Konfigurieren der TACACS+-Geräteadministration auf Palo Alto mit der ISE

Inhalt

Einleitung

In diesem Dokument wird die TACACS+-Konfiguration auf Palo Alto mit der Cisco ISE beschrieben.

Voraussetzungen

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

- Cisco ISE und TACACS+-Protokoll.
- Palo Alto-Firewall.

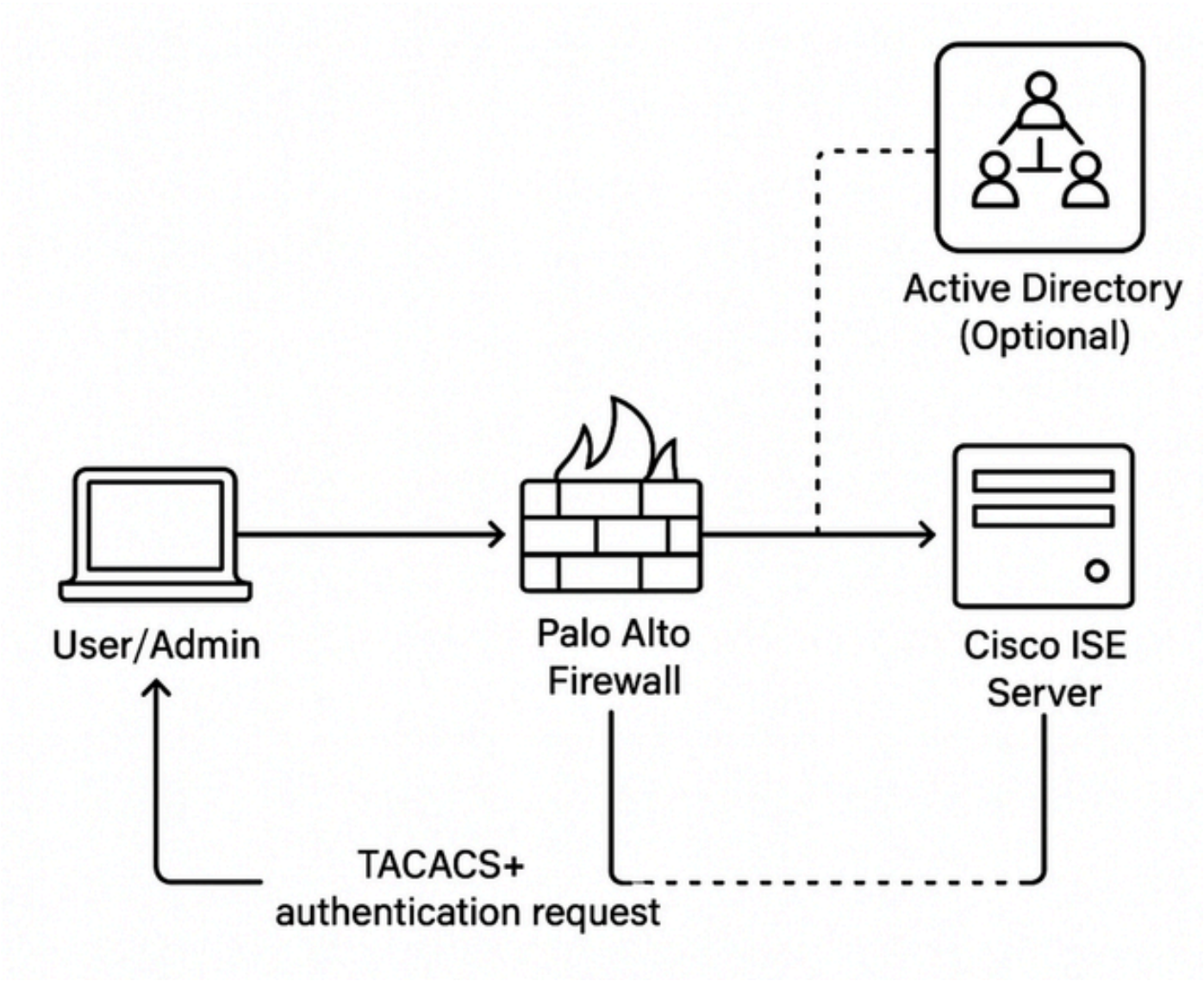
Verwendete Komponenten

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

- Palo Alto Firewall Version 10.1.0
- Cisco Identity Services Engine (ISE) Version 3.3 Patch 4

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.

Netzwerkdiagramm



Authentifizierungsablauf

1. Der Administrator meldet sich bei der Palo Alto Firewall an.

2. Palo Alto sendet eine TACACS+-Authentifizierungsanforderung an die Cisco ISE.

3. Cisco ISE:

- Wenn AD integriert ist, fragt es AD nach Authentifizierung und Autorisierung ab.
- Wenn kein AD vorhanden ist, werden lokale Identitätsspeicher oder Richtlinien verwendet.
- Die Cisco ISE sendet eine Autorisierungsantwort an Palo Alto, die auf den konfigurierten Richtlinien basiert.

- Der Administrator erhält Zugriff mit der entsprechenden Privilegstufe.

Konfigurieren

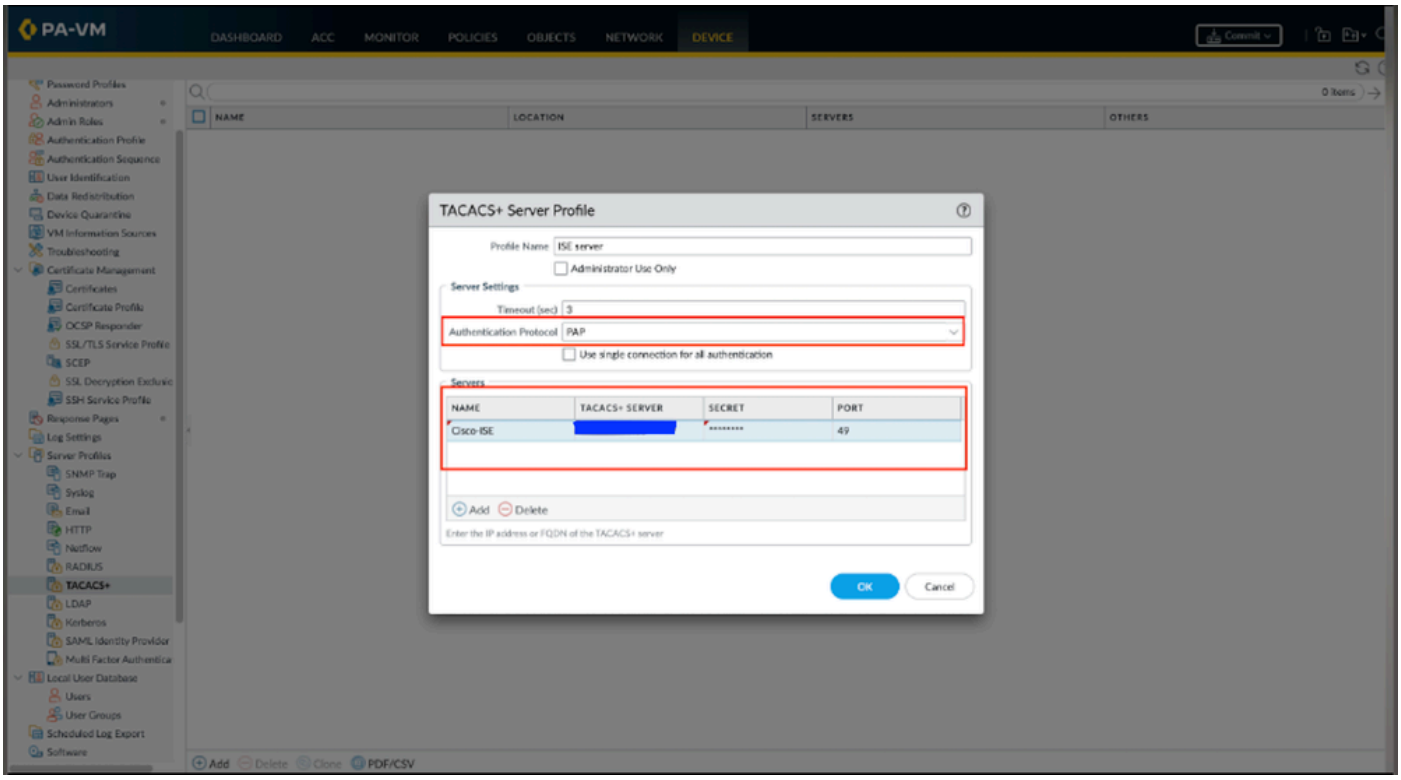
Abschnitt 1: Konfigurieren der Palo Alto Firewall für TACACS+

Schritt 1: Hinzufügen eines TACACS+-Serverprofils

Das Profil definiert, wie die Firewall mit dem TACACS+-Server verbunden wird.

1. Wählen Sie Device > Server Profiles > TACACS+ oder Panorama > Server Profiles > TACACS+ auf Panorama aus, und fügen Sie ein Profil hinzu.
2. Geben Sie einen Profilnamen zur Identifizierung des Serverprofils ein.
3. (Optional) Wählen Sie Administrator Use Only (Nur Administrator verwenden) aus, um den Zugriff auf Administratoren einzuschränken.
4. Geben Sie ein Zeitüberschreitungsintervall in Sekunden ein, nach dem eine Authentifizierungsanforderung ein Zeitüberschreitungsintervall aufweist (Standardwert ist 3). Bereich ist 1-20).
5. Wählen Sie das Authentifizierungsprotokoll (der Standardwert ist CHAP) aus, das von der Firewall für die Authentifizierung beim TACACS+-Server verwendet wird. 
6. Fügen Sie jeden TACACS+-Server hinzu, und gehen Sie wie folgt vor:
    1. Ein Name zum Identifizieren des Servers.
    2. Die IP-Adresse oder der FQDN des TACACS+ Servers. Wenn Sie einen Server mit einem FQDN-Adressobjekt identifizieren und anschließend die Adresse ändern, müssen Sie die Änderung bestätigen, damit die neue Serveradresse wirksam wird.
    3. Ein Geheimnis und Geheimnis bestätigen, um Benutzernamen und Kennwörter zu verschlüsseln.
    4. Der Server-Port für Authentifizierungsanforderungen (Standardwert: 49). Klicken Sie auf OK, um das Serverprofil zu speichern.

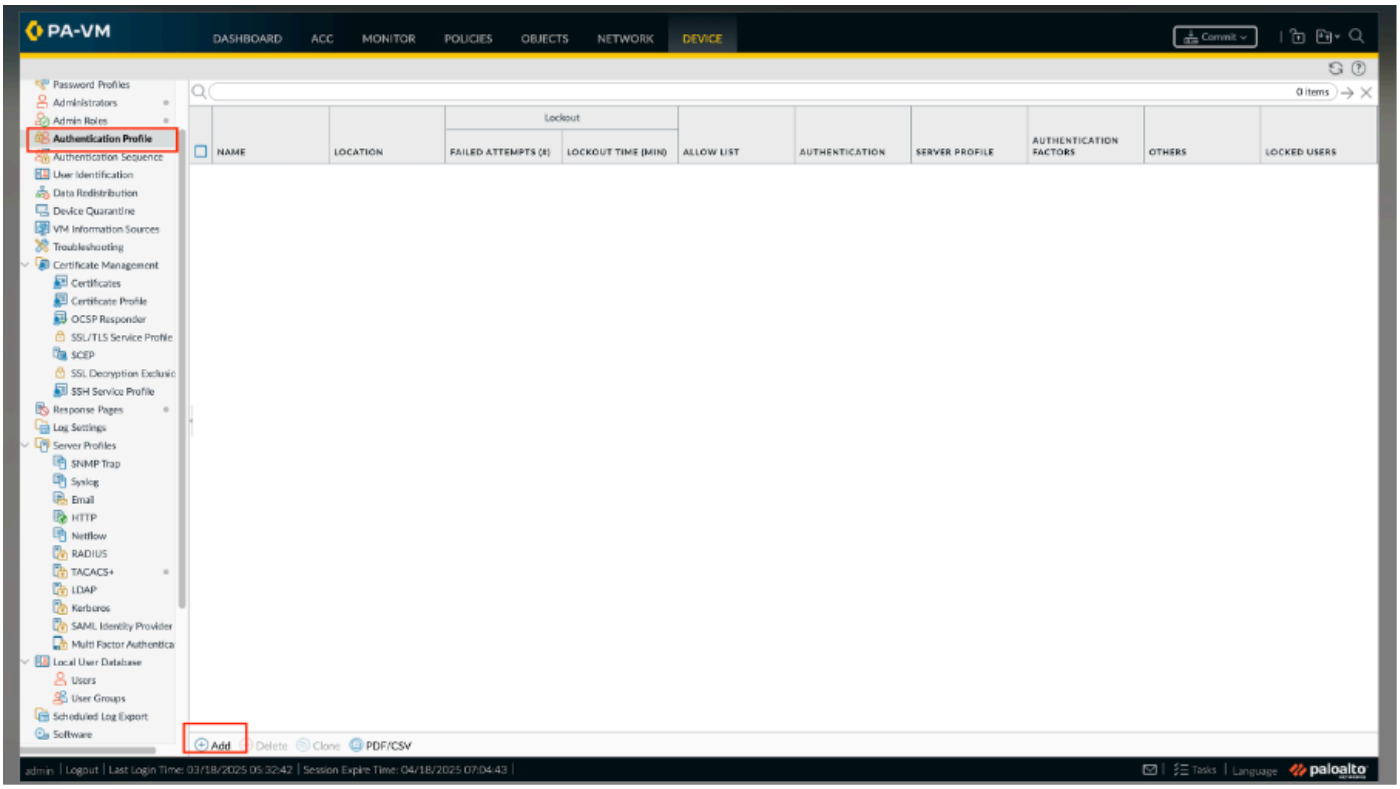
7. Klicken Sie auf OK, um das Serverprofil zu speichern.

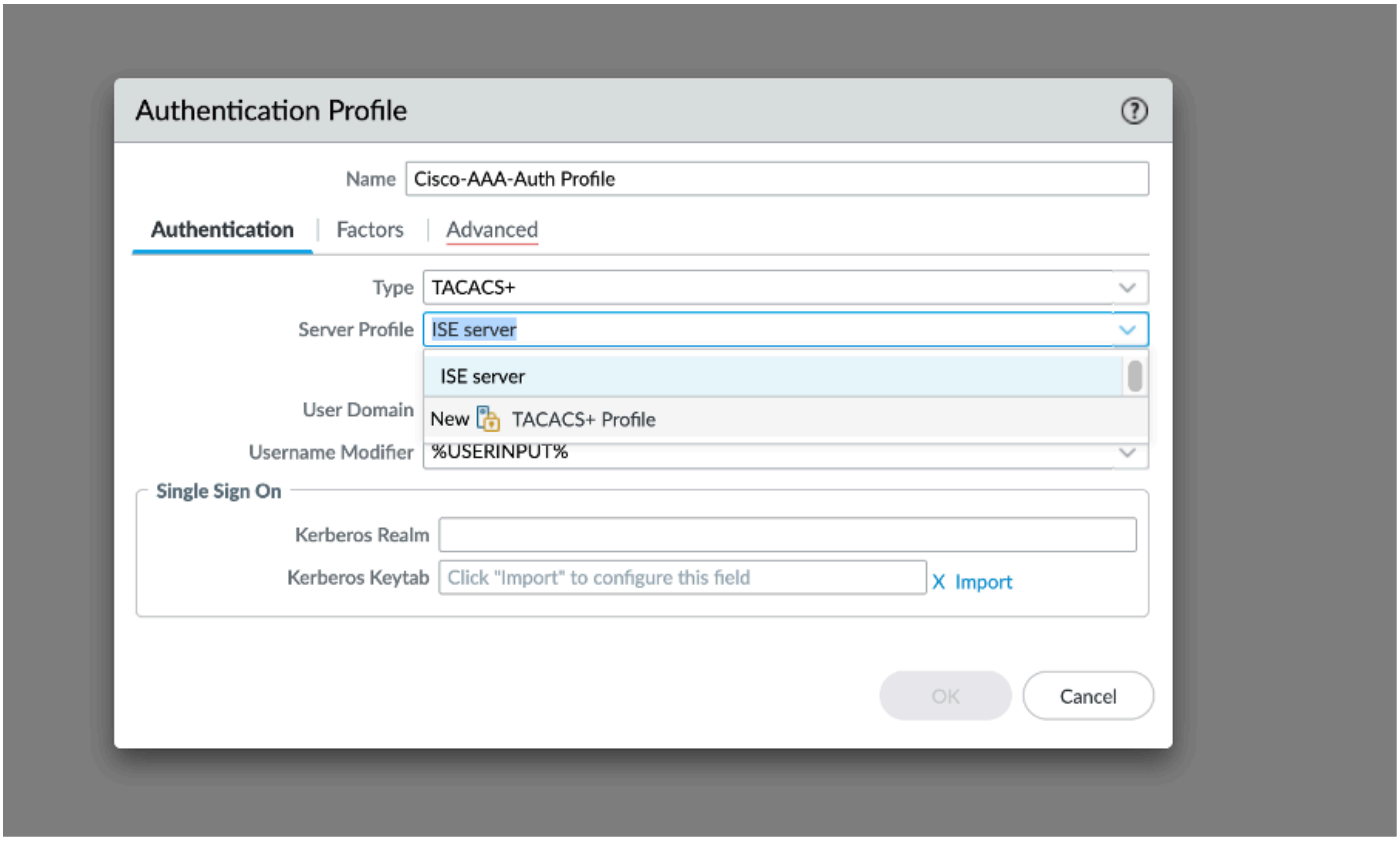


Schritt 2: Weisen Sie das TACACS+-Serverprofil einem Authentifizierungsprofil zu.

Das Authentifizierungsprofil definiert die Authentifizierungseinstellungen, die einer Reihe von Benutzern gemeinsam sind.

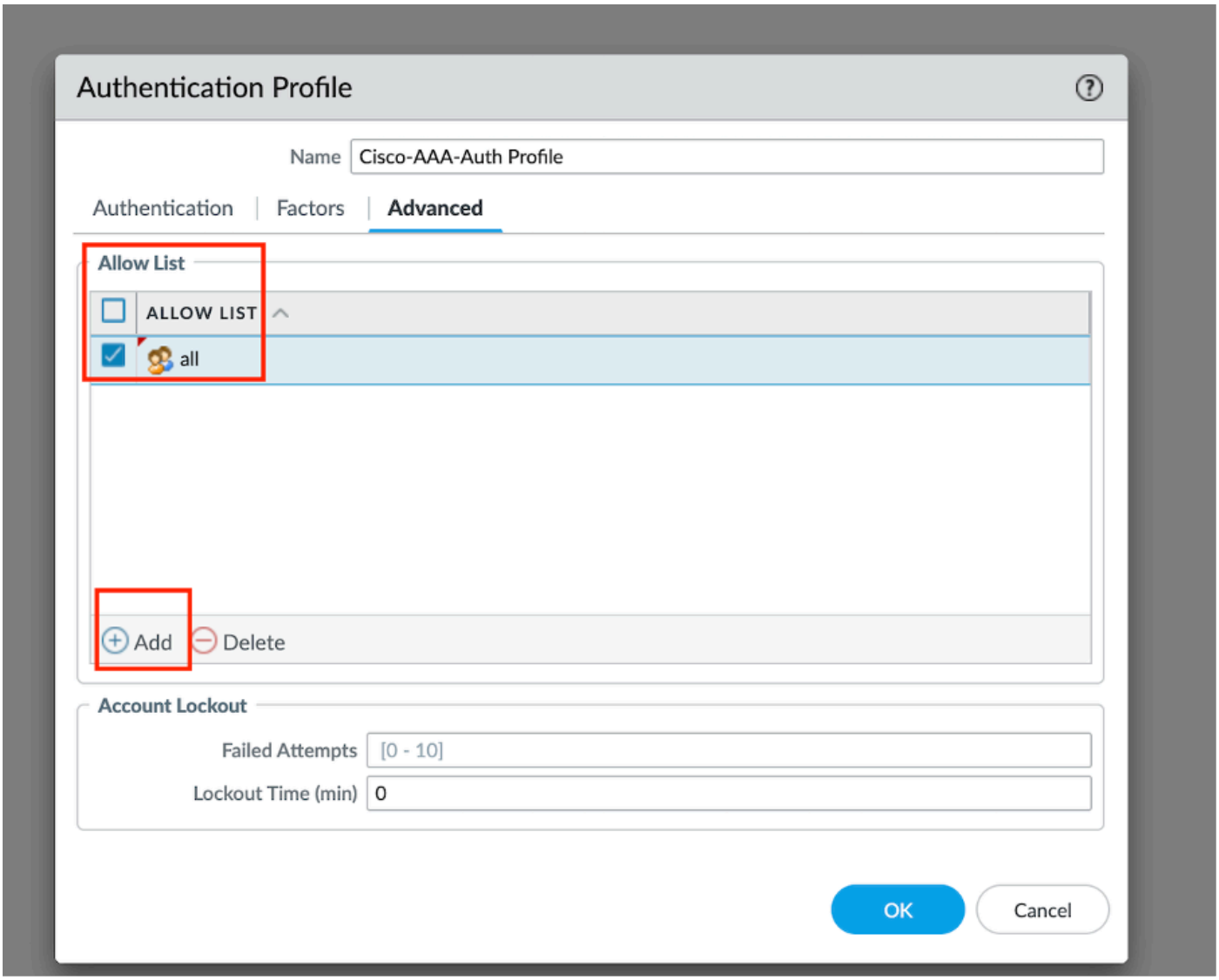
1. Wählen Sie Device > Authentication Profile aus, und fügen Sie ein Profil hinzu.
    1. Geben Sie einen Namen für das Profil ein.
    2. Legen Sie für Type (Typ) TACACS+ fest.
    3. Wählen Sie das von Ihnen konfigurierte Serverprofil aus.
    4. Wählen Sie Retrieve user group from TACACS+ (Benutzergruppe aus TACACS+ abrufen) aus, um Benutzergruppeninformationen von VSAs zu erfassen, die auf dem TACACS+-Server definiert sind.





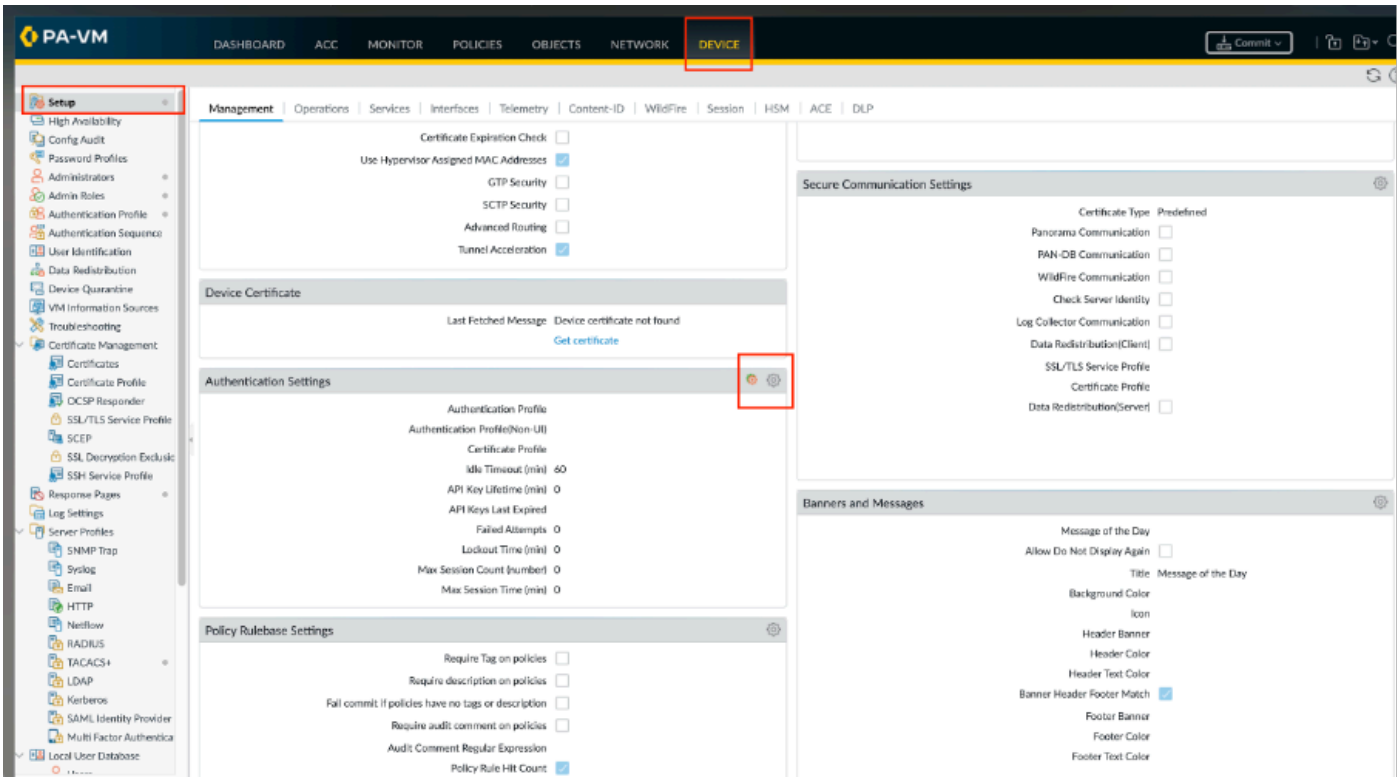
Die Firewall stimmt mit den Gruppeninformationen überein, indem die Gruppen verwendet werden, die Sie in der Zulassungsliste des Authentifizierungsprofils angeben.

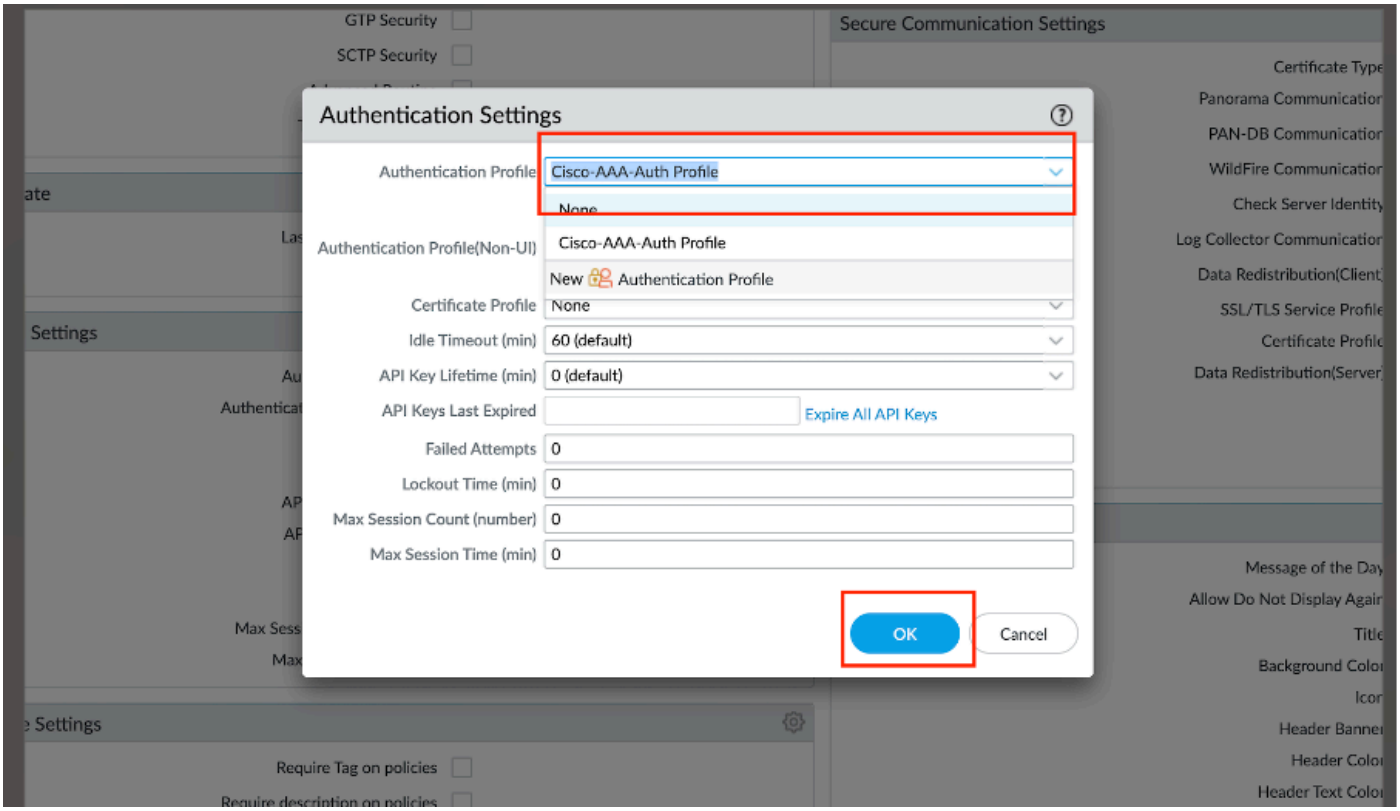
1. Wählen Sie Erweitert aus, und fügen Sie in der Zulassungsliste die Benutzer und Gruppen hinzu, die sich mit diesem Authentifizierungsprofil authentifizieren können.
2. Klicken Sie auf OK, um das Authentifizierungsprofil zu speichern.



Schritt 3: Konfigurieren Sie die Firewall so, dass das Authentifizierungsprofil für alle Administratoren verwendet wird.

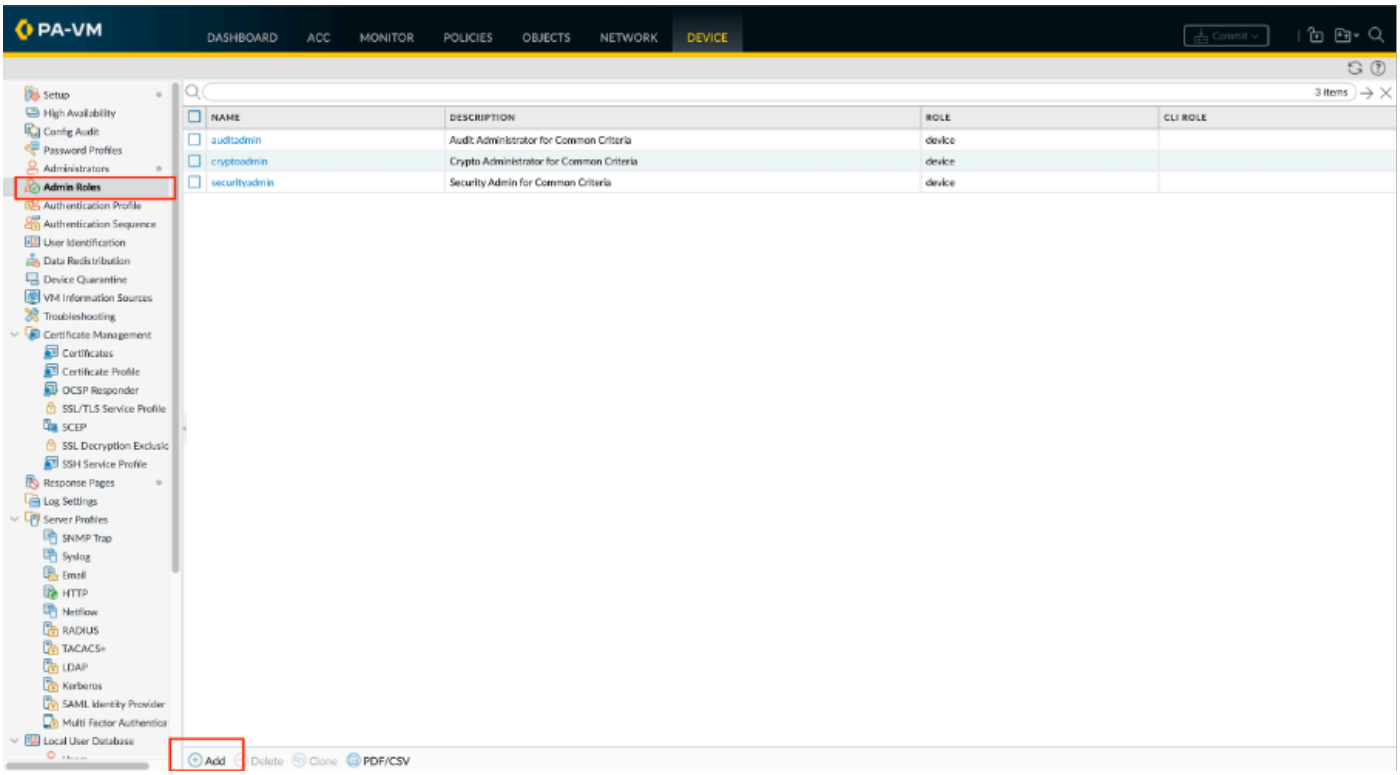
1. Wählen Sie Device > Setup > Management aus, und bearbeiten Sie die Authentifizierungseinstellungen.
2. Wählen Sie das konfigurierte Authentifizierungsprofil aus, und klicken Sie auf OK.



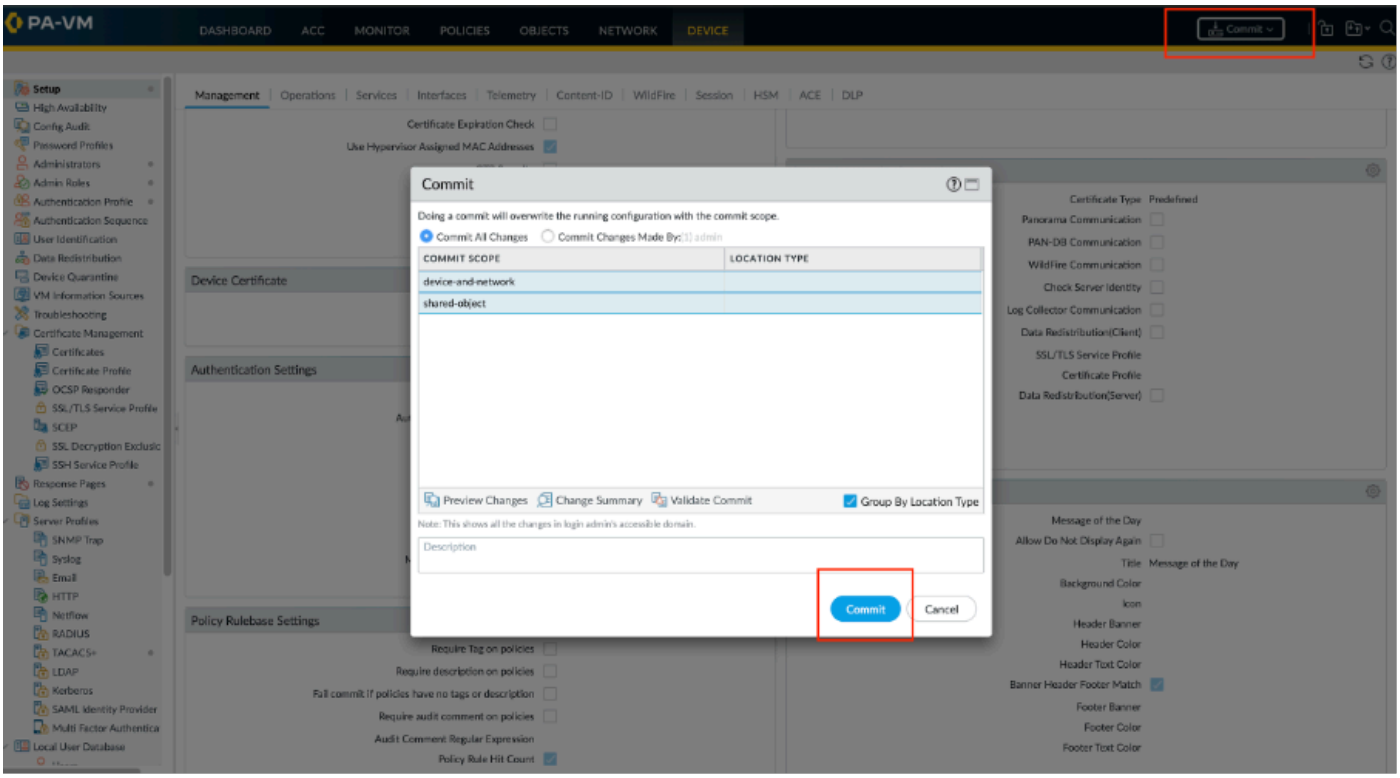


Schritt 4: Konfigurieren eines Admin-Rollenprofils

Wählen Sie Device > Admin Roles aus, und klicken Sie auf Add. Geben Sie einen Namen zur Identifizierung der Rolle ein.



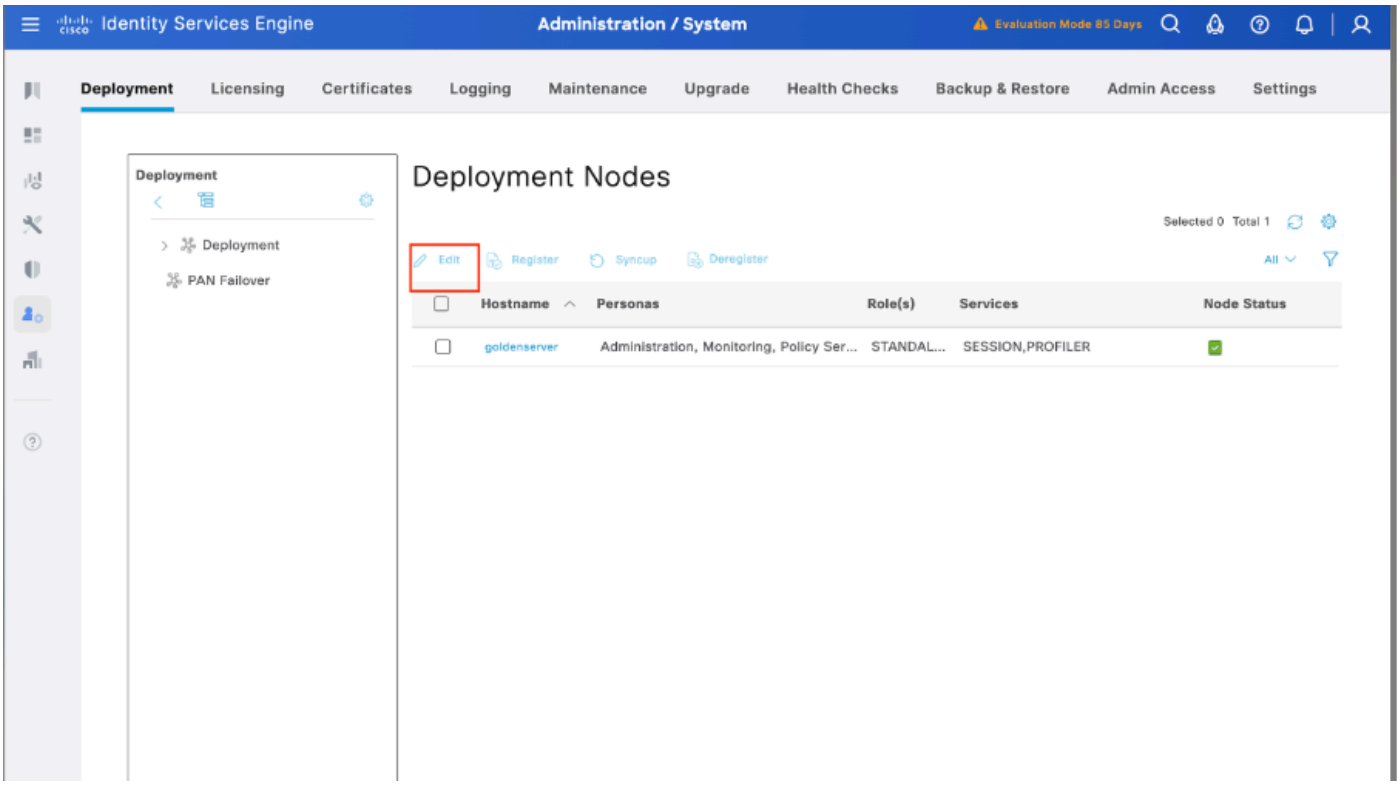
Schritt 5: Bestätigen Sie Ihre Änderungen, um sie auf der Firewall zu aktivieren.



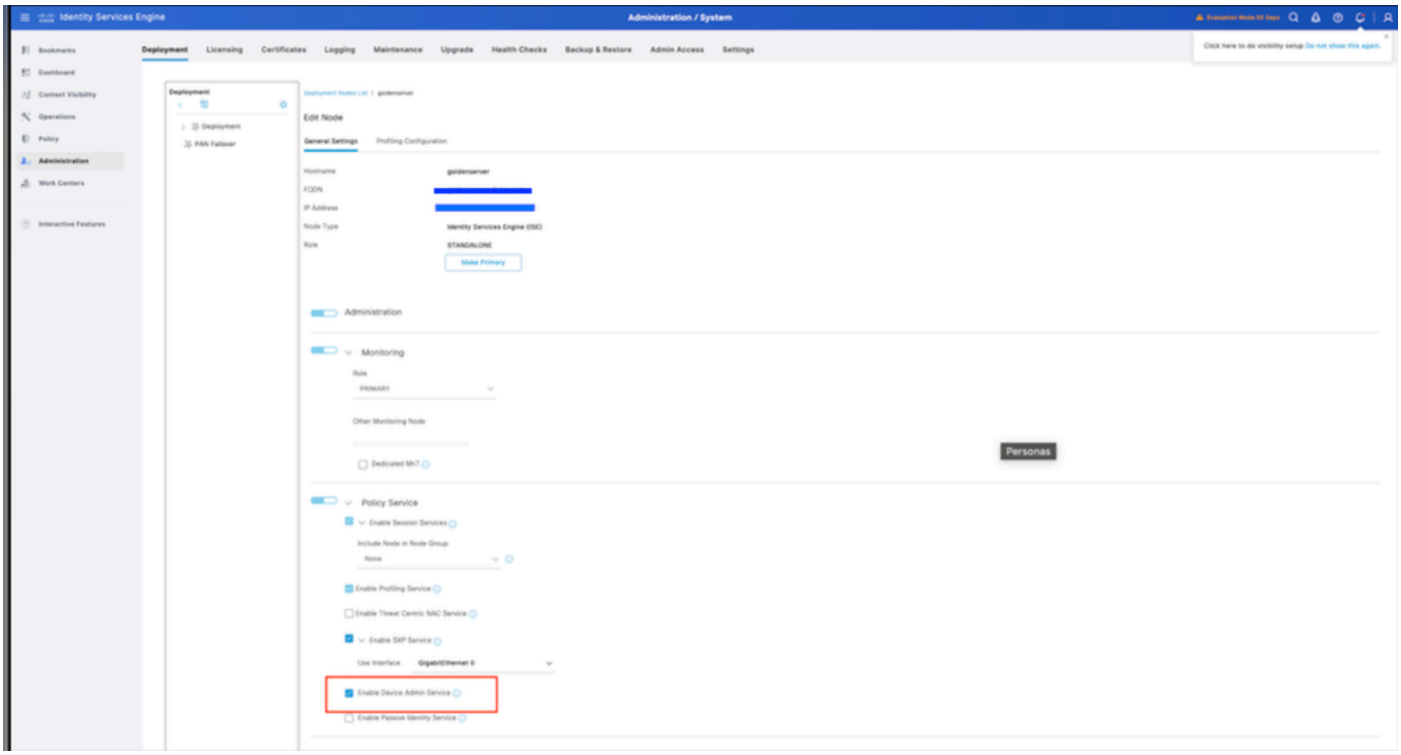
Abschnitt 2: TACACS+-Konfiguration auf der ISE

Schritt 1: Im ersten Schritt wird überprüft, ob die Cisco ISE über die erforderlichen Funktionen für die TACACS+-Authentifizierung verfügt. Vergewissern Sie sich dazu, dass die Funktion für den Geräteadministratordienst auf dem gewünschten Policy Service Node (PSN) aktiviert ist. Navigieren Sie zu Administration > System > Deployment, wählen Sie den entsprechenden

Knoten aus, auf dem ISE die TACACS+-Authentifizierung verarbeitet, und klicken Sie auf Edit, um die Konfiguration zu überprüfen.

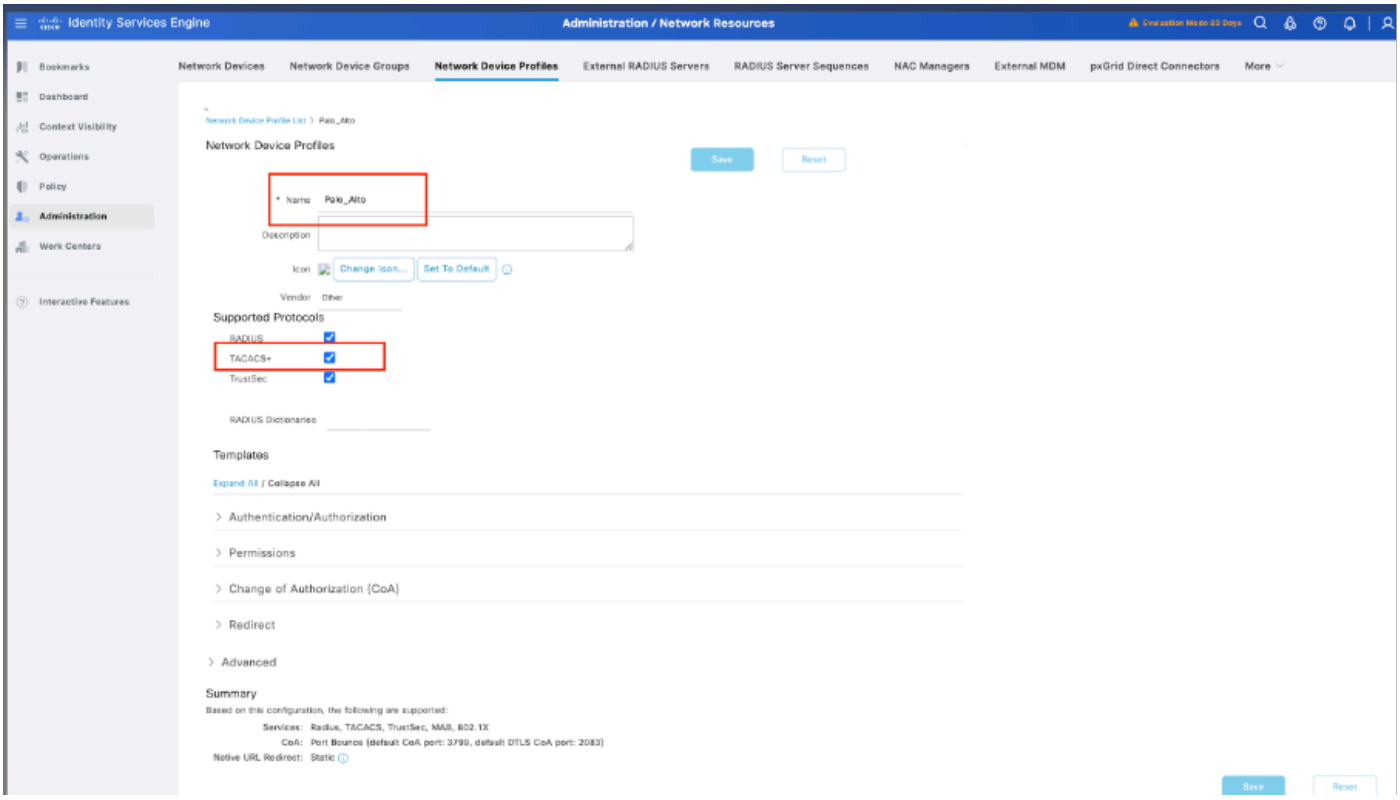


Schritt 2: Scrollen Sie nach unten, um nach der Device Administration Service-Funktion zu suchen. Beachten Sie, dass zur Aktivierung dieser Funktion die Rolle des Richtliniendiensts auf dem Knoten aktiv sein muss, zusammen mit den verfügbaren TACACS+-Lizenzen in der Bereitstellung. Aktivieren Sie das Kontrollkästchen, um die Funktion zu aktivieren, und speichern Sie dann die Konfiguration.



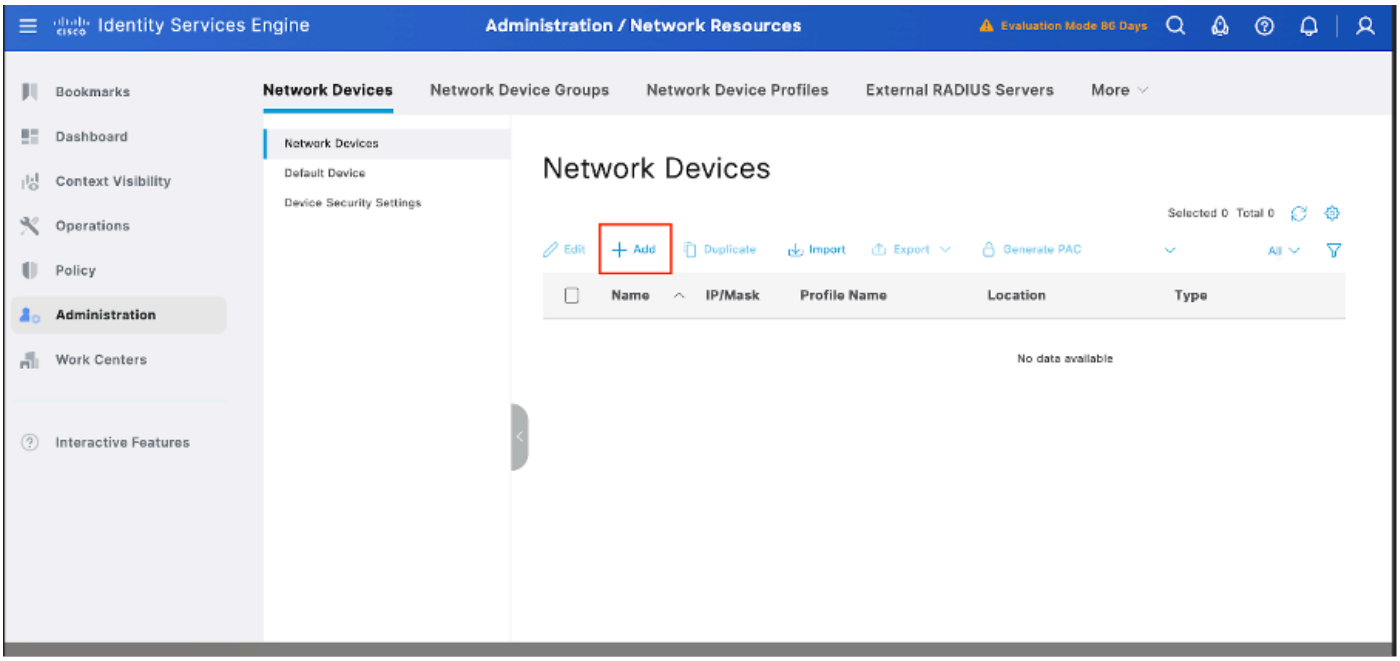
Schritt 3: Konfigurieren des Palo Alto-Netzwerkgeräteprofils für die Cisco ISE

Navigieren Sie zu Administration > Network Resources > Network Device Profile. Klicken Sie auf Hinzufügen, und geben Sie den Namen (Palo Alto) an, und aktivieren Sie TACACS+ unter den unterstützten Protokollen.



Schritt 4: Hinzufügen von Palo Alto als Netzwerkgerät.

1. Navigieren Sie zu Administration > Network Resources > Network Devices > +Add.



2. Klicken Sie auf Hinzufügen, und geben Sie folgende Details ein:

Name: Palo-Alto

IP-Adresse: <Palo-Alto-IP>

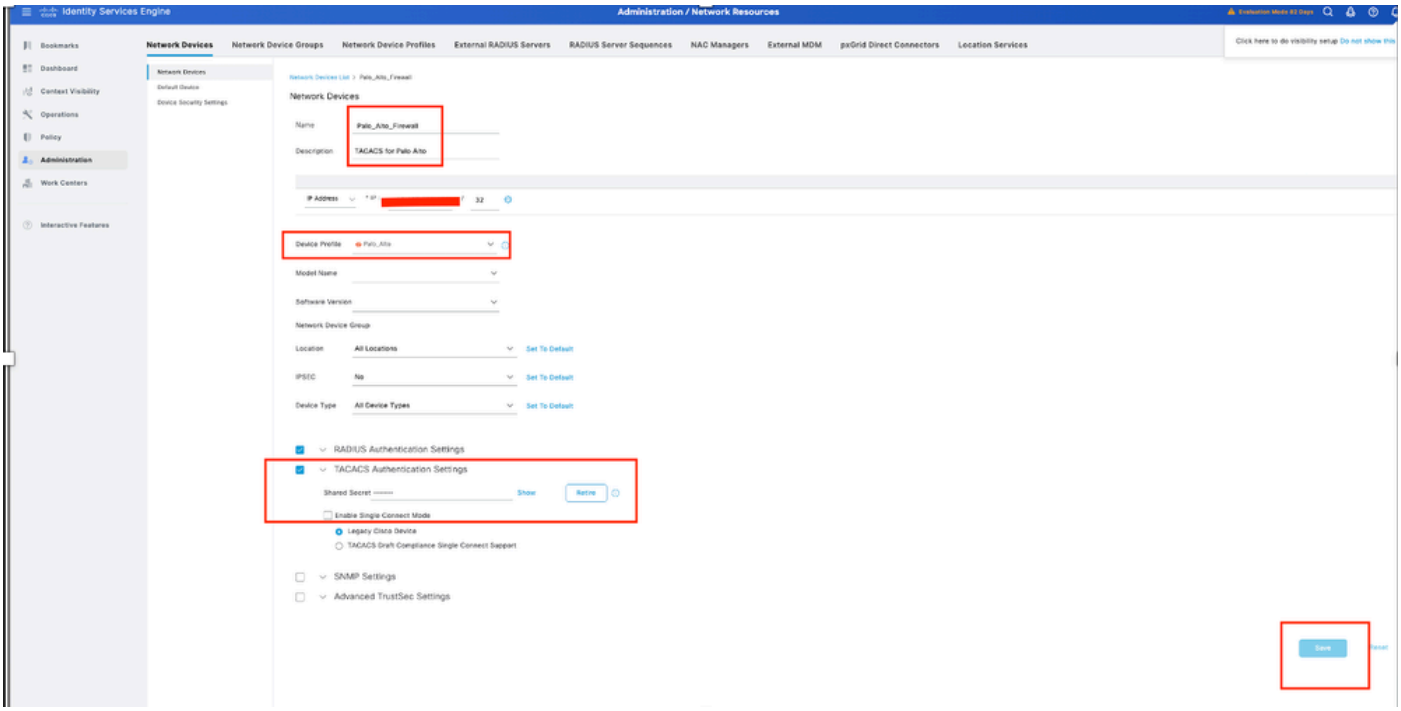
Netzwerk-Geräteprofil: Palo Alto auswählen

TACACS-Authentifizierungseinstellungen:

TACACS+-Authentifizierung aktivieren

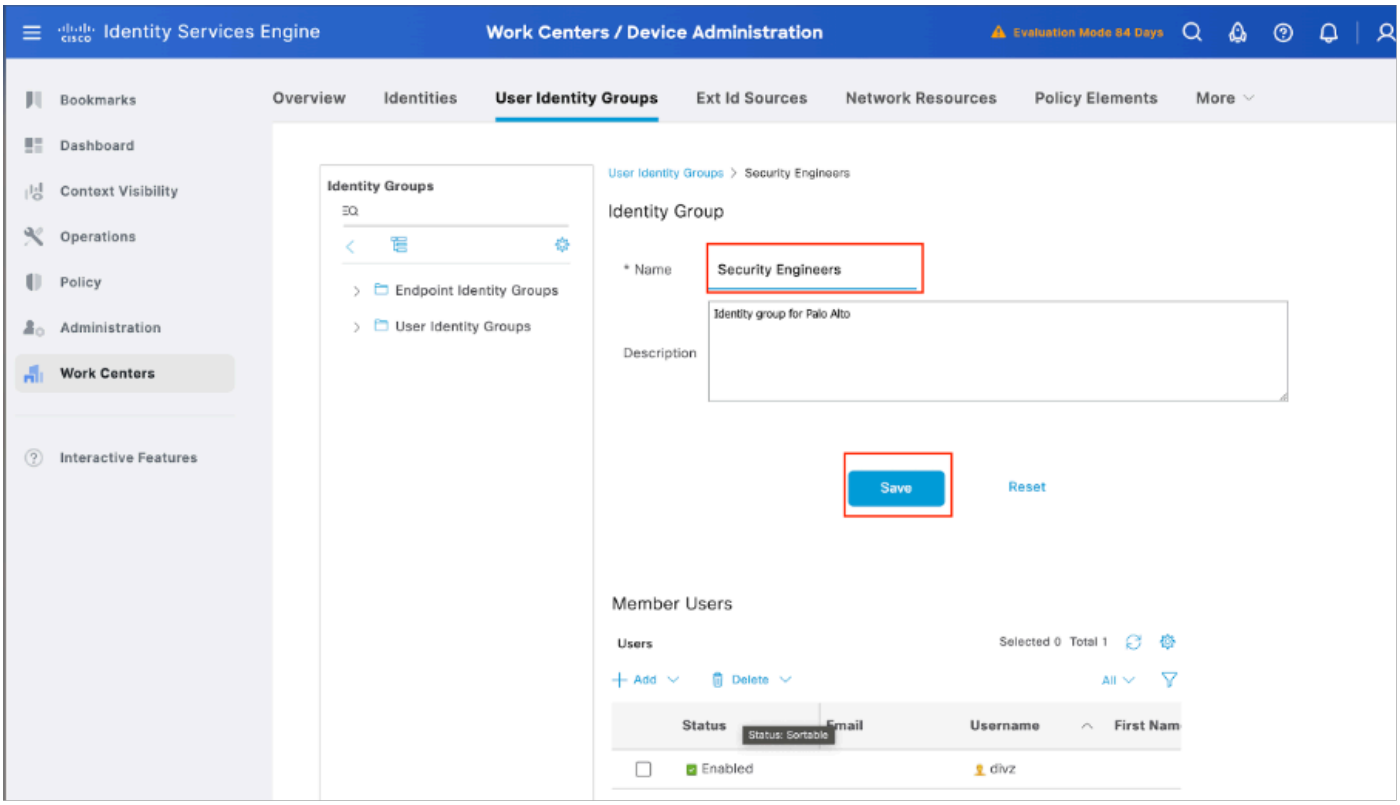
Geben Sie den gemeinsamen Schlüssel ein (muss mit der Palo Alto-Konfiguration übereinstimmen).

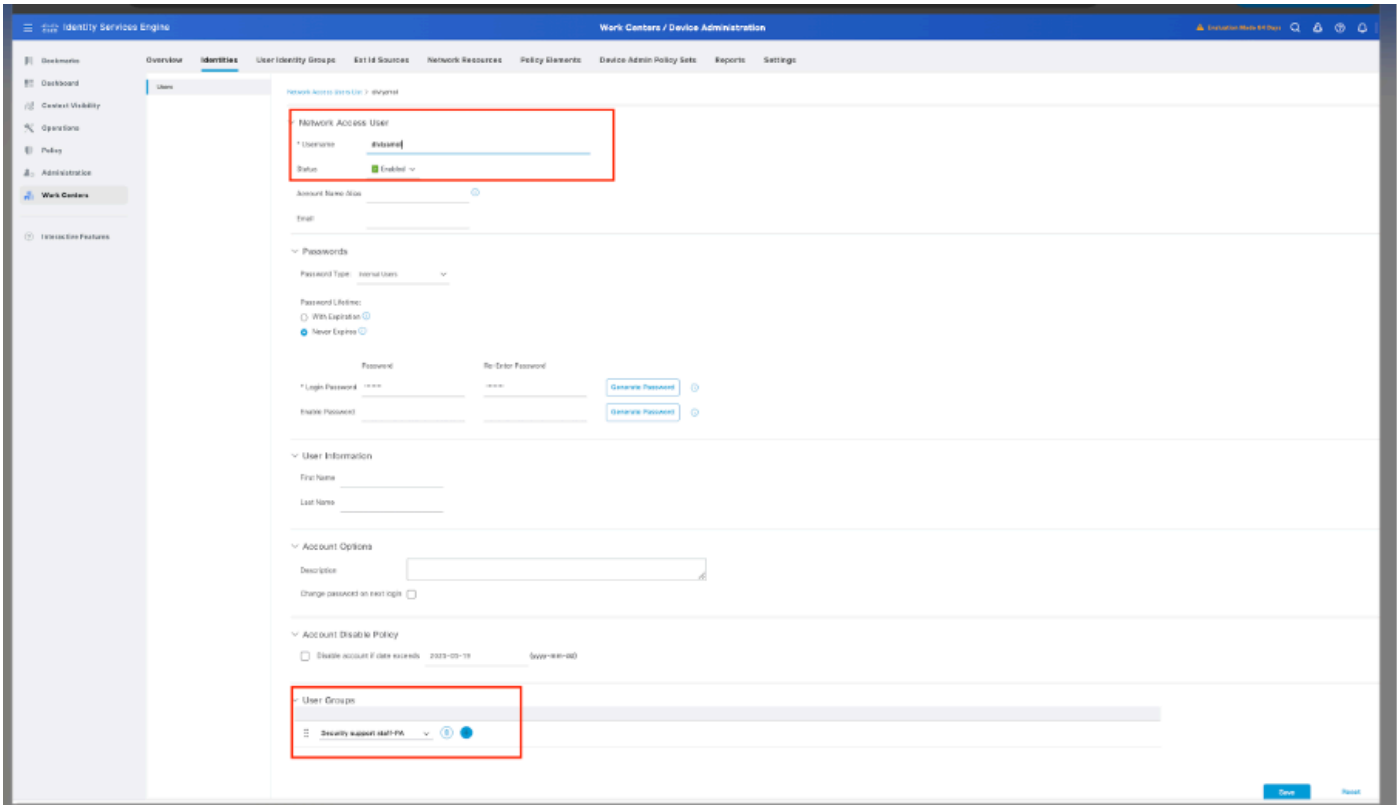
Klicken Sie auf Speichern.

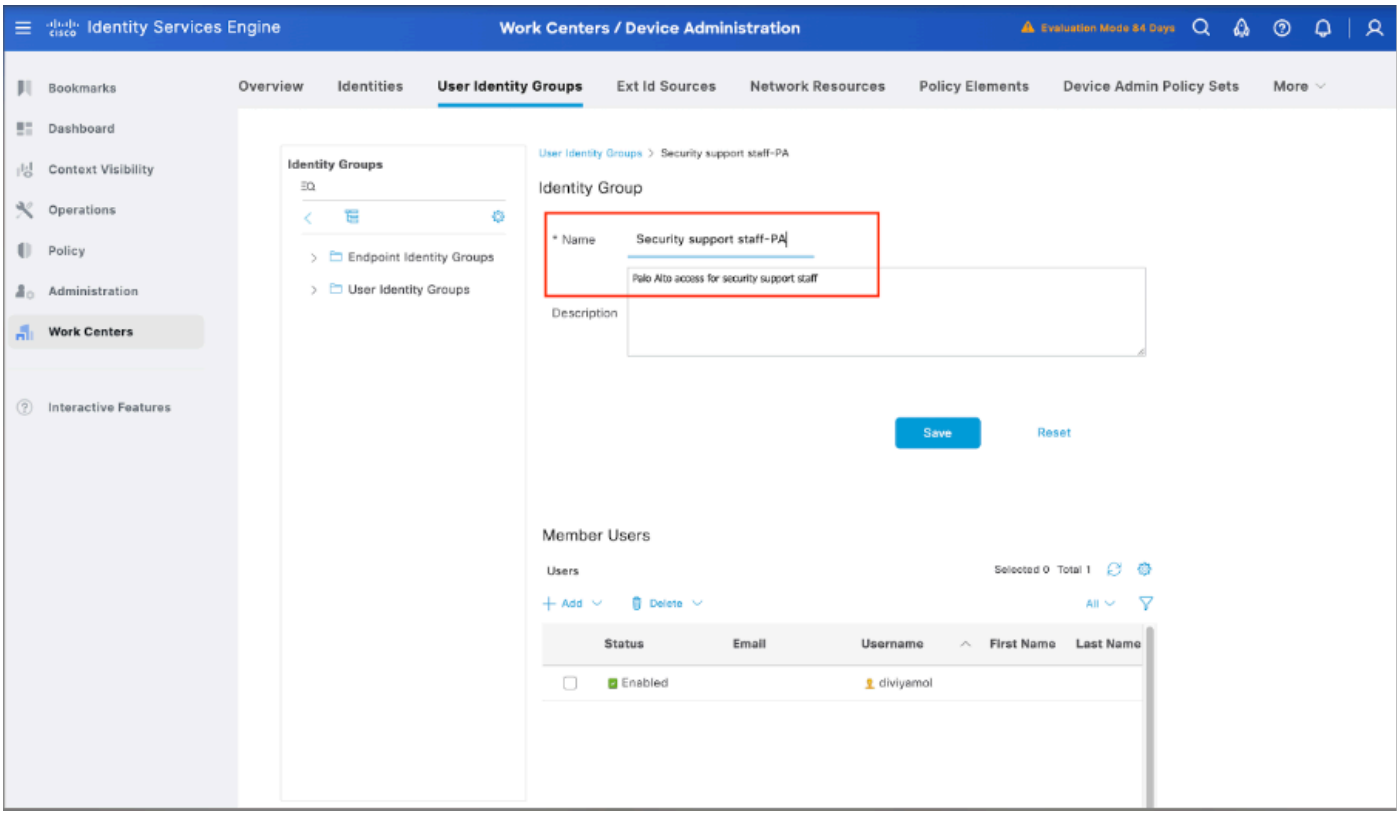


Schritt 5: Erstellen von Benutzeridentitätsgruppen

Navigieren Sie zu Work Centers > Device Administration > User Identity Groups, und klicken Sie dann auf Add (Hinzufügen), und geben Sie den Namen der Benutzergruppe an.


Identity Services Engine
Work Centers / Device Administration
Evaluation Mode 84 Days
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Features
Overview
Identities
User Identity Groups
Ext Id Sources
Network Resources
Policy Elements
More
Identity Groups
Endpoint Identity Groups
User Identity Groups
User Identity Groups > Security Engineers
Identity Group
* Name
Security Engineers
Description
Identity group for Palo Alto
Save
Reset
Member Users
Users
Selected 0 Total 1
Add
Delete
All
Status
Email
Username
First Nam
Status: Sortable
Enabled
divz

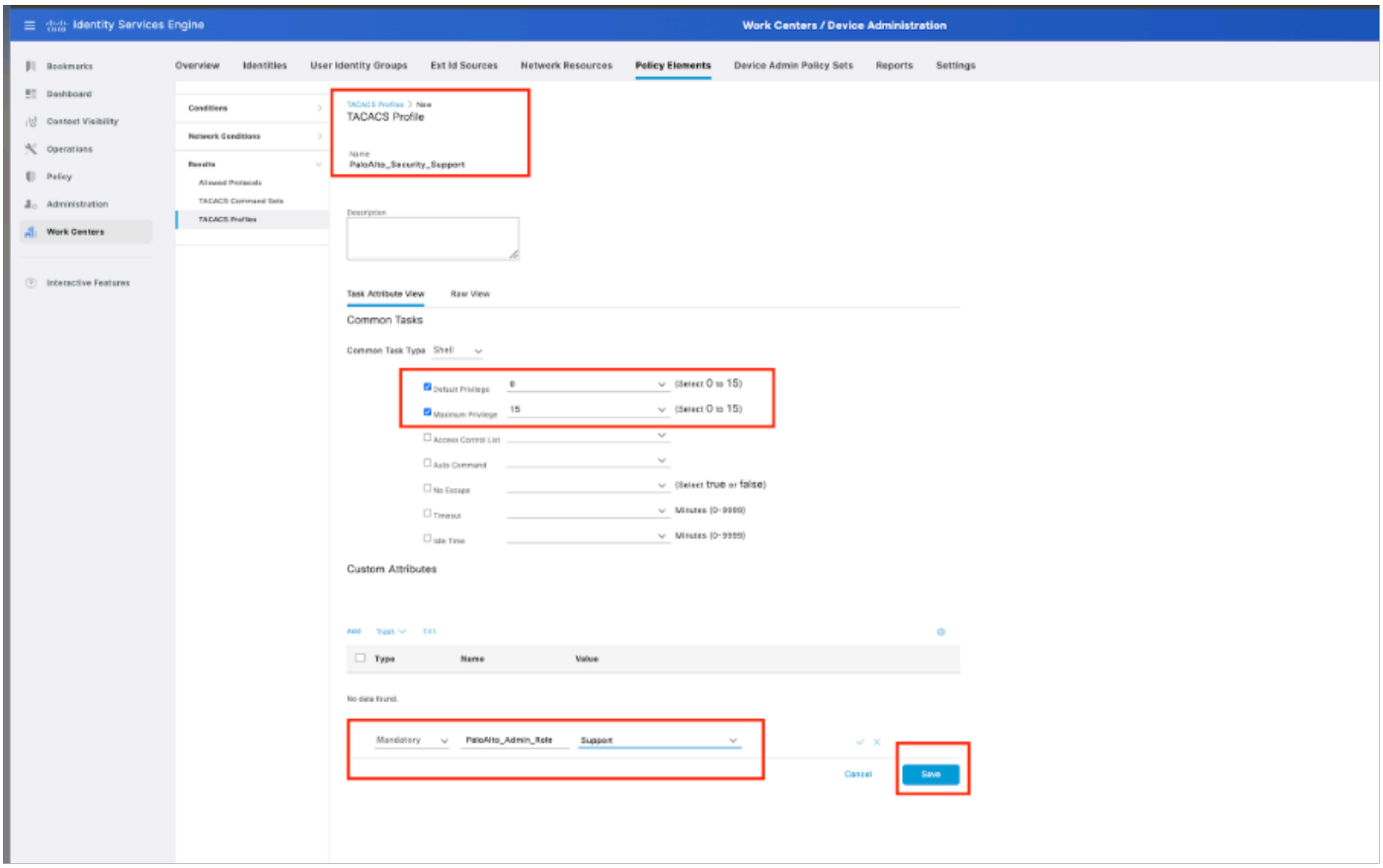

Identity Services Engine
Work Centers / Device Administration
Network Access User
Passwords
User Information
Account Options
Account Disable Policy
User Groups

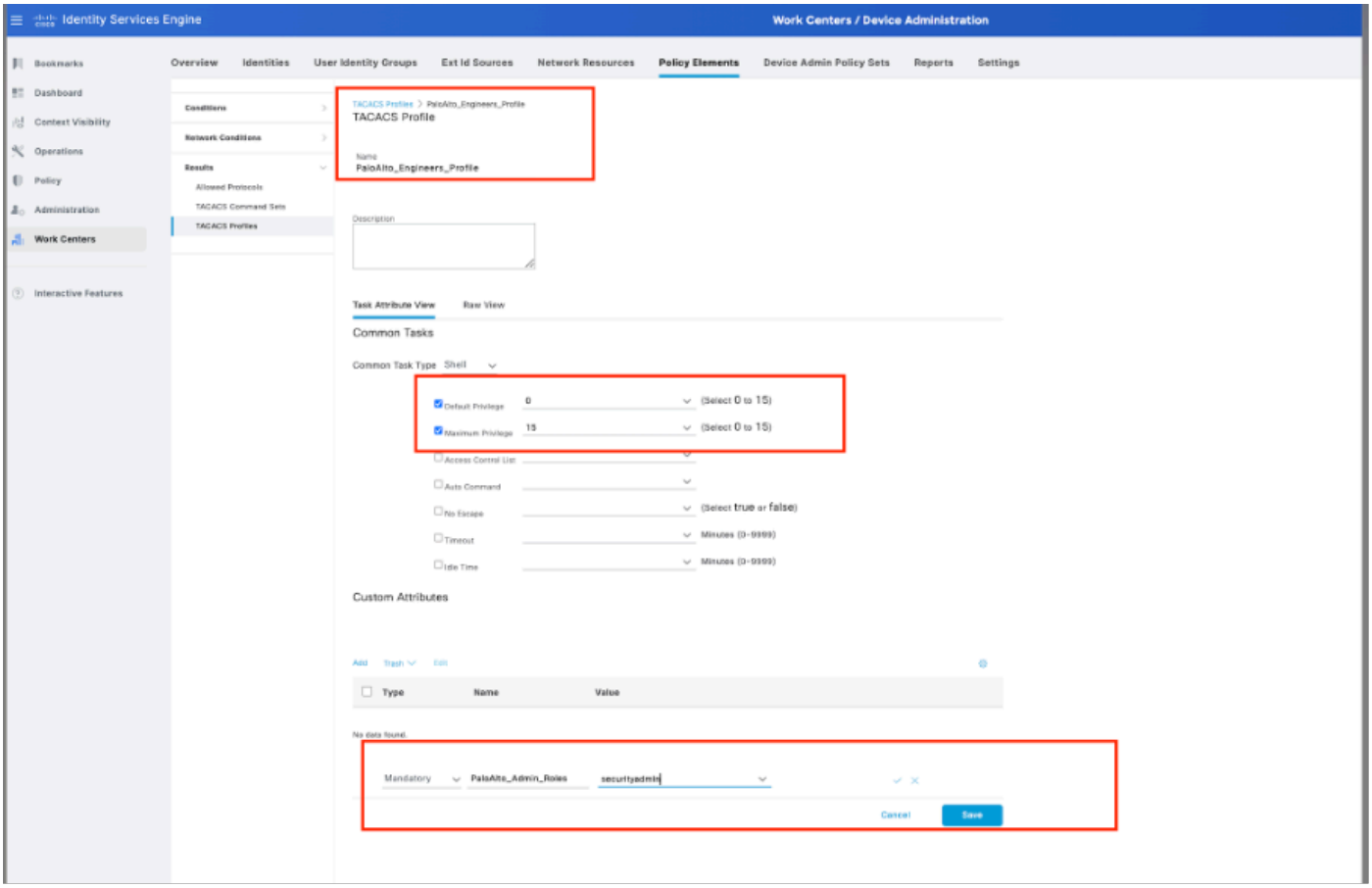


Schritt 6: Konfigurieren eines TACACS-Profils

Als Nächstes konfigurieren Sie ein TACACS-Profil, in dem Sie Einstellungen wie die Privilegstufe und Timeout-Einstellungen konfigurieren können. Navigieren Sie zu Work Centers > Device Administration -> Policy Elements -> Results -> TACACS Profiles.

Klicken Sie auf Hinzufügen, um ein neues TACACS-Profil zu erstellen. Geben Sie dem Profil einen guten Namen.





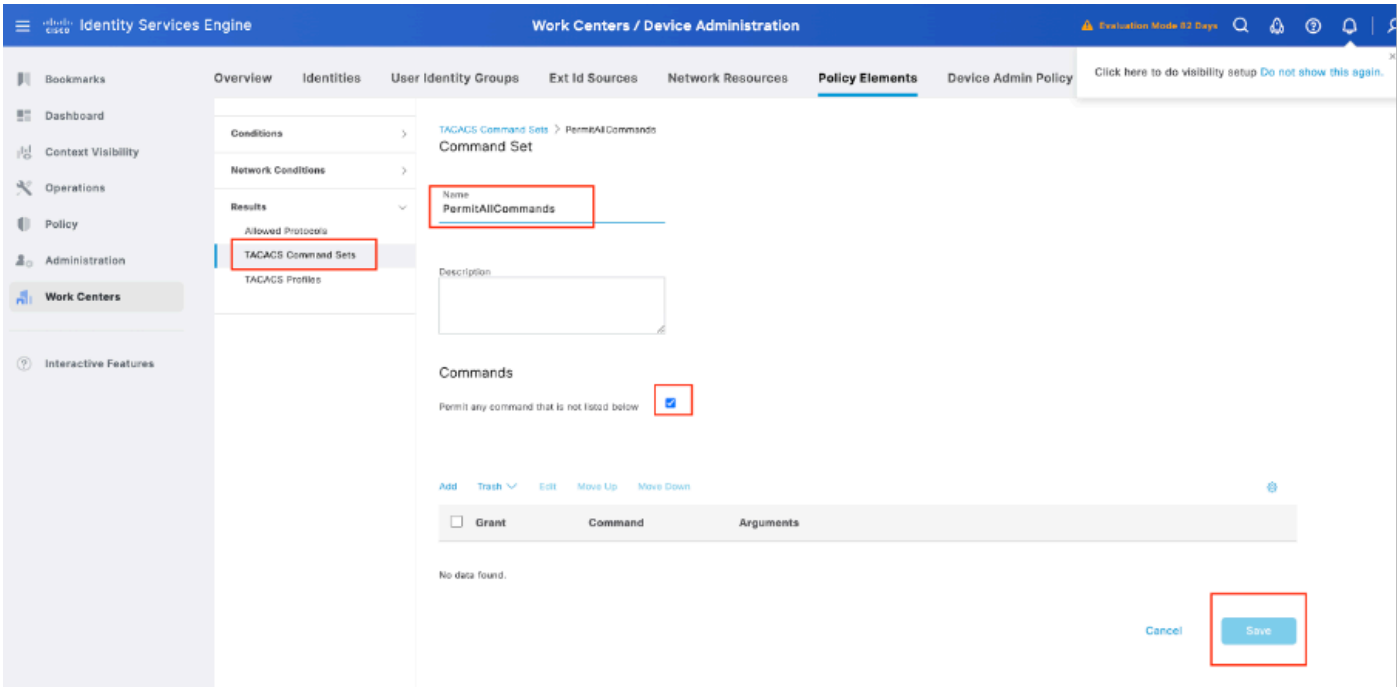
Schritt 6: Konfigurieren von TACACS-Befehlssätzen

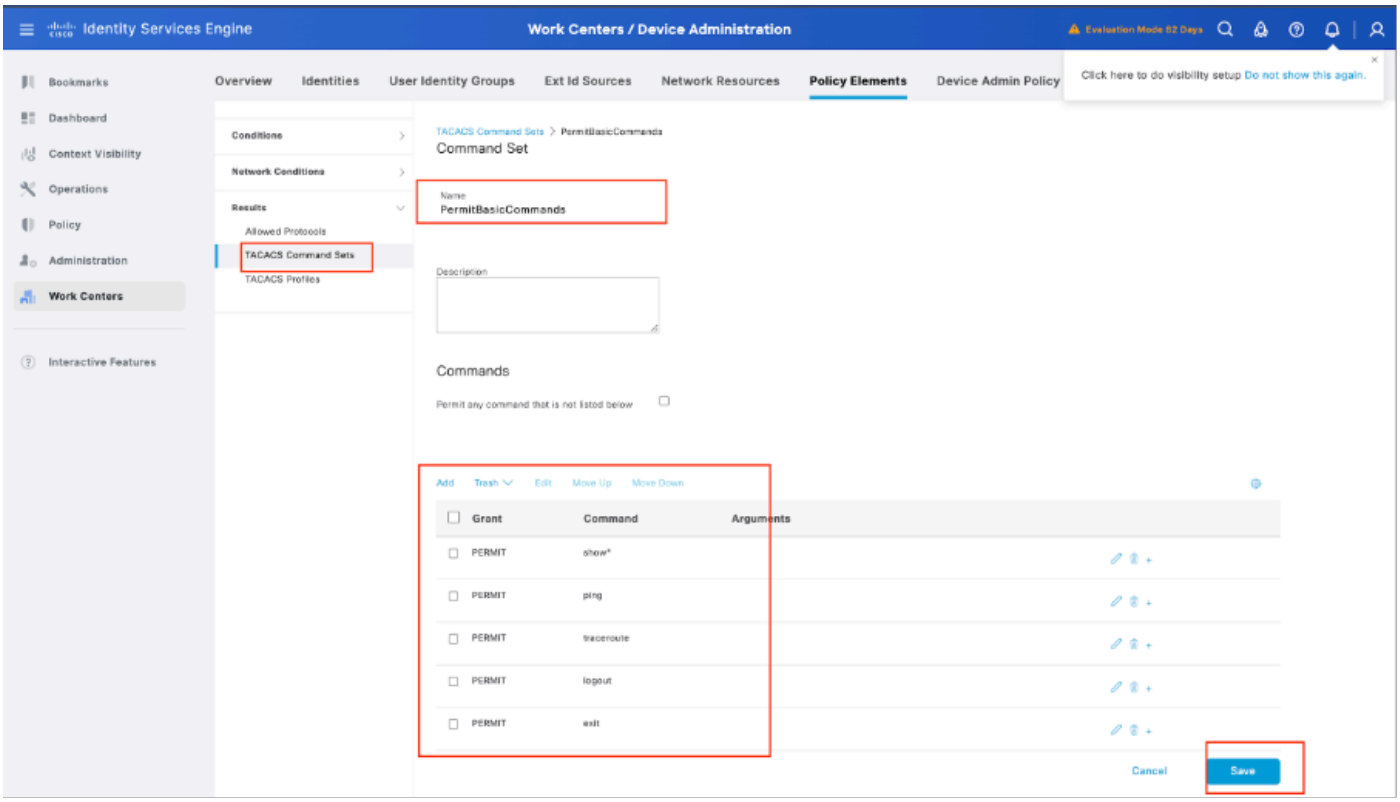
Nun ist es an der Zeit zu konfigurieren, welche Befehle Benutzer verwenden dürfen. Da Sie

beiden Anwendungsfällen die Berechtigungsstufe 15 zuweisen können, die den Zugriff auf alle verfügbaren Befehle ermöglicht, verwenden Sie TACACS-Befehlssätze, um die verwendbaren Befehle zu begrenzen.

Navigieren Sie zu Work Centers > Device Administration > Policy Elements > Results -> TACACS Command Sets. Klicken Sie auf Hinzufügen, um einen neuen TACACS-Befehlssatz zu erstellen und ihm den Namen PermitAllCommands zu geben. Wenden Sie diesen TACACS-Befehlssatz für die Sicherheitsunterstützung an.

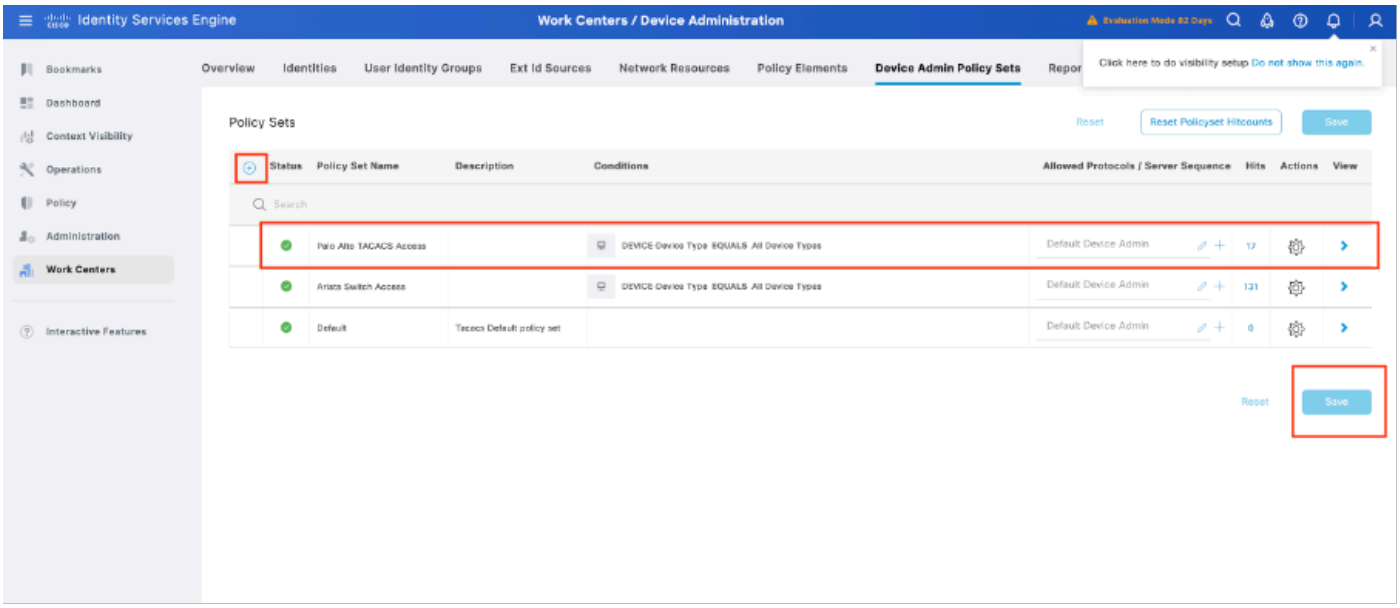
In diesem TACACS-Befehlssatz müssen Sie lediglich das Kontrollkästchen Befehle zulassen aktivieren, das unten nicht aufgeführt ist.





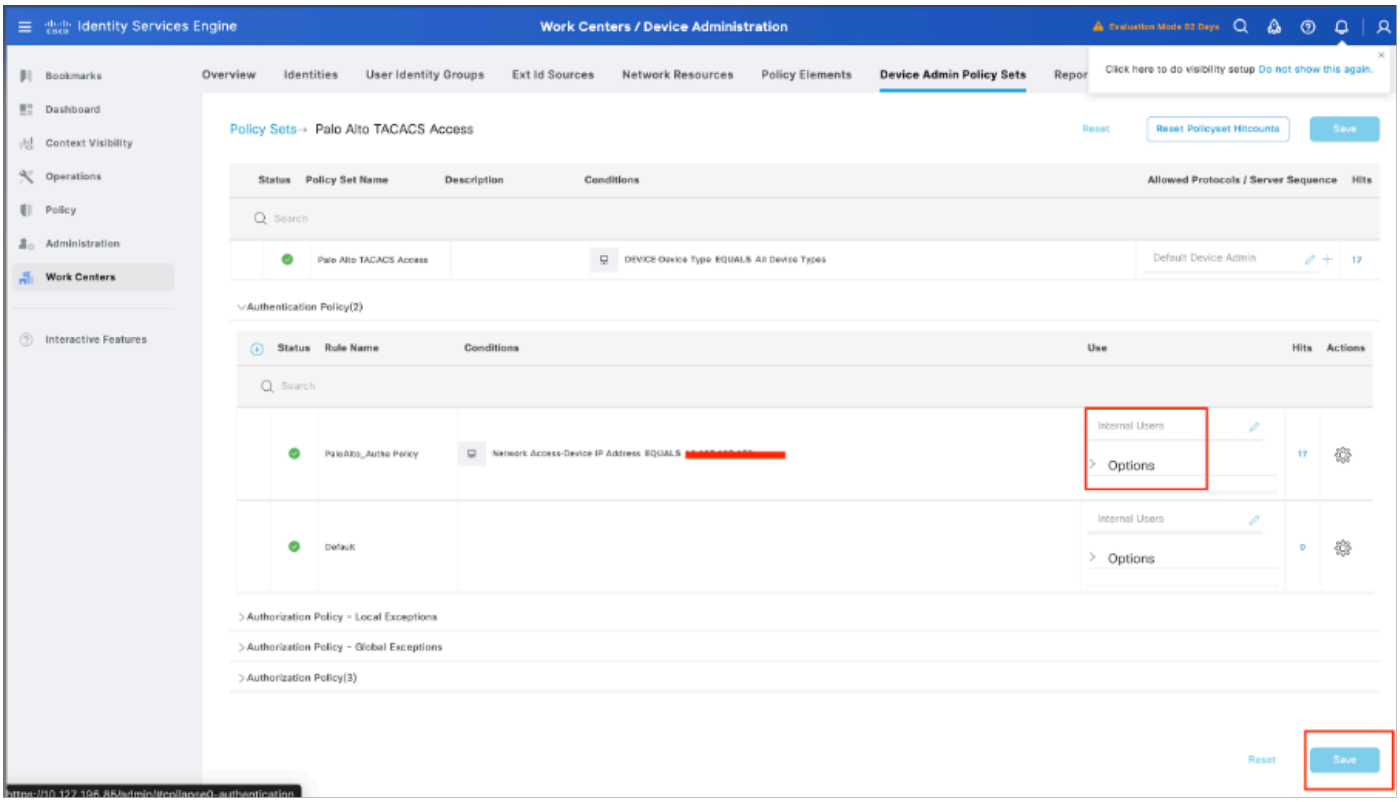
Schritt 7: Erstellen Sie ein Gerät Admin Policy Set für Ihren Palo Alto verwendet werden, Navigieren Sie im Menü Work Centers > Device Administration > Device Admin Policy Sets, klicken Sie auf die Hinzufügen + Symbol.

Schritt 8: Benennen Sie diesen neuen Richtliniensatz, fügen Sie Bedingungen hinzu, die von den Merkmalen der TACACS+-Authentifizierungen abhängen, die von der Palo Alto Firewall aus durchgeführt werden, und wählen Sie Zulässige Protokolle > Standardgeräteadministrator. Speichern Sie Ihre Konfiguration.

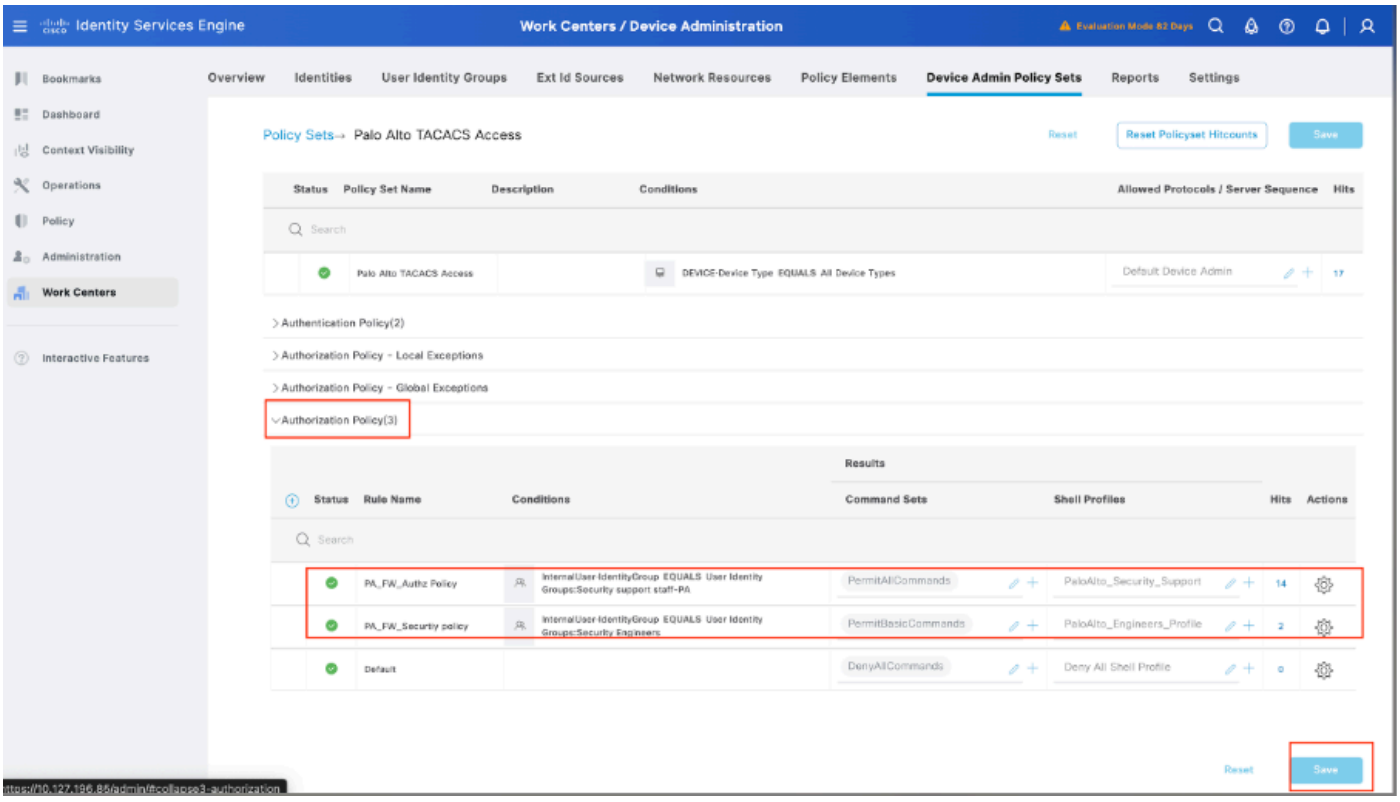


Schritt 9: Wählen Sie in der Option > view (Ansicht) und dann im Abschnitt Authentication Policy (Authentifizierungsrichtlinie) die externe Identitätsquelle aus, die Cisco ISE verwendet, um den Benutzernamen und die Anmeldeinformationen für die Authentifizierung in der Palo Alto Firewall

abzufragen. In diesem Beispiel entsprechen die Anmeldeinformationen internen Benutzern, die in der ISE gespeichert sind.



Schritt 10: Blättern Sie nach unten bis zum Abschnitt "Autorisierungsrichtlinie", bis die Standardrichtlinie angezeigt wird, wählen Sie das Zahnradsymbol aus, und fügen Sie eine Regel oben ein.



Schritt 11: Benennen Sie die neue Autorisierungsregel, fügen Sie Bedingungen für den Benutzer

hinzu, der bereits als Gruppenmitgliedschaft authentifiziert wurde, und speichern Sie die Konfiguration im Abschnitt "Shell Profiles" (Shell-Profile), und fügen Sie das zuvor konfigurierte TACACS-Profil hinzu.

Überprüfung

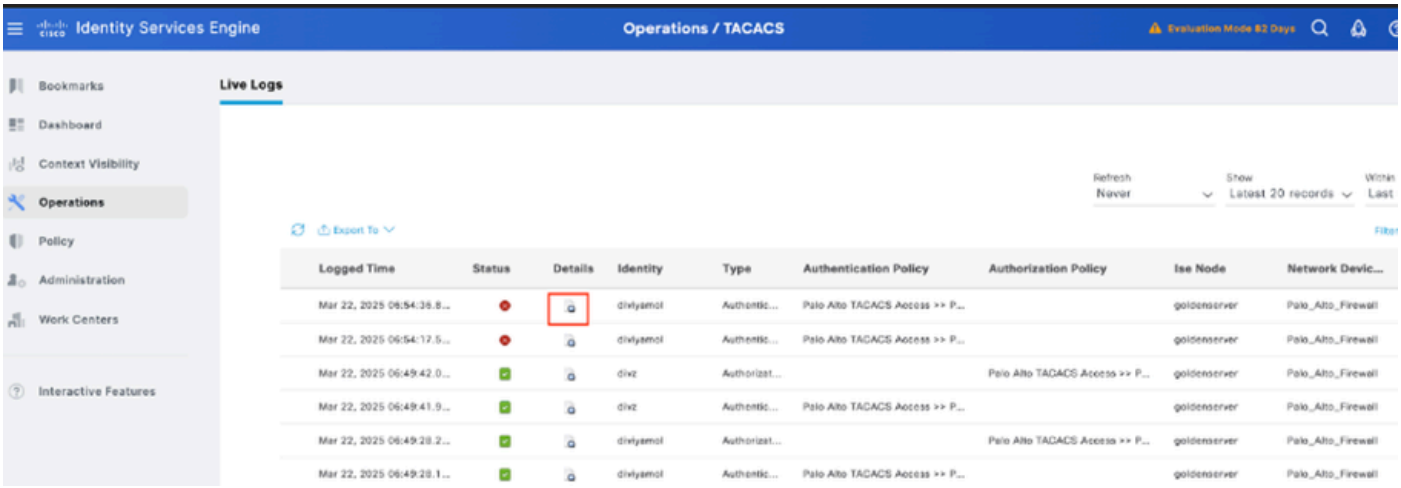
ISE-Prüfung

Schritt 1: Überprüfen Sie, ob die TACACS+-Wartungsfreundlichkeit ausgeführt wird. Dies kann wie folgt eingecheckt werden:

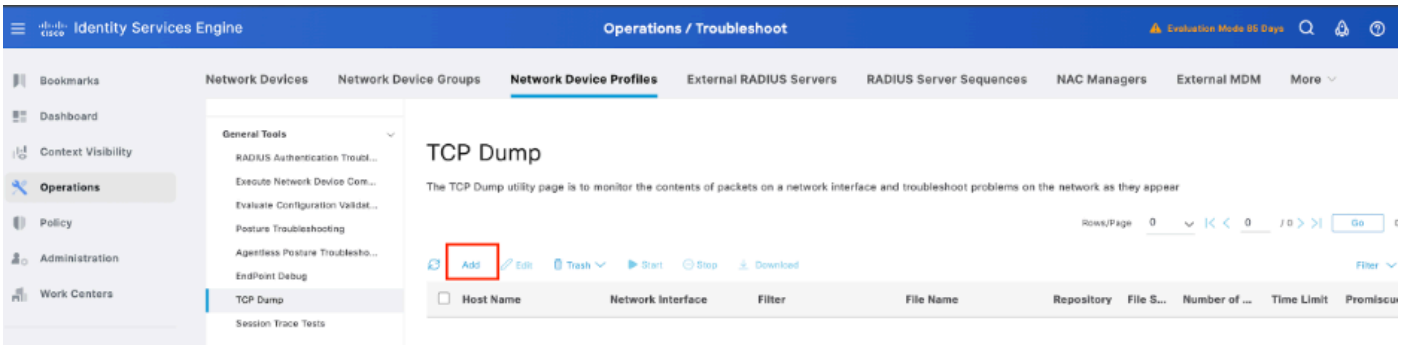
- GUI: Überprüfen Sie, ob der Knoten mit dem Dienst GERÄTEADMIN unter Administration -> System -> Deployment aufgeführt ist.
- CLI: Führen Sie den Befehl show ports aus. | einschließlich 49, um zu bestätigen, dass es Verbindungen im TCP-Port gibt, die zu TACACS+ gehören.

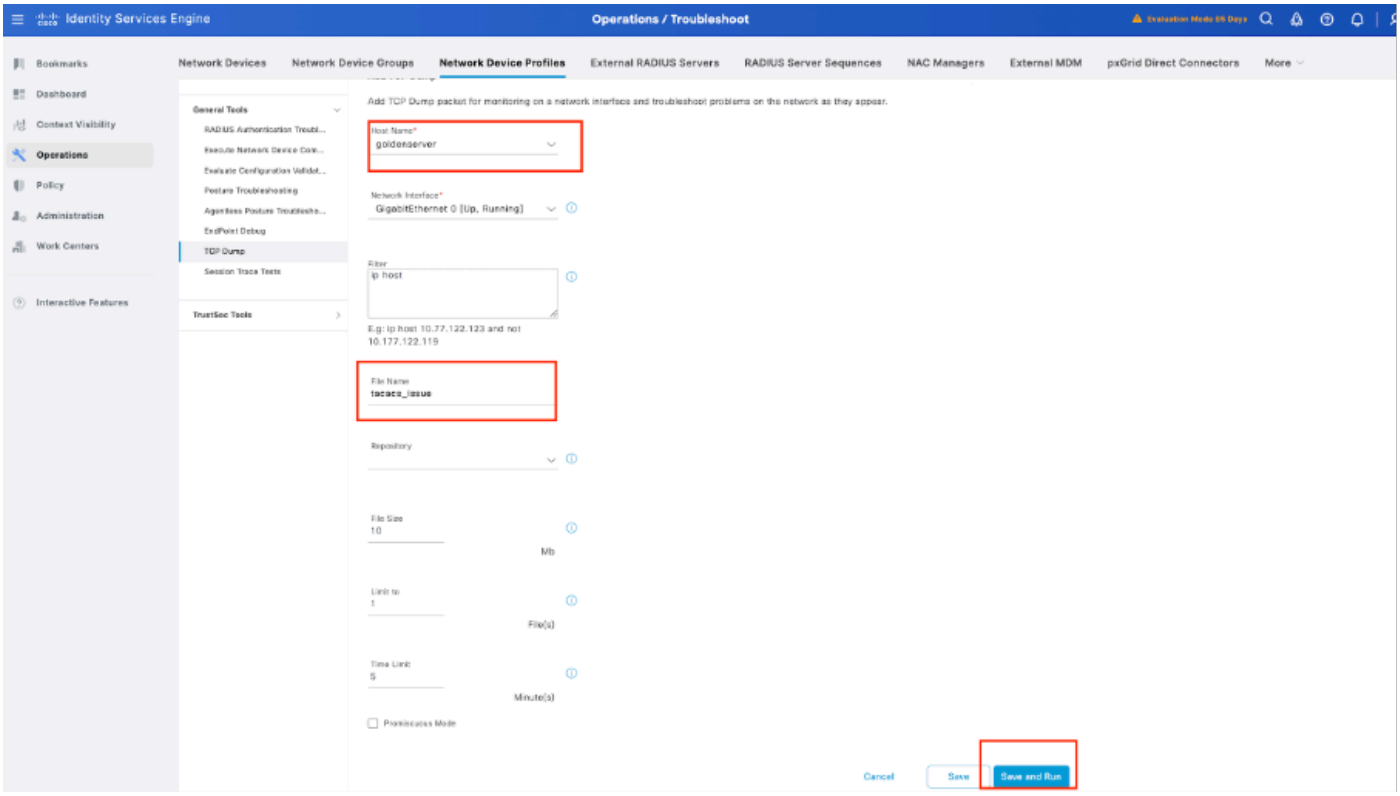
Schritt 2: Bestätigen Sie, ob Live-Protokolle mit TACACS+-Authentifizierungsversuchen vorhanden sind: Dies kann im Menü Operationen -> TACACS -> Live-Protokolle überprüft werden.

Abhängig vom Fehlergrund können Sie die Konfiguration anpassen oder die Fehlerursache beheben.

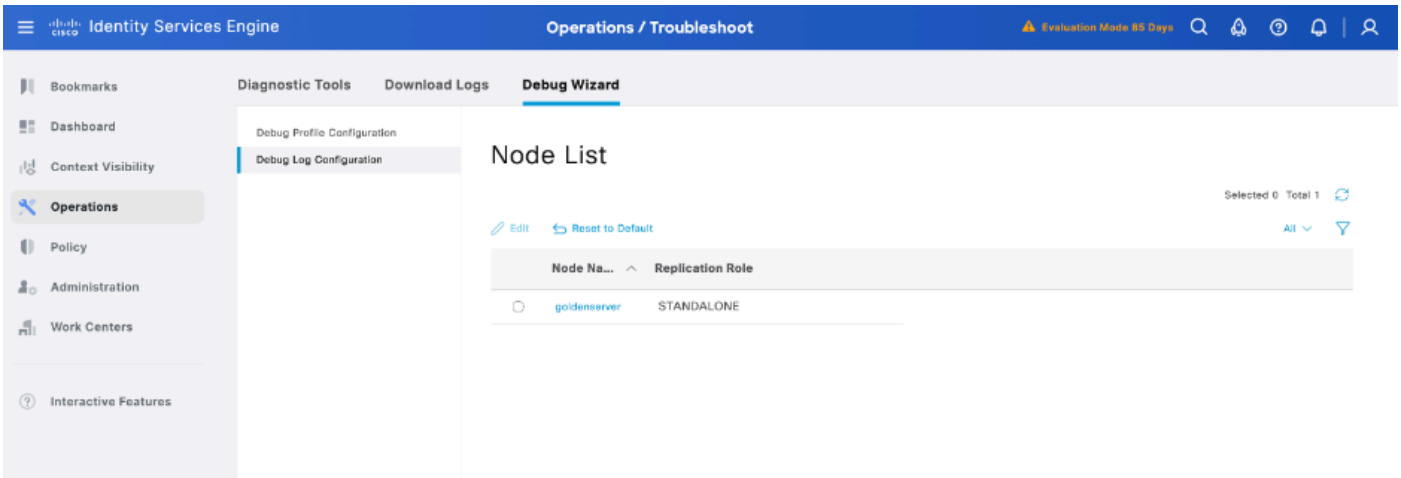


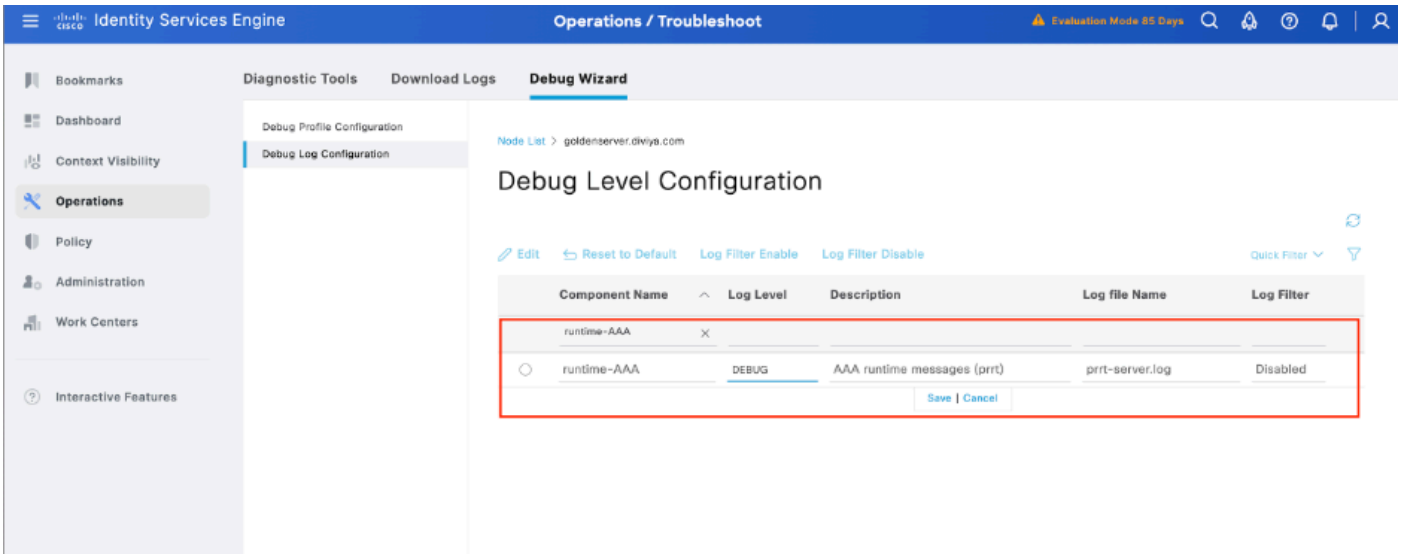
Schritt 3: Falls kein Live-Protokoll angezeigt wird, fahren Sie mit der Paketerfassung fort, navigieren Sie zum Menü Vorgänge > Fehlerbehebung > Diagnosetools > Allgemeine Tools > TCP-Dump, und wählen Sie Hinzufügen.





Schritt 4. Aktivieren Sie die Komponente Laufzeit-AAA im Debugging innerhalb des PSN, von wo aus die Authentifizierung durchgeführt wird in Operationen > Fehlerbehebung > Debug-Assistent > Debug-Protokollkonfiguration, wählen Sie PSN-Knoten, wählen Sie dann Weiter in Bearbeiten-Taste .





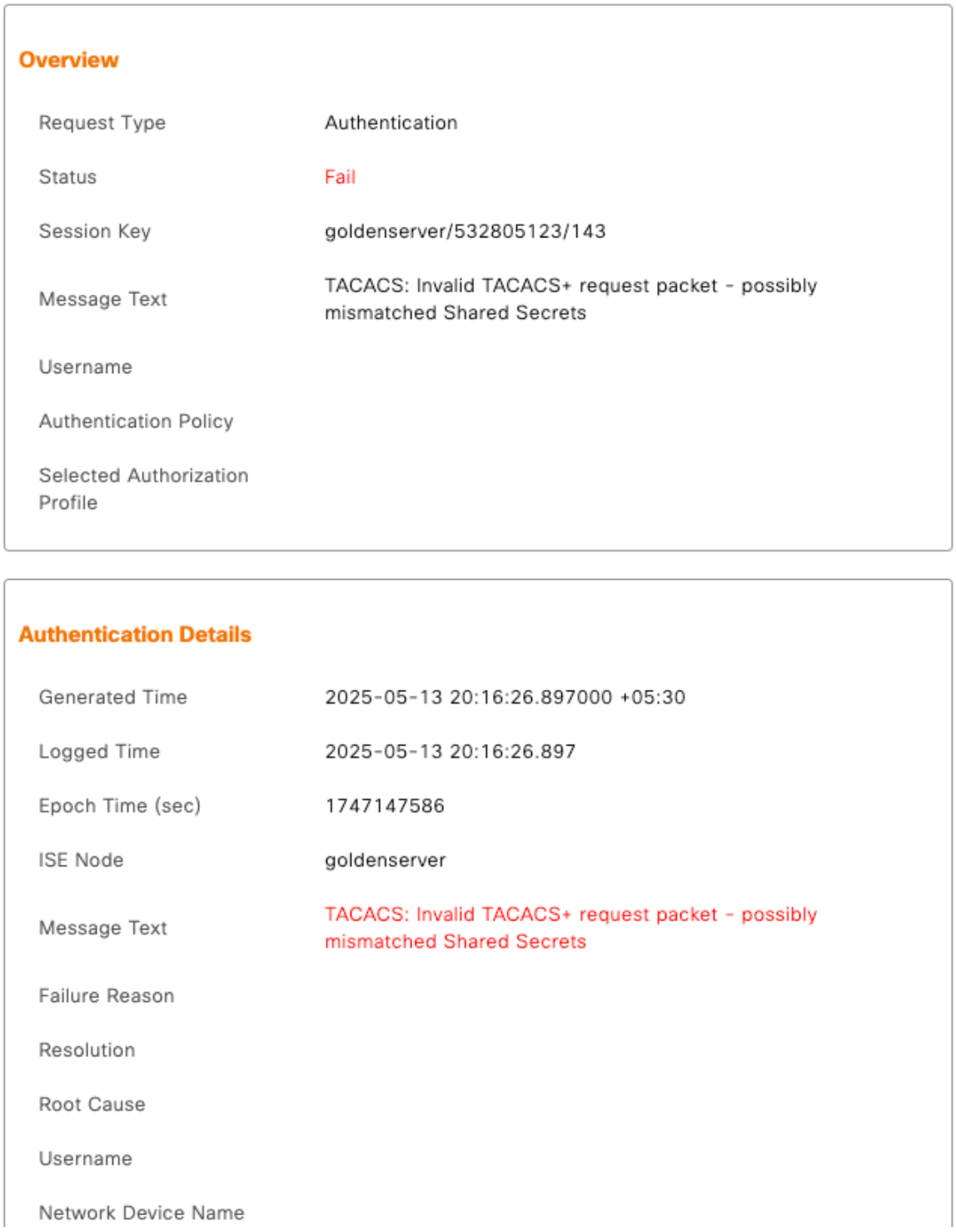
Identifizieren Sie die Laufzeit-AAA-Komponente, legen Sie deren Protokollierungsebene auf debug fest, reproduzieren Sie das Problem, und analysieren Sie die Protokolle für weitere Untersuchungen.

Fehlerbehebung

TACACS Ungültiges TACACS+-Anforderungspaket - möglicherweise nicht übereinstimmende freigegebene Schlüssel

Problem

Die TACACS+-Authentifizierung zwischen der Cisco ISE und der Palo Alto-Firewall (oder einem anderen Netzwerkgerät) schlägt mit der folgenden Fehlermeldung fehl:
"Ungültiges TACACS+-Anforderungspaket - möglicherweise nicht übereinstimmende Shared Secrets"



Overview

Request Type	Authentication
Status	Fail
Session Key	goldenserver/532805123/143
Message Text	TACACS: Invalid TACACS+ request packet - possibly mismatched Shared Secrets
Username	
Authentication Policy	
Selected Authorization Profile	

Authentication Details

Generated Time	2025-05-13 20:16:26.897000 +05:30
Logged Time	2025-05-13 20:16:26.897
Epoch Time (sec)	1747147586
ISE Node	goldenserver
Message Text	TACACS: Invalid TACACS+ request packet - possibly mismatched Shared Secrets
Failure Reason	
Resolution	
Root Cause	
Username	
Network Device Name	

Dies verhindert erfolgreiche administrative Anmeldeversuche und kann die Gerätezugriffskontrolle durch zentrale Authentifizierung beeinträchtigen.

Mögliche Ursachen

- Eine Diskrepanz zwischen dem auf der Cisco ISE und der Palo Alto Firewall oder dem Netzwerkgerät konfigurierten gemeinsamen geheimen Schlüssel.
- Die TACACS+-Serverkonfiguration auf dem Gerät ist falsch (z. B. falsche IP-Adresse, falscher Port oder falsches Protokoll).

Lösung

Es gibt mehrere mögliche Lösungen für dieses Problem:

1. Überprüfen Sie den gemeinsamen geheimen Schlüssel:

- Auf der Cisco ISE:
  Navigieren Sie zu Administration > Network Resources > Network Devices, wählen Sie das betroffene Gerät aus, und bestätigen Sie den gemeinsamen geheimen Schlüssel.

- Palo Alto Firewall:
  Gehen Sie zu Device > Server Profiles > TACACS+ (Gerät > Serverprofile > TACACS+), und stellen Sie sicher, dass der gemeinsame geheime Schlüssel exakt übereinstimmt, einschließlich Groß- und Kleinschreibung und Sonderzeichen.

2. Aktivieren Sie TACACS+ Server Settings:

- Stellen Sie sicher, dass die richtige IP-Adresse und der richtige Port (der Standardwert ist 49) der Cisco ISE im TACACS+-Profil der Firewall konfiguriert sind.

- Stellen Sie sicher, dass der Protokolltyp TACACS+ (nicht RADIUS) 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.