

Toediening van TACACS+-apparaten configureren op Palo Alto met ISE

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Gebruikte componenten](#)

[Netwerkdigram](#)

[verificatiestroom](#)

[Configureren](#)

[Sectie 1: Palo Alto Firewall configureren voor TACACS+](#)

[Sectie 2: TACACS+-configuratie op ISE](#)

[Verifiëren](#)

[ISE-beoordeling](#)

[Probleemoplossing](#)

[TACACS: ongeldig TACACS+-aanvraagpakket – mogelijk niet-overeenkomende gedeelde geheimen](#)

[Probleem](#)

[Mogelijke oorzaken](#)

[Oplossing](#)

Inleiding

Dit document beschrijft de TACACS+ Configuratie op Palo Alto met Cisco ISE.

Voorwaarden

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco ISE en TACACS+ protocol.
- Firewall van Palo Alto.

Gebruikte componenten

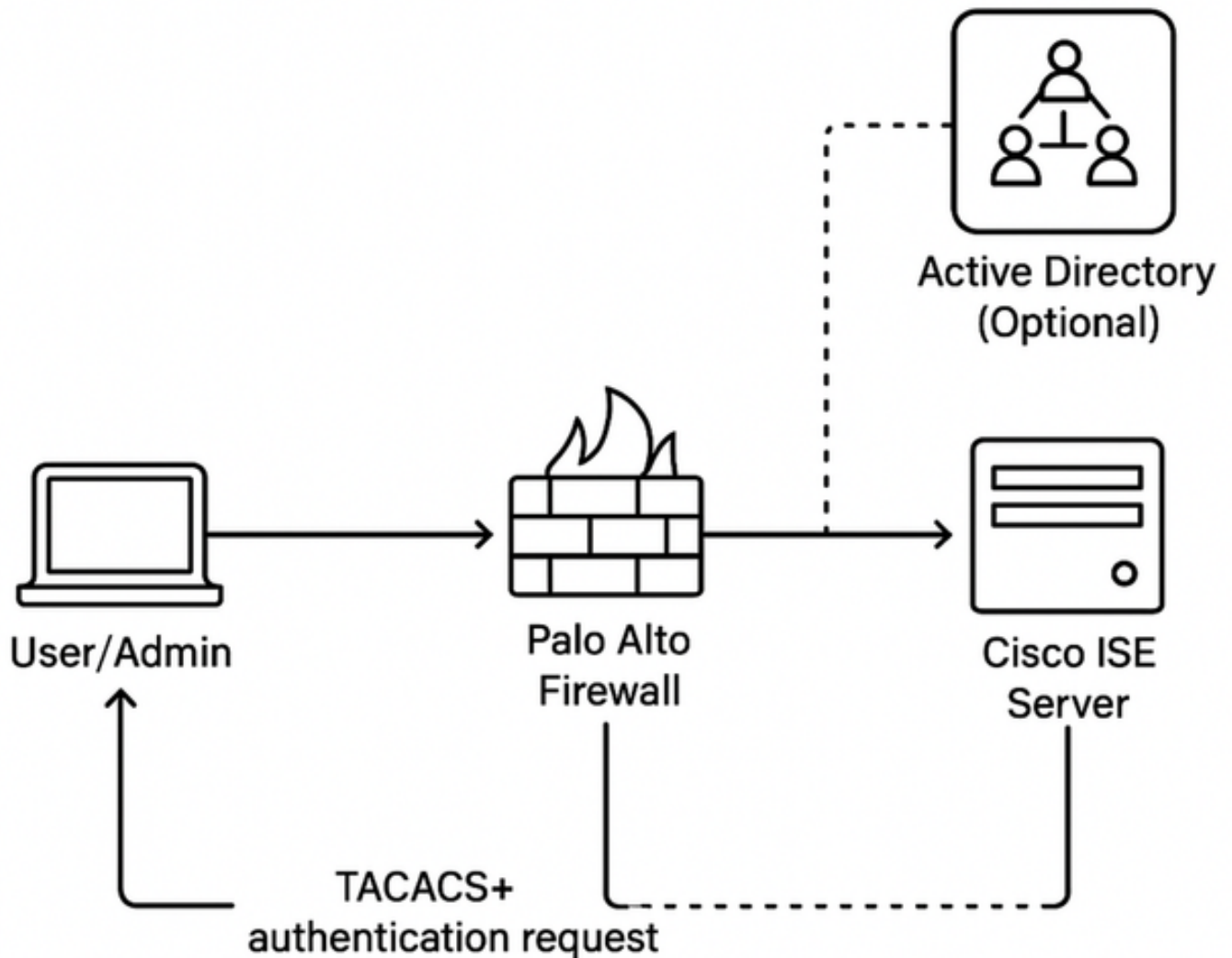
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Netwerkdigram



verificatiestroom

1. De beheerder meldt zich aan bij de Palo Alto-firewall.
2. Palo Alto stuurt een TACACS+-verificatieverzoek naar Cisco ISE.
3. Cisco ISE:
 - Als AD is geïntegreerd, wordt door AD een query uitgevoerd voor verificatie en autorisatie.
 - Als er geen AD is, wordt gebruik gemaakt van lokale identiteitswinkels of beleidsregels.
 - Cisco ISE stuurt een autorisatiereactie naar Palo Alto op basis van het geconfigureerde beleid.
 - De beheerder krijgt toegang met het juiste voorkeursniveau.

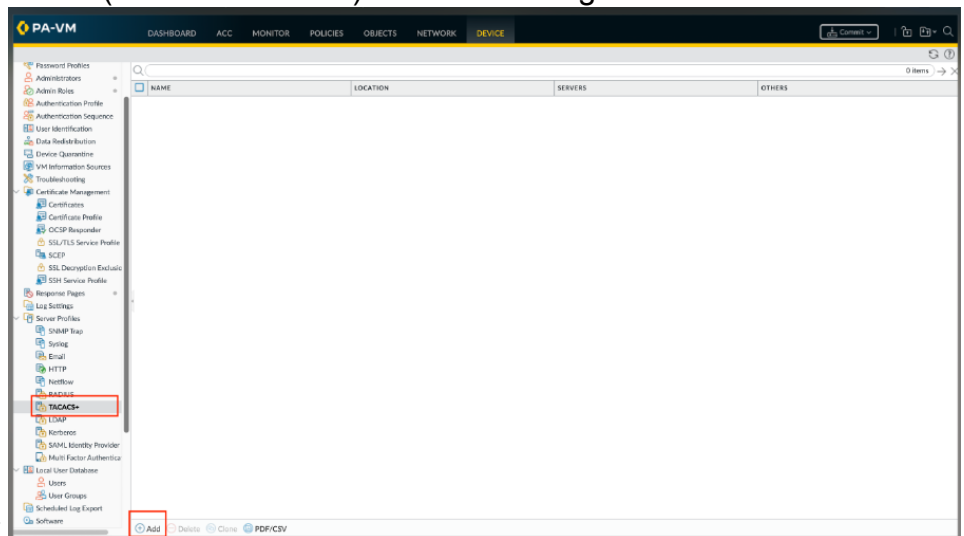
Configureren

Sectie 1: Palo Alto Firewall configureren voor TACACS+

Stap 1. Voeg een TACACS+-serverprofiel toe.

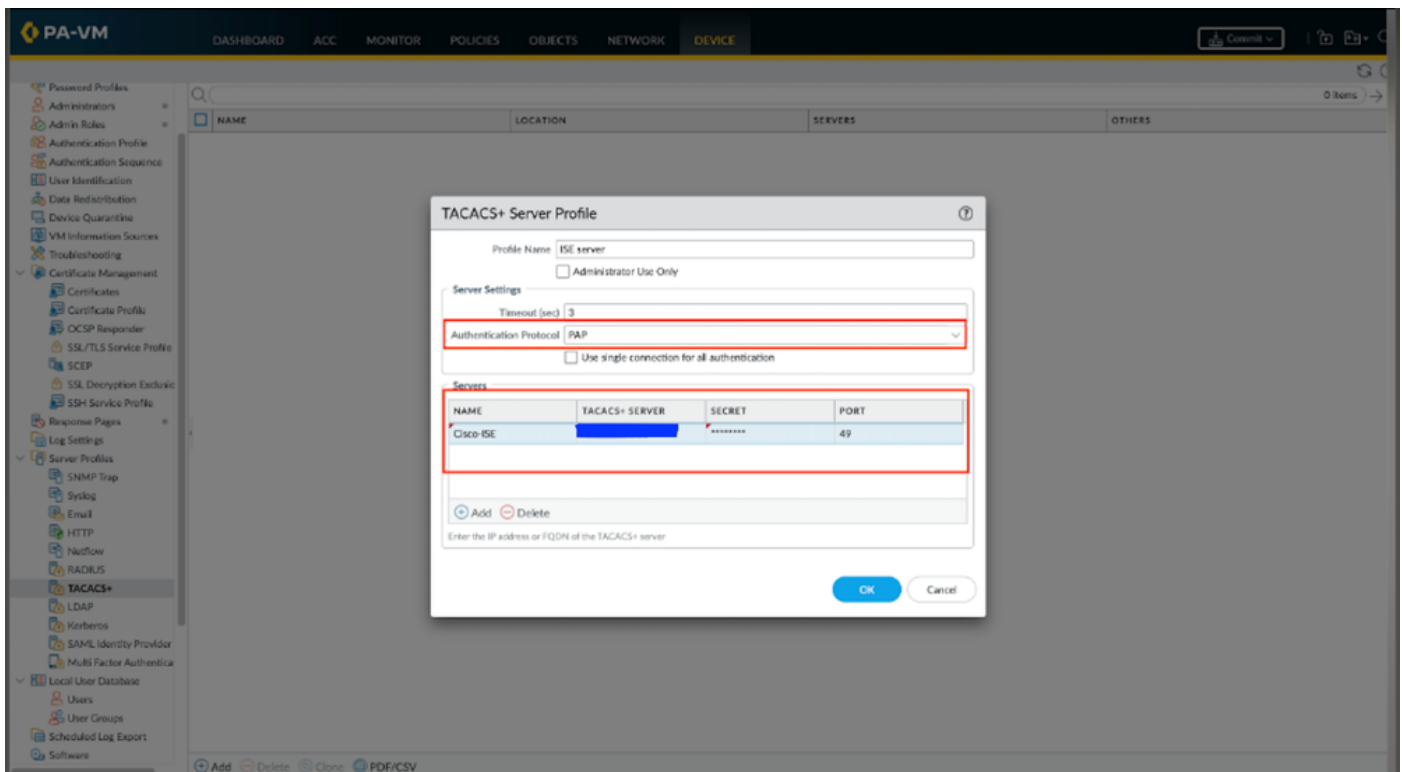
In het profiel wordt gedefinieerd hoe de firewall verbinding maakt met de TACACS+-server.

1. Selecteer Apparaat > Serverprofielen > TACACS+ of Panorama > Serverprofielen > TACACS+ op Panorama en voeg een profiel toe.
2. Voer een profielnaam in om het serverprofiel te identificeren.
3. (Optioneel) Selecteer Alleen gebruiken door beheerder om de toegang tot beheerders te beperken.
4. Voer een time-outinterval in seconden in, waarna een verificatieverzoek een time-out krijgt (standaard 3; bereik 1-20).
5. Selecteer het verificatieprotocol (standaard CHAP) dat de firewall gebruikt voor de verificatie



van de TACACS+-server.

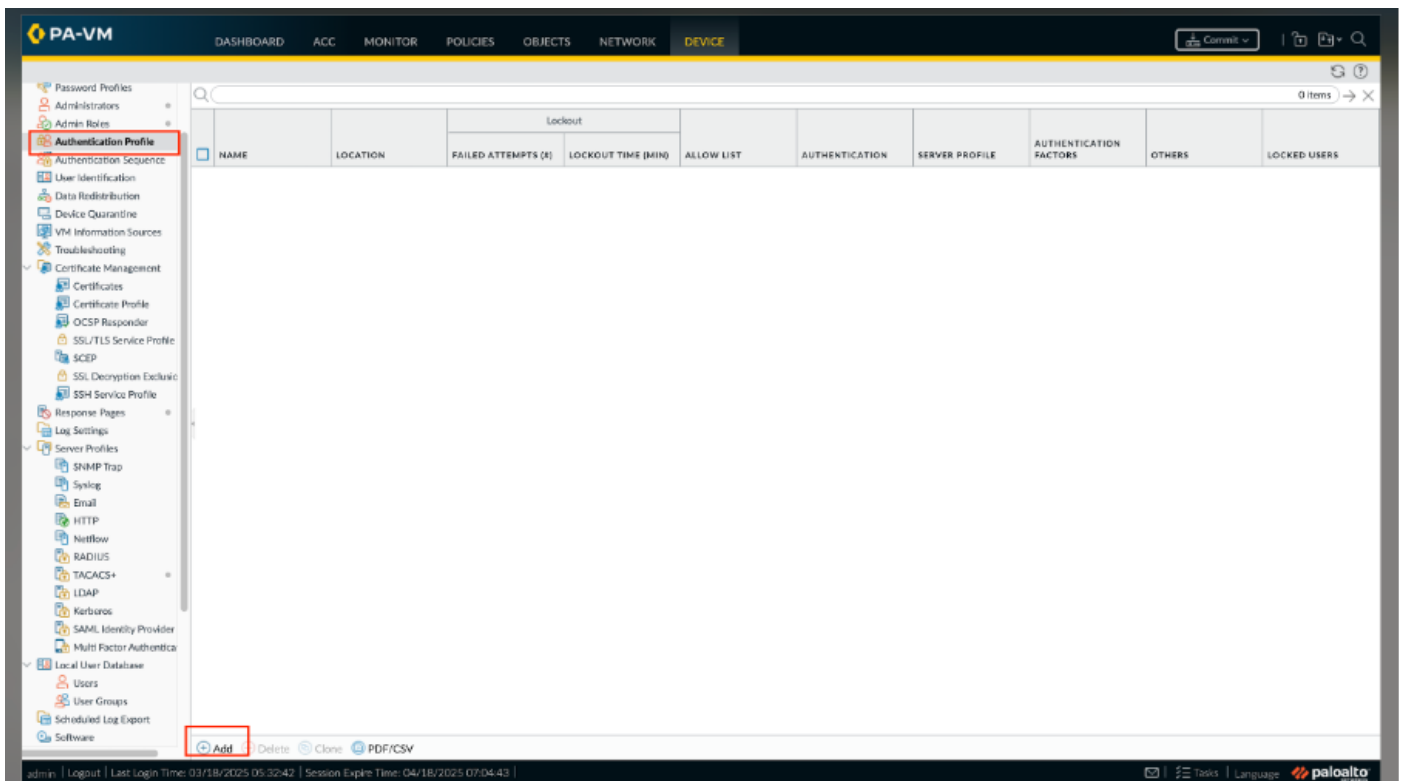
6. Voeg elke TACACS+-server toe en voer de volgende stappen uit:
 1. Een naam om de server te identificeren.
 2. Het IP-adres van de TACACS+-server of FQDN. Als u een FQDN-adresobject gebruikt om de server te identificeren en u vervolgens het adres wijzigt, moet u de wijziging vastleggen zodat het nieuwe serveradres van kracht wordt.
 3. Een geheim bevestigen en bevestigen om gebruikersnamen en wachtwoorden te versleutelen.
 4. De serverpoort voor verificatieverzoeken (standaard is 49). Klik op OK om het serverprofiel op te slaan.
7. Klik op OK om het serverprofiel op te slaan.



Stap 2. Wijs het TACACS+-serverprofiel toe aan een verificatieprofiel.

Het verificatieprofiel definieert de verificatie-instellingen die gemeenschappelijk zijn voor een set gebruikers.

1. Selecteer Apparaat > Verificatieprofiel en voeg een profiel toe.
 1. Voer een naam in om het profiel te identificeren
 2. Stel het type in op TACACS+.
 3. Selecteer het serverprofiel dat u hebt ingesteld.
 4. Selecteer Gebruikersgroep ophalen van TACACS+ om gebruikersgroepinformatie te verzamelen van VSA's die zijn gedefinieerd op de TACACS+-server.



Authentication Profile

Name: Cisco-AAA-Auth Profile

Authentication | Factors | Advanced

Type: TACACS+

Server Profile: ISE server

User Domain: New TACACS+ Profile

Username Modifier: %USERINPUT%

Single Sign On

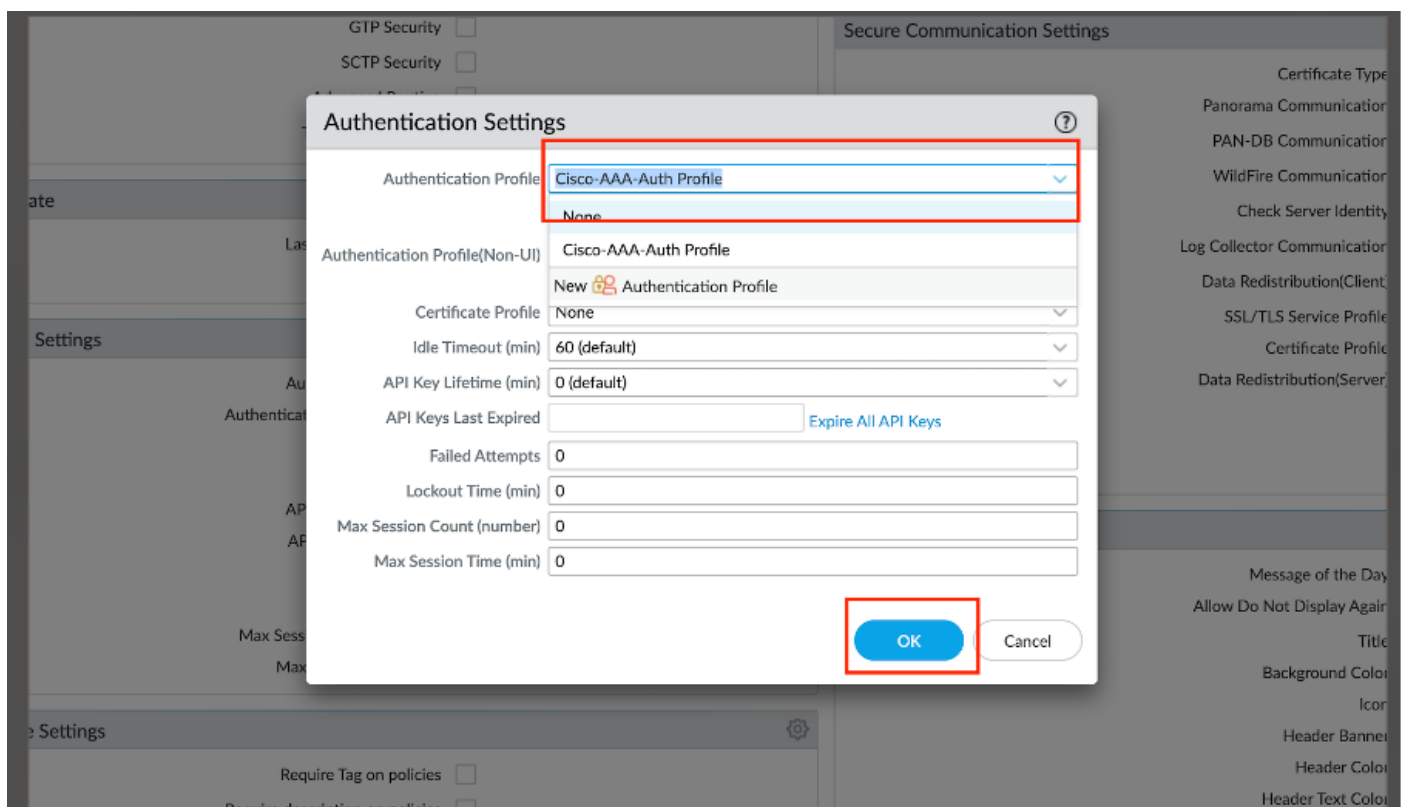
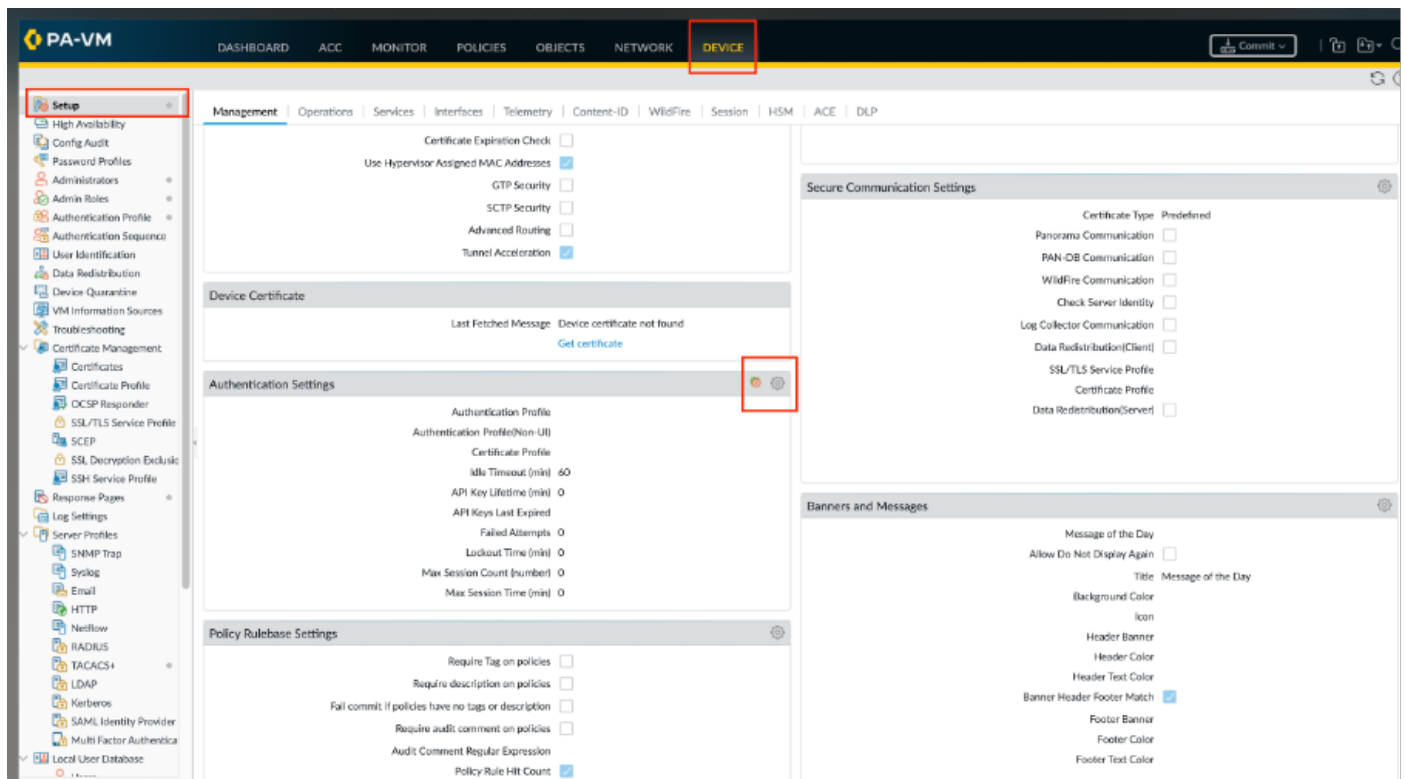
Kerberos Realm:

Kerberos Keytab: Click "Import" to configure this field [X Import](#)

OK Cancel

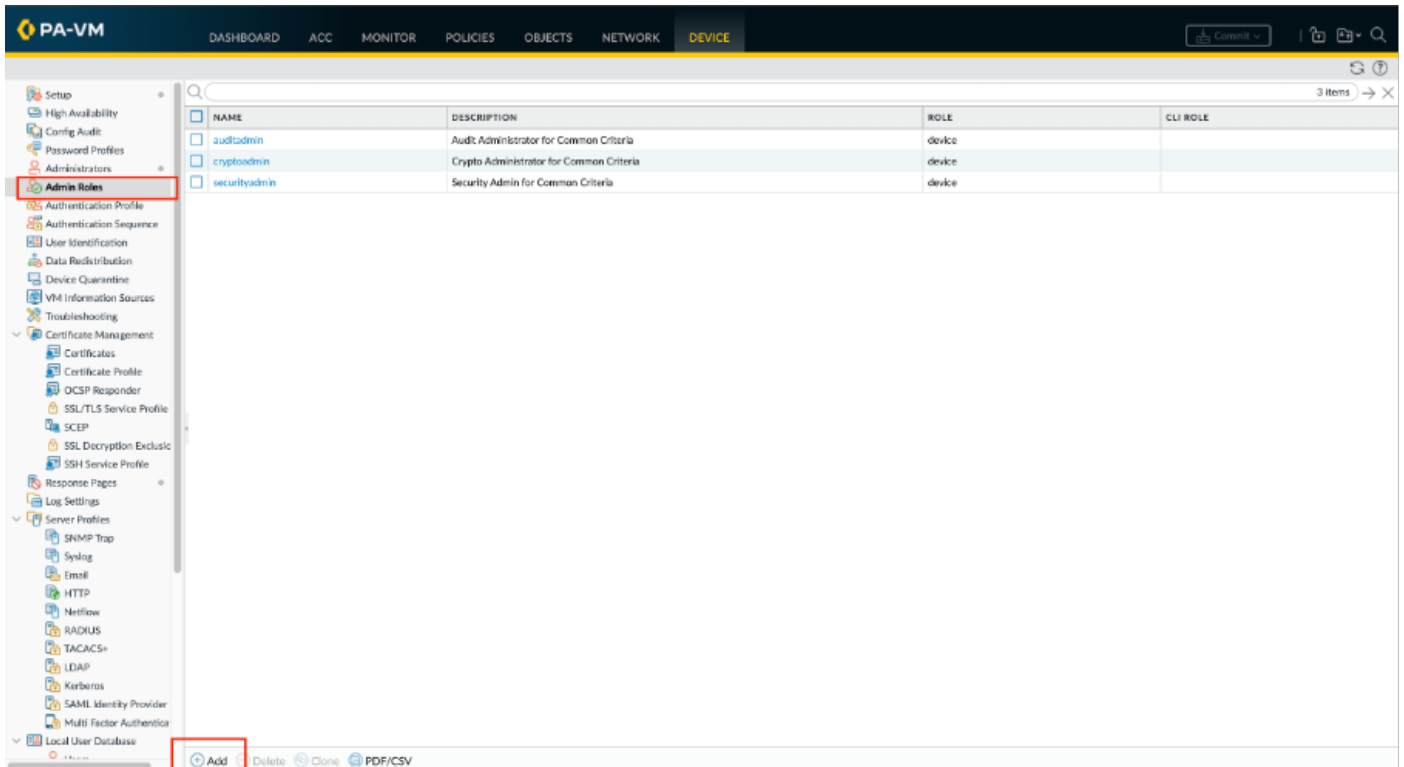
De firewall komt overeen met de groepsinformatie met de groepen die u opgeeft in de lijst Toestaan van het verificatieprofiel.

1. Selecteer Geavanceerd en voeg in de lijst Toestaan de gebruikers en groepen toe die met dit verificatieprofiel kunnen worden geverifieerd.
2. Klik op OK om het verificatieprofiel op te slaan.

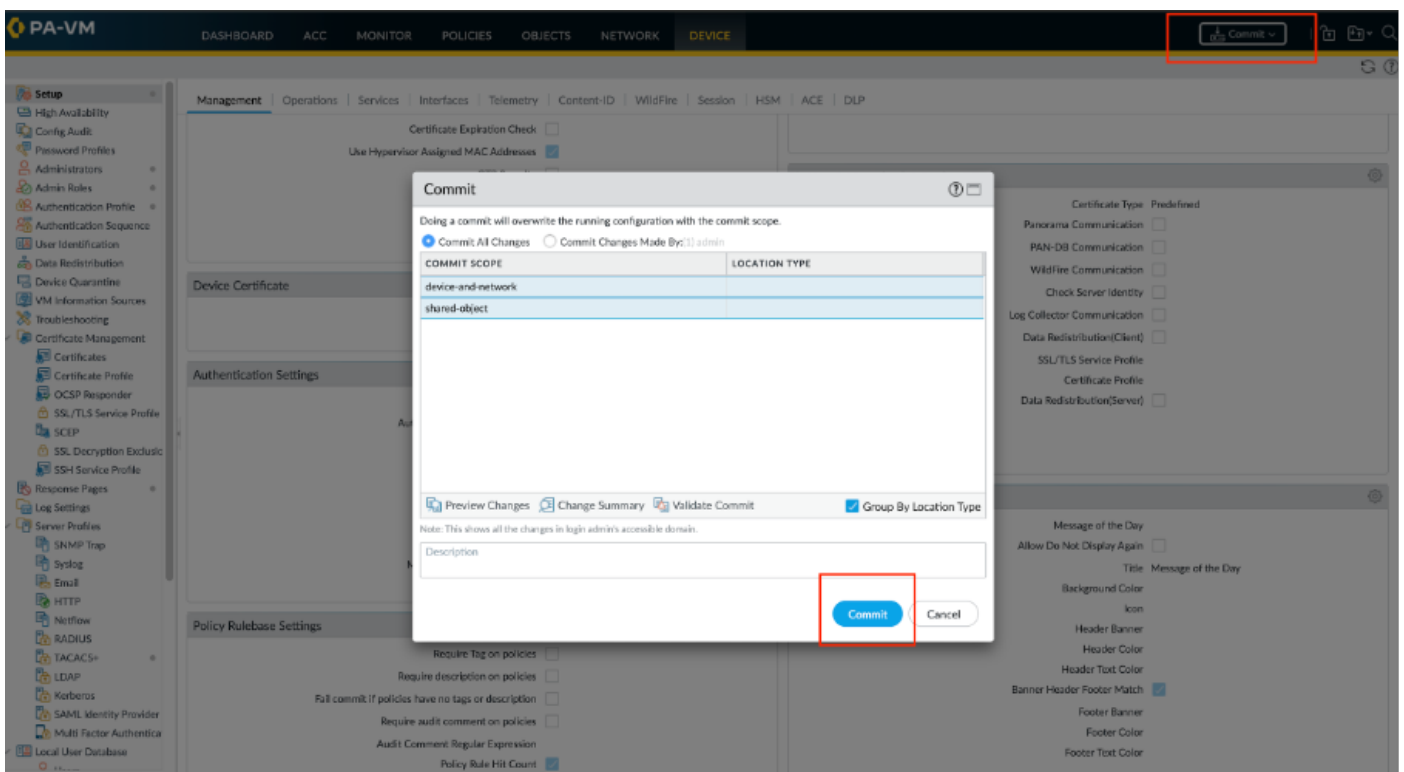


Stap 4. Een beheerdersrolprofiel configureren.

Selecteer Apparaat > Beheerrollen en klik op Toevoegen. Voer een naam in om de rol te identificeren.



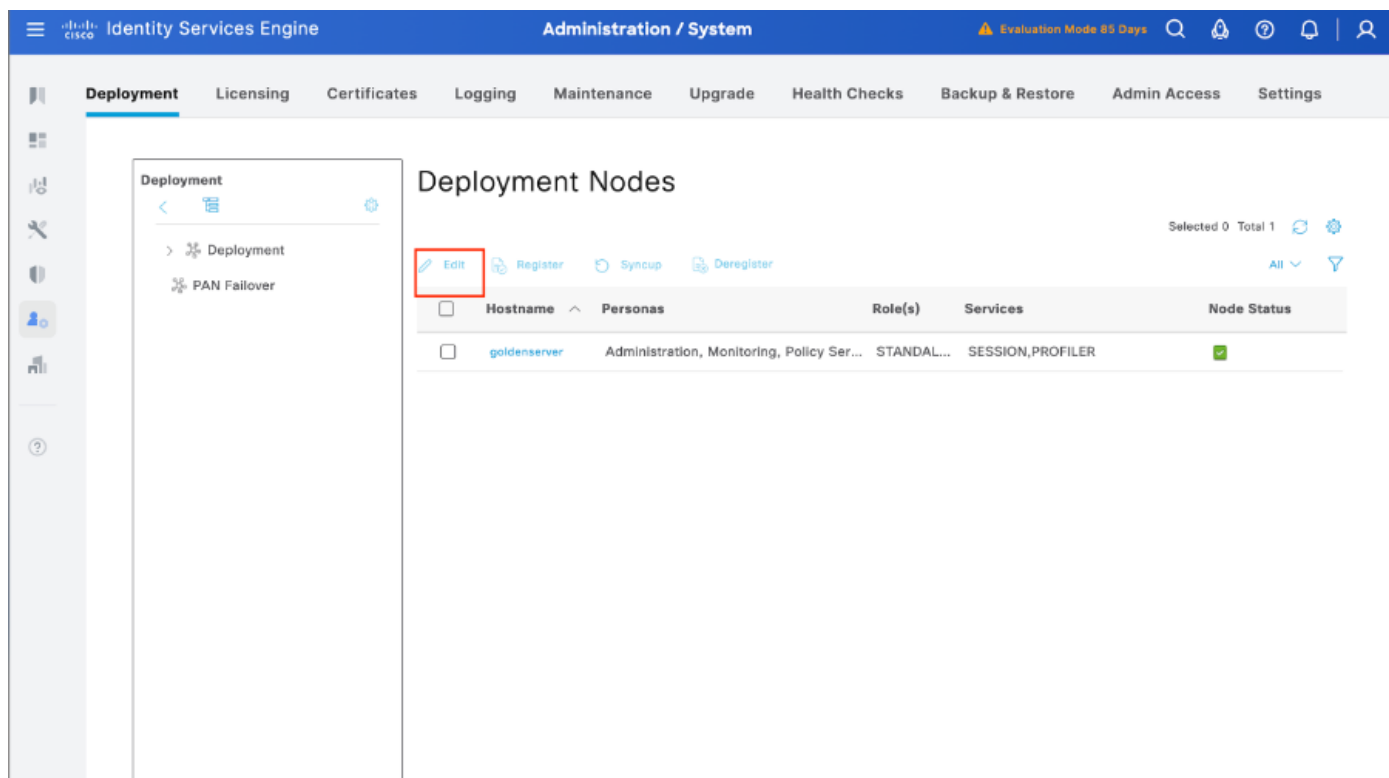
Stap 5. Wijzig de instellingen om deze te activeren in de firewall.



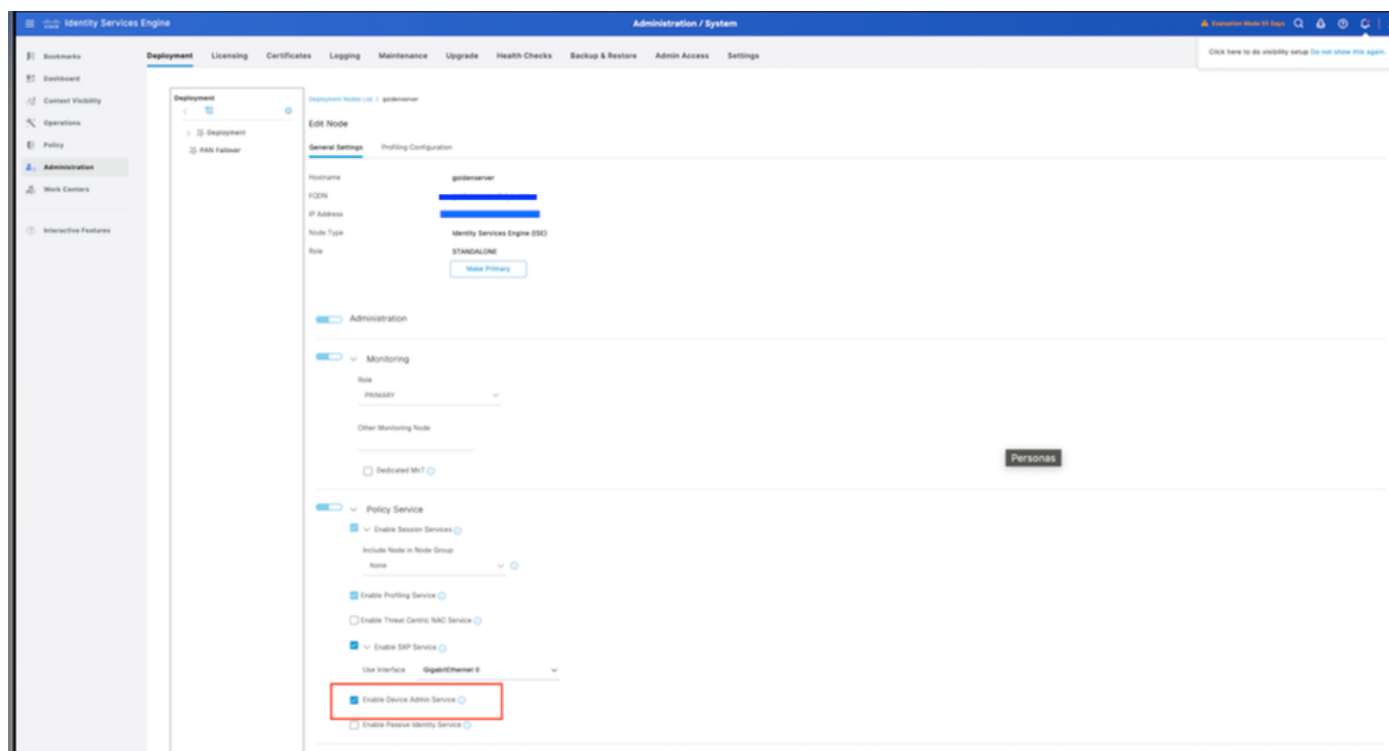
Sectie 2: TACACS+-configuratie op ISE

Stap 1. De eerste stap is om na te gaan of Cisco ISE over de nodige mogelijkheden beschikt om de TACACS+-verificatie af te handelen. Bevestig hiervoor dat de functie Apparaatbeheerservice is ingeschakeld in de gewenste beleidsserviceknooppunt (PSN). Navigeer naar Beheer > Systeem > Implementatie, selecteer het juiste knooppunt waar ISE TACACS+-verificatie verwerkt en klik op

Bewerken om de configuratie te bekijken.



Stap 2. Blader omlaag om de functie Apparaatbeheerservice te vinden. Houd er rekening mee dat als u deze functie inschakelt, de persona van de Beleidsservice actief moet zijn op de node, samen met de beschikbare TACACS+-licenties in de implementatie. Schakel het selectievakje in om de functie in te schakelen en sla de configuratie vervolgens op.



Stap 3. Configureer het Palo Alto Network Device Profile voor Cisco ISE.

Ga naar Beheer > Netwerkbronnen > Netwerkapparaatprofiel. Klik op Toevoegen en vermeld de naam (Palo Alto) en schakel TACACS+ in onder ondersteunde protocollen.

The screenshot shows the 'Network Device Profiles' configuration page in the Cisco ISE Administration console. The 'Name' field is highlighted with a red box and contains 'Palo_Alto'. Below it, the 'Supported Protocols' section has 'TACACS+' checked, also highlighted with a red box. The 'Summary' section at the bottom lists supported services: Radius, TACACS, TrustSec, MAB, and RADIUS.

Stap 4. Palo Alto toevoegen als netwerkapparaat.

1. Navigeer naar Beheer > Netwerkbronnen > Netwerkapparaten > +Toevoegen.

The screenshot shows the 'Network Devices' page in the Cisco ISE Administration console. The '+ Add' button is highlighted with a red box. Below the button is a table with the following columns: Name, IP/Mask, Profile Name, Location, and Type. The table is currently empty, and the text 'No data available' is displayed at the bottom.

2. Klik op Toevoegen en voer de volgende gegevens in:

Naam: Palo-Alto

IP-adres: <Palo-Alto IP>

Network Device Profile: selecteer Palo Alto

TACACS-verificatie-instellingen:

TACACS+-verificatie inschakelen

Voer het gedeelde geheim in (moet overeenkomen met de Palo Alto-configuratie)

Klik op Save (Opslaan).

The screenshot shows the 'Network Device Profile' configuration page in the Palo Alto Networks Identity Services Engine (ISE) interface. The page is titled 'Administration / Network Resources' and 'Network Devices'. The 'Network Device Profile' section is selected, and the 'Palo_Alto_Firewall' profile is being edited. The 'Name' field is 'Palo_Alto_Firewall' and the 'Description' is 'TACACS for Palo Alto'. The 'IP Address' is '10.10.10.32'. The 'Device Profile' is 'Palo_Alto'. The 'Model Name' and 'Software Version' fields are empty. The 'Network Device Group' is 'All Locations'. The 'Location' is 'All Locations'. The 'IPSEC' is 'No'. The 'Device Type' is 'All Device Types'. The 'TACACS Authentication Settings' section is expanded, showing a 'Shared Secret' field with a 'Show' button and a 'Legacy Cisco Device' checkbox. The 'Save' button is at the bottom right.

Stap 5. Gebruikersidentiteitsgroepen maken.

Navigeer naar Werkcentra > Apparaatbeheer > Gebruikersidentiteitsgroepen en klik vervolgens op Toevoegen en geef de naam voor de gebruikersgroep op.

Identity Services Engine

Work Centers / Device Administration

Evaluation Mode 94 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

EQ

< > ⚙

> Endpoint Identity Groups

> User Identity Groups

User Identity Groups > Security Engineers

Identity Group

* Name Security Engineers

Identity group for Palo Alto

Description

Save Reset

Member Users

Users

Selected 0 Total 1

+ Add - Delete

All

Status: Sortable

Email Username First Nam

☐ Enabled divz

Identity Services Engine

Work Centers / Device Administration

Evaluation Mode 94 Days

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Features

Overview

Identities

User Identity Groups

Ext Id Sources

Network Resources

Policy Elements

Device Admin Policy Sets

Reports

Settings

Network Access Service > divznet

Network Access User

* Username divznet

Status Enabled

Account Name divz

Email

Passwords

Password Type Internal Users

Password Lifetime

With Expiration Never Expires

Password

Re-Enter Password

* Login Password

Enable Password

Generate Password

Generate Password

User Information

First Name

Last Name

Account Options

Description

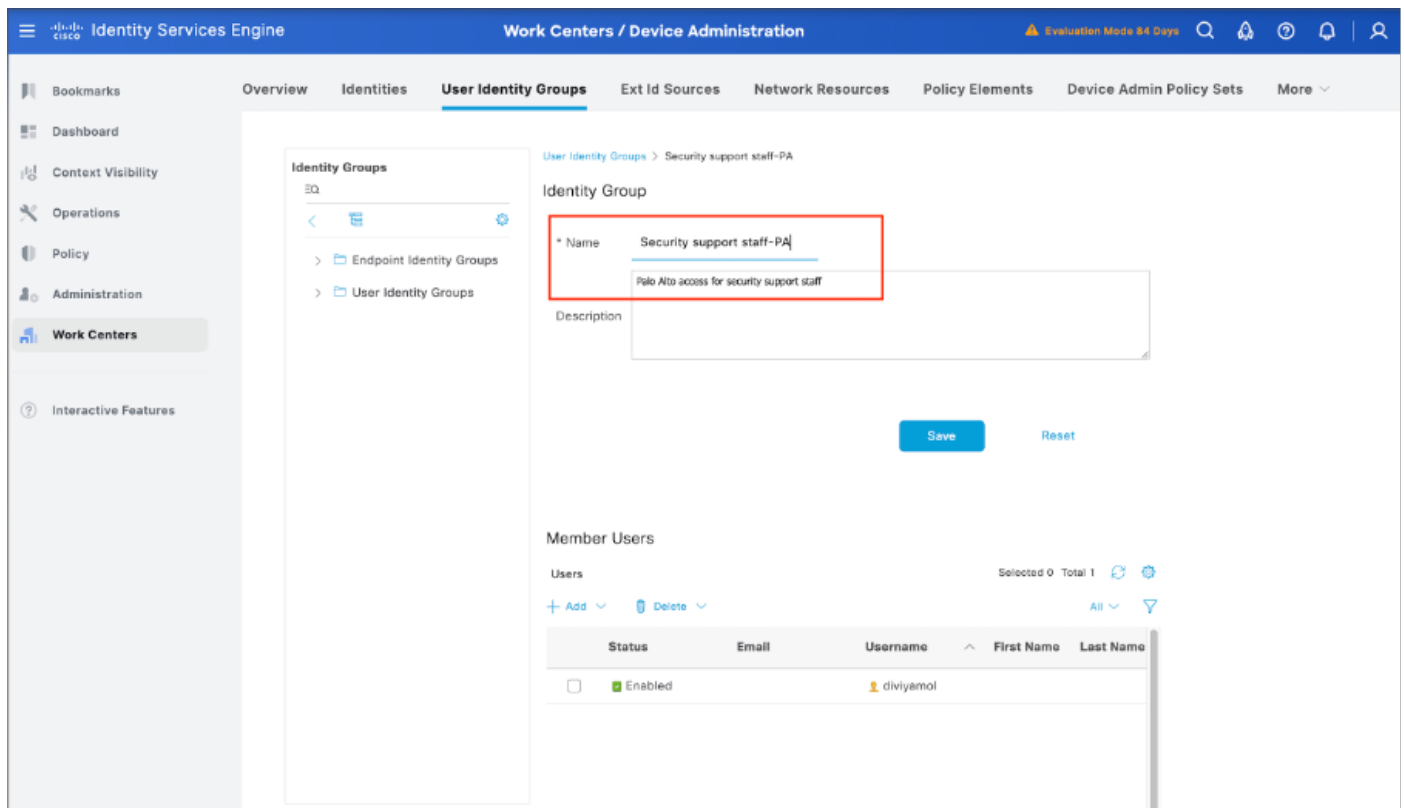
Change password on next login

Account Disable Policy

Disable account if date exceeds 2023-03-19

User Groups

Security support staff PK



Stap 6. Een TACACS-profiel configureren.

Vervolgens configureert u een TACACS-profiel, waarin u instellingen zoals Privilege Level en time-outinstellingen kunt configureren. Navigeer naar Werkcentra > Apparaatbeheer -> Beleidselementen -> Resultaten -> TACACS-profielen.

Klik op Toevoegen om een nieuw TACACS-profiel te maken. Geef het profiel een goede naam.

Identity Services Engine Work Centers / Device Administration

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

Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Features

Conditions TACACS Profiles > New TACACS Profile

Network Conditions

Results Name PaloAlto_Security_Support

Allowed Protocols TACACS Command Sets TACACS Profiles

Description

Task Attribute View Raw View

Common Tasks

Common Task Type Shell

Default Privilege 0 (Select 0 to 15)

Maximum Privilege 15 (Select 0 to 15)

Access Control List

Auto Command

No Escape (Select true or false)

Timeout Minutes (0-9999)

Idle Time Minutes (0-9999)

Custom Attributes

Add Type Value

No data found.

Mandatory PaloAlto_Admin_Role Support

Cancel Save

Identity Services Engine Work Centers / Device Administration

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

Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Features

Conditions TACACS Profiles > PaloAlto_Engineers_Profile TACACS Profile

Network Conditions

Results Name PaloAlto_Engineers_Profile

Allowed Protocols TACACS Command Sets TACACS Profiles

Description

Task Attribute View Raw View

Common Tasks

Common Task Type Shell

Default Privilege 0 (Select 0 to 15)

Maximum Privilege 15 (Select 0 to 15)

Access Control List

Auto Command

No Escape (Select true or false)

Timeout Minutes (0-9999)

Idle Time Minutes (0-9999)

Custom Attributes

Add Type Value

No data found.

Mandatory PaloAlto_Admin_Role securityadmin

Cancel Save

Stap 6. TACACS-opdrachtsets configureren.

Nu is het tijd om te configureren welke commando's gebruikers mogen gebruiken. Aangezien u

beide use cases het Privilege Level 15 kunt toekennen, dat toegang geeft tot elke beschikbare opdracht, kunt u TACACS-opdrachtsets gebruiken om te beperken welke opdrachten kunnen worden gebruikt.

Navigeer naar Werkcentra > Apparaatbeheer > Beleidselementen > Resultaten -> TACACS-opdrachtsets. Klik op Toevoegen om een nieuwe TACACS-opdrachtset te maken en geef deze de naam PermitAllCommands. Pas deze TACACS-opdrachtset voor beveiligingsondersteuning toe.

Het enige dat u in deze TACACS-opdrachtset hoeft te configureren, is het selectievakje voor Toestemming aanvinken voor opdrachten die hieronder niet worden vermeld.

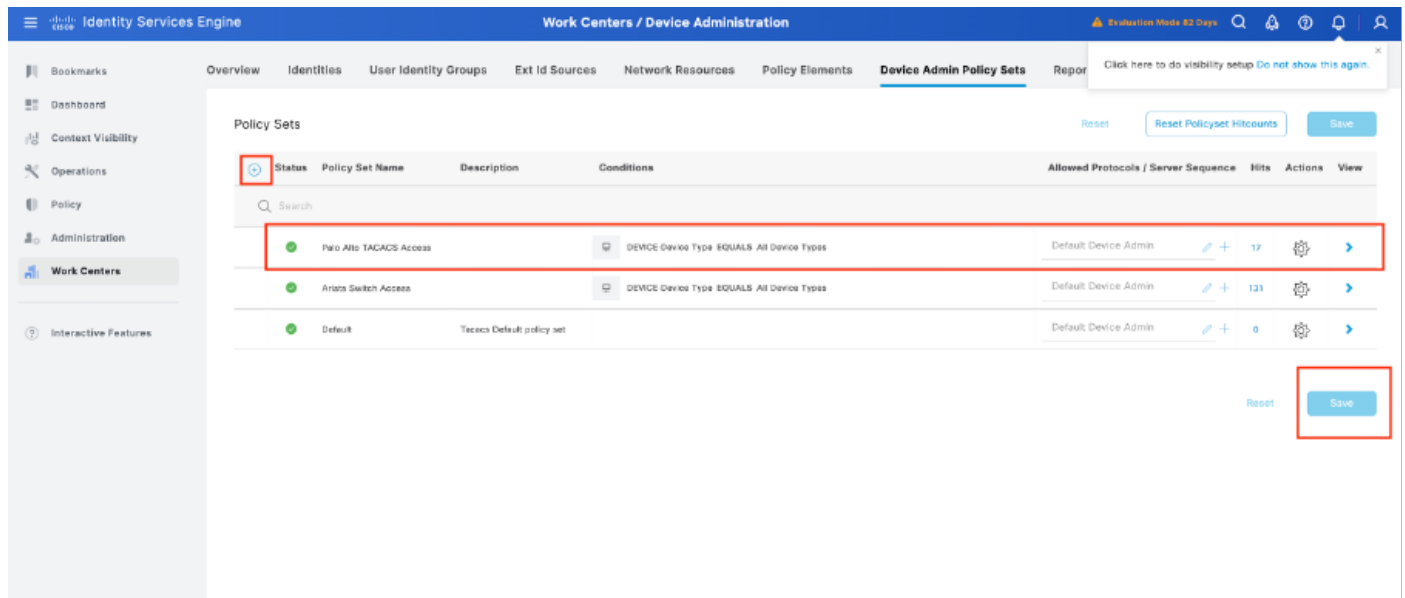
The screenshot shows the 'Identity Services Engine' interface with the 'Work Centers / Device Administration' tab selected. The left sidebar contains a navigation menu with 'Work Centers' highlighted. The main content area is divided into a left sidebar with 'TACACS Command Sets' selected and a main panel. The main panel shows the configuration for a 'TACACS Command Set' named 'PermitAllCommands'. The 'Name' field is filled with 'PermitAllCommands'. The 'Description' field is empty. The 'Commands' section has a checkbox labeled 'Permit any command that is not listed below' which is checked. Below this is a table with columns 'Grant', 'Command', and 'Arguments'. The table is empty, with a message 'No data found.' below it. At the bottom right, there are 'Cancel' and 'Save' buttons.

The screenshot shows the 'Identity Services Engine' interface with the 'Work Centers / Device Administration' tab selected. The left sidebar contains a navigation menu with 'Work Centers' highlighted. The main content area is divided into a left sidebar with 'TACACS Command Sets' selected and a main panel. The main panel shows the configuration for a 'TACACS Command Set' named 'PermitBasicCommands'. The 'Name' field is filled with 'PermitBasicCommands'. The 'Description' field is empty. The 'Commands' section has a checkbox labeled 'Permit any command that is not listed below' which is unchecked. Below this is a table with columns 'Grant', 'Command', and 'Arguments'. The table contains five rows of data, each with a 'PERMIT' grant and a specific command. At the bottom right, there are 'Cancel' and 'Save' buttons.

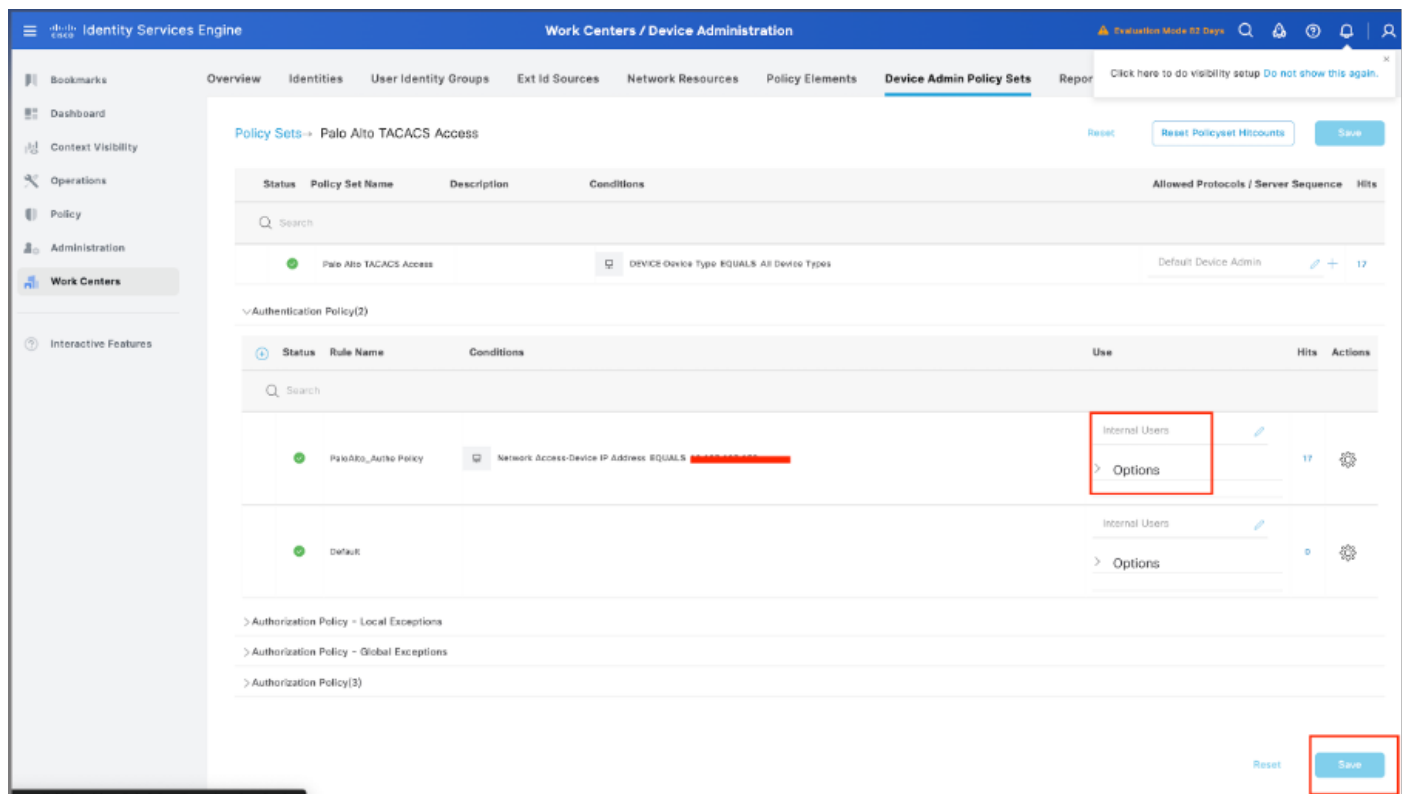
Grant	Command	Arguments
PERMIT	show*	
PERMIT	ping	
PERMIT	tracoute	
PERMIT	logout	
PERMIT	exit	

Stap 7. Maak een Device Admin Policy Set voor uw Palo Alto, navigeer in het menu Work Centers > Device Administration > Device Admin Policy Sets, klik op het Add + pictogram.

Stap 8. Geef deze nieuwe beleidsset een naam, voeg voorwaarden toe afhankelijk van de kenmerken van de TACACS+-verificaties die worden uitgevoerd vanuit de Palo Alto Firewall en selecteer als Toegestane protocollen > Standaardapparaatbeheer. Sla uw configuratie op.



Stap 9. Selecteer in de optie > bekijken en selecteer vervolgens in het gedeelte Authenticatiebeleid de externe identiteitsbron die Cisco ISE gebruikt om de gebruikersnaam en referenties voor verificatie op te vragen in de Palo Alto Firewall. In dit voorbeeld komen de referenties overeen met interne gebruikers die zijn opgeslagen in ISE.



Stap 10. Blader omlaag tot de sectie Autorisatiebeleid tot het standaardbeleid, selecteer het tandwielpictogram en plaats een regel hierboven.

The screenshot shows the Palo Alto Identity Services Engine (ISE) interface. The main heading is 'Work Centers / Device Administration'. The left sidebar contains navigation options like Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration, Work Centers, and Interactive Features. The main content area is titled 'Policy Sets -> Palo Alto TACACS Access'. It features a table with columns: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, and Hits. A red box highlights the 'Authorization Policy(3)' section, which contains three rows: 'PA_FW_Authz Policy', 'PA_FW_Security policy', and 'Default'. The 'PA_FW_Authz Policy' row is highlighted with a red box, showing its conditions, command sets, and shell profiles. The 'Save' button at the bottom right is also highlighted with a red box.

Stap 11. Geef de nieuwe autorisatieregel een naam, voeg voorwaarden toe met betrekking tot de gebruiker die al is geverifieerd als groepslidmaatschap en voeg in het gedeelte Shell-profielen het eerder geconfigureerde TACACS-profiel toe en sla de configuratie op.

Verifiëren

ISE-beoordeling

Stap 1. Controleer of de TACACS+-service actief is. Dit kan worden ingecheckt:

- GUI: Controleer of de node is vermeld bij de service DEVICE ADMIN in Beheer -> Systeem -> Implementatie.
- CLI: Voer de opdracht show ports uit | neem 49 op om te bevestigen dat er verbindingen in de TCP-poort zijn die behoren tot TACACS+

```
goldenserver/admin#show ports | include 49
```

```
tcp: [REDACTED]
```

Stap 2. Bevestig of er live logs zijn met betrekking tot TACACS+ authenticatie pogingen: dit kan worden gecontroleerd in het menu Operations -> TACACS -> Live logs.

Afhankelijk van de reden van de storing kunt u uw configuratie aanpassen of de oorzaak van de storing aanpakken.

Identity Services Engine									
Operations / TACACS									
Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Features Live Logs									
Export To Refresh Never Show Latest 20 records Window Last									
Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Isa Node	Network Device	
Mar 22, 2025 06:54:38.8...			diviyamol	Authentic...	Palo Alto TACACS Access >> P...		goldenserver	Palo_Alto_Firewall	
Mar 22, 2025 06:54:17.5...			diviyamol	Authentic...	Palo Alto TACACS Access >> P...		goldenserver	Palo_Alto_Firewall	
Mar 22, 2025 06:49:42.0...			divi	Authorizat...		Palo Alto TACACS Access >> P...	goldenserver	Palo_Alto_Firewall	
Mar 22, 2025 06:49:41.9...			divi	Authentic...	Palo Alto TACACS Access >> P...		goldenserver	Palo_Alto_Firewall	
Mar 22, 2025 06:49:28.2...			diviyamol	Authorizat...		Palo Alto TACACS Access >> P...	goldenserver	Palo_Alto_Firewall	
Mar 22, 2025 06:49:28.1...			diviyamol	Authentic...	Palo Alto TACACS Access >> P...		goldenserver	Palo_Alto_Firewall	

Stap 3. Als u geen live logboek ziet, gaat u verder met het vastleggen van pakketten en navigeert u naar het menu **Bewerkingen > Problemen oplossen > Diagnostische hulpmiddelen > Algemene hulpmiddelen > TCP-dump**, selecteer **Toevoegen**.

Identity Services Engine									
Operations / Troubleshoot									
Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM More									
General Tools RADIUS Authentication Troub... Execute Network Device Com... Evaluate Configuration Validat... Posture Troubleshooting Agentless Posture Troublesho... Endpoint Debug TCP Dump Session Trace Tests TCP Dump The TCP Dump utility page is to monitor the contents of packets on a network interface and troubleshoot problems on the network as they appear Rows/Page 0 << 0 / 0 >> Go Add Edit Trash Start Stop Download Filter									
Host Name	Network Interface	Filter	File Name	Repository	File S...	Number of ...	Time Limit	Promiscu	

Identity Services Engine									
Operations / Troubleshoot									
Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Features Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM pxGrid Direct Connectors More									
General Tools RADIUS Authentication Troub... Execute Network Device Com... Evaluate Configuration Validat... Posture Troubleshooting Agentless Posture Troublesho... Endpoint Debug TCP Dump Session Trace Tests TCP Dump Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear. Host Name* goldenserver Network Interface* GigabitEthernet 0 [Up, Running] Filter ip host E.g: ip host 10.77.122.123 and not 10.177.122.119 File Name tsccac_issue Repository File Size 10 Mb Limit to 1 File(s) Time Limit 5 Minute(s) ☐ Promiscuous Mode Cancel Save Save and Run									

Stap 4. Schakel de component runtime-AAA in voor foutopsporing binnen de PSN van waaruit de verificatie wordt uitgevoerd in **Operations > Troubleshoot > Debug Wizard > Debug log**

Identity Services Engine

Operations / Troubleshoot

Evaluation Mode 85 Days

Search

Help

Refresh

Close

Logout

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Features

Diagnostic Tools

Download Logs

Debug Wizard

Debug Profile Configuration

Debug Log Configuration

Node List

Selected 0 Total 1

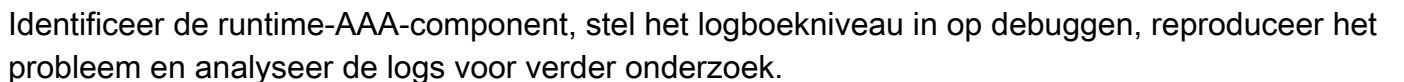
Edit

Reset to Default

All

Filter

Node Name	Replication Role
☐ goldenserver	STANDALONE



TACACS: ongeldig TACACS+-aanvraagpakket – mogelijk niet-overeenkomende gedeelde geheimen

De TACACS+-verificatie tussen de Cisco ISE en de Palo Alto-firewall (of een ander netwerkkapparaat) mislukt met de foutmelding:
"Ongeldig TACACS+-aanvraagpakket - mogelijk niet-overeenkomende gedeelde geheimen"

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	

Dit voorkomt succesvolle administratieve aanmeldingspogingen en kan invloed hebben op de toegangscontrole van het apparaat door middel van gecentraliseerde verificatie.

Mogelijke oorzaken

- Een mismatch in het gedeelde geheim dat is geconfigureerd op Cisco ISE en de Palo Alto-firewall of het netwerkapparaat.
- Onjuiste TACACS+-serverconfiguratie op het apparaat (zoals verkeerd IP-adres, poort of protocol).

Oplossing

Er zijn verschillende mogelijke oplossingen voor dit probleem:

1. Controleer het gedeelde geheim:

- Over Cisco ISE:
Navigeer naar Beheer > Netwerkbronnen > Netwerkapparaten, selecteer het betreffende apparaat en bevestig het gedeelde geheim.
- Op de Palo Alto firewall:
Ga naar Apparaat > Serverprofielen > TACACS+ en zorg ervoor dat het gedeelde geheim exact overeenkomt, inclusief hoofdletters en speciale tekens.

2. Controleer de instellingen van de TACACS+-server:

- Controleer of het juiste IP-adres en de juiste poort (standaard is 49) van Cisco ISE zijn geconfigureerd in het TACACS+-profiel van de firewall.
- Controleer of het protocoltype TACACS+ is (niet RADIUS).

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.