Konfigurieren des APIC für die Geräteadministration mit ISE und TACACS+

Inhalt

Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten

Konfigurieren

- Netzwerkdiagramm
- Authentifizierungsverfahren
- APIC-Konfiguration
- ISE-Konfiguration

Überprüfung

Fehlerbehebung

Einleitung

In diesem Dokument wird das Verfahren zur Integration des APIC in die ISE für die Benutzerauthentifizierung durch den Administrator mit dem TACACS+-Protokoll beschrieben.

Voraussetzungen

Anforderungen

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

- Application Policy Infrastructure Controller (APIC)
- Identity Services Engine (ISE)
- TACACS-Protokoll

Verwendete Komponenten

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

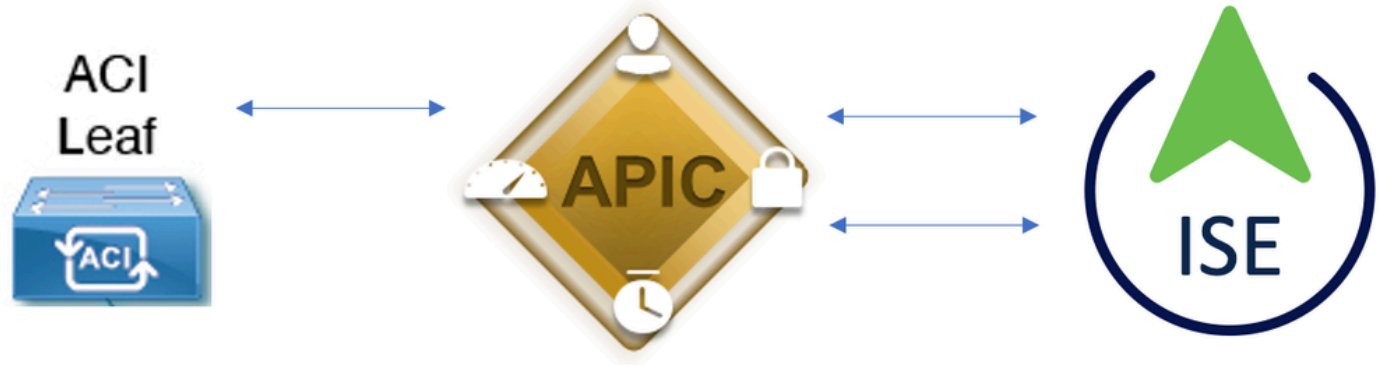
- APIC Version 4.2(7u)
- ISE Version 3.2 Patch 1

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.

Konfigurieren

Netzwerkdiagramm



Integrationsdiagramm

Authentifizierungsverfahren

Schritt 1:Melden Sie sich mit Administratoranmeldeinformationen bei der APIC-Anwendung an.

Schritt 2: Der Authentifizierungsprozess wird ausgelöst, und die ISE überprüft die Anmeldeinformationen lokal oder über Active Directory.

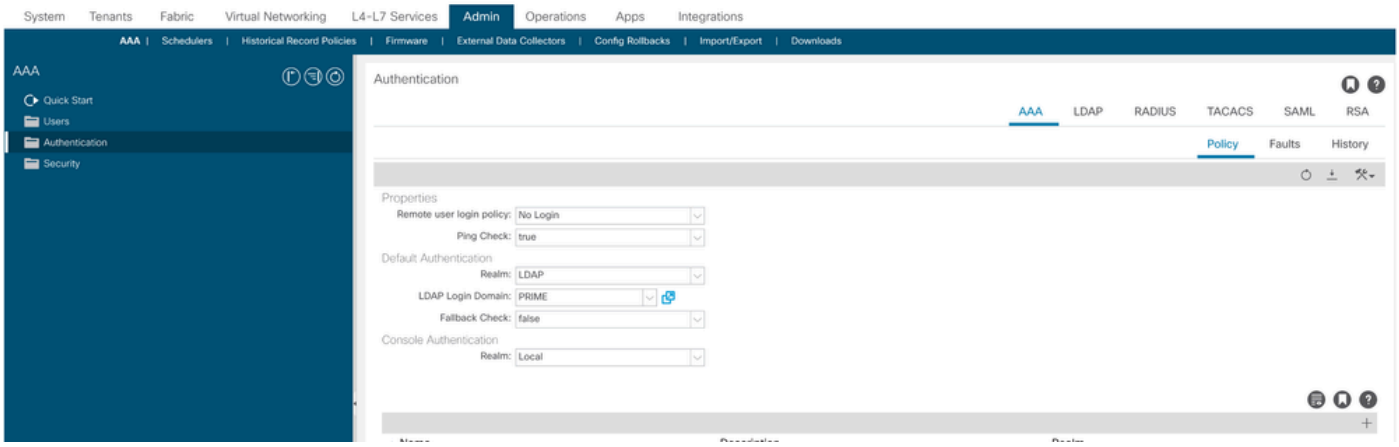
Schritt 3: Nach erfolgreicher Authentifizierung sendet die ISE ein Erlaubnispaket, um den Zugriff auf den APIC zu autorisieren.

Schritt 4: Die ISE zeigt ein erfolgreiches Authentifizierungs-Liveprotokoll an.

Anmerkung: Der APIC repliziert die TACACS+-Konfiguration auf Leaf-Switches, die Teil der Fabric sind.

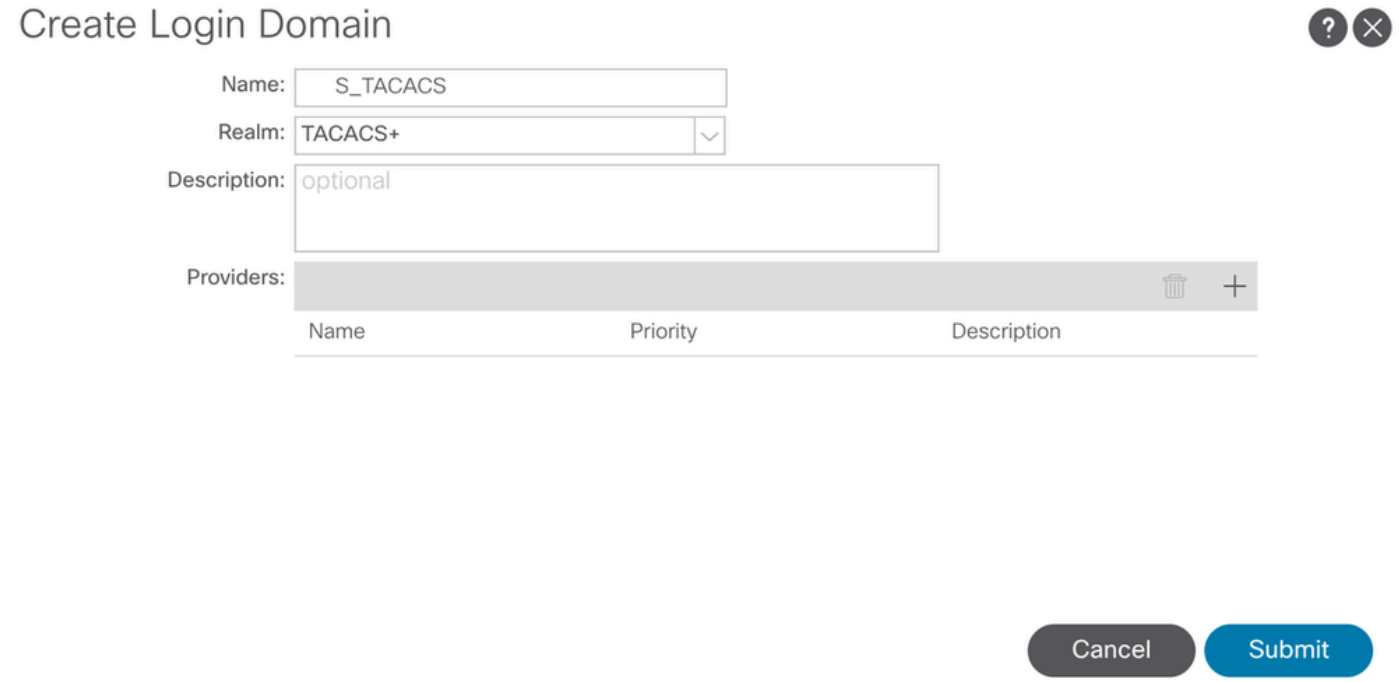
APIC-Konfiguration

Schritt 1: Navigieren Sie zuAdmin > AAA > Authentication > AAA+, und wählen Sie das Symbol aus, um eine neue Anmelde-Domäne zu erstellen.

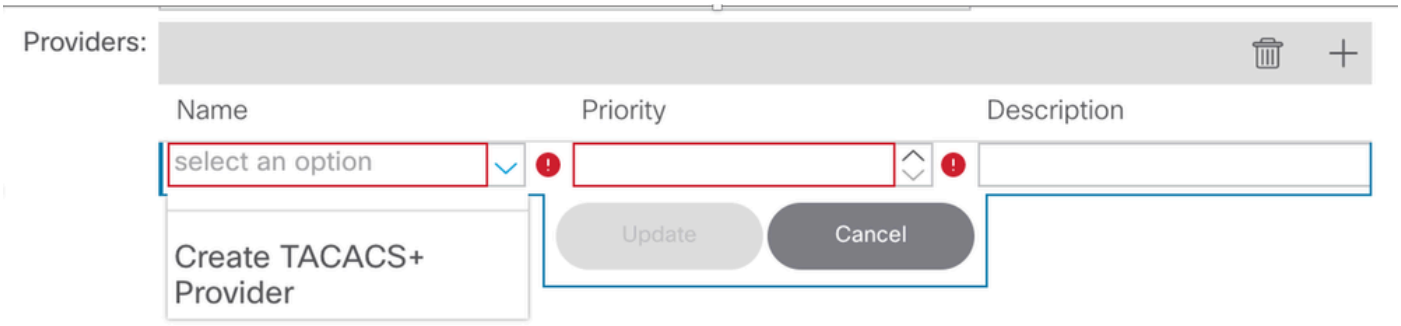


Administratorkonfiguration für APIC-Anmeldung

Schritt 2. Definieren Sie einen Namen und einen Bereich für die neue Anmeldungsdomäne und klicken Sie unter Anbieter auf, um einen neuen Anbieter zu erstellen. Klicken+Sie auf Anbieter.



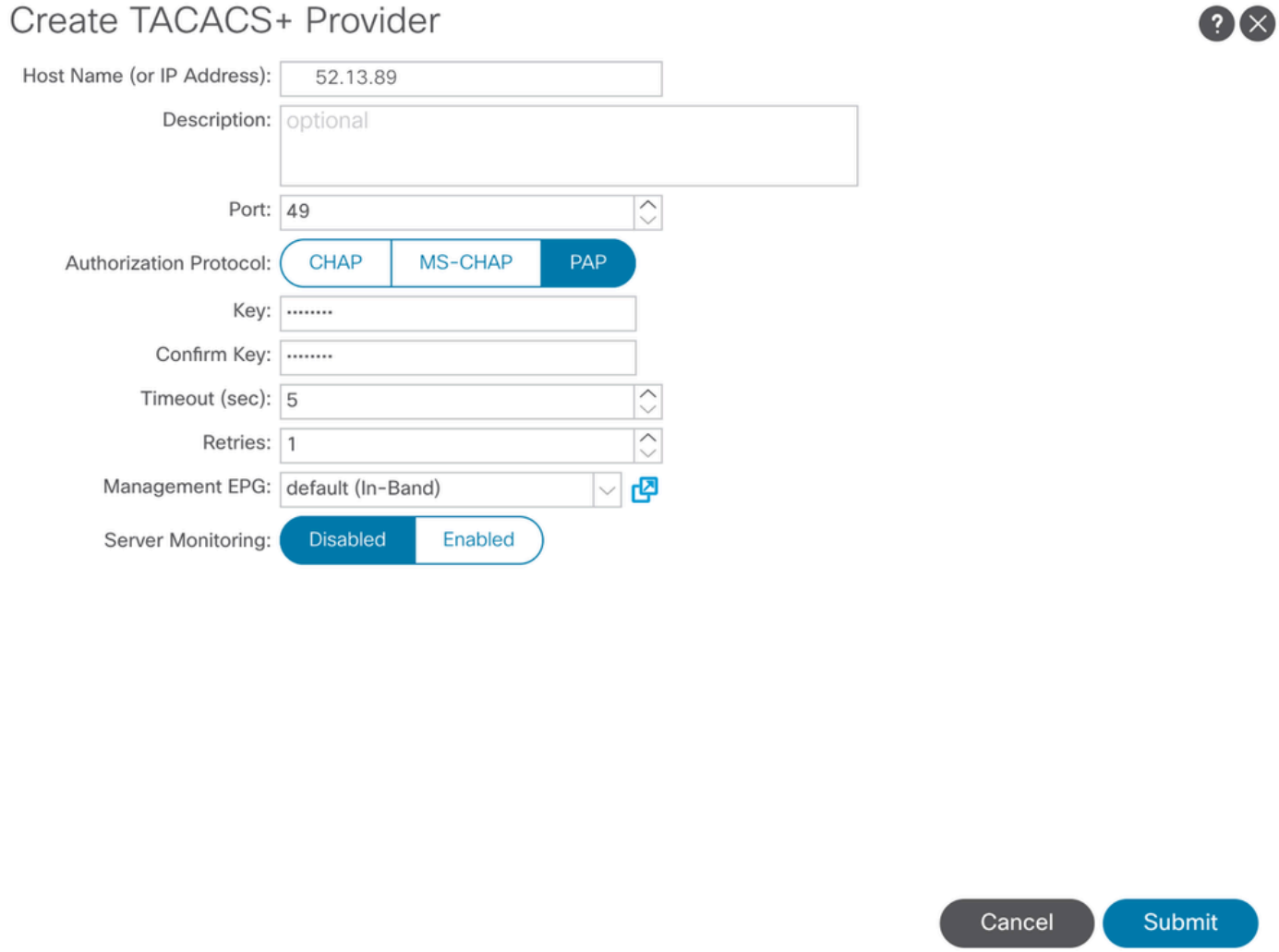
APIC-Anmeldeadministrator



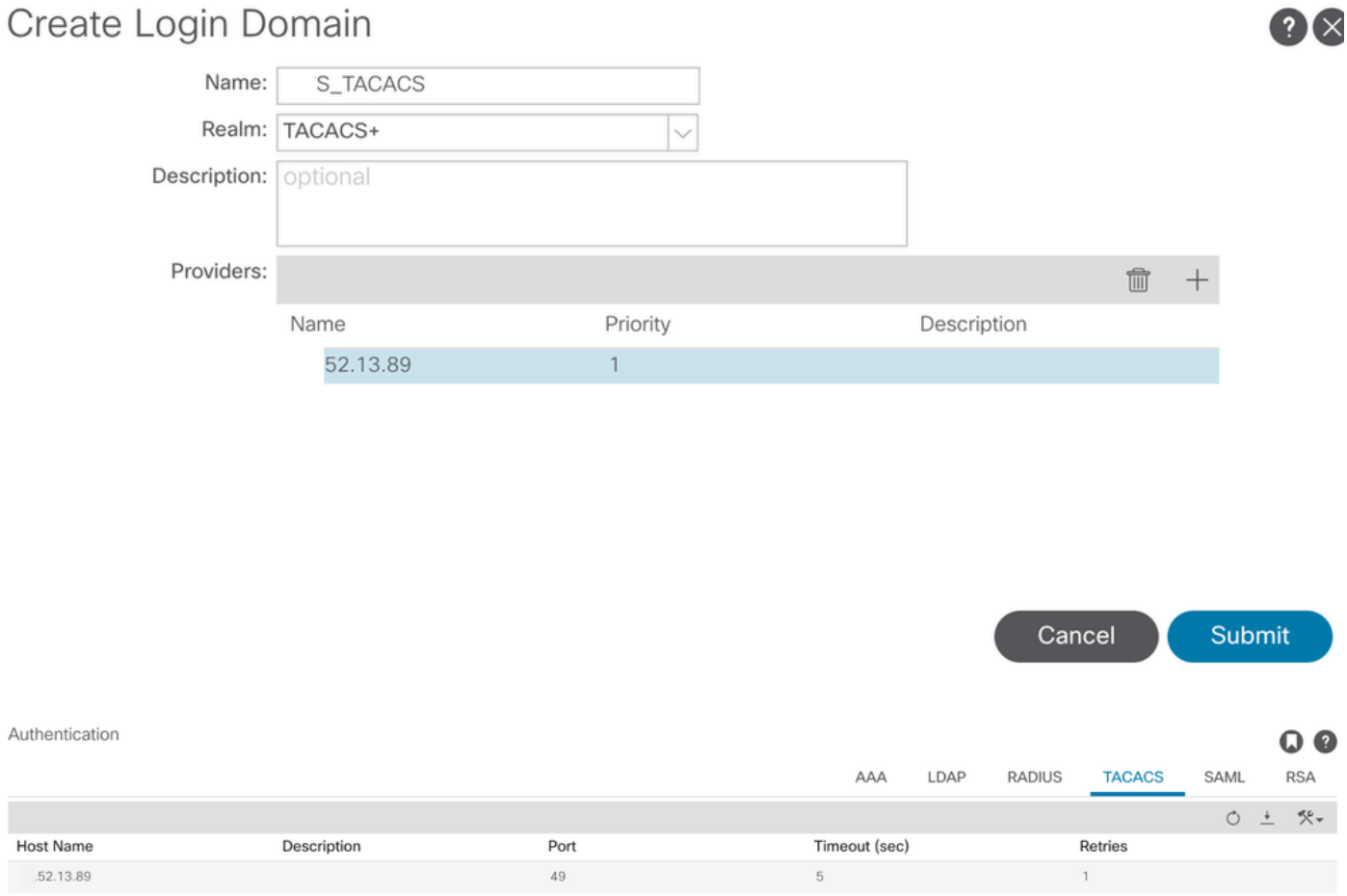
APIC TACACS-Anbieter

Schritt 3: Definieren Sie die ISE-IP-Adresse oder den Hostnamen, definieren Sie einen

gemeinsamen geheimen Schlüssel, und wählen Sie die Management Endpoint Policy Group (EPG) aus. Klicken Sie,Submitum den TACACS+-Anbieter für die Anmeldung als Administrator hinzuzufügen.



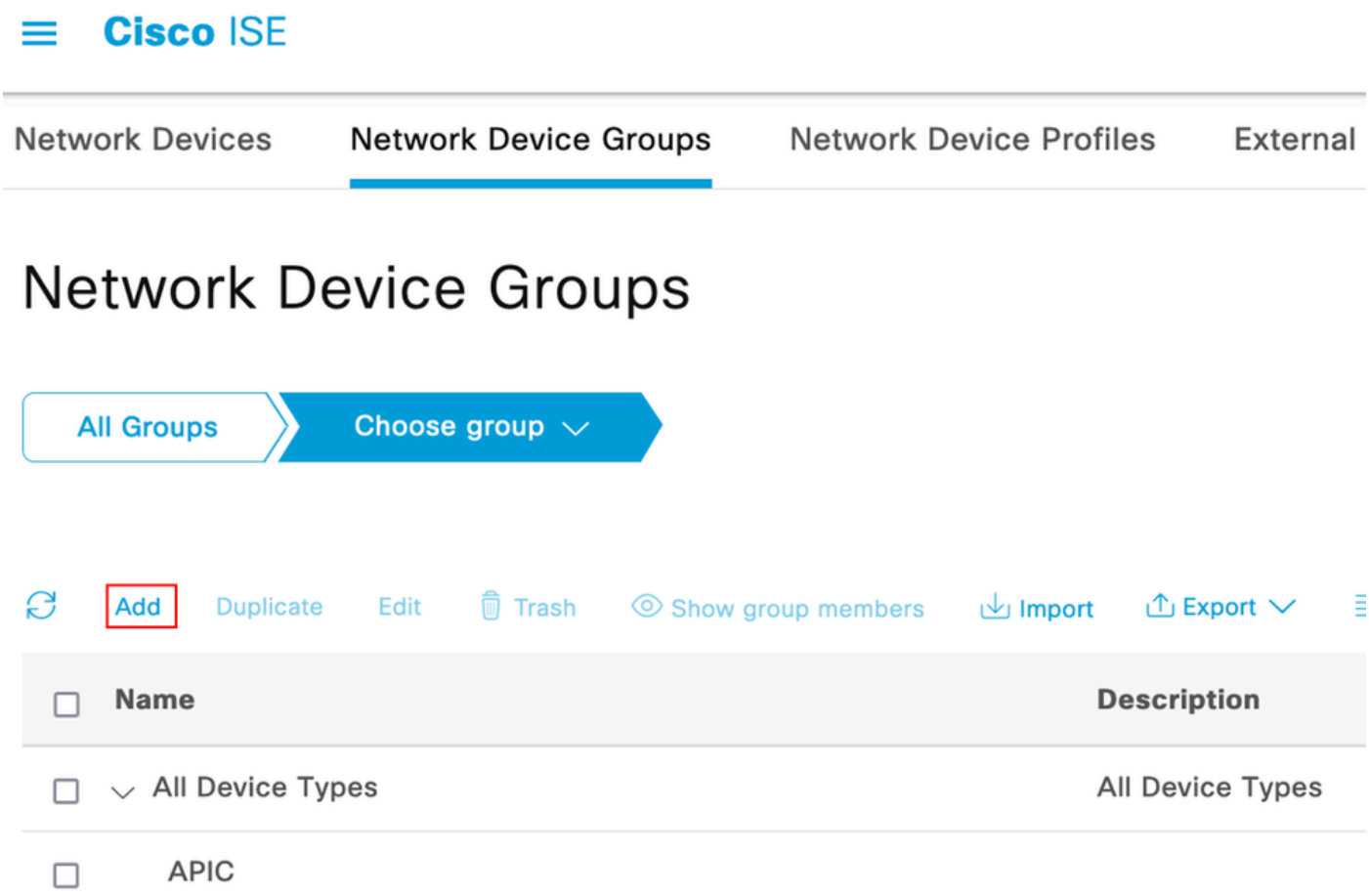
APIC TACACS Provider-Einstellungen



TACACS-Anbieteransicht

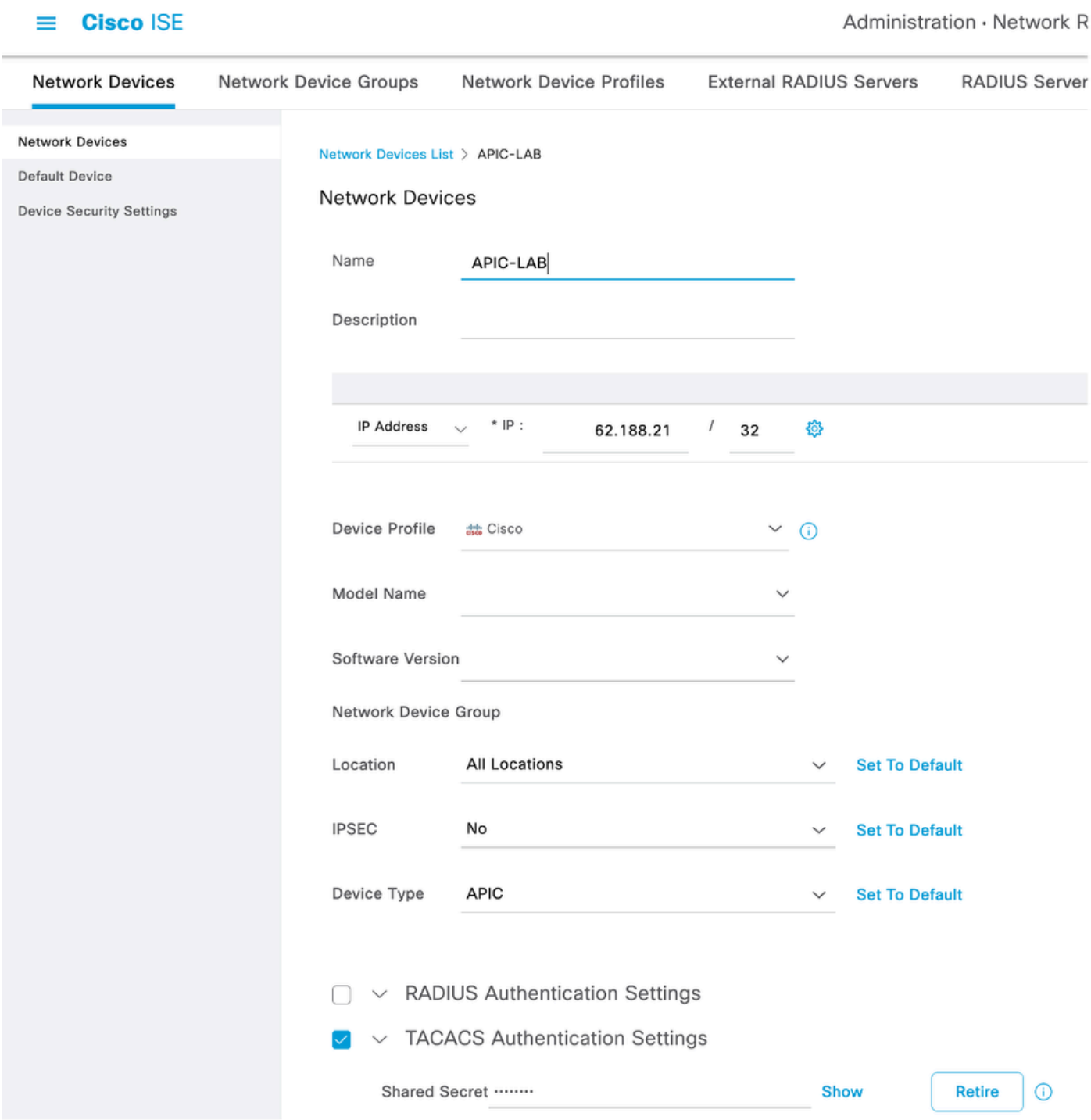
ISE-Konfiguration

Schritt 1: Navigieren Sie zu ☰>Administration > Network Resources > Network Device Groups. Erstellen Sie unter "Alle Gerätetypen" eine Netzwerk-Gerätegruppe.



ISE-Netzwerk-Gerätegruppen

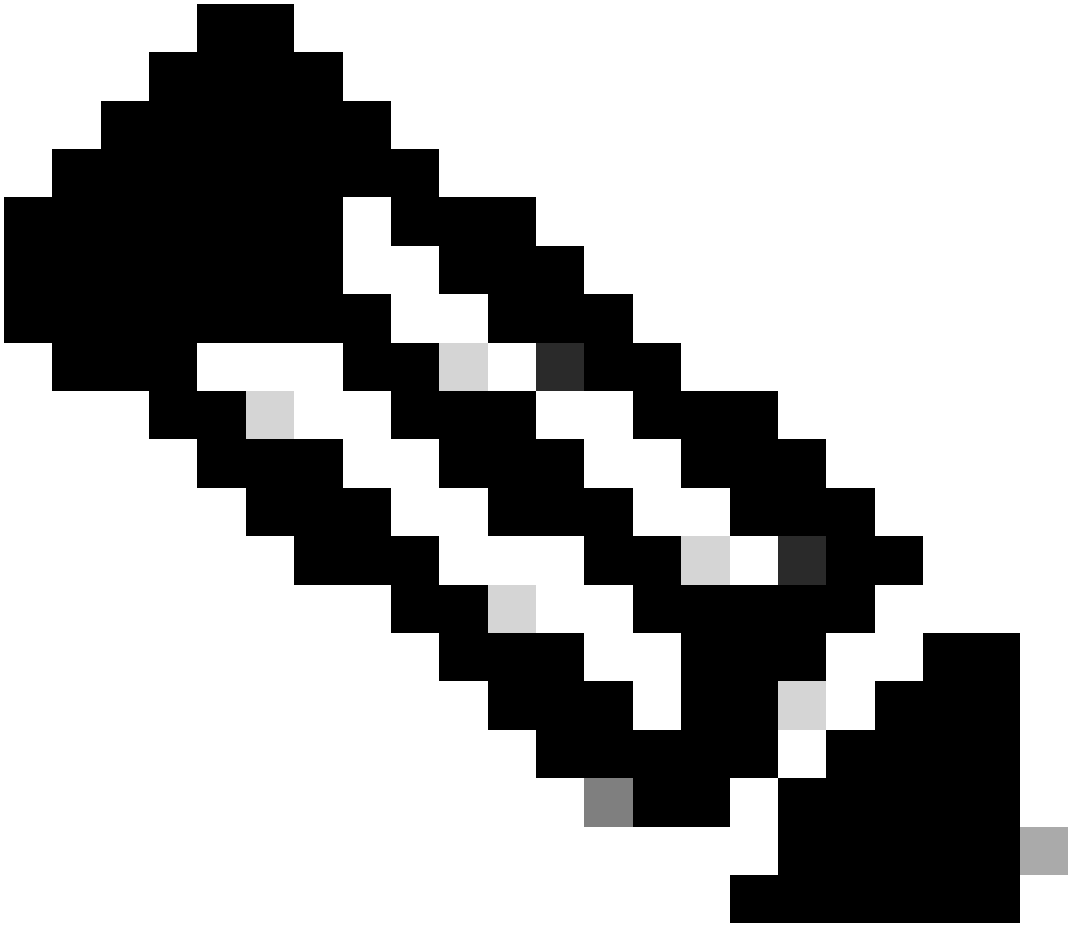
Schritt 2. Navigieren Sie zuAdministration > Network Resources > Network Devices. AddWählen Sie Definieren des APIC-Namens und der IP-Adresse, wählen Sie APIC unter Device Type (Gerätetyp) und TACACS+ (TACACS+) aus, und definieren Sie das Kennwort für die APIC TACACS+ Provider-Konfiguration. Klicken Sie auf .Submit



Wiederholen Sie die Schritte 1 und 2 für Leaf-Switches.

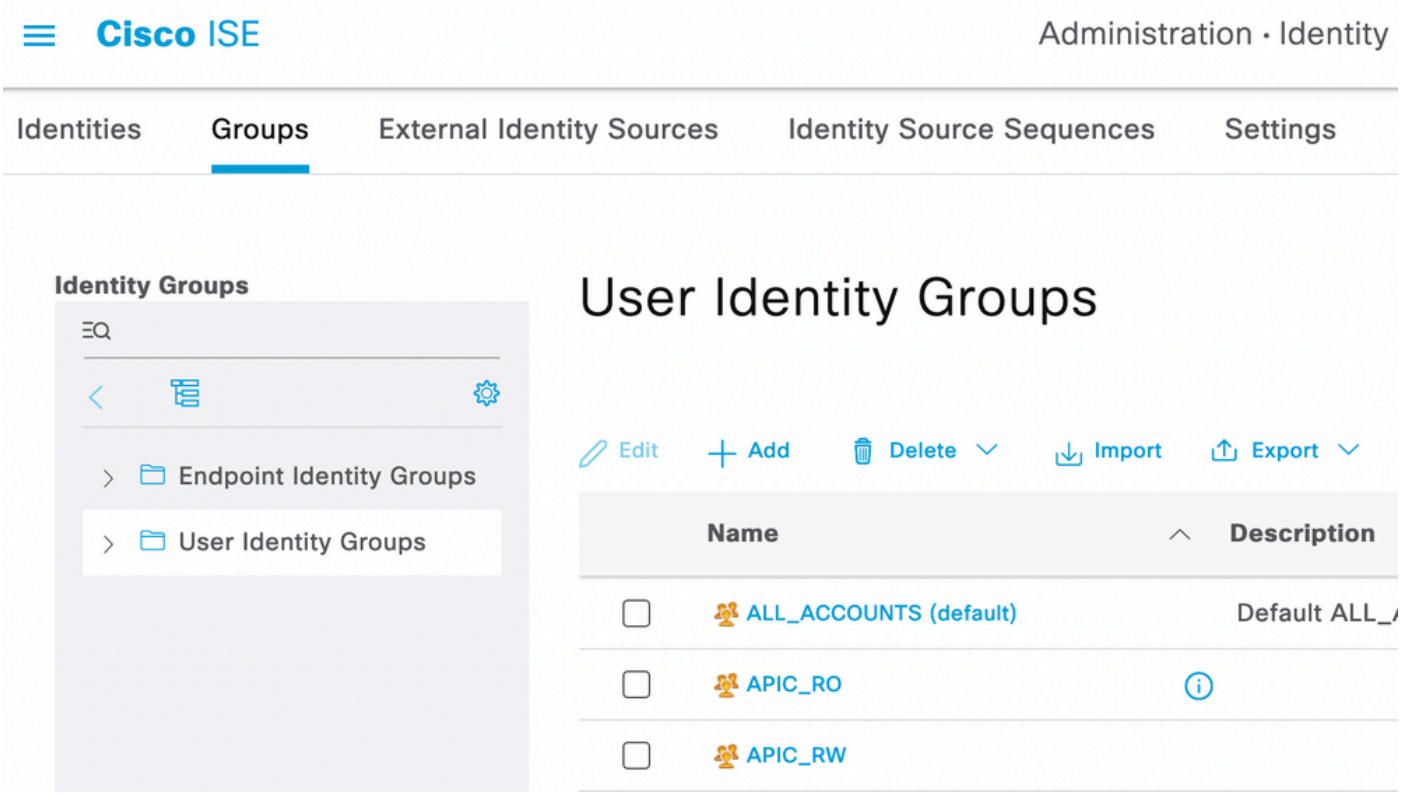
Schritt 3: Verwenden Sie die Anweisungen auf diesem Link, um die ISE in Active Directory zu integrieren.

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/217351-ad-integration-for-cisco-ise-gui-and-cli.html



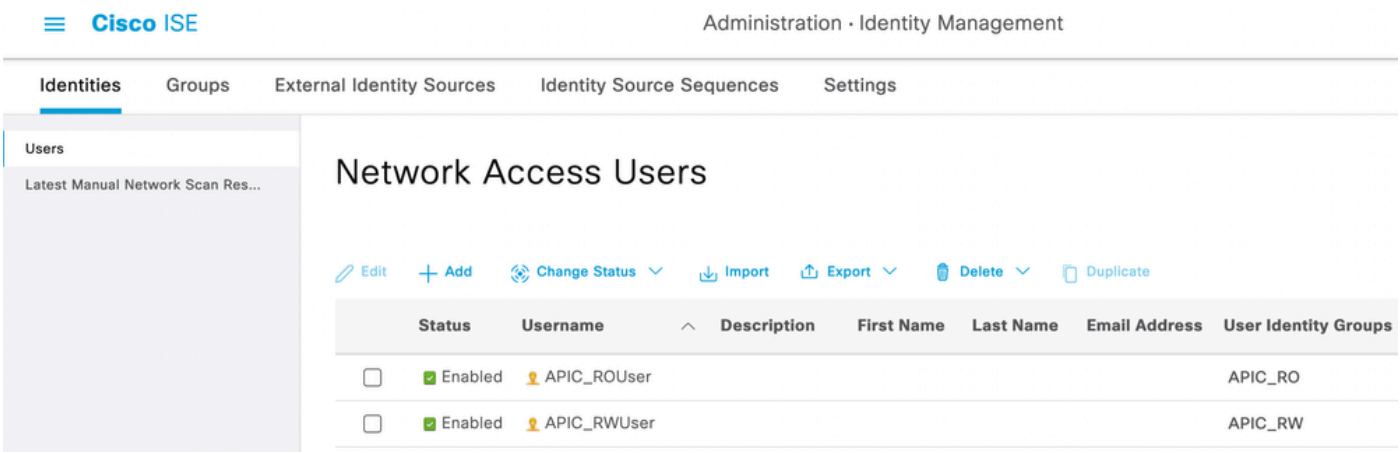
Anmerkung: In diesem Dokument sind interne Benutzer und AD-Administratorgruppen als Identitätsquellen enthalten. Der Test wird jedoch mit der Identitätsquelle der internen Benutzer durchgeführt. Das Ergebnis ist für AD-Gruppen identisch.

Schritt 4. (Optional) Navigieren Sie zu ☰ >Administration > Identity Management > Groups. Wählen SieUser Identity Groups und klicken Sie auf Add. Erstellen Sie eine Gruppe für schreibgeschützte Admin-Benutzer und Admin-Benutzer.

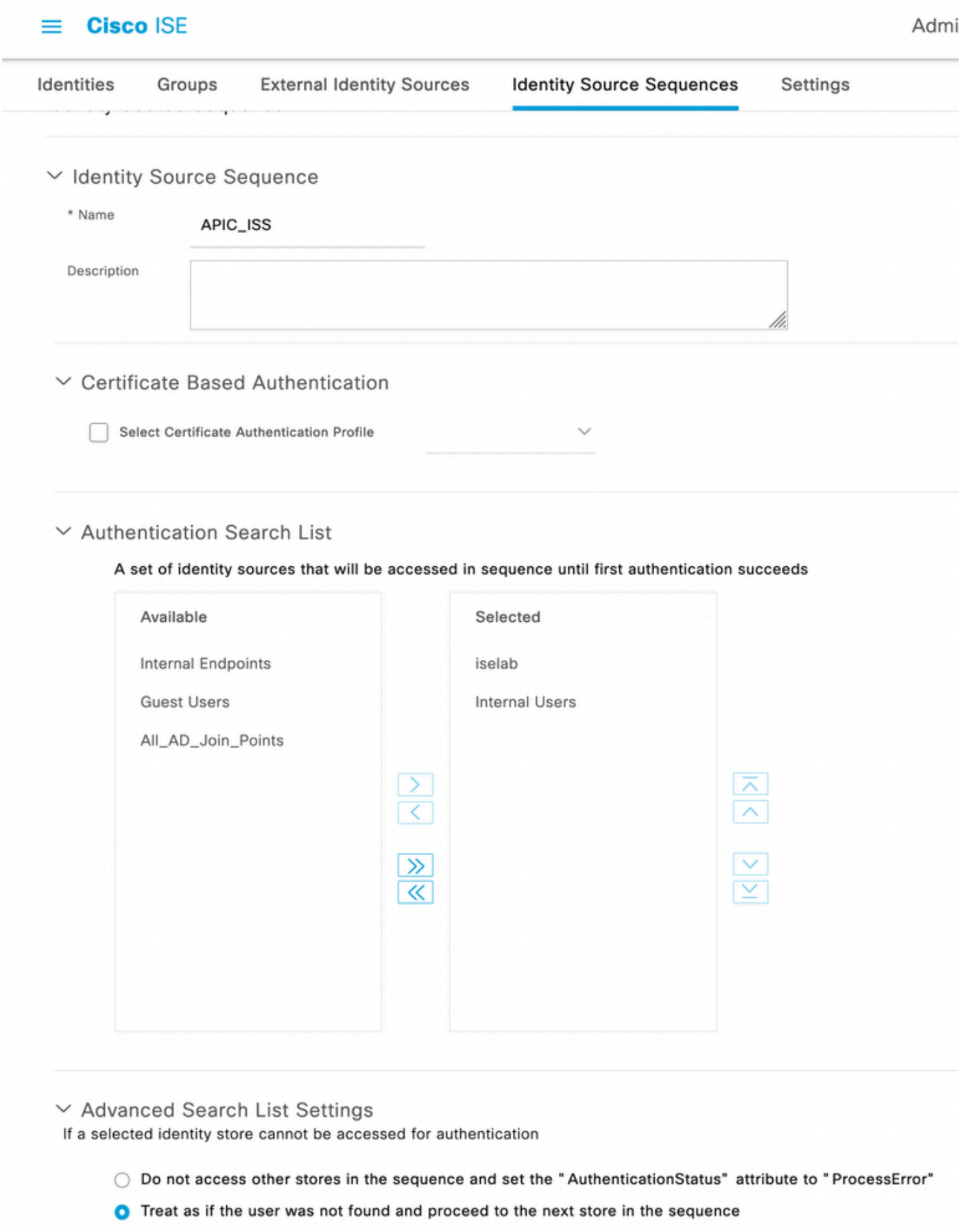


Identitätsgruppe

Schritt 5. (Optional) Navigieren Sie zu ☰>Klicken Sie aufAdministration > Identity Management > Identity.,Addund erstellen Sie einenRead Only AdminBenutzer und einenAdminBenutzer. Weisen Sie jeden Benutzer jeder in Schritt 4 erstellten Gruppe zu.



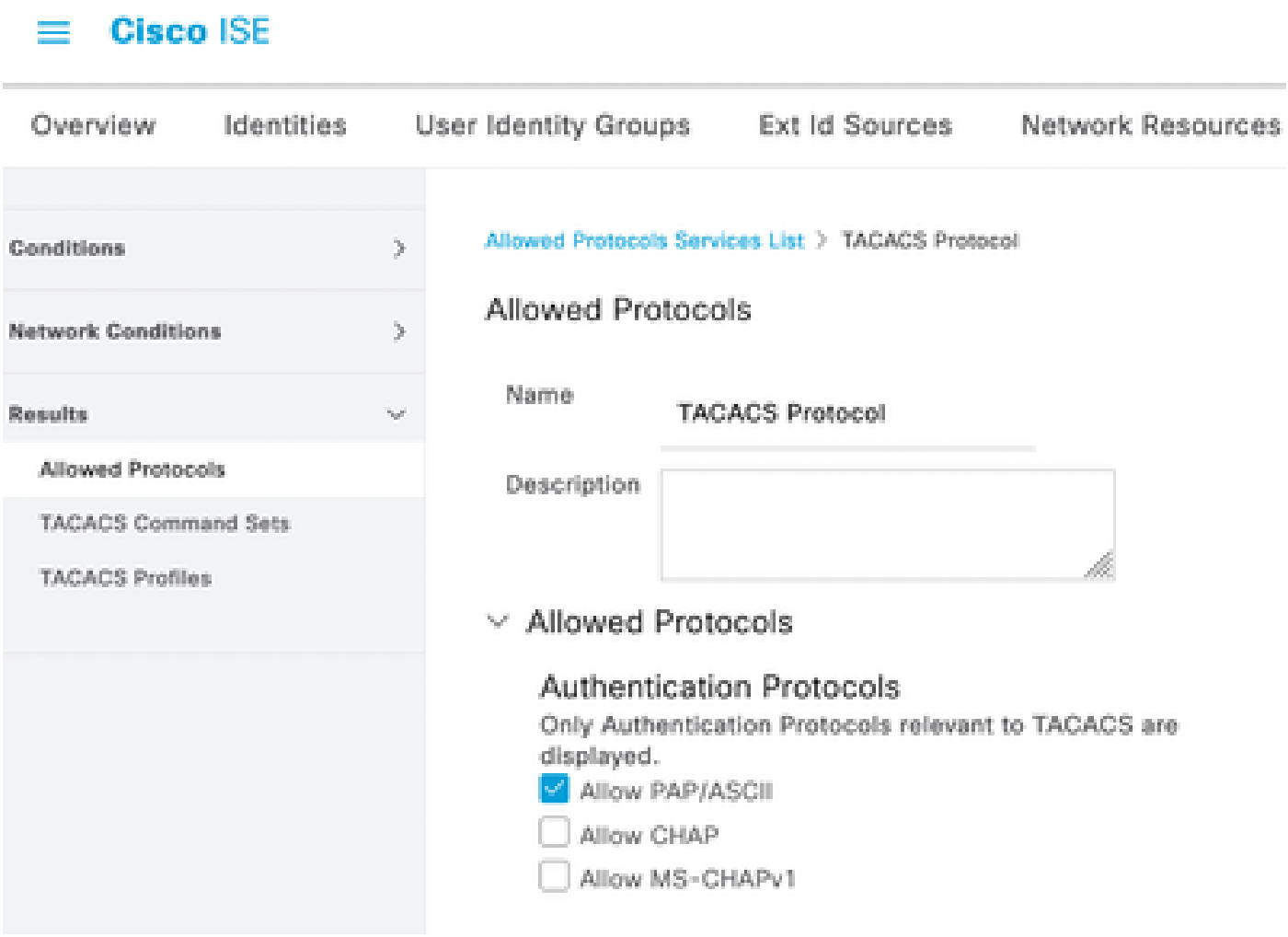
Schritt 6: Navigieren Sie zu ☰ >Administration > Identity Management > Identity Source Sequence. Wählen SieAdd, definieren Sie einen Namen, und wählen Sie in der ListeAD Join PointsundInternal UsersIdentitätsquelle aus. Wählen SieTreat as if the user was not found and proceed to the next store in the sequenceunterAdvanced Search List Settingsaus, und klicken Sie aufSave.



Identitätsquellensequenz

>7. Navigieren Sie zu ☰**Work Centers** > **Device Administration** > **Policy Elements** > **Results** > **Allowed Protocols**. Wählen

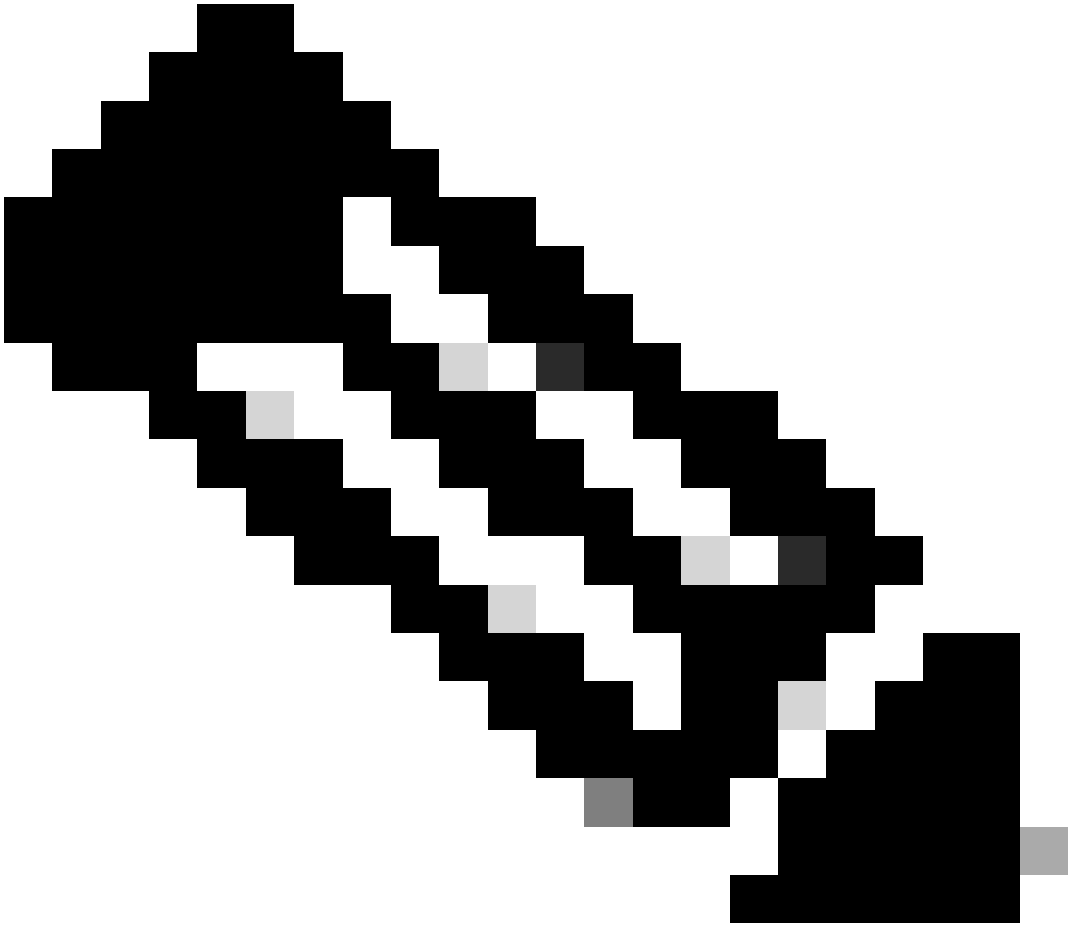
Sie Hinzufügen aus, definieren Sie einen Namen, und deaktivieren Sie CHAP zulassen und MS-CHAPv1 aus der Liste der Authentifizierungsprotokolle zulassen. Wählen Sie Speichern aus.



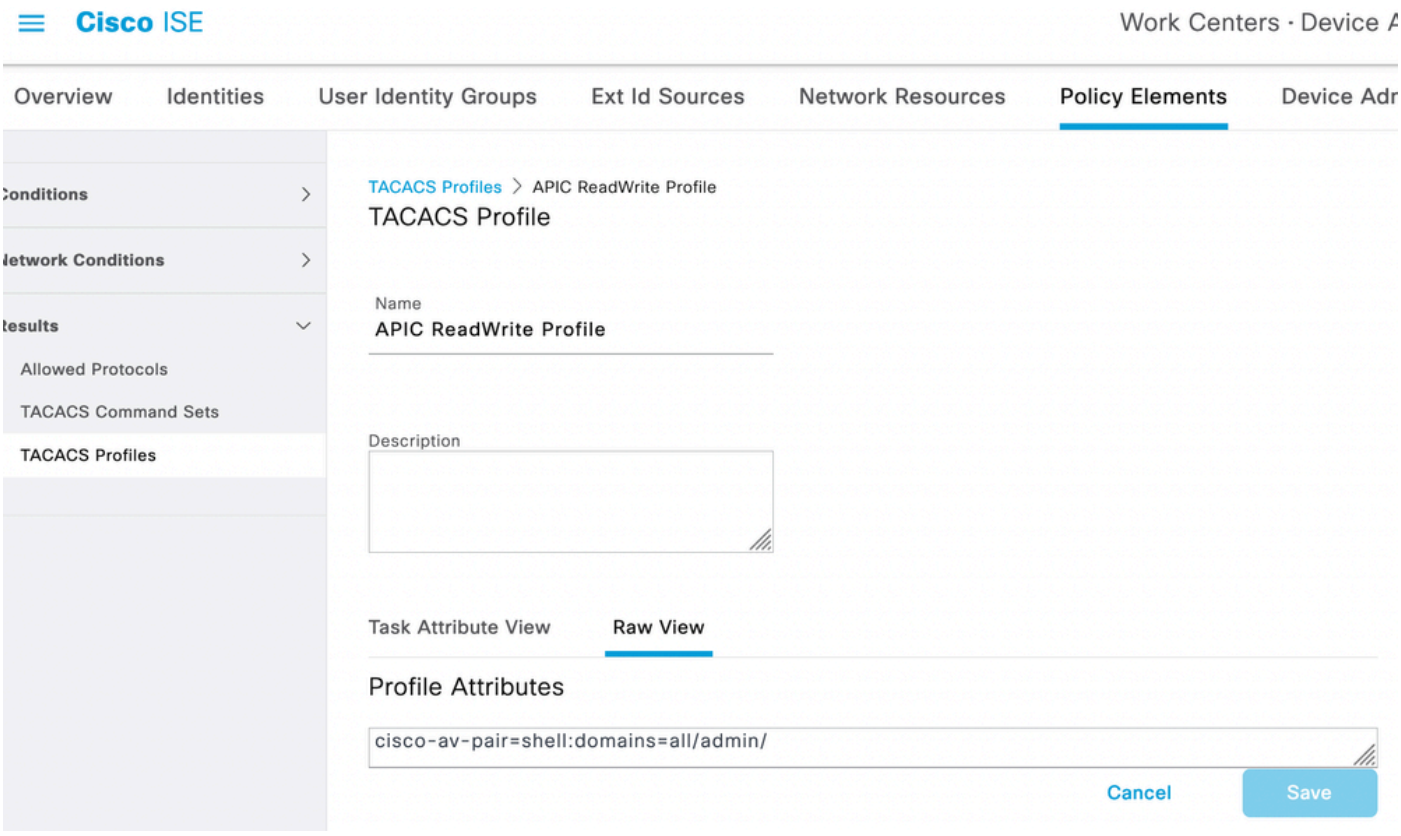
TACACS-Zulässigkeitsprotokoll

8. Navigieren Sie zu ☰ >Work Centers > Device Administration > Policy Elements > Results > TACACS Profile. Klicken Sie auf,addund erstellen Sie zwei Profile basierend auf den Attributen in der Liste unterRaw View. Klicken Sie auf .Save

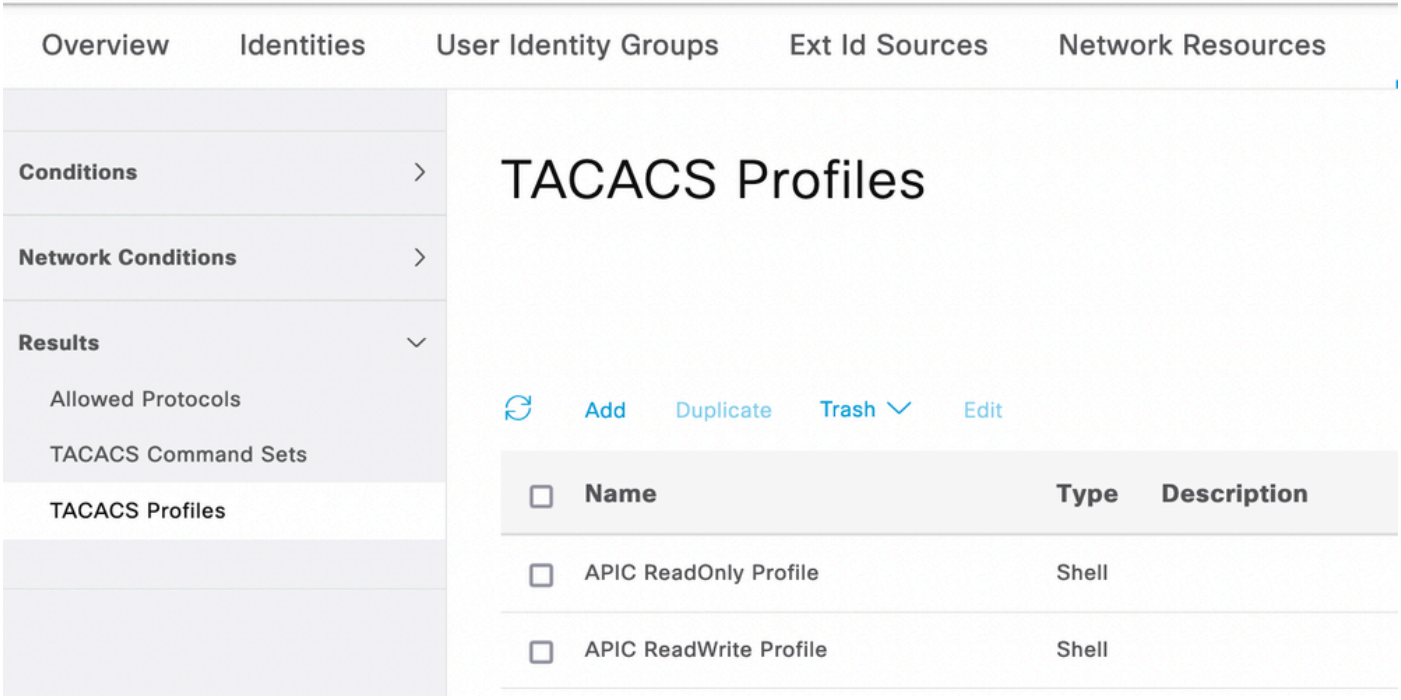
- Administrator: cisco-av-pair=shell:domains=all/admin/
- Schreibgeschützter Administratorbenutzer: cisco-av-pair=shell:domains=all//read-all



Anmerkung: Bei Leerzeichen oder zusätzlichen Zeichen schlägt die Autorisierungsphase fehl.

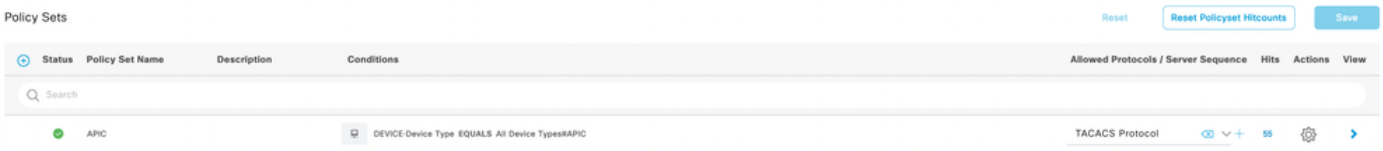


TACACS-Profil



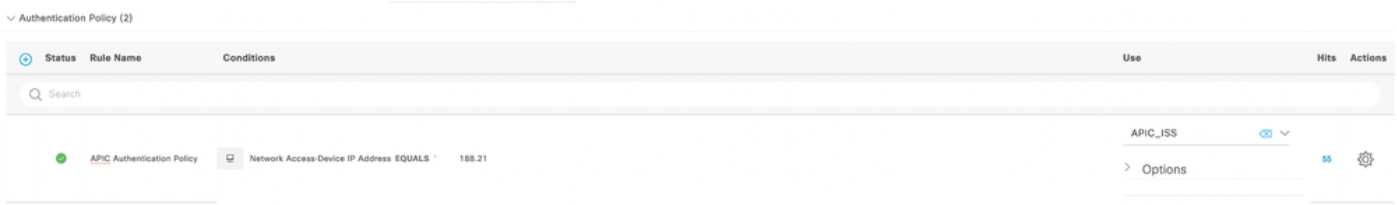
TACACS-Admin- und schreibgeschützte Admin-Profile

Schritt 9: Navigieren Sie zu ☰>Work Centers > Device Administration > Device Admin Policy Set. Erstellen Sie einen neuen Richtliniensatz, definieren Sie einen Namen, und wählen Sie den in Schritt 1 erstellten GerätetypAPICaus. Wählen Sie in Schritt 7. erstellt als zulässiges ProtokollTACACS Protocolaus, und klicken Sie aufSave.

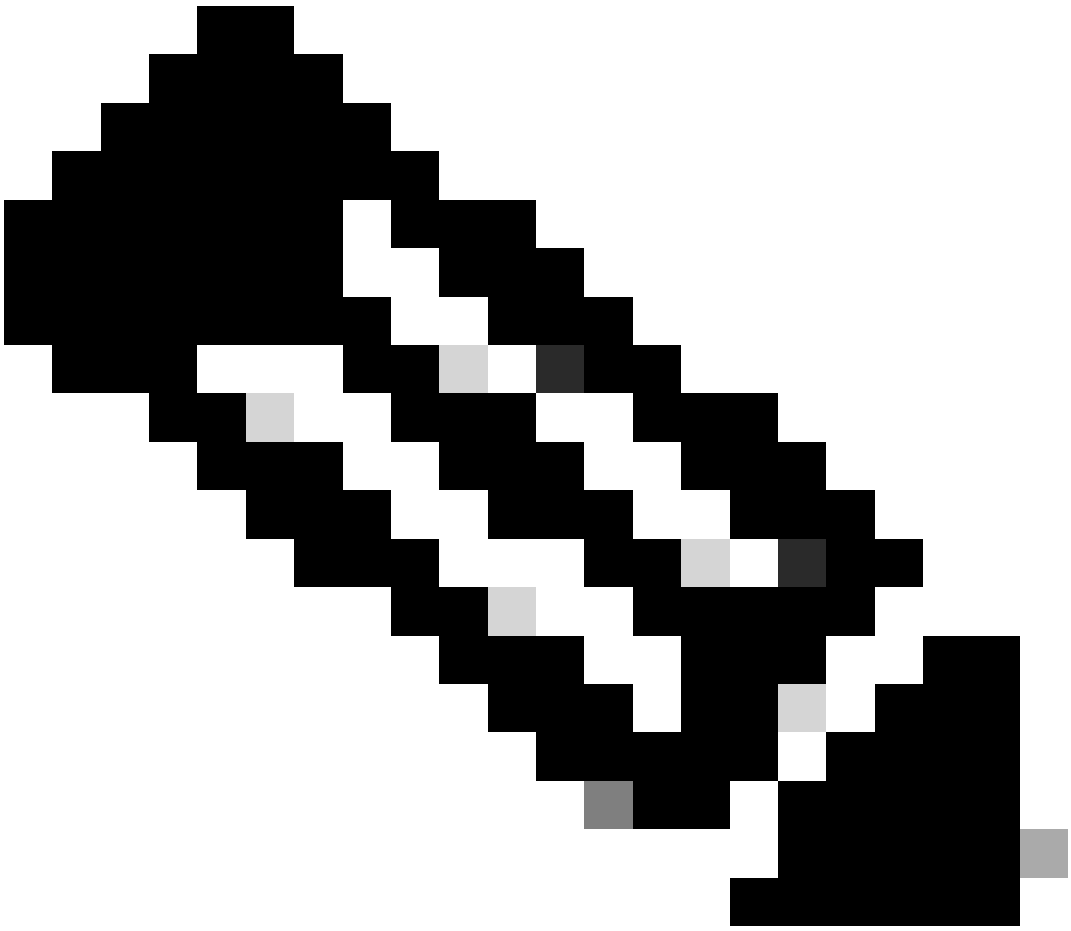


TACACS-Richtliniensatz

Schritt 10: Klicken Sie unter "NeuPolicy Set" auf den Pfeil nach rechts>, und erstellen Sie eine Authentifizierungsrichtlinie. Definieren Sie einen Namen, und wählen Sie die IP-Adresse des Geräts als Bedingung aus. Wählen Sie dann die in Schritt 6 erstellte Identitätsquellensequenz aus.

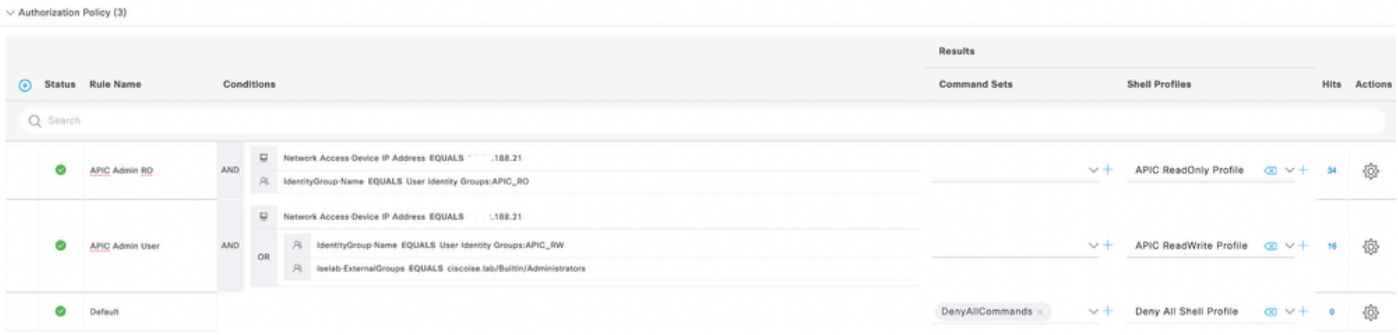


Authentifizierungsrichtlinie



Anmerkung: Location oder andere Attribute können als Authentifizierungsbedingung verwendet werden.

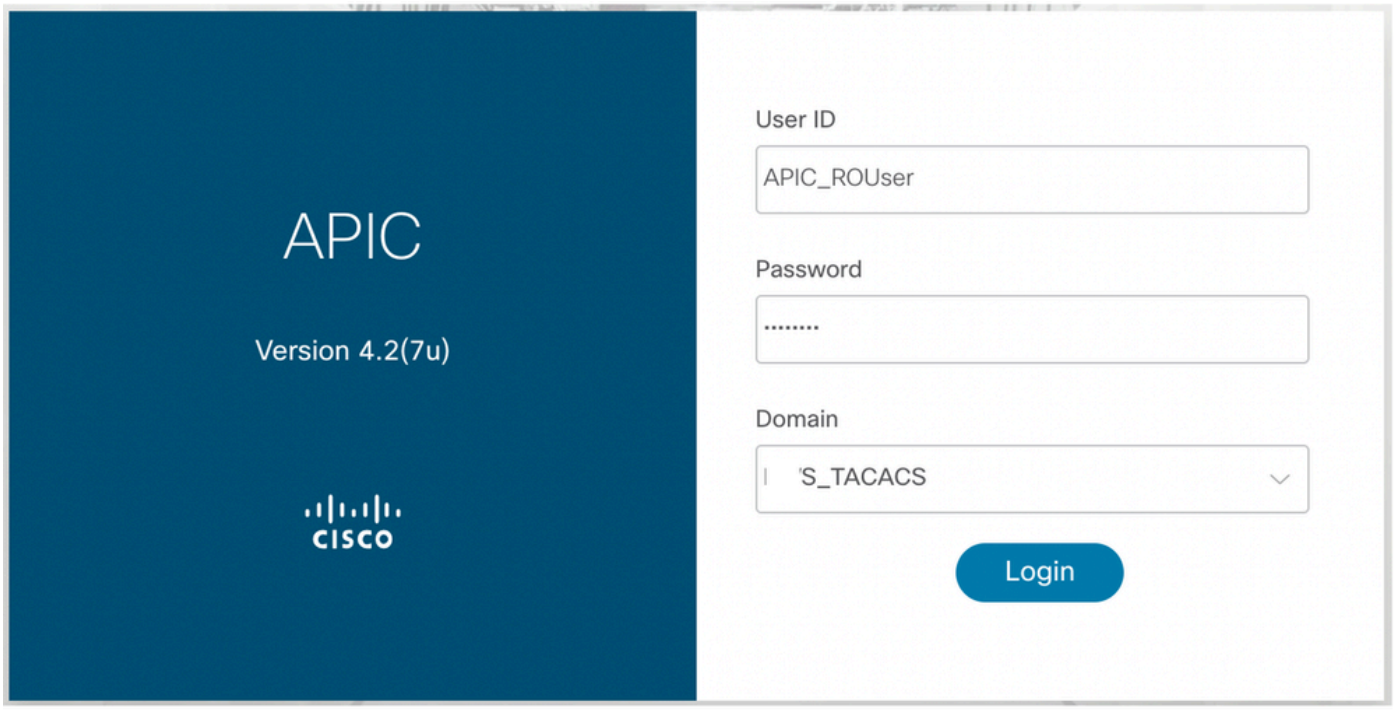
Schritt 11: Erstellen Sie ein Autorisierungsprofil für jeden Admin-Benutzertyp, definieren Sie einen Namen, und wählen Sie einen internen Benutzer und/oder eine AD-Benutzergruppe als Bedingung aus. Es können zusätzliche Bedingungen wie der APIC verwendet werden. Wählen Sie für jede Autorisierungsrichtlinie das passende Shell-Profil aus, und klicken Sie aufSave.



TACACS-Autorisierungsprofil

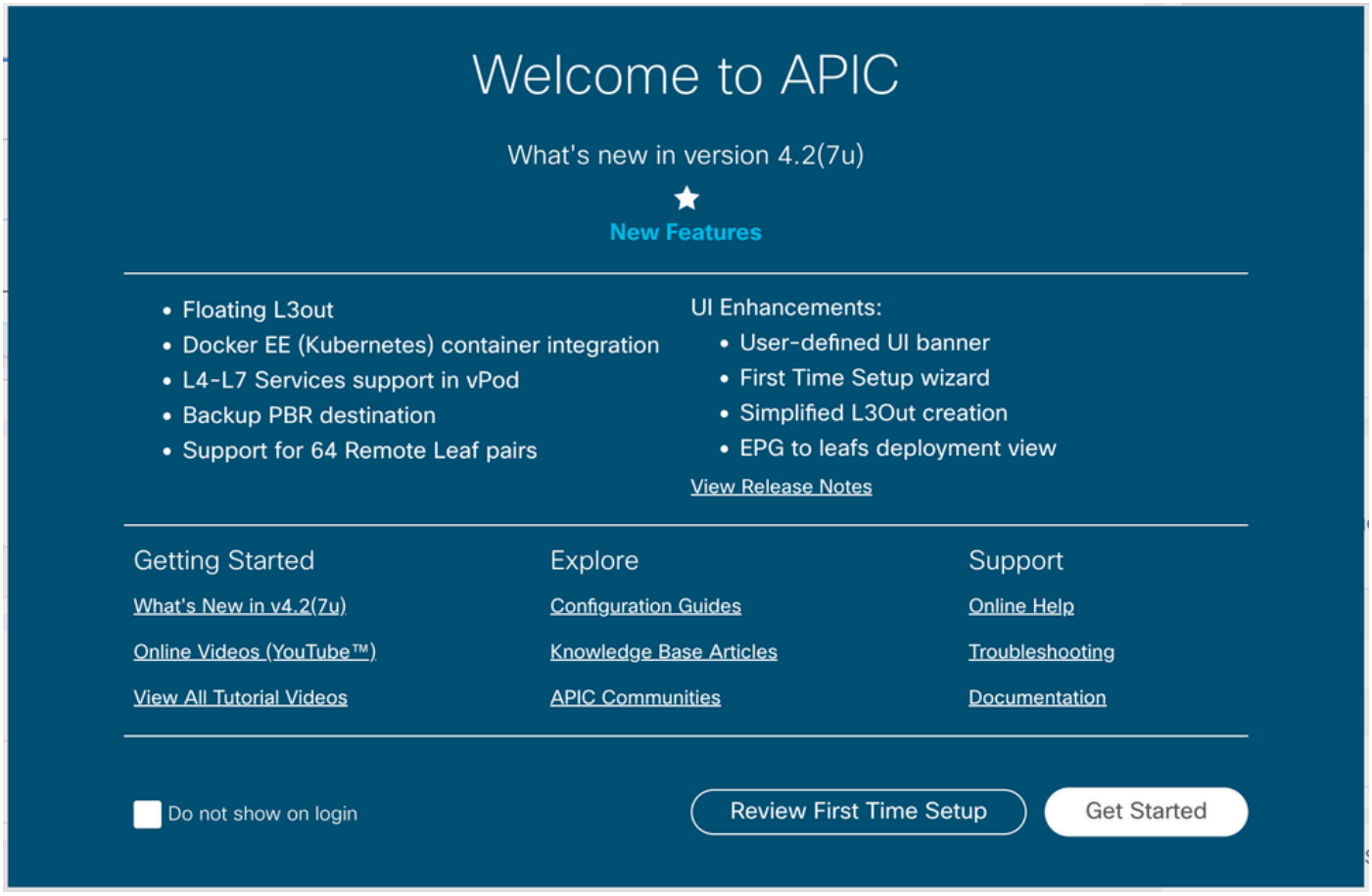
Überprüfung

Schritt 1: Melden Sie sich auf der APIC-Benutzeroberfläche mit den Anmeldeinformationen für den Benutzeradministrator an. Wählen Sie in der Liste die Option TACACS aus.



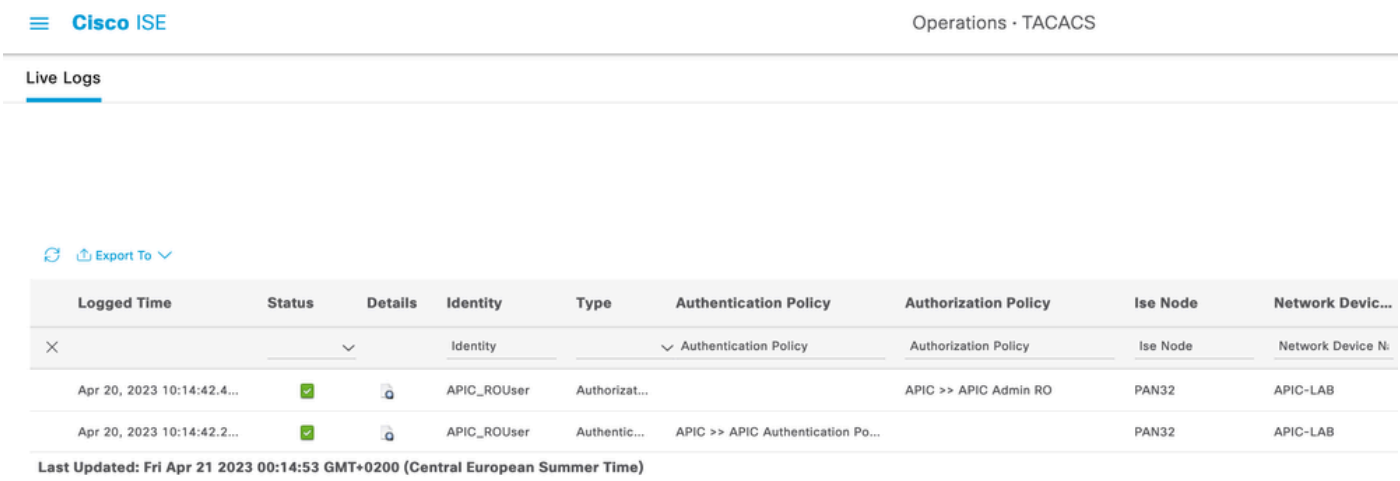
APIC-Anmeldung

Schritt 2: Überprüfen, ob der Zugriff auf die APIC-Benutzeroberfläche und die Anwendung der richtigen Richtlinien auf die TACACS Live-Protokolle gewährleistet sind



APIC-Willkommensmeldung

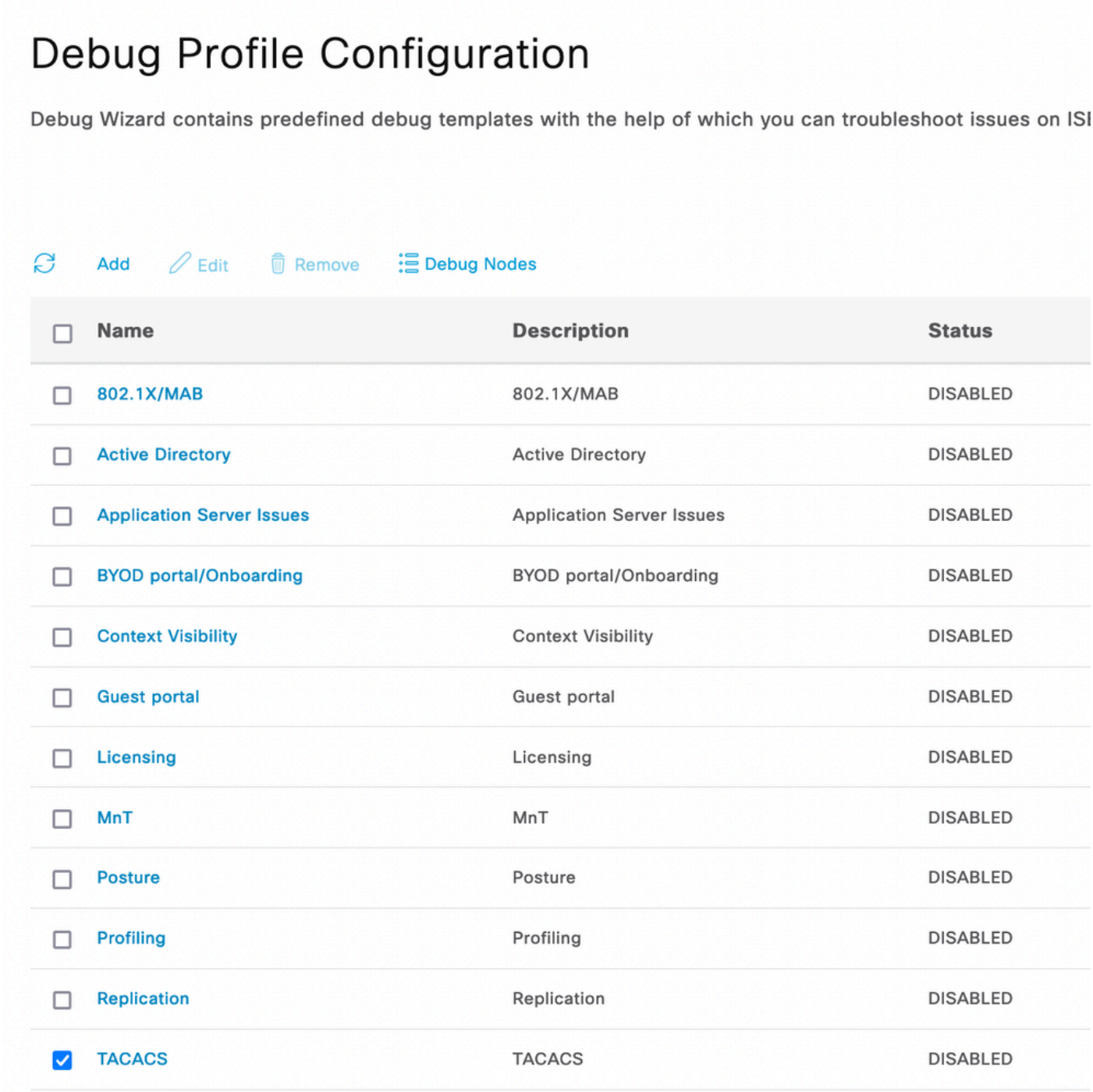
Wiederholen Sie die Schritte 1 und 2 für schreibgeschützte Administratorbenutzer.



TACACS+ Live-Protokolle

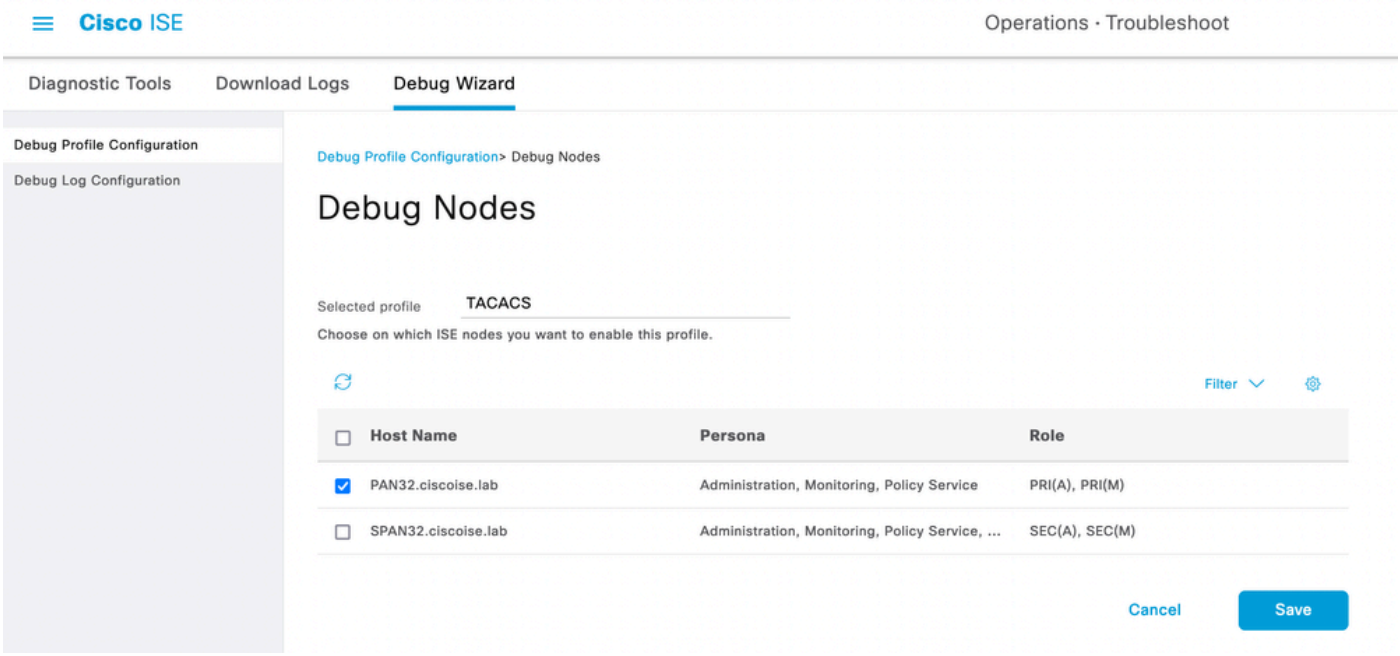
Fehlerbehebung

Schritt 1: Navigieren Sie zu ☰ >Operations > Troubleshoot > Debug Wizard. Wählen SieTACACSund klicken Sie auf Debug Nodes.



Konfiguration des Debugprofils

Schritt 2. Wählen Sie den Knoten, der den Datenverkehr empfängt, und klicken Sie aufSave.



Auswahl der Debug-Knoten

Schritt 3: Führen Sie einen neuen Test durch, und laden Sie die Protokolle herunter,Operations > Troubleshoot > Download logs wie folgt:

```
AcsLogs,2023-04-20 22:17:16,866,DEBUG,0x7f93cabc7700,cntx=0004699242,sesn=PAN32/469596415/70,CPMSession
```

Falls die Debugging-Informationen keine Authentifizierungs- und Autorisierungsinformationen enthalten, überprüfen Sie Folgendes:

1. Der Geräteverwaltungsdienst ist auf dem ISE-Knoten aktiviert.
2. Die richtige ISE-IP-Adresse wurde der APIC-Konfiguration hinzugefügt.
3. Falls sich eine Firewall in der Mitte befindet, stellen Sie sicher, dass Port 49 (TACACS) zulässig ist.

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.