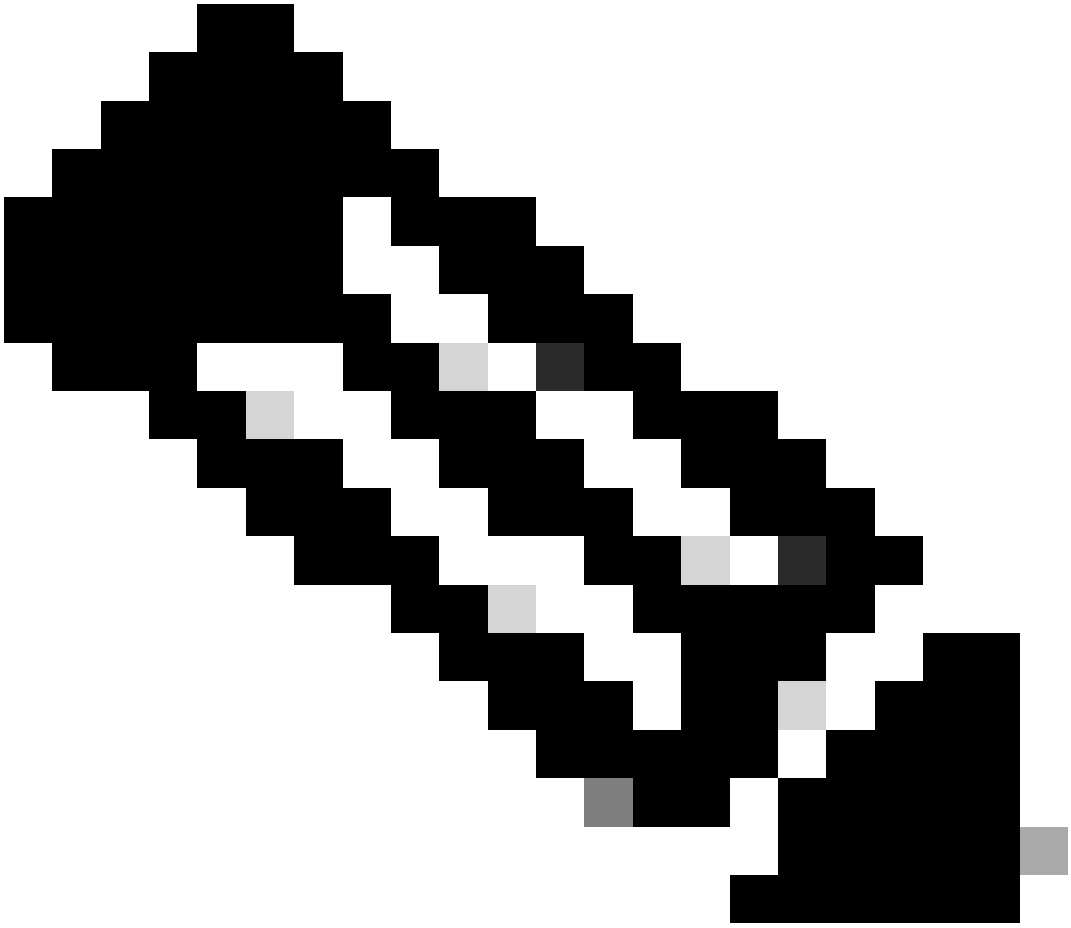
- Fügen Sie einen Profilnamen hinzu.
- Fügen Sie ein benutzerdefiniertes Attribut wie folgt hinzu:

- Typ: Mandatory (Obligatorisch)
- Name: cisco-av-pair
- Wert: Role=SUPER-ADMIN-ROLE

- Speichern Sie das Profil.



TACACS+-Profil



Anmerkung: Cisco Catalyst Center unterstützt externe AAA-Server (Authentication, Authorization and Accounting) für die Zugriffskontrolle. Wenn Sie einen externen Server für die Authentifizierung und Autorisierung externer Benutzer verwenden, können Sie die externe Authentifizierung im Cisco Catalyst Center aktivieren. Die AAA-Standardattributeinstellung stimmt mit dem Standardbenutzerprofilattribut überein.

Der AAA-Standardattributwert für das TACACS-Protokoll ist cisco-av-pair.

Der standardmäßige AAA-Attributwert des RADIUS-Protokolls ist Cisco-AVPair.

Eine Änderung ist nur erforderlich, wenn der AAA-Server über ein benutzerdefiniertes Attribut im Benutzerprofil verfügt. Auf dem AAA-Server lautet das Format des AAA-Attributwerts Role=role1. Auf dem Cisco Identity Services Engine (Cisco ISE)-Server kann der Benutzer beim Konfigurieren des RADIUS- oder TACACS-Profils cisco av-pair als AAA-Attribut auswählen oder eingeben.

Sie können das AAA-Attribut beispielsweise manuell als cisco-av-pair=Role=SUPER-ADMIN-ROLE oder Cisco-AVPair=Role=SUPER-ADMIN-ROLE auswählen und

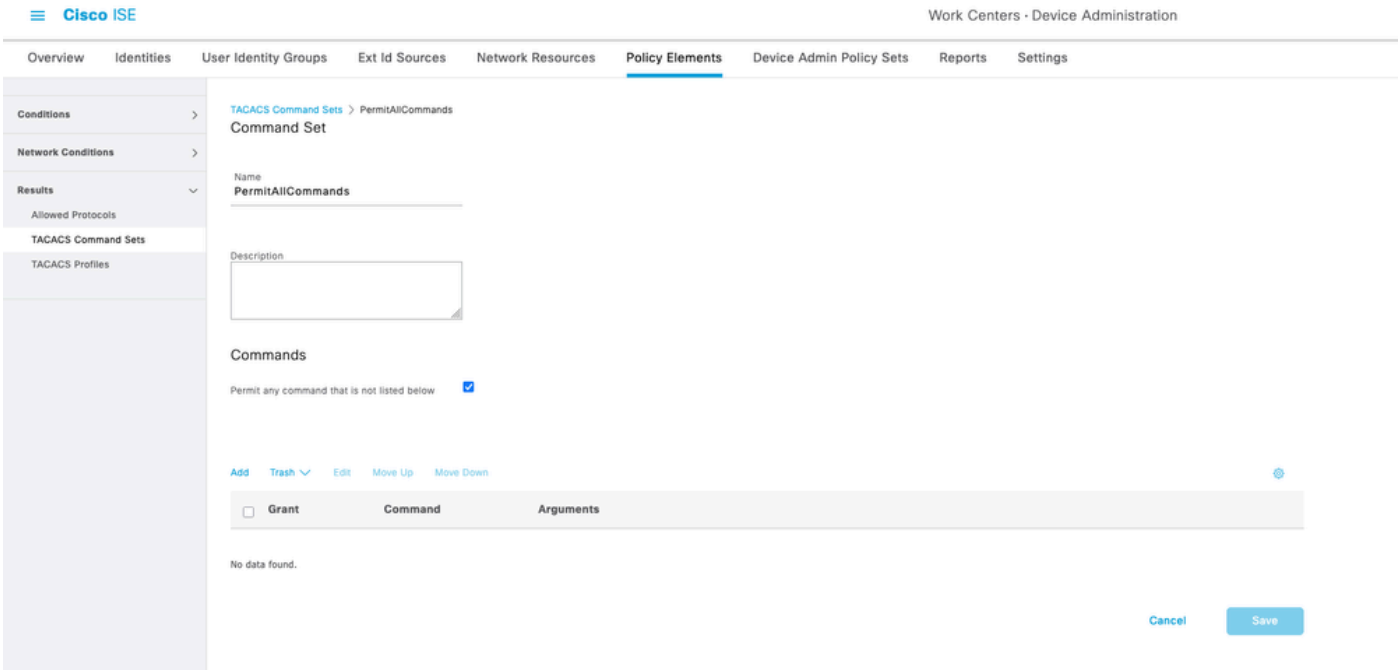
konfigurieren.

2. Erstellen Sie einen TACACS+-Befehlssatz.

- Navigieren Sie zu:

Work Centers > Device Administration > Policy Elements > Results > TACACS Command Sets

- Fügen Sie einen Namen hinzu.
- Aktivieren Sie die Option Befehle zulassen, die unten nicht aufgeführt sind.
- Speichern Sie den Befehlssatz.



TACACS-Befehlssätze

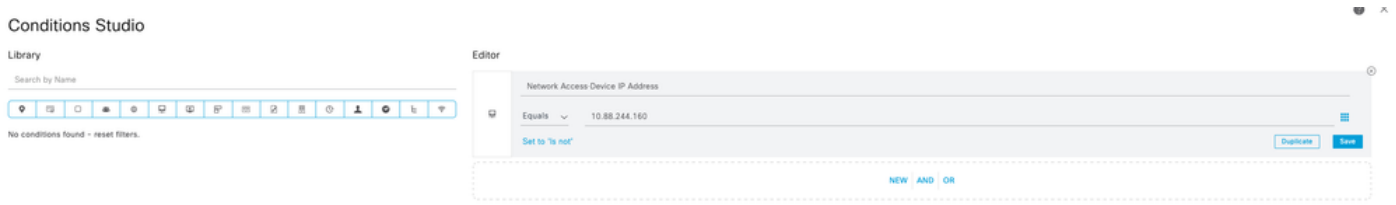
Konfigurieren von TACACS+-Richtlinien

1. Erstellen Sie einen neuen TACACS+-Richtliniensatz.

- Navigieren Sie zu:

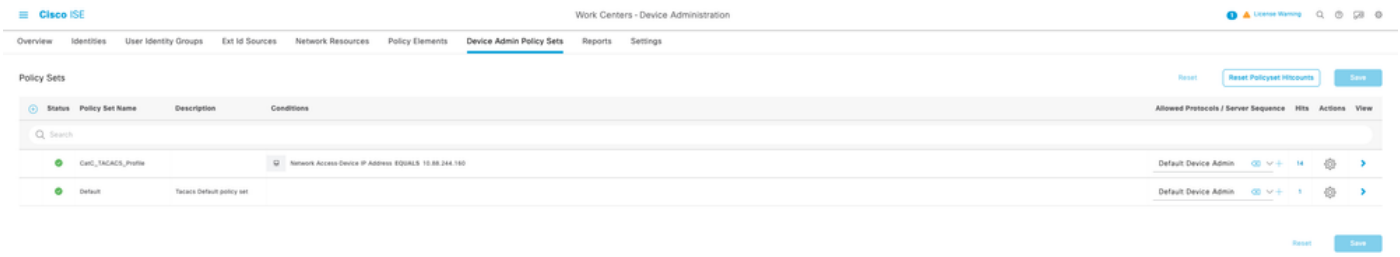
Work Centers > Device Administration > Device Admin Policy Set

- Fügen Sie einen Namen für den Policy Set hinzu.
- Konfigurieren Sie die Bedingung.
  - In diesem Beispiel entspricht die Bedingung der Catalyst Center-IP-Adresse.



Catalyst Center-IP-Adresse

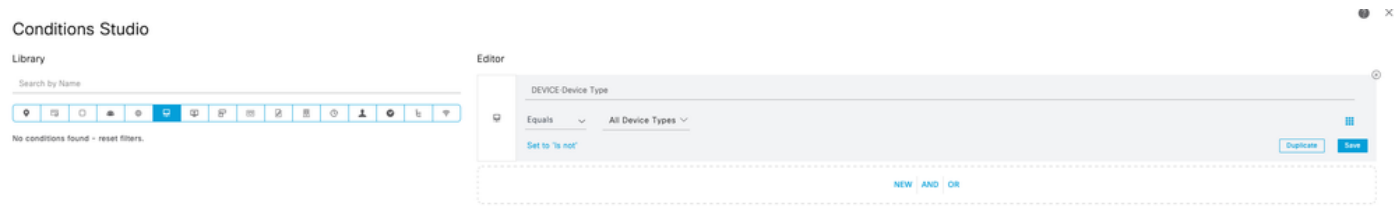
1.3 Wählen Sie auf der Registerkarte Allowed Protocols / Server Sequence (Zulässige Protokolle/Serversequenz) Default Device Admin (Standardgeräteadministrator) aus.



Standard-Geräteadministrator auswählen

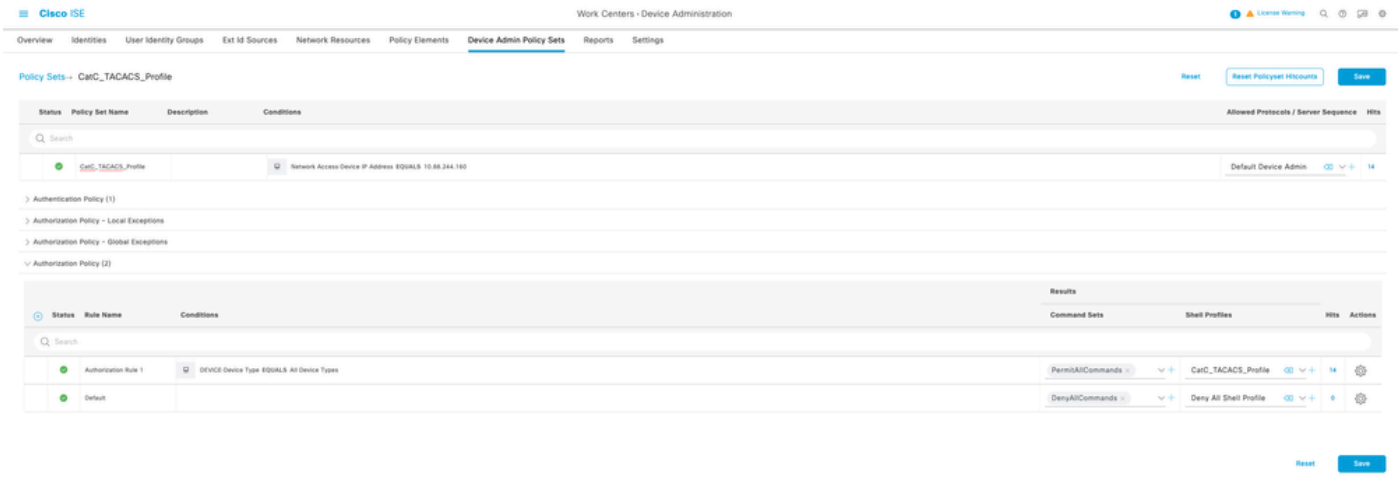
2. Konfigurieren Sie den Richtliniensatz.

- Klicken Sie auf den Pfeil (>) rechts, um den Richtliniensatz zu erweitern und zu konfigurieren.
- Fügen Sie eine neue Regel unter Autorisierungsrichtlinie hinzu.
- Konfigurieren Sie die neue Regel wie folgt:
  - Name: Geben Sie einen beschreibenden Regelnamen ein.
  - Bedingung: In diesem Beispiel stimmte die Bedingung mit Alle Gerätetypen überein.



Alle Gerätetypen

- Befehlssatz: Wählen Sie den zuvor erstellten TACACS+-Befehlssatz aus.
- Shell-Profil: Wählen Sie das zuvor erstellte TACACS+-Profil aus.



TACACS+-Befehlssatz

Cisco Catalyst Center

Konfigurieren des ISE-/AAA-Servers

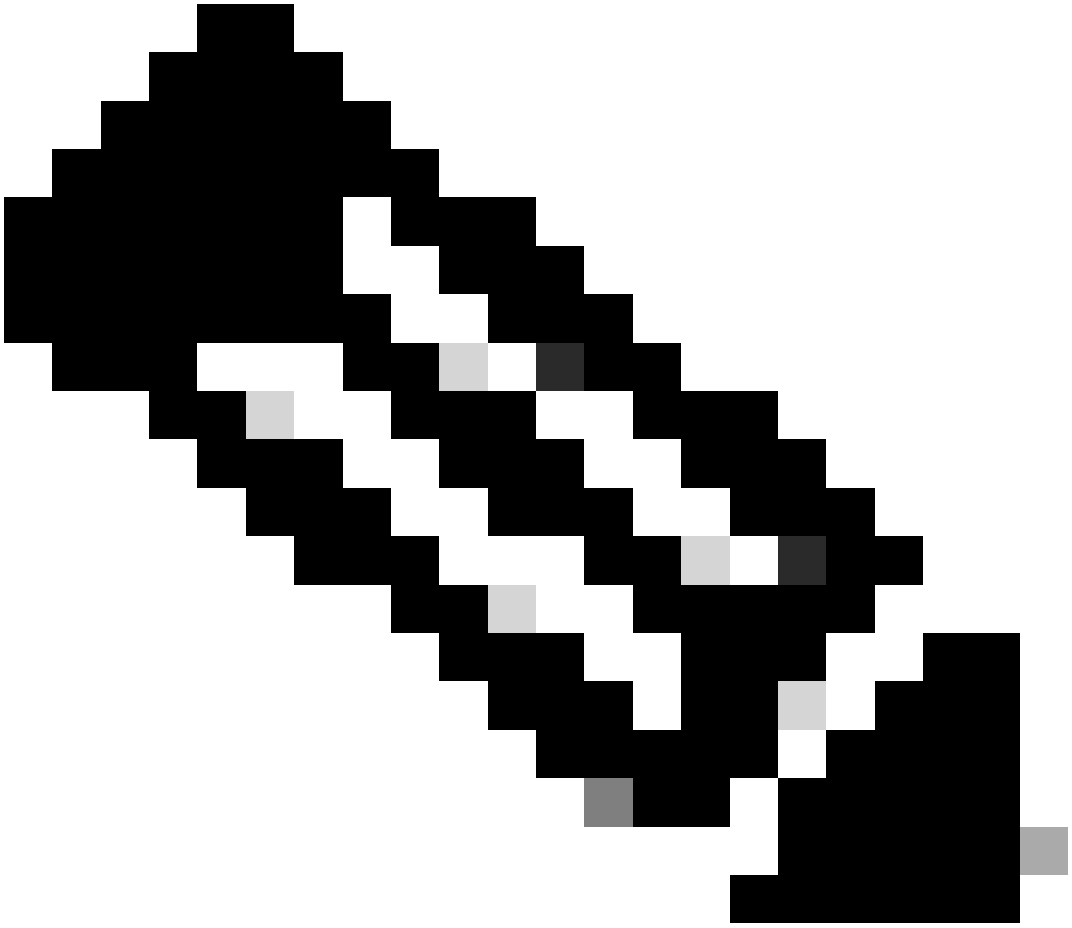
1. Melden Sie sich bei der Catalyst Center-Webschnittstelle an.

   - Navigieren Sie zu:

Hauptmenü > System > Einstellungen > Externe Dienste > Authentifizierung und Richtlinienserver

2. Fügen Sie einen neuen Server hinzu. Sie können entweder ISE oder AAA auswählen.

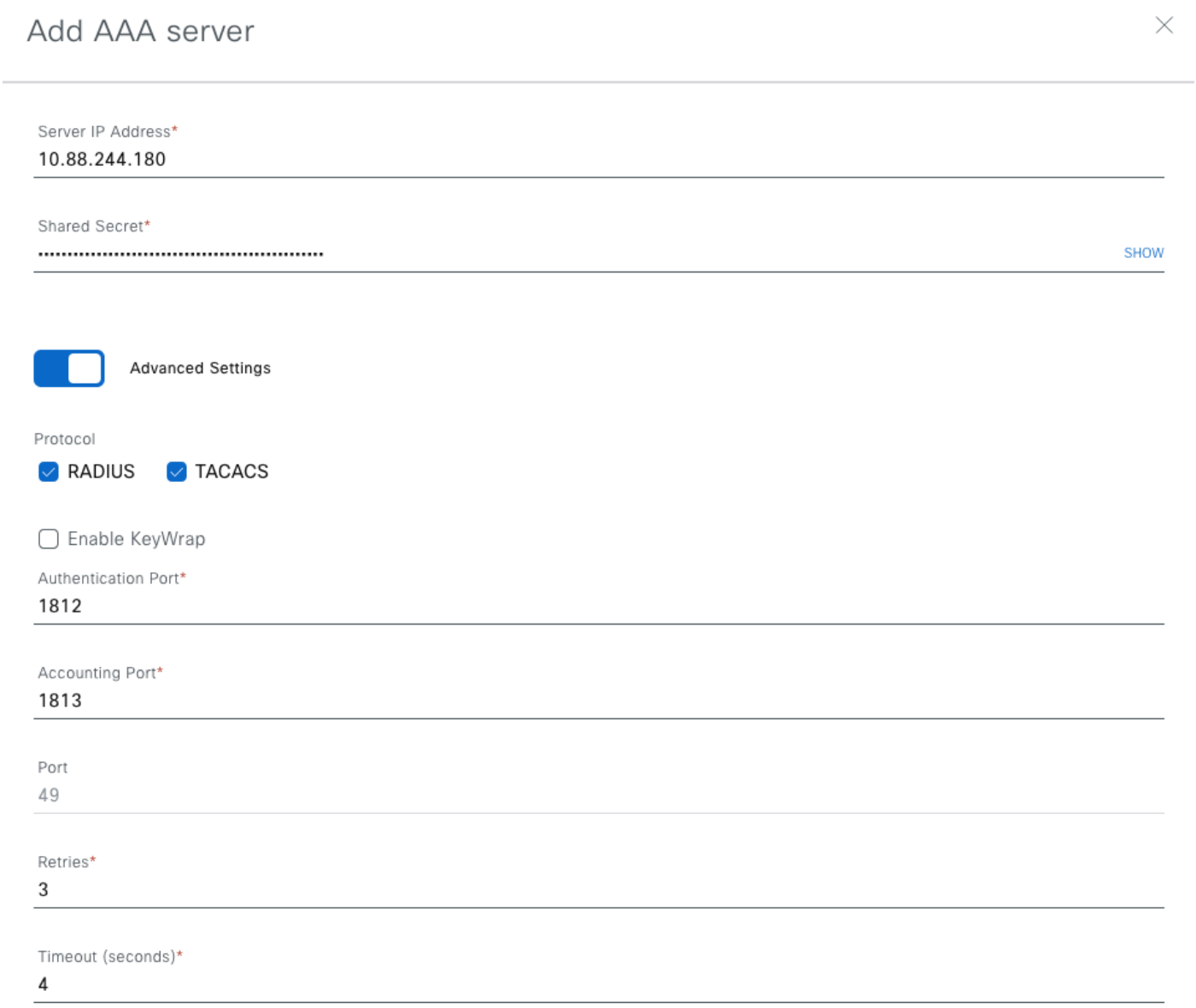
   - Für diese Demo wird die AAA-Serveroption verwendet.



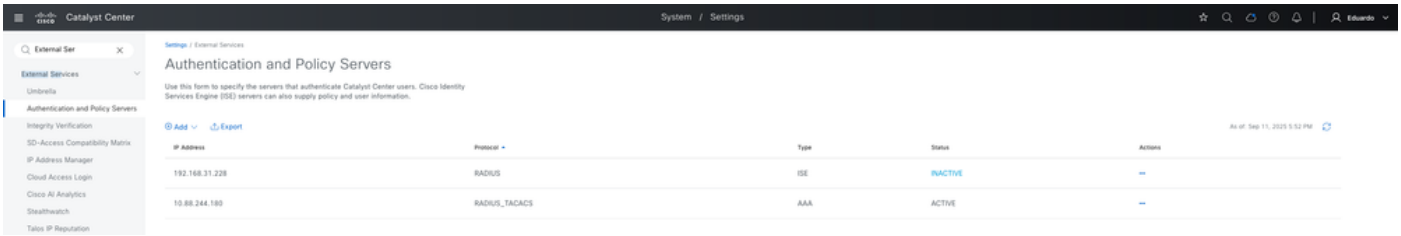
Anmerkung: In einem Catalyst Center-Cluster kann nur ein ISE-Cluster konfiguriert werden.

3. Konfigurieren Sie diese Optionen und speichern Sie dann:

- Geben Sie die IP-Adresse des AAA-Servers ein.
- Fügen Sie den gemeinsamen geheimen Schlüssel hinzu (derselbe geheime Schlüssel, der in der Cisco ISE-Netzwerkressource konfiguriert wurde).
- Erweiterte Einstellungen auf Ein umschalten.
- Aktivieren Sie die Option TACACS.



Authentifizierungs- und Richtlinienserver



Erweiterte Einstellungen

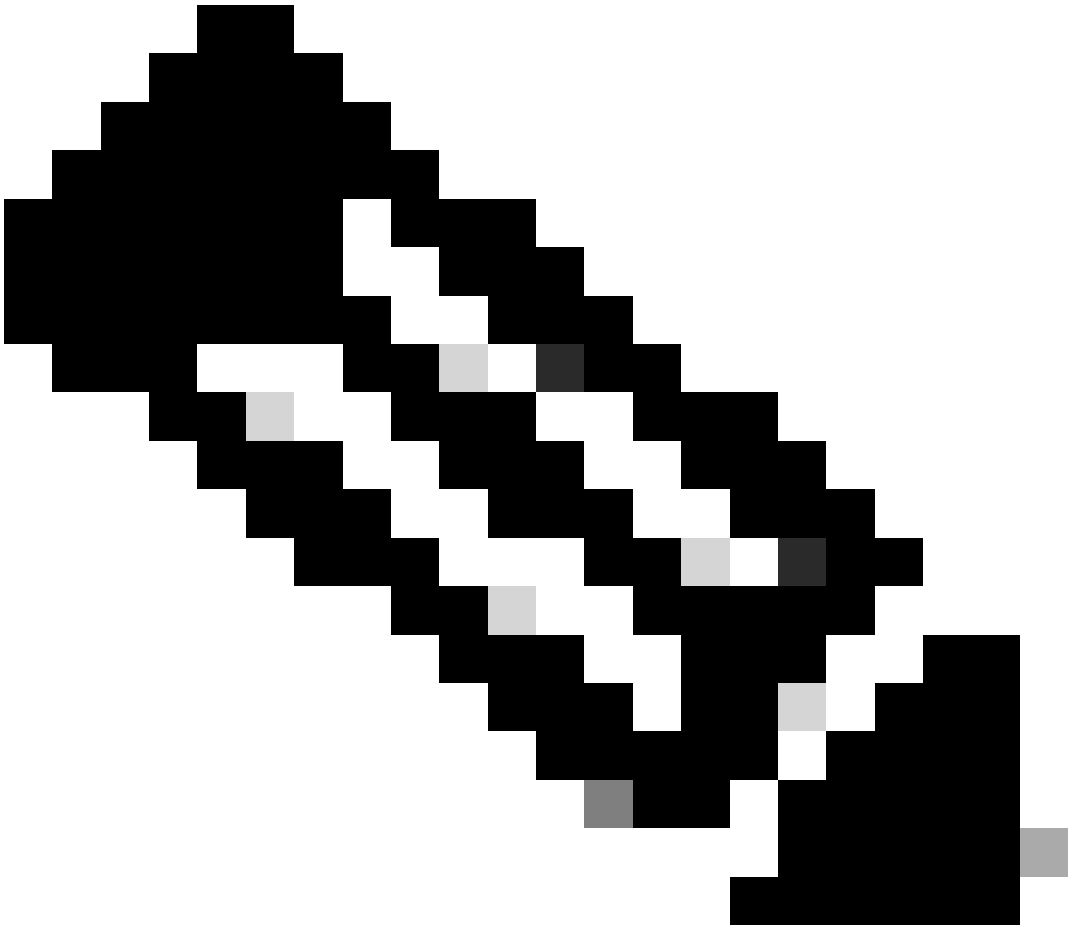
Aktivieren und Konfigurieren der externen Authentifizierung

1. Navigieren Sie zur Seite Externe Authentifizierung:

   Hauptmenü > System > Benutzer & Rolle > Externe Authentifizierung

2. Fügen Sie das AAA-Attribut cisco-av-pair hinzu, und klicken Sie auf Aktualisieren, um die

Änderungen zu speichern.



> Anmerkung: Dieser Schritt ist nicht obligatorisch, da das Standardattribut für TACACS+ bereits cisco-av-pair ist. Es wird jedoch als Best Practice erachtet, diesen Schritt explizit zu konfigurieren.

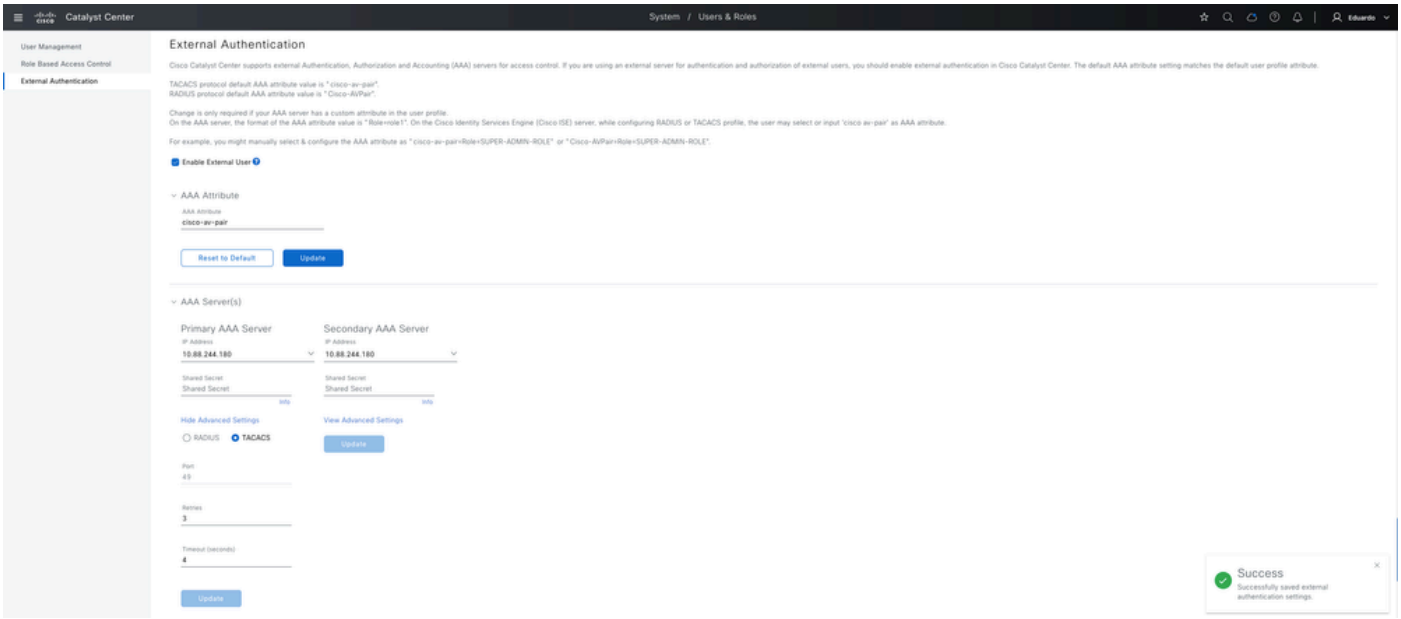
---

3. Wählen Sie unter Primary AAA Server (Primärer AAA-Server) den zuvor konfigurierten AAA-Server aus.

- Klicken Sie auf Erweiterte Einstellungen anzeigen, um weitere Optionen anzuzeigen.
- Wählen Sie die Option TACACS+ aus.
- Geben Sie den in der Netzwerkressource der Cisco ISE konfigurierten gemeinsamen geheimen Schlüssel ein.
- Klicken Sie auf Aktualisieren, um die Änderungen zu speichern.

4. Aktivieren Sie das Kontrollkästchen Externer Benutzer.

- Dadurch wird die Konfiguration automatisch gespeichert.



Externe Authentifizierung

Überprüfung

1. Öffnen Sie eine neue Browser-Sitzung, oder verwenden Sie den Inkognito-Modus, und melden Sie sich bei der Catalyst Center-Webseite mit dem in Cisco ISE konfigurierten Benutzerkonto an.

2. Bestätigen Sie im Catalyst Center, dass die Anmeldung erfolgreich war.

Anmelden Konfigurieren Catalyst Center Externe Authentifizierung TACACS mit ISE

3. Validieren Sie die Protokolle der Cisco ISE:

   Vorgänge > TACACS > Live-Protokolle

- Authentifizierungsstatus: Bestehen
- Autorisierungsstatus: Bestehen

Live-Protokolle

4. Vergleichen Sie in den Autorisierungsdetails die folgende Ausgabe:

    - Nachrichtentext: Geräteverwaltung: Sitzungsautorisierung erfolgreich
    - Alle Antwortattribute: cisco-av-pair=Role=SUPER-ADMIN-ROLE

Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

Authorization Attributes

All Request Attribues	
All Response Attribues	cisco-av-pair=Role=SUPER-ADMIN-ROLE

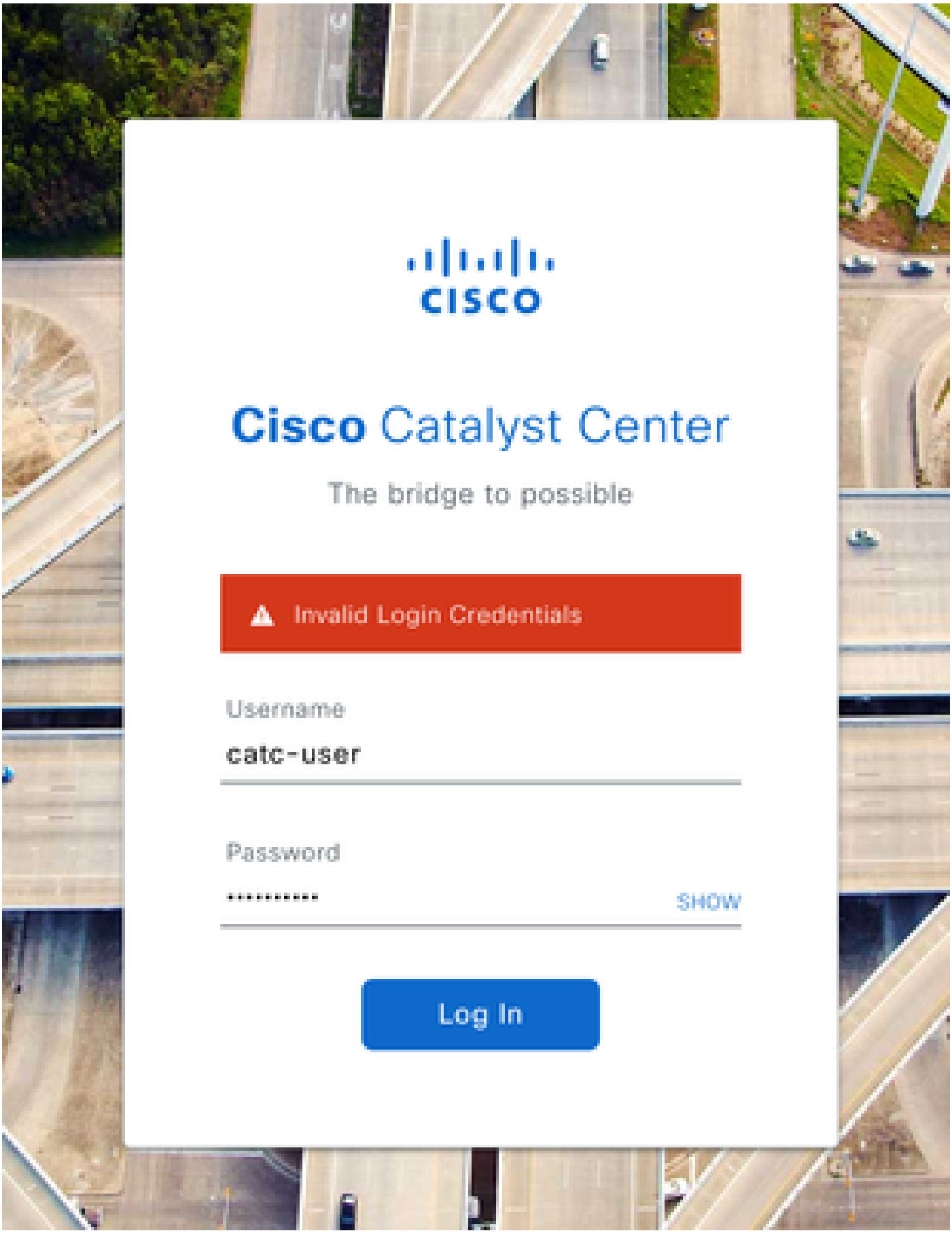
cisco-av-pair=Rolle=SUPER-ADMIN-ROLE

Fehlerbehebung

Im Folgenden finden Sie einige häufige Probleme, auf die Sie während der Integration stoßen können, und wie Sie diese identifizieren können:

1. Attributfehlkonfiguration

Symptom in Catalyst Center: Ungültige Anmeldeinformationen



Attributfehlkonfiguration

- Symptom in Cisco ISE (TACACS-Protokolle):

- Authentifizierung: Bestehen
- Autorisierung: Bestehen

Attributfehlkonfiguration

- Mögliche Ursachen:
  - Im Attributwert ist ein Leerzeichen vorhanden.

Beispiel:

Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

Authorization Attributes

All Request Attribues	
All Response Attribues	cisco-av-pair=Role=SUPER-ADMIN-ROLE

Attributfehlkonfiguration

- Das Attribut ist falsch konfiguriert, das Schlüsselwort Role= fehlt.

  Beispiel:

Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

Authorization Attributes

All Request Attribues	
All Response Attribues	cisco-av-pair=Role=SUPER-ADMIN-ROLE

Attributfehlkonfiguration

2. Nicht übereinstimmender gemeinsamer geheimer Schlüssel

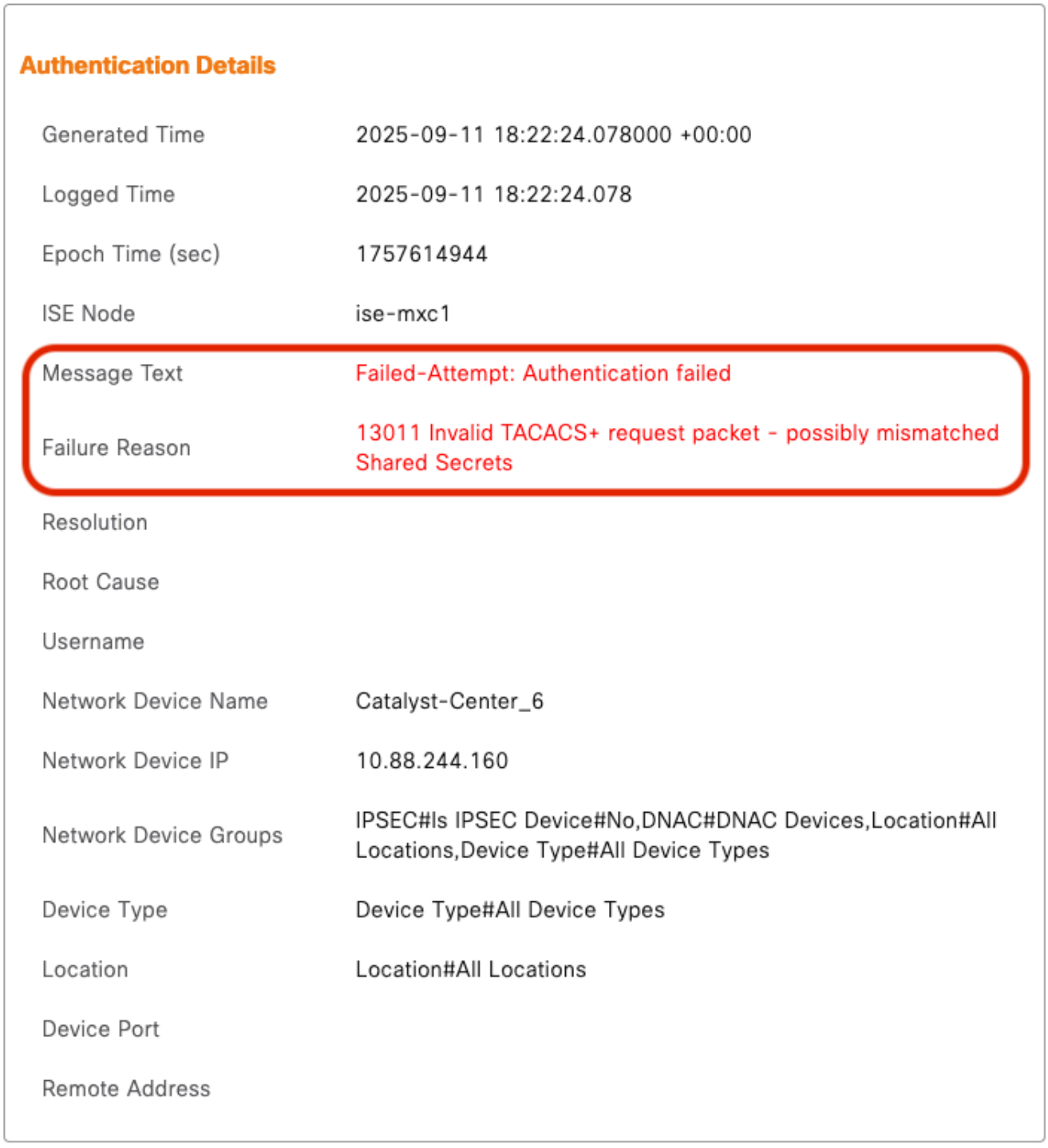
- Symptom: Authentifizierungspakete fallen zwischen Catalyst Center und der Cisco ISE aus.

- Mögliche Ursache: Der in den Netzwerkressourcen der ISE konfigurierte gemeinsame geheime Schlüssel stimmt nicht mit dem in Catalyst Center > Externe Authentifizierung konfigurierten Schlüssel überein.

So überprüfen Sie:

- Überprüfen Sie die Netzwerkressourcenkonfiguration in der ISE.
- Vergleichen Sie den gemeinsamen geheimen Schlüssel mit der Konfiguration unter Catalyst Center > External Authentication.

Beispiel:



Authentication Details

Generated Time	2025-09-11 18:22:24.078000 +00:00
Logged Time	2025-09-11 18:22:24.078
Epoch Time (sec)	1757614944
ISE Node	ise-mxc1
Message Text	Failed-Attempt: Authentication failed
Failure Reason	13011 Invalid TACACS+ request packet - possibly mismatched Shared Secrets
Resolution	
Root Cause	
Username	
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	
Remote Address	

Nicht übereinstimmender gemeinsamer Schlüssel

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.