

# Configure TACACS+ Device Administration on Palo Alto with ISE

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

### [Components Used](#)

### [Network Diagram](#)

[Authentication Flow](#)

### [Configure](#)

[Section 1: Configure Palo Alto Firewall for TACACS+](#)

[Section 2: TACACS+ Configuration on ISE](#)

### [Verify](#)

[ISE Review](#)

### [Troubleshooting](#)

[TACACS: Invalid TACACS+ Request Packet – Possibly Mismatched Shared Secrets](#)

[Problem](#)

[Possible Causes](#)

[Solution](#)

---

## Introduction

This document describes TACACS+ Configuration on Palo Alto with Cisco ISE.

## Prerequisites

Cisco recommends that you have knowledge of these topics:

- Cisco ISE and TACACS+ protocol.
- Palo Alto firewall.

## Components Used

The information in this document is based on these software and hardware versions:

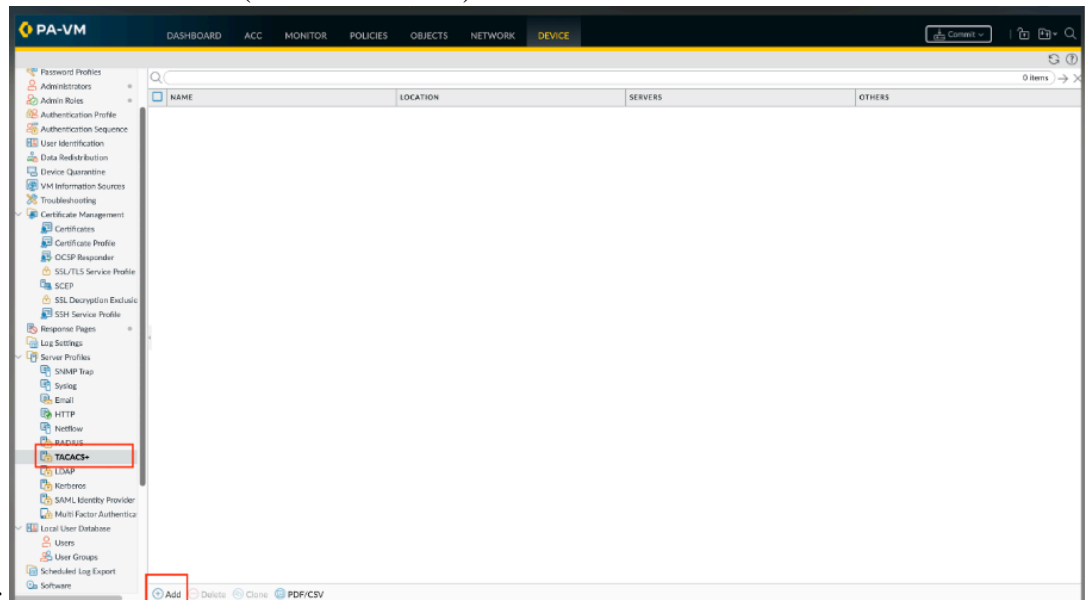
- Palo Alto Firewall version 10.1.0
- Cisco Identity Services Engine (ISE) version 3.3 Patch 4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Network Diagram

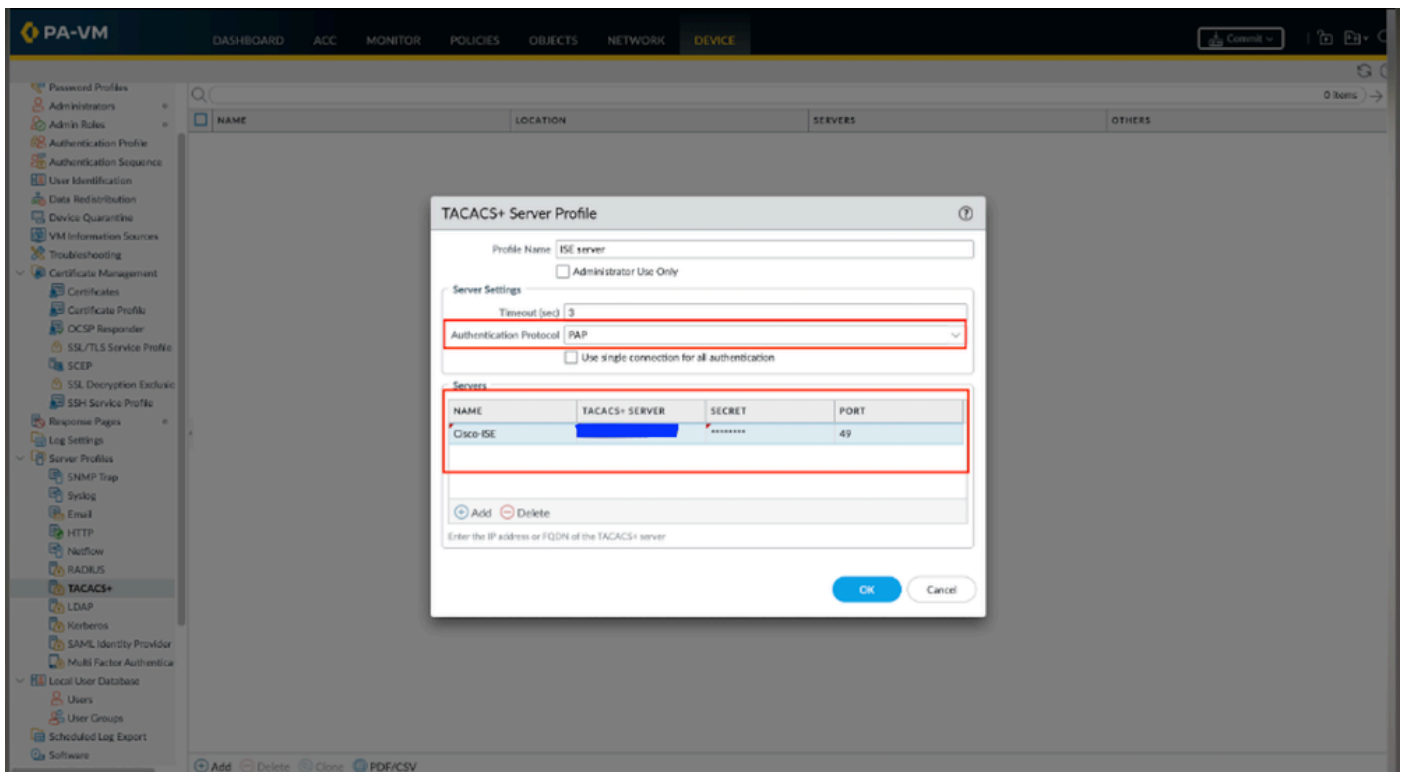


1. Select **Device > Server Profiles > TACACS+ or Panorama > Server Profiles > TACACS+** on Panorama and **Add** a profile.
2. Enter a Profile Name to identify the server profile.
3. (Optional) Select **Administrator Use Only** to restrict access to administrators.
4. Enter a Timeout interval in seconds after which an authentication request times out (default is 3; range is 1–20).
5. Select the **Authentication Protocol** (default is CHAP) that the firewall uses to authenticate to the



TACACS+ server.

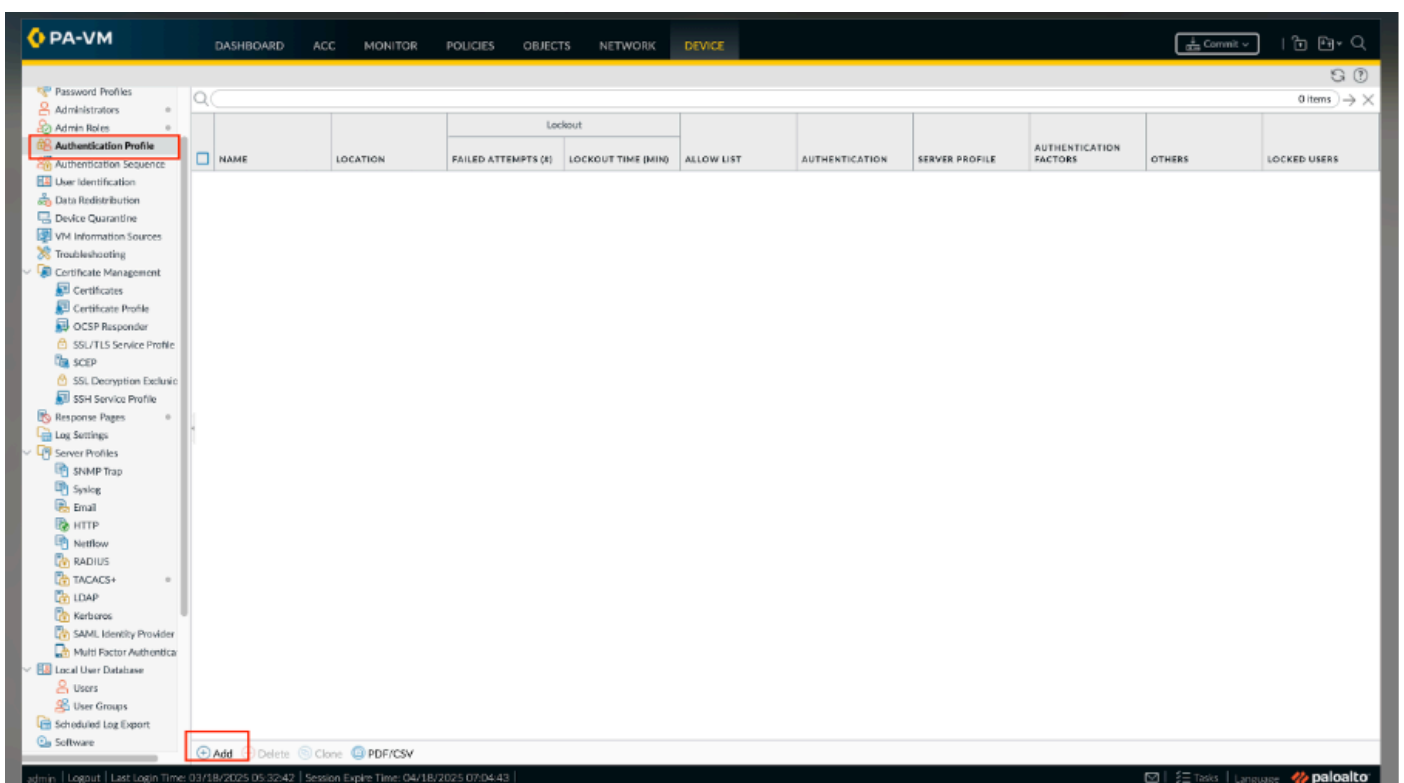
6. Add each TACACS+ server and perform these steps:
  1. A **Name** to identify the server.
  2. The TACACS+ Server IP address or FQDN. If you use an FQDN address object to identify the server and you subsequently change the address, you must commit the change for the new server address to take effect.
  3. A Secret and Confirm Secret to encrypt usernames and passwords.
  4. The server Port for authentication requests (default is 49). Click OK to save the server profile.
7. Click OK to save the server profile.



Step 2. Assign the TACACS+ server profile to an authentication profile.

The authentication profile defines the authentication settings that are common to a set of users.

1. Select **Device > Authentication Profile** and **Add** a profile.
  1. Enter a Name to identify the profile
  2. Set the Type to TACACS+.
  3. Select the Server Profile you configured.
  4. Select Retrieve user group from TACACS+ to collect user group information from VSAs defined on the TACACS+ server.



**Authentication Profile** ⓘ

Name

**Authentication** | Factors | Advanced

Type

Server Profile   
ISE server

User Domain

Username Modifier

**Single Sign On**

Kerberos Realm

Kerberos Keytab  [X Import](#)

OK Cancel

The firewall matches the group information using the groups you specify in the Allow List of the authentication profile.

1. Select **Advanced** and in the Allow List, **Add** the users and groups that can authenticate with this authentication profile.
2. Click **OK** to save the authentication profile.

Authentication Profile

Name Cisco-AAA-Auth Profile

Authentication | Factors | **Advanced**

**Allow List**

<input type="checkbox"/>	ALLOW LIST ^
<input checked="" type="checkbox"/>	all

+ Add - Delete

**Account Lockout**

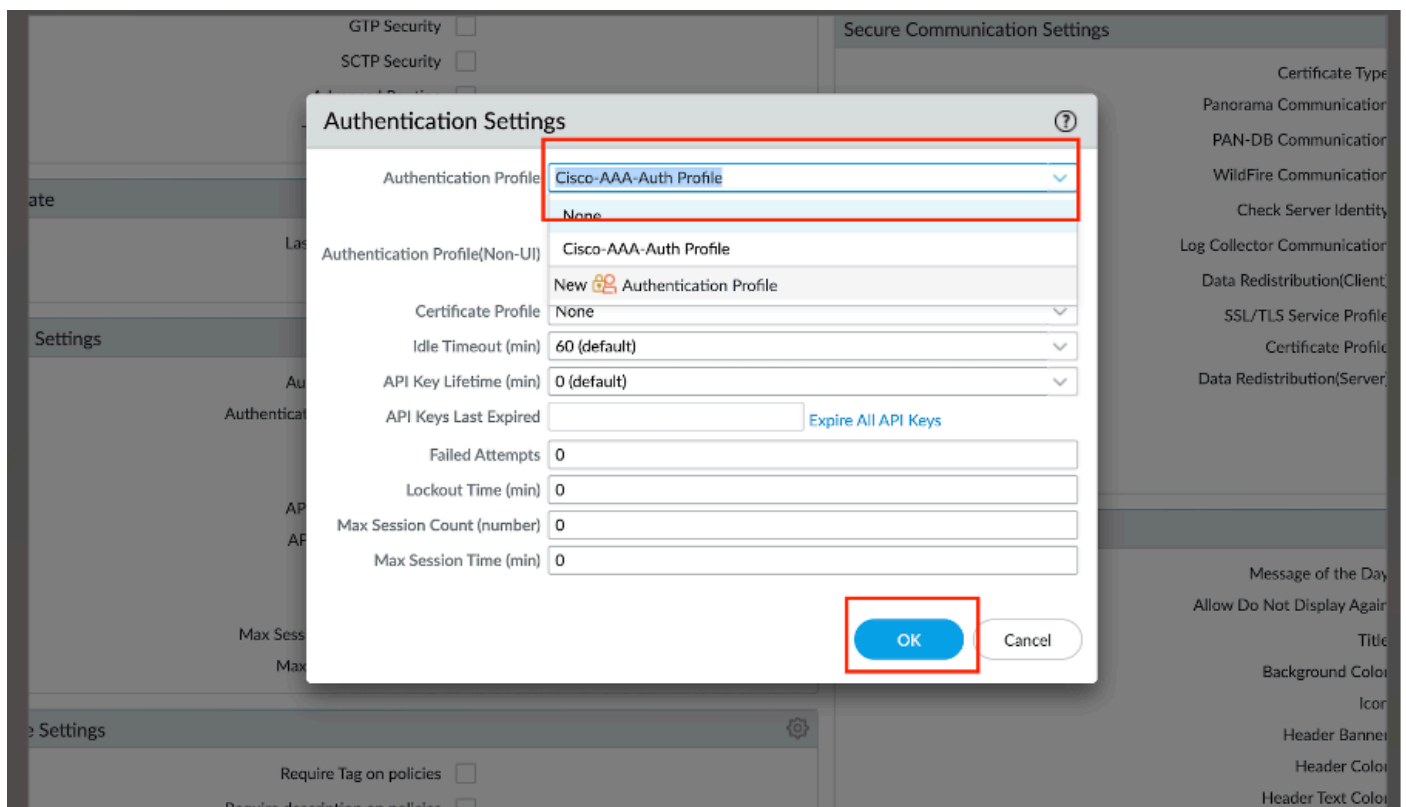
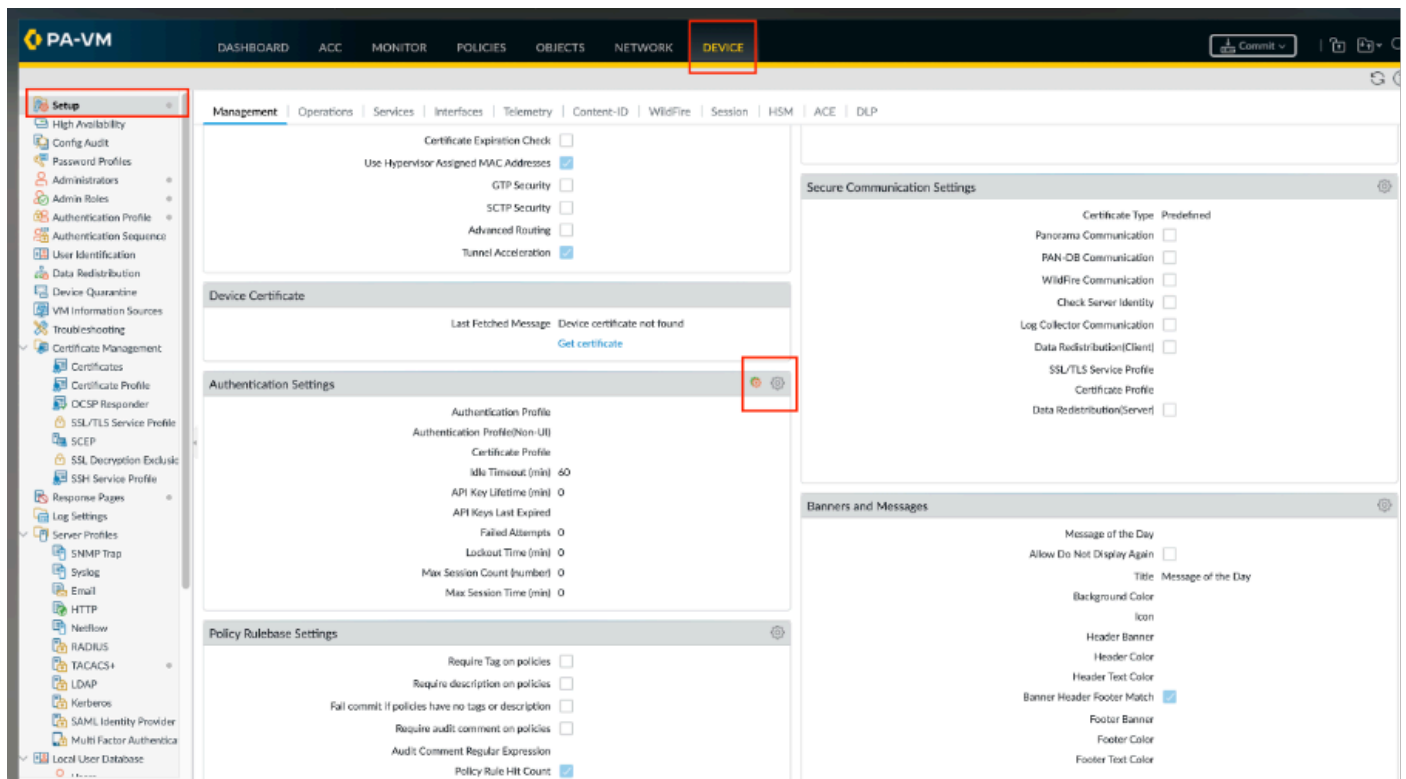
Failed Attempts [0 - 10]

Lockout Time (min) 0

OK Cancel

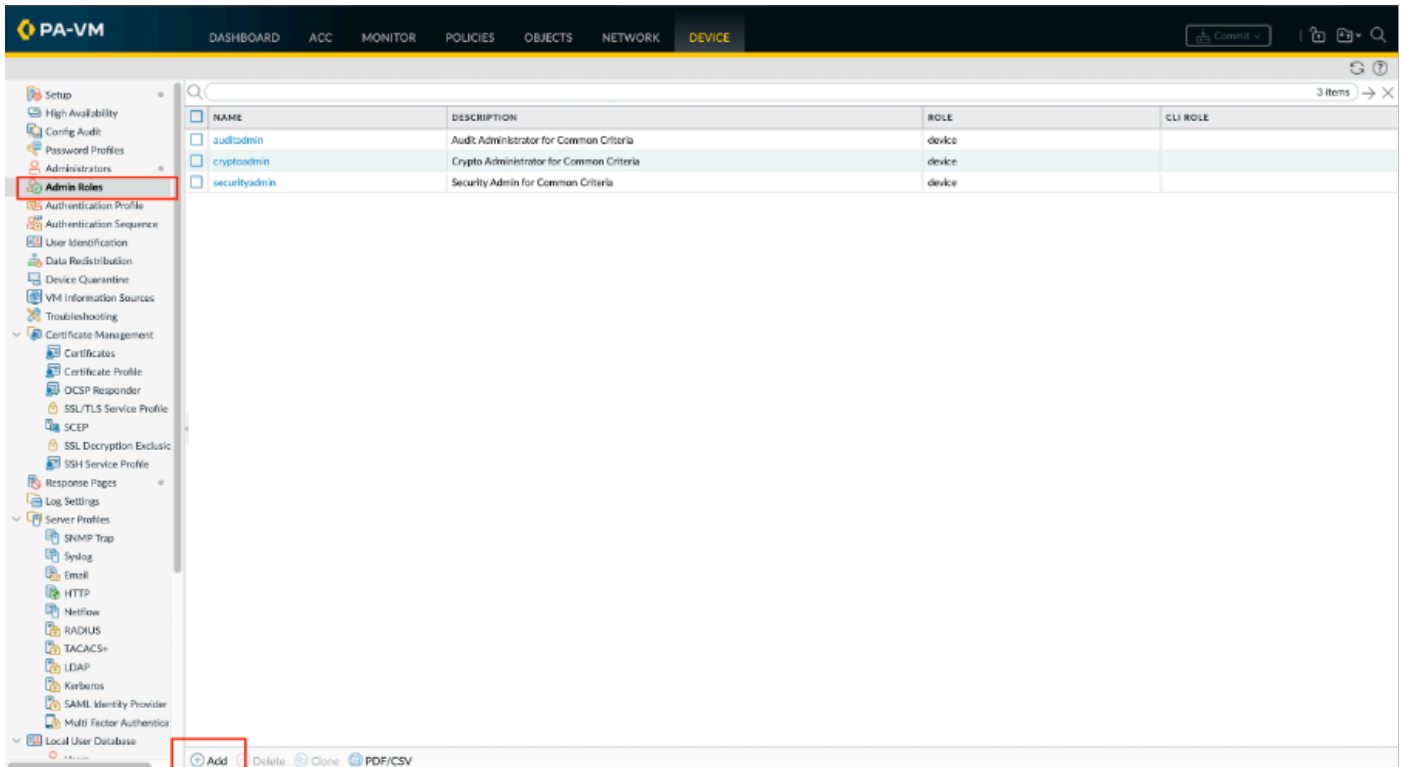
Step 3. Configure the firewall to use the authentication profile for all administrators.

1. Select **Device > Setup > Management** and edit the **Authentication Settings**.
2. Select the **Authentication Profile** you configured and click **OK**.

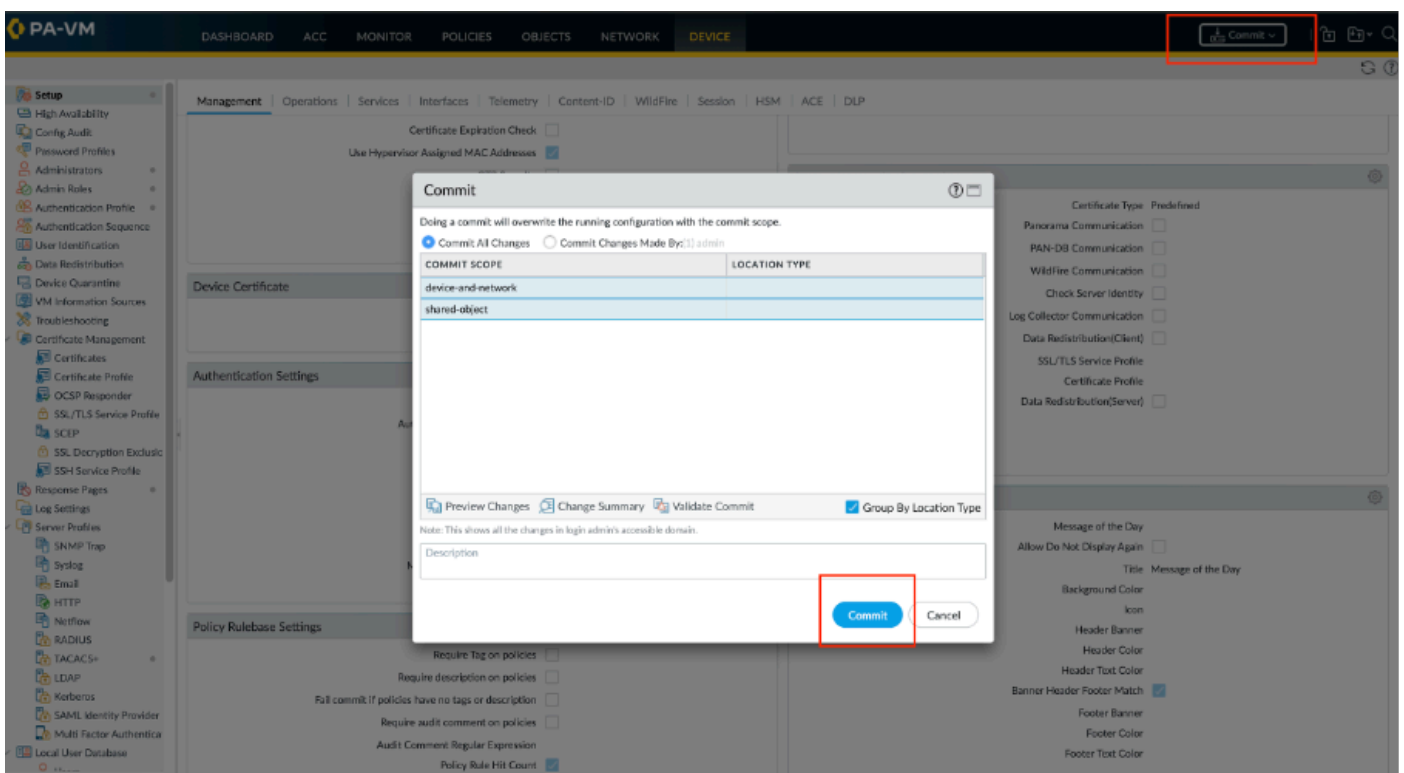


Step 4. Configure an Admin Role Profile.

Select **Device > Admin Roles** and click **Add**. Enter a **Name** to identify the role.



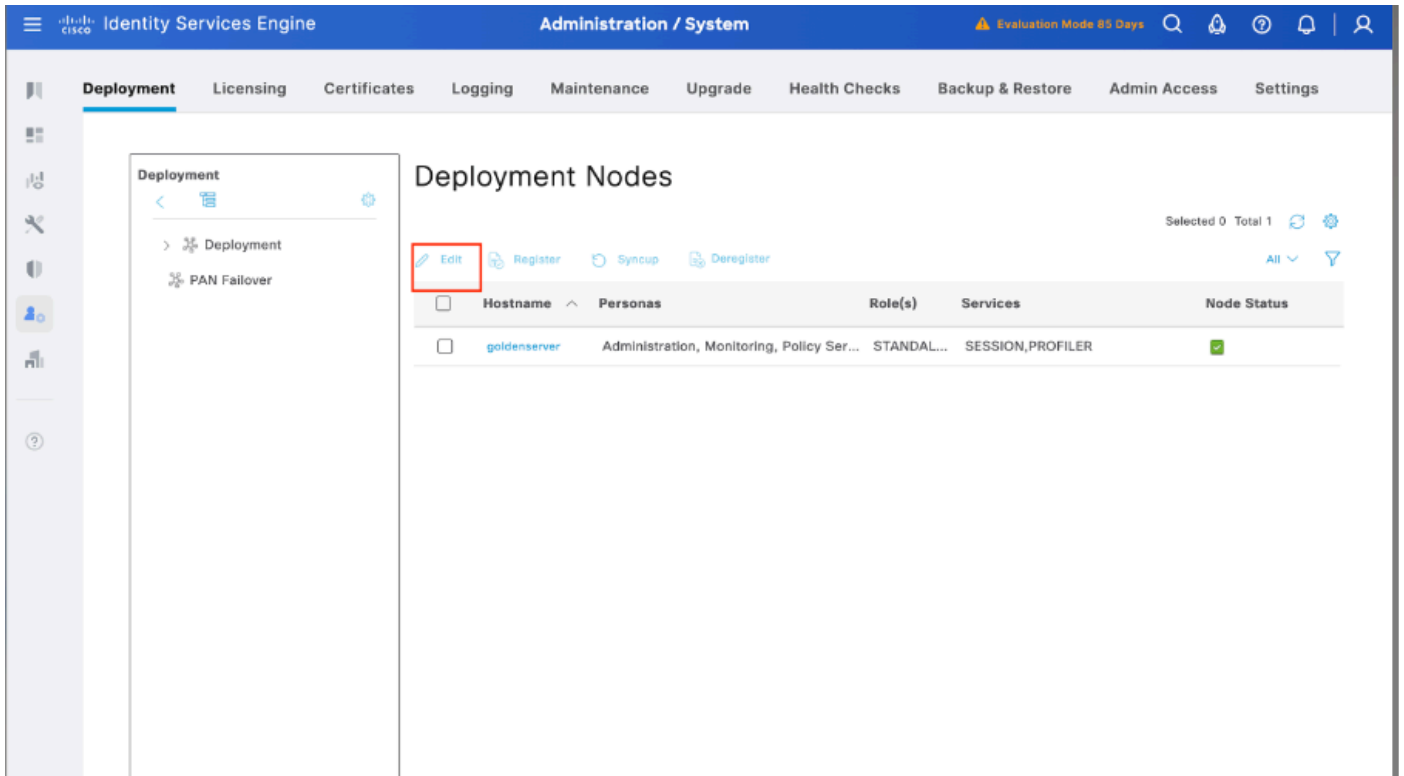
Step 5. Commit your changes to activate them on the firewall.



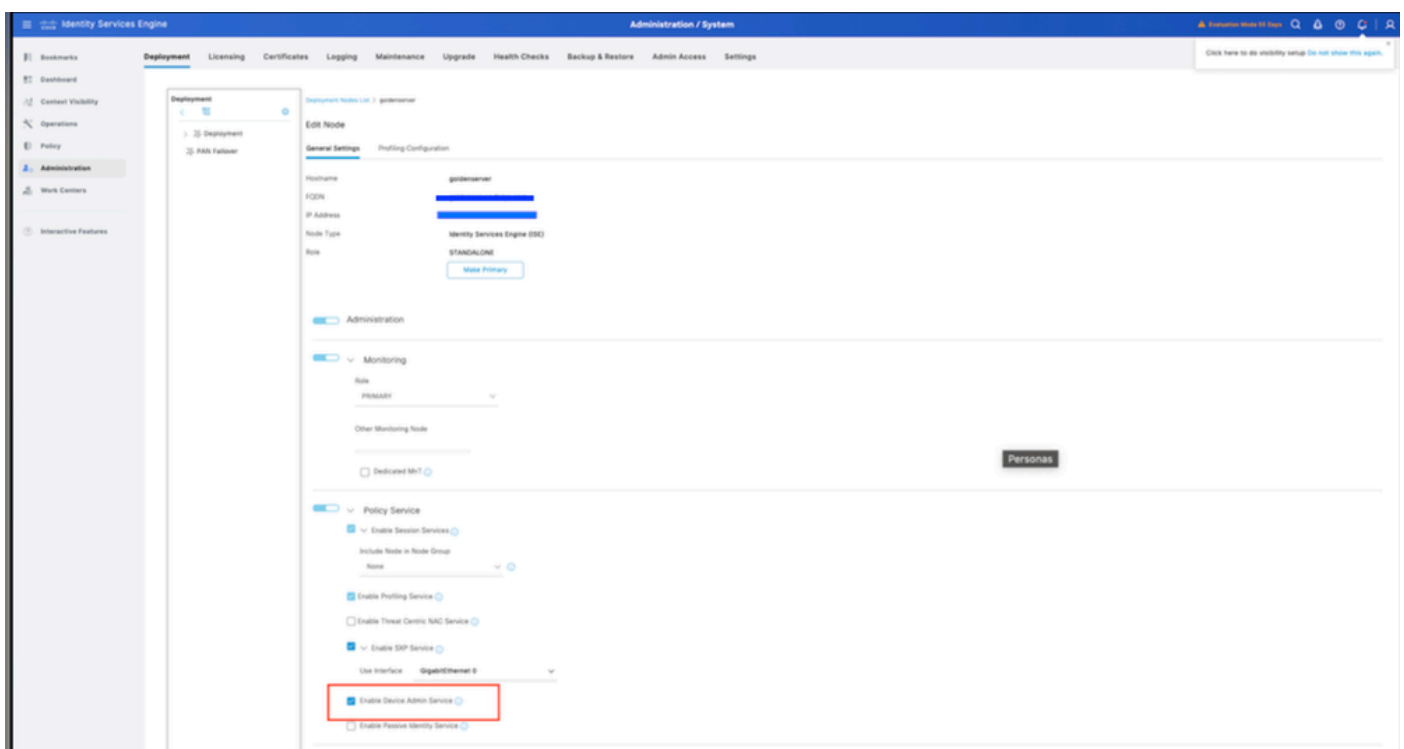
## Section 2: TACACS+ Configuration on ISE

Step 1. The initial step is to verify whether Cisco ISE has the necessary capabilities to handle TACACS+ authentication. To do this, confirm that the desired Policy Service Node (PSN) has the Device Admin Service feature enabled. Navigate to **Administration > System > Deployment**, select the appropriate node where ISE processes TACACS+ authentication, and click Edit to review its configuration.





Step 2. Scroll down to locate the Device Administration Service feature. Note that enabling this feature requires the Policy Service persona to be active on the node, along with available TACACS+ licenses in the deployment. Select the checkbox to enable the feature, then save the configuration.



Step 3. Configure Palo Alto Network Device Profile for Cisco ISE.

Navigate to **Administration > Network Resources > Network device profile**. Click **Add** and mention the name (Palo Alto) and enable TACACS+ under supported protocols.

Identity Services Engine Administration / Network Resources

Network Device Profiles

Name: **Palo\_Alto**

Description:

Icon: [Change icon...](#) [Set To Default](#)

Vendor: **Palo Alto**

Supported Protocols:

- ☒ RADIUS
- ☒ **TACACS+**
- ☒ TrustSec

RADIUS Dictionaries:

Templates:

- [Expand All / Collapse All](#)
- [Authentication/Authorization](#)
- [Permissions](#)
- [Change of Authorization \(CoA\)](#)
- [Redirect](#)
- [Advanced](#)

Summary:

Based on this configuration, the following are supported:

- Services: Radius, TACACS, TrustSec, MAB, EoL, IX
- CoA: Port Based (default CoA port: 3799, default DTLS CoA port: 2083)
- Native URL Redirect: [Static](#)

[Save](#) [Reset](#)

Step 4. Add Palo Alto as a Network Device.

1. Navigate to **Administration > Network Resources > Network Devices > +Add**.

Identity Services Engine Administration / Network Resources

Network Devices

Network Devices

Default Device

Device Security Settings

Network Devices

Selected 0 Total 0

[Edit](#) [+ Add](#) [Duplicate](#) [Import](#) [Export](#) [Generate PAC](#)

Name	IP/Mask	Profile Name	Location	Type
No data available				

2. Click **Add** and enter these details:

Name: Palo-Alto

IP Address: <Palo-Alto IP>

Network Device Profile: select Palo Alto

TACACS Authentication Settings:

## Enable TACACS+ Authentication

Enter the Shared Secret (must match Palo Alto configuration)

Click **Save**.

The screenshot shows the 'Administration / Network Resources' page in the Identity Services Engine. The 'Network Devices' section is active, showing a configuration for 'Palo\_Alto\_Firewall'. The 'TACACS+ Authentication Settings' section is highlighted with a red box, showing the 'Shared Secret' field and the 'Save' button. The 'Device Profile' is set to 'Palo\_Alto'. The 'IP Address' is set to '10.10.10.10'. The 'Device Type' is set to 'All Device Types'. The 'TACACS+ Authentication Settings' section is expanded, showing the 'Shared Secret' field and the 'Save' button. The 'Save' button is highlighted with a red box.

## Step 5. Create User Identity Groups.

Navigate to **Work Centers > Device Administration > User Identity Groups**, then click **Add** and specify the name for the user group.

The screenshot shows the 'Work Centers / Device Administration' page in the Identity Services Engine. The 'User Identity Groups' section is active, showing a configuration for 'Security Engineers'. The 'Name' field is highlighted with a red box, and the 'Save' button is also highlighted with a red box. The 'Description' field contains the text 'Identity group for Palo Alto'. The 'Member Users' section shows a table with columns for Status, Email, Username, and First Name. The table contains one row with the user 'divz'.

**Network Access User**

\* Username: diviyamol

Status: Enabled

Account Name Alias: \_\_\_\_\_

Email: \_\_\_\_\_

**Passwords**

Password Type: Internal Users

Password Lifespan:   
☐ With Expiration   
☒ Never Expires

\* Login Password: \_\_\_\_\_ Re-Enter Password: \_\_\_\_\_ Generate Password   
 Enable Password: \_\_\_\_\_ Generate Password

**User Information**

First Name: \_\_\_\_\_   
 Last Name: \_\_\_\_\_

**Account Options**

Description: \_\_\_\_\_   
 Change password on next sign: ☐

**Account Disable Policy**

☐ Disable account if date exceeds: 2023-03-18 (over-ride)

**User Groups**

Security support staff-PA

Save Reset

**User Identity Groups**

Identity Group

\* Name: Security support staff-PA   
 Palo Alto access for security support staff

Description: \_\_\_\_\_

Save Reset

**Member Users**

Users: Selected 0 Total 1 Refresh Settings

+ Add Delete All Filter

Status	Email	Username	First Name	Last Name
<input checked="" type="checkbox"/> Enabled		diviyamol		

Step 6. Configure A TACACS Profile.

Next up is configuring a TACACS Profile, which is where you can configure settings such as Privilege Level and timeout settings. Navigate to **Work Centers > Device Administration -> Policy Elements -> Results -> TACACS Profiles**.

Click **Add** to create a new TACACS Profile. Give the profile a good name.

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 Task Edit

Type	Name	Value
No data found.		

Mandatory PaloAlto\_Admin\_Rate 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 Task Edit

Type	Name	Value
No data found.		

Mandatory PaloAlto\_Admin\_Roles securityadmin

Cancel Save

Step 6. Configure TACACS Command Sets.

Now, it is time to configure which commands users are allowed to be use. Since you can grant both of these

use cases the Privilege Level 15, which gives access to every command available, use TACACS Command Sets to limit which commands can be used.

Navigate to **Work Centers > Device Administration > Policy Elements > Results -> TACACS Command Sets**. Click **Add** to create a new TACACS Command Set and name it PermitAllCommands. Apply this TACACS Command Set for Security Support.

The only thing you need to configure in this TACACS Command Set is to check the box for **Permit any command that is not listed below**.

The screenshot shows the 'Identity Services Engine' interface with the 'Work Centers / Device Administration' section active. The 'Policy Elements' tab is selected, and the 'TACACS Command Sets' sub-tab is highlighted. A new command set named 'PermitAllCommands' is being created. The 'Name' field is filled with 'PermitAllCommands'. The 'Description' field is empty. Under the 'Commands' section, the checkbox 'Permit any command that is not listed below' is checked. The 'Add' button is visible at the bottom right of the command list area. The 'Save' button is highlighted with a red box.

The screenshot shows the 'Identity Services Engine' interface with the 'Work Centers / Device Administration' section active. The 'Policy Elements' tab is selected, and the 'TACACS Command Sets' sub-tab is highlighted. A new command set named 'PermitBasicCommands' is being created. The 'Name' field is filled with 'PermitBasicCommands'. The 'Description' field is empty. Under the 'Commands' section, the checkbox 'Permit any command that is not listed below' is unchecked. The 'Add' button is visible at the bottom right of the command list area. The 'Save' button is highlighted with a red box.

Grant	Command	Arguments
<input type="checkbox"/>	PERMIT	show*
<input type="checkbox"/>	PERMIT	ping
<input type="checkbox"/>	PERMIT	traceroute
<input type="checkbox"/>	PERMIT	logout
<input type="checkbox"/>	PERMIT	exit

Step 7. Create a Device Admin Policy Set to be used for your Palo Alto, Navigate the menu **Work Centers > Device Administration > Device Admin Policy Sets**, Click the **Add** + icon.

Step 8. Name this new Policy Set, add conditions depending upon the characteristics of the TACACS+ authentications that is ongoing from the Palo Alto Firewall, and select as **Allowed Protocols > Default Device Admin**. Save your configuration.

The screenshot shows the 'Device Admin Policy Sets' configuration page in the Palo Alto Networks Identity Services Engine. The 'Policy Sets' table is visible, with the following data:

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
On	Palo Alto TACACS Access		DEVICE Device Type EQUALS All Device Types	Default Device Admin	17		
On	Armit Switch Access		DEVICE Device Type EQUALS All Device Types	Default Device Admin	131		
On	Default	Tacacs Default policy set		Default Device Admin	0		

The 'Save' button at the bottom right is highlighted with a red box.

Step 9. Select in the > **view** option, then in the Authentication Policy section, select the external identity source that Cisco ISE uses to query the username and credentials for authentication on the Palo Alto Firewall. In this example, the credentials correspond to Internal Users stored within ISE.

The screenshot shows the 'Authentication Policy' configuration page in the Palo Alto Networks Identity Services Engine. The 'Authentication Policy' section is expanded, showing the following data:

Status	Rule Name	Conditions	Use	Hits	Actions
On	PaloAlto_Auto Policy	Network Access-Device IP Address EQUALS 10.10.10.10	Internal Users > Options	17	
On	Default		Internal Users > Options	0	

The 'Options' dropdown menu for the 'PaloAlto\_Auto Policy' rule is highlighted with a red box.

Step 10. Scroll down until the section named Authorization Policy until the Default policy, select the gear icon, and then insert one rule above.

Identity Services Engine Work Centers / Device Administration Evaluation Mode 82 Days

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

Policy Sets → Palo Alto TACACS Access

Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Palo Alto TACACS Access		DEVICE-Device Type EQUALS All Device Types	Default Device Admin	17

> Authentication Policy(2)  
 > Authorization Policy - Local Exceptions  
 > Authorization Policy - Global Exceptions  
 < Authorization Policy(3)

Status	Rule Name	Conditions	Results			Hits	Actions
			Command Sets	Shell Profiles			
✓	PA_FW_Authz Policy	Internal/User Identity Group EQUALS User Identity Groups:Security support staff-PA	PermitAllCommands	PaloAlto_Security_Support	14		
✓	PA_FW_Security policy	Internal/User Identity Group EQUALS User Identity Groups:Security Engineers	PermitBasicCommands	PaloAlto_Engineers_Profile	2		
✓	Default		DenyAllCommands	Deny All Shell Profile	0		

Reset Save

https://10.127.186.85/admin/#collapse3-authorization

Step 11. Name the new Authorization Rule, add conditions concerning the user that is authenticated already as group membership, and in the Shell Profiles section add the TACACS profile that you configured previously, save the configuration.

## Verify

### ISE Review

Step 1. Review if the TACACS+ serviceability is running, this can be checked in:

- GUI: Review if you have the node listed with the service DEVICE ADMIN in **Administration -> System -> Deployment**.
- CLI: Run the command **show ports | include 49** to confirm that there are connections in the TCP port that belong to TACACS+

```
goldenserver/admin#show ports | include 49
tcp: [REDACTED]
```

Step 2. Confirm if there are live logs concerning TACACS+ authentications attempts : this can be checked in the menu **Operations -> TACACS -> Live logs**.

Depending upon the failure reason you can adjust your configuration or address the cause of failure.



Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device...
Mar 22, 2025 06:54:35.8...	<span style="color: red;">●</span>		diviyamol	Authentic...	Palo Alto TACACS Access >> P...		goldenserver	Palo_Alto_Firewall
Mar 22, 2025 06:54:17.5...	<span style="color: red;">●</span>		diviyamol	Authentic...	Palo Alto TACACS Access >> P...		goldenserver	Palo_Alto_Firewall
Mar 22, 2025 06:49:42.0...	<span style="color: green;">●</span>		divi	Authorizat...		Palo Alto TACACS Access >> P...	goldenserver	Palo_Alto_Firewall
Mar 22, 2025 06:49:41.9...	<span style="color: green;">●</span>		divi	Authentic...	Palo Alto TACACS Access >> P...		goldenserver	Palo_Alto_Firewall
Mar 22, 2025 06:49:28.2...	<span style="color: green;">●</span>		diviyamol	Authorizat...		Palo Alto TACACS Access >> P...	goldenserver	Palo_Alto_Firewall
Mar 22, 2025 06:49:28.1...	<span style="color: green;">●</span>		diviyamol	Authentic...	Palo Alto TACACS Access >> P...		goldenserver	Palo_Alto_Firewall

Step 3. In case you don't see any live log, proceed to take a packet capture navigate to the menu **Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump**, select **Add**.

**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

Host Name	Network Interface	Filter	File Name	Repository	File S...	Number of ...	Time Limit	Promiscu
-----------	-------------------	--------	-----------	------------	-----------	---------------	------------	----------

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 **tacacs\_issue**

Repository

File Size 10 Mb

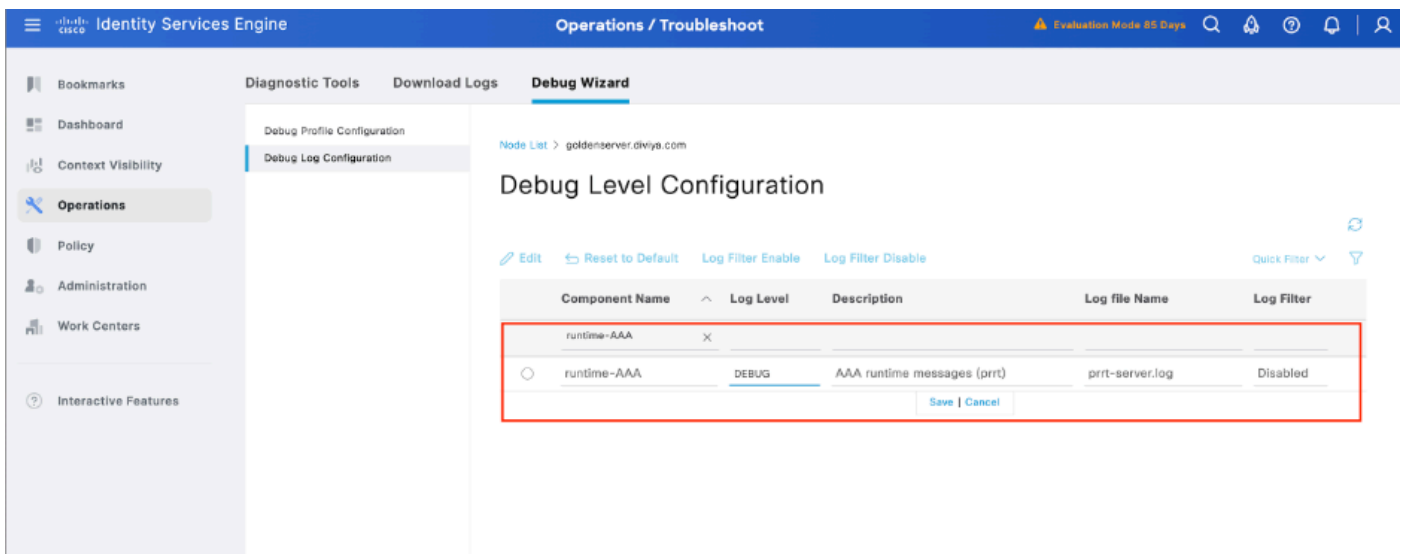
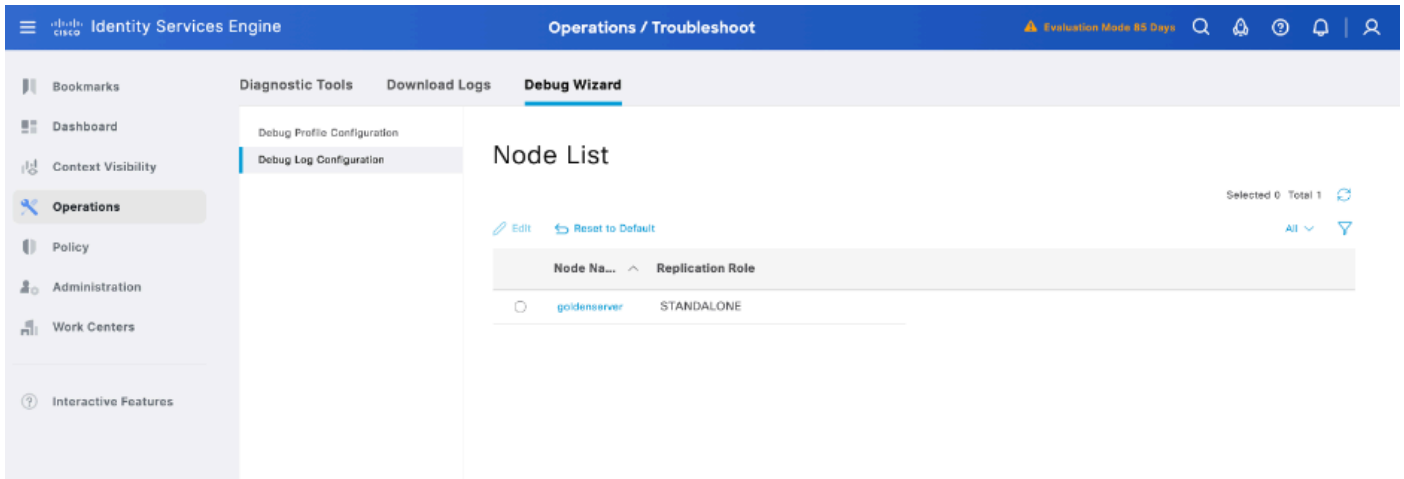
Limit to 1 File(s)

Time Limit 5 Minute(s)

☐ Promiscuous Mode

Cancel Save **Save and Run**

Step 4. Enable the component runtime-AAA in debug within the PSN from where the authentication is being performed in **Operations > Troubleshoot > Debug Wizard > Debug log configuration**, select PSN node , select then next in edit button .



Identify the **runtime-AAA** component, set its logging level to **debug**, reproduce the issue, and analyse the logs for further investigation.

## Troubleshooting

### TACACS: Invalid TACACS+ Request Packet – Possibly Mismatched Shared Secrets

#### Problem

TACACS+ authentication between the Cisco ISE and the Palo Alto firewall (or any network device) fails with the error message:

**"Invalid TACACS+ request packet - possibly mismatched 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	

This prevents successful administrative login attempts and can impact device access control through centralized authentication.

## Possible Causes

- A mismatch in the shared secret configured on Cisco ISE and the Palo Alto firewall or network device.
- Incorrect TACACS+ server configuration on the device (such as wrong IP address, port, or protocol).

## Solution

There are several possible resolutions for this issue:

1. Verify the Shared Secret:

- On Cisco ISE:  
Navigate to Administration > Network Resources > Network Devices, select the affected device, and confirm the shared secret.
- On the Palo Alto firewall:  
Go to Device > Server Profiles > TACACS+, and ensure the shared secret matches exactly, including case and special characters.

2. Check TACACS+ Server Settings:

- Ensure the correct IP address and port (default is 49) of Cisco ISE are configured in the firewall's TACACS+ profile.
- Confirm that the protocol type is TACACS+ (not RADIUS).