

Palo Alto ىلع TACACS+ ةزهجأ ةرادإ نيوكت ISE مادختساب

تايوتحمل

[ةمدقملا](#)

[ةيساسالاب لطلتلا](#)

[ةمدختسملا تانوكملا](#)

[ةكبش ليل يطي طختلا مسرلا](#)

[ةقداصملا قفدت](#)

[نيوكتلا](#)

[Palo Alto ل TACACS+ ةيامح رادج نيوكت: 1 مسقلا](#)

[ISE ىلع TACACS+ نيوكت: 2 مسقلا](#)

[ةحصلا نم ققحتلا](#)

[ISE ةعجارم](#)

[اهجالص او عا طخال افاشكتسا](#)

[ةقباطت مريغ ةكرتشملا رارسال نيوكت دق - ةجل اصريغ TACACS+ بلط ةمزح: TACACS:](#)

[ةلكشملا](#)

[ةلمتحملا بابسالا](#)

[لجلا](#)

ةمدقملا

Cisco ISE مادختساب وتلا ولاب ىلع TACACS+ نيوكت دنتسملا اذه فصوي.

ةيساسالاب لطلتلا

ةيلاتلا عيضاوملاب ةفرعم لكي دل نيوكت ناب Cisco ي صوت:

- Cisco نم TACACS+ و ISE لوكوتورب
- Palo Alto ةيامح رادج

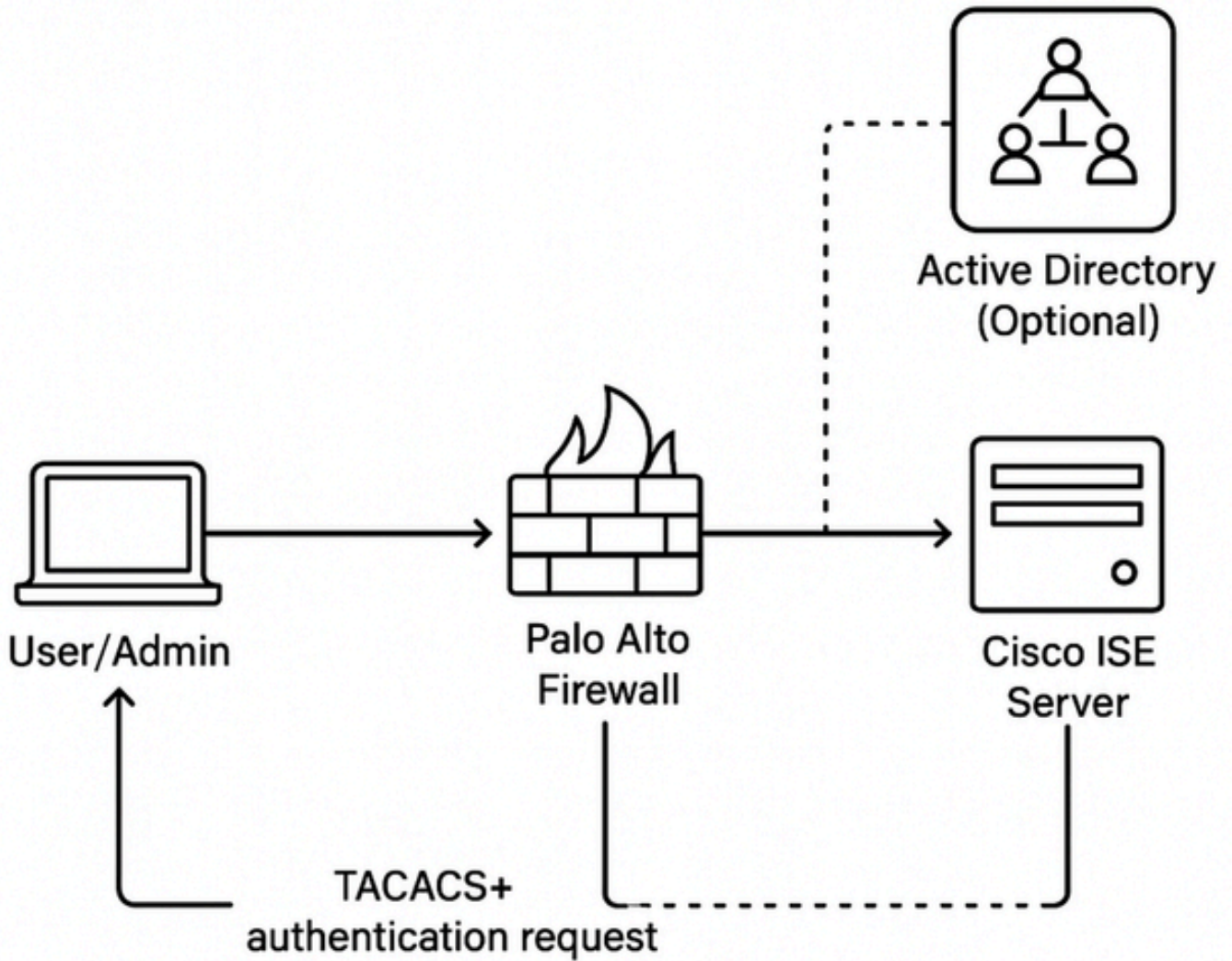
ةمدختسملا تانوكملا

ةيلاتلا ةيداملا تانوكملا وجماربل تارادصا ىل دنتسملا اذه في ةدراولا تامولعمل دنتست:

- 10.1.0 رادصلا Palo Alto ةيامح رادج
- Cisco Identity Services Engine (ISE)، 3.3 Patch 4 رادصلا

ةصاخ ةيلمعم ةئيب في ةدوجوملا ةزهجال نم دنتسملا اذه في ةدراولا تامولعمل عاشنإ مت تناك اذإ. (يضا رتفا) حوسمم نيوكتب دنتسملا اذه في ةمدختسملا ةزهجال عيمج تأدب رما يال لمتمحمل ريثأتلل كمهف نم دكأتف، ليغشتلا دي قكتكبش

ةكبش ل ل ي ط ي ط خ ت ل ا م س ر ل ا



ةق د ا ص م ل ا ق ف د ت

1. Palo Alto ةي ا م ح ر ا د ج ل ل ا ل و خ د ل ا ل ي ج س ت ب ل و ؤ س م ل ا م و ق ي .

2. Cisco ISE ل ل ا TACACS+ ةق د ا ص م ب ل ط و ت ل ا و ل ا ب ل س ر ي .

3. Cisco ISE:

- ض ي و ف ت ل ا و ةق د ا ص م ل ل A D م ل ع ت س ي ه ن ا ف ، A D ج م د ة ل ا ح ي ف .
- ت ا س ا ي س ل ا و ا ة ي ل ح م ل ا ة ي و ه ل ن ز ا خ م م د خ ت س ي ه ن ا ف ، ن ا ل ع ا ك ا ن ه ن ك ي م ل ا ذ ا .
- م ت ي ت ل ا ت ا س ا ي س ل ا ل ا ا د ا ن ت س ا P a l o A l t o ل ل ا ل ي و خ ت ة ب ا ج ت س ا C i s c o I S E ل س ر ي . ا ه ن ي و ك ت .
- ب س ا ن م ل ا ز ا ي ت م ا ل ا ي و ت س م ع م ل و ص و ل ا ل ع ل و ؤ س م ل ا ل ص ح ي .

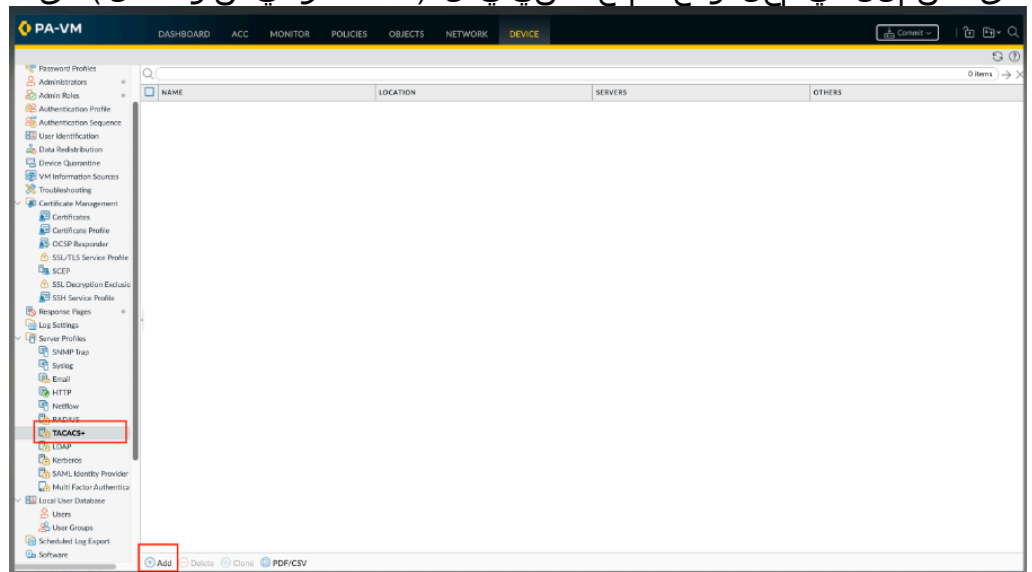
ن ي و ك ت ل ا

Palo Alto J TACACS+ ةيامح راج نيوك ت: 1 مسقلا

TACACS+ مداخ فيرعت فلم فضا 1. ةوطخلا

TACACS+ مداخ ةيامحلا راج ليصوت ةيفيك فيرعتلا فلم ددحي

1. > مداخلا فيرعت تافلم > اماروناب و TACACS+ > مداخلا فيرعت تافلم > زاهج ددح. فيرعت فلم فضا امارونابلا لىل TACACS+.
2. مداخلا فيرعت فلم فيرعتلا فيرعتلا فلم مسا لخدأ.
3. نيلوؤسملا لىل لوصول ديقتل طقف لوؤسملا مادختسا ددح (ي رايتخا).
4. وه يضارتفالا) ةقداصملا بلط ةلهم اهدعب يهتنت يتلا يناوثللاب ةلهملا ةرتف لخدأ. (1-20 وه ىدملا؛ 3).
5. ةقداصملا ةيامحلا راج هم دختسي يذلا (CHAP وه يضارتفالا) ةقداصملا لوكوتورب ددح.

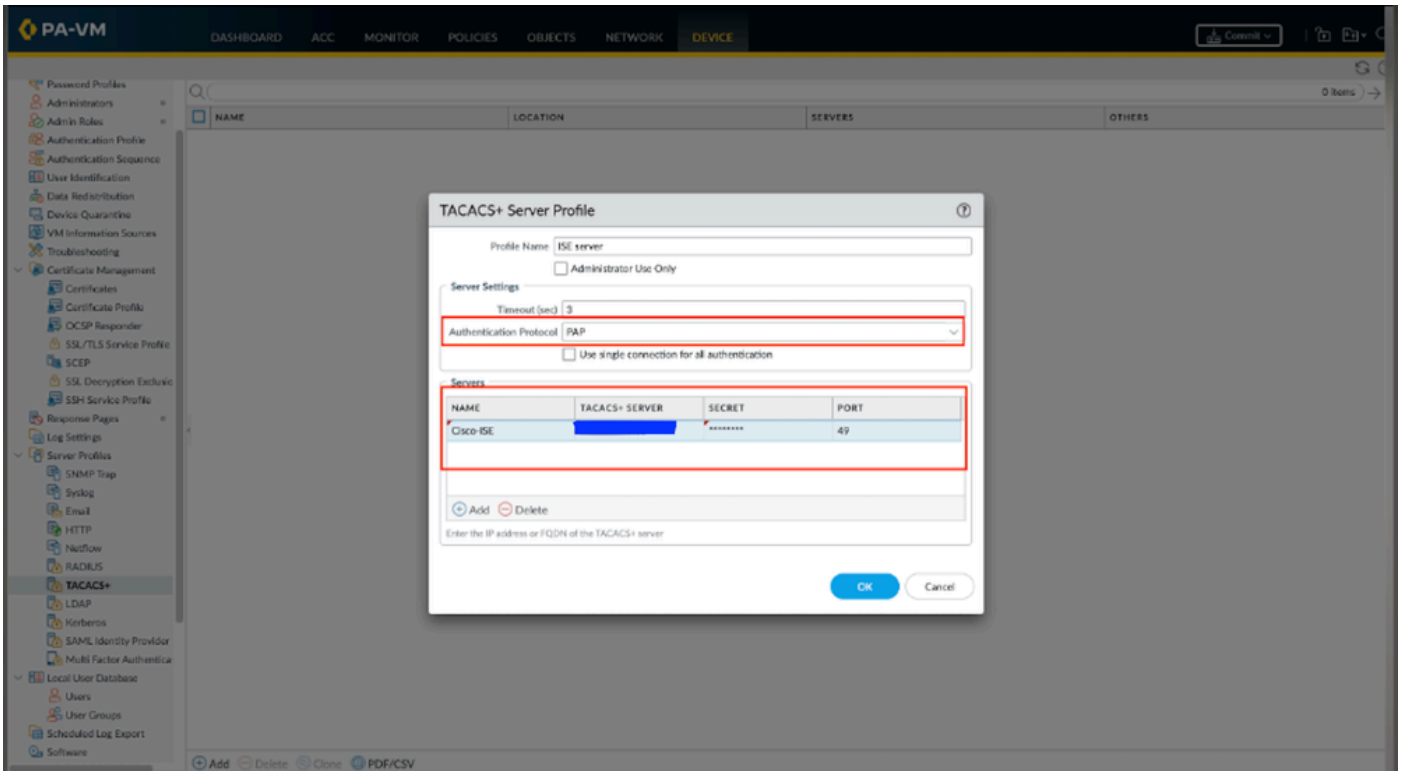


TACACS+ مداخ لىل

6. ةيلاتلا تاوطخلا ذيفنتو TACACS+ مداخ لك ةفاضلا:

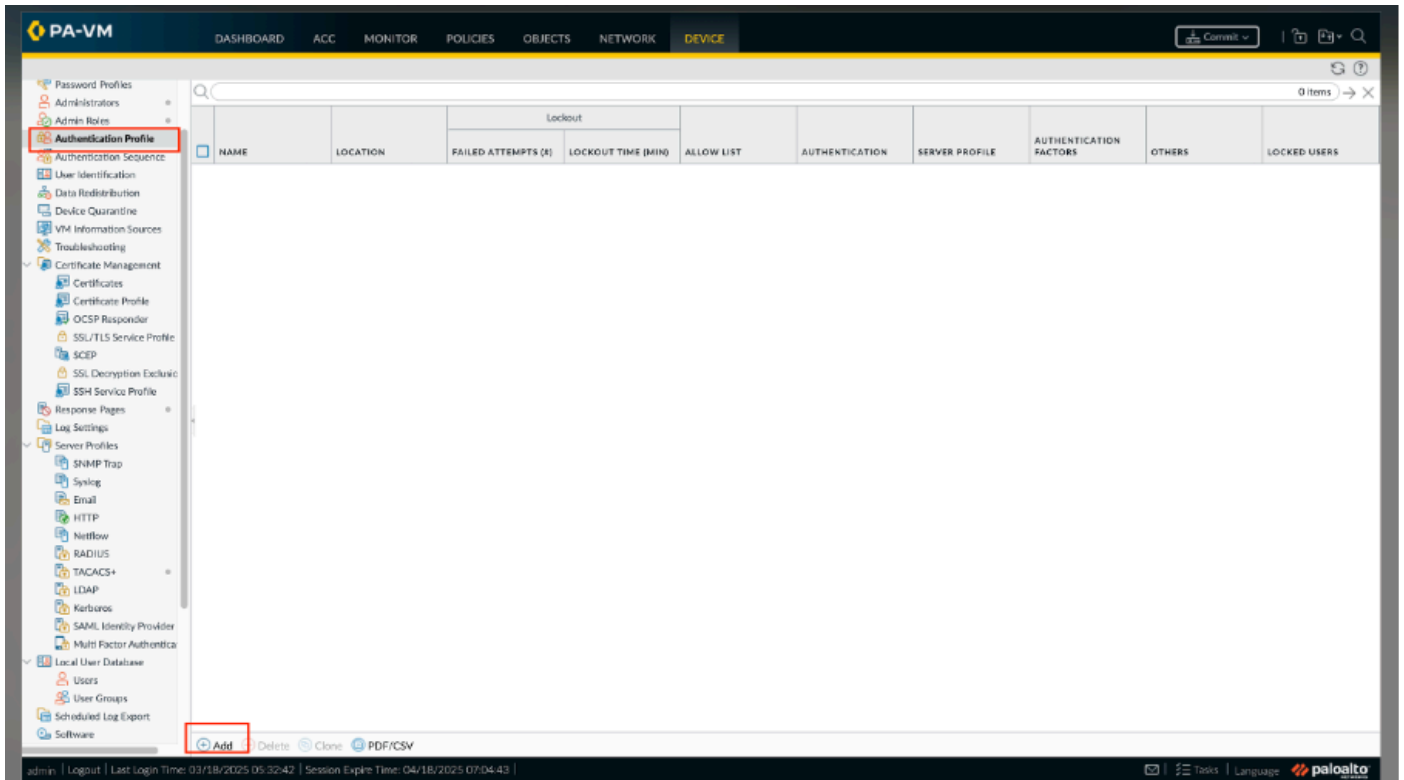
1. مداخلا فيرعتلا مسا.
2. ناووع نئاك مدختست تنك اذا FQDN و TACACS+ مداخ صاخلا IP ناووع كيلىل بجيف، كلذدعب ناووعلا ريغيغتب تمق مئ مداخلا لىل فرعتلا FQDN لوعفملا يراس ديدجلا مداخلا ناووع حبصيل ريغيغتلا ذيفنت رورملا تاملكو ني مدختسملا ءامسا ريغشتل ديكأت رس.
3. ظفحل قفاوم لىل رقنا. (49 وه يضارتفالا) ةقداصملا تابلل مل مداخلا ذفنم.
4. مداخلا فيرعت فلم.

7. مداخلا فيرعت فلم ظفحل قفاوم قوف رقنا.



ةقداصم فيرعت فلم ىلإ TACACS+ مداخ فيرعت فلم نييعتب مق 2. ةوطخلا
نم دختسمل نم ةومجمل ةعئاشلا ةقداصملا تاداعل ةقداصملا فيرعت فلم ددحي

1. فيرعت فلم ةفاضل ةقداصملا فيرعت فلم > زاهج ددح.
 1. فيصوتلا فيرعتل امسا لخدأ
 2. TACACS+ ىل عونلا نييعتب مق
 3. هنيوكتب تمق يذلا مداخلا فيرعت فلم ددح
 4. ةومجمل تامولعم عمجل TACACS+ نم ني دختسمل ةومجمل دادرسل ددح
TACACS+ مداخلا ىل ةفرعمل VSA تاكبش نم ني دختسمل



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

حاصل الةمئاق في اهدحت يتل تاوموم ال م ادخت ساب ةوموم ال تامول عم ةيامل راج قباطي ةقداصلم فيرعت فلمب

- قداصل نأ نكمي يتل تاوموم ال او نيمدختسم ال فضا، حاصل الةمئاق في ةومومت دح. اذه ةقداصلم فيرعت فلم عم
- ةقداصلم في صوت ظفحل قفاوم يلع رقنا.

Authentication Profile

NameCisco-AAA-Auth Profile

Authentication | Factors | **Advanced**

Allow List

☐

ALLOW LIST ^

☒all

+ Add

- Delete

Account Lockout

Failed Attempts[0 - 10]

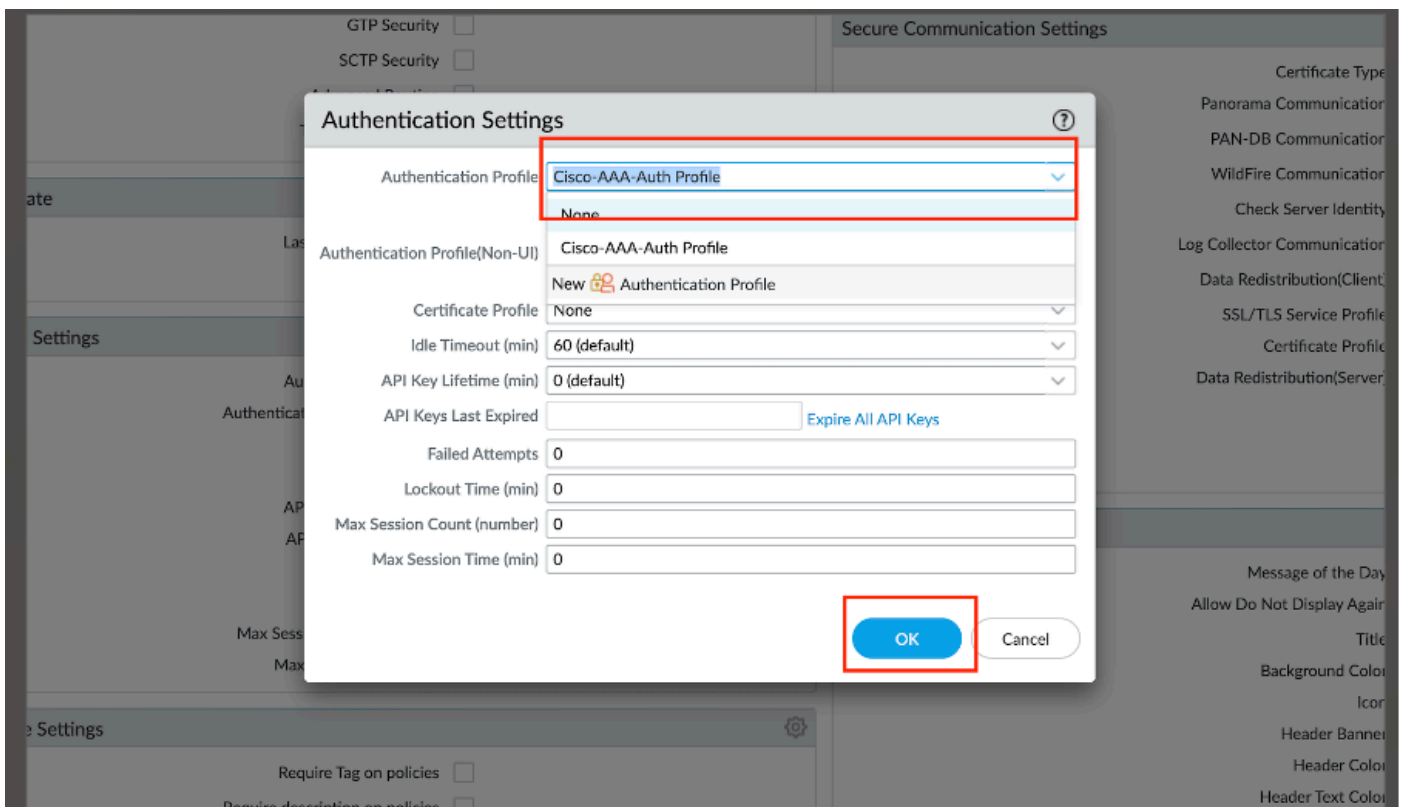
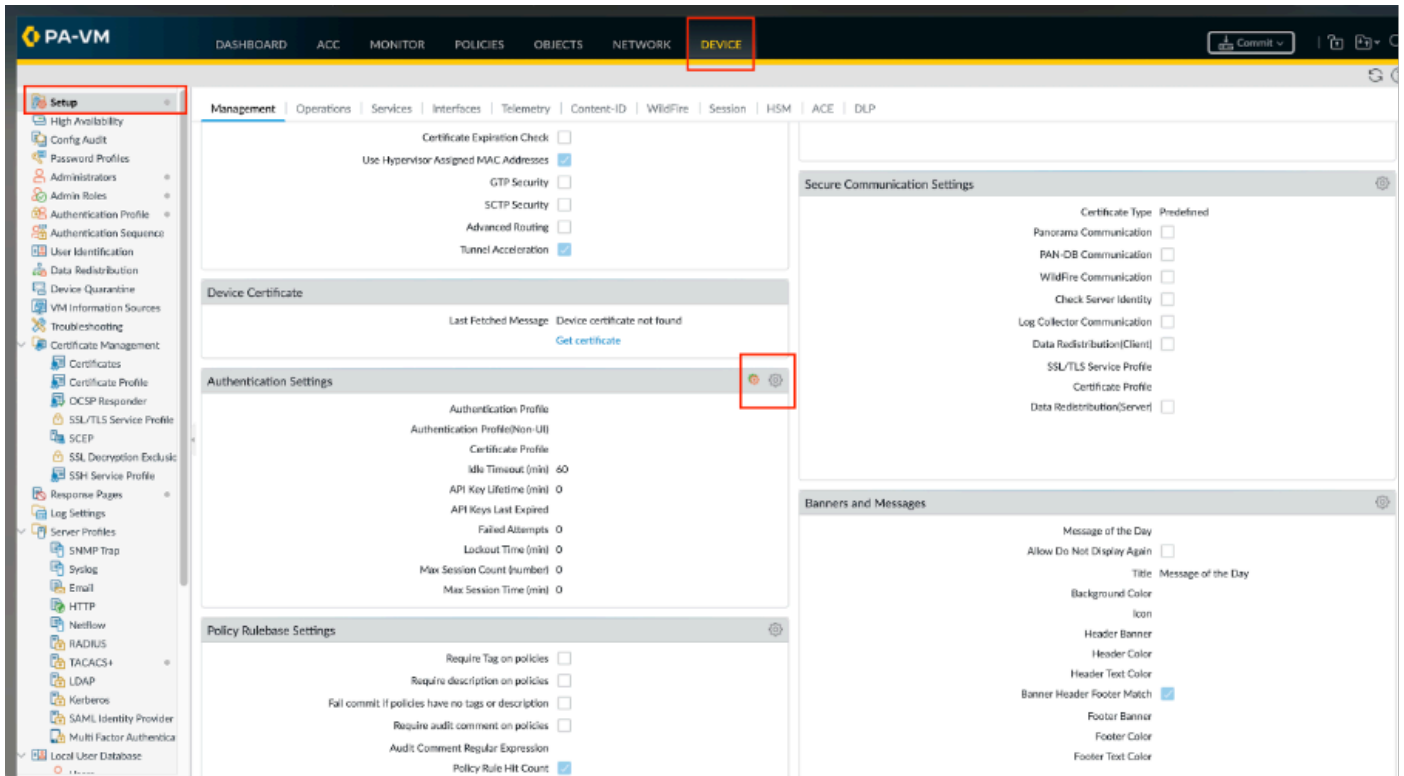
Lockout Time (min)0

OK

Cancel

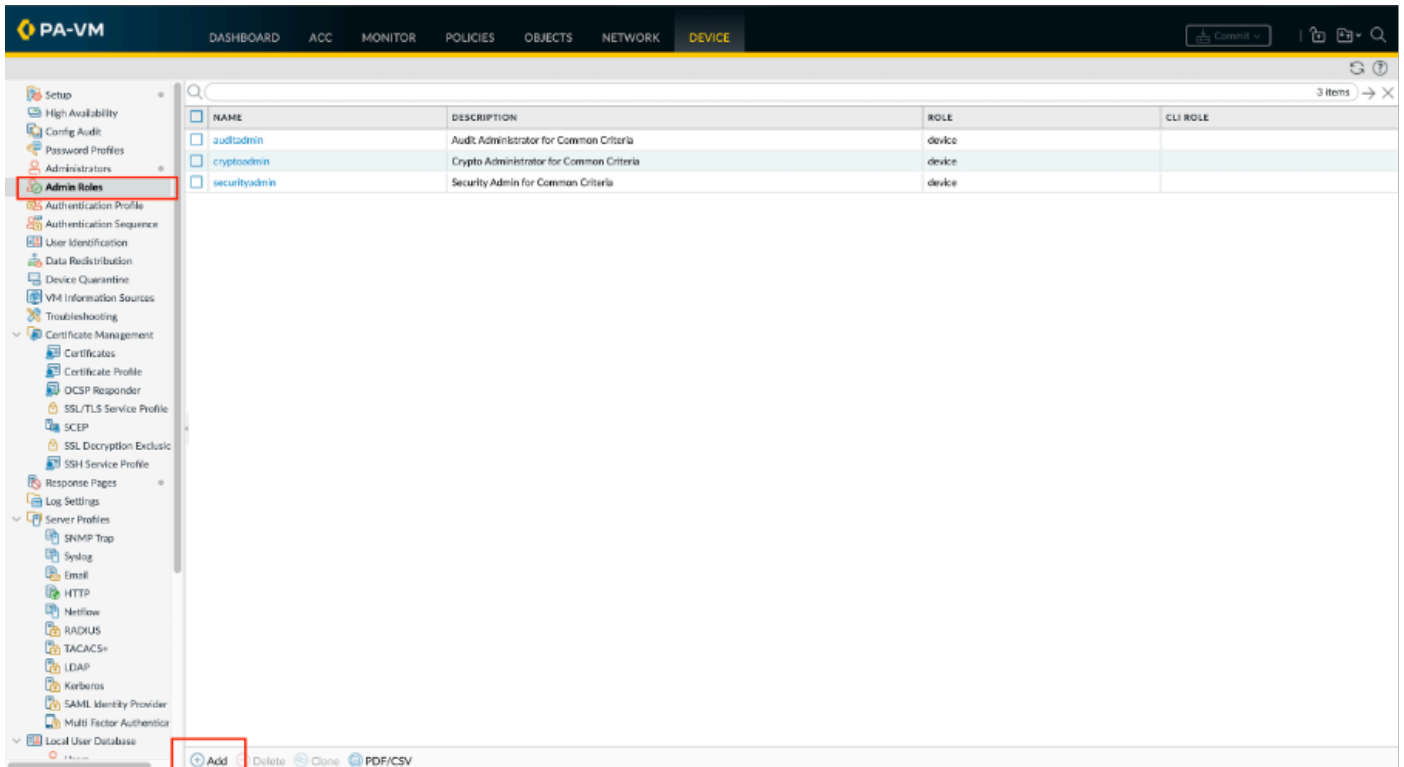
نيلوؤسمل اعمجل ةقداصلم ال فيرعت فلم مادختسال ةيامل راج نيوكتب مق 3. ةوطخل

- ةقداصلم ال تادادعل ريحتو ةرادا > دادعإ > زاهج ددح.
- قفاوم ىلع رقنا مئ هنيوكتب تمق يذلا ةقداصلم ال فيرعت فلم ددح.

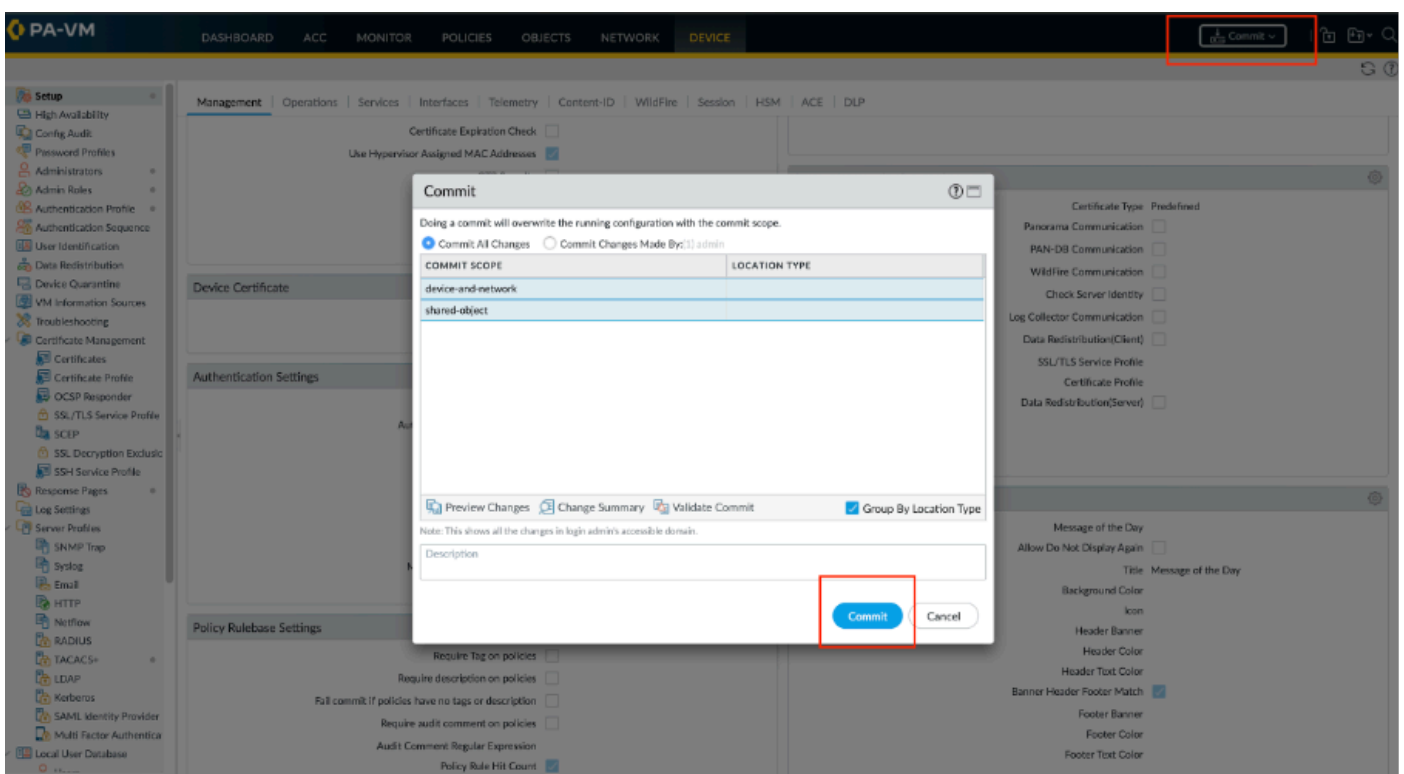


لوؤسمال رود فيرعت فلم نيوك ت. 4 ةوطخل

رودلا دي دحتل امسا لخدأ. ةفاضل رقناو لوؤسمال راودأ > زاخ دح

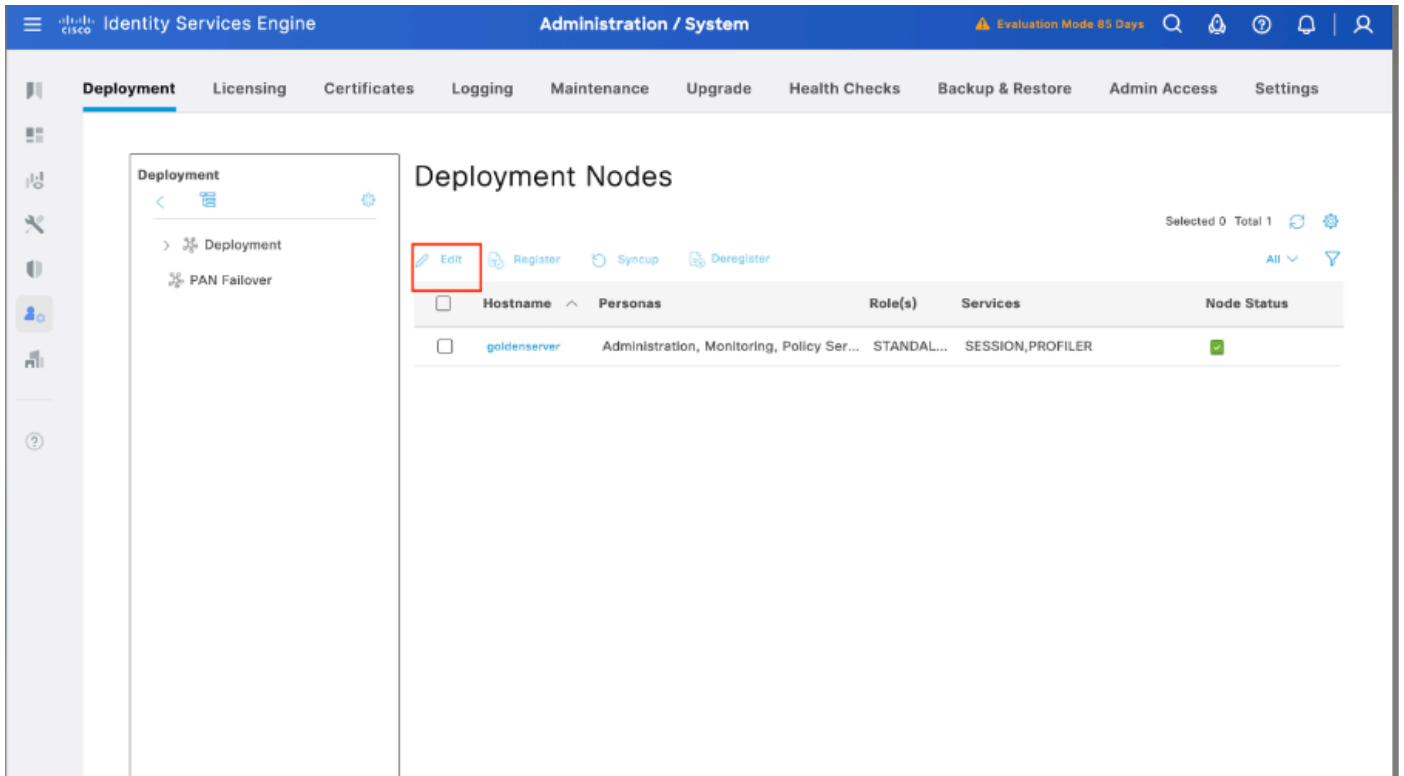


ةي امحل رادج ىل ع اهطي شنتل اهتيرج ايتل تاريغيغتلا ذيفنتب مق 5 ةوطخل

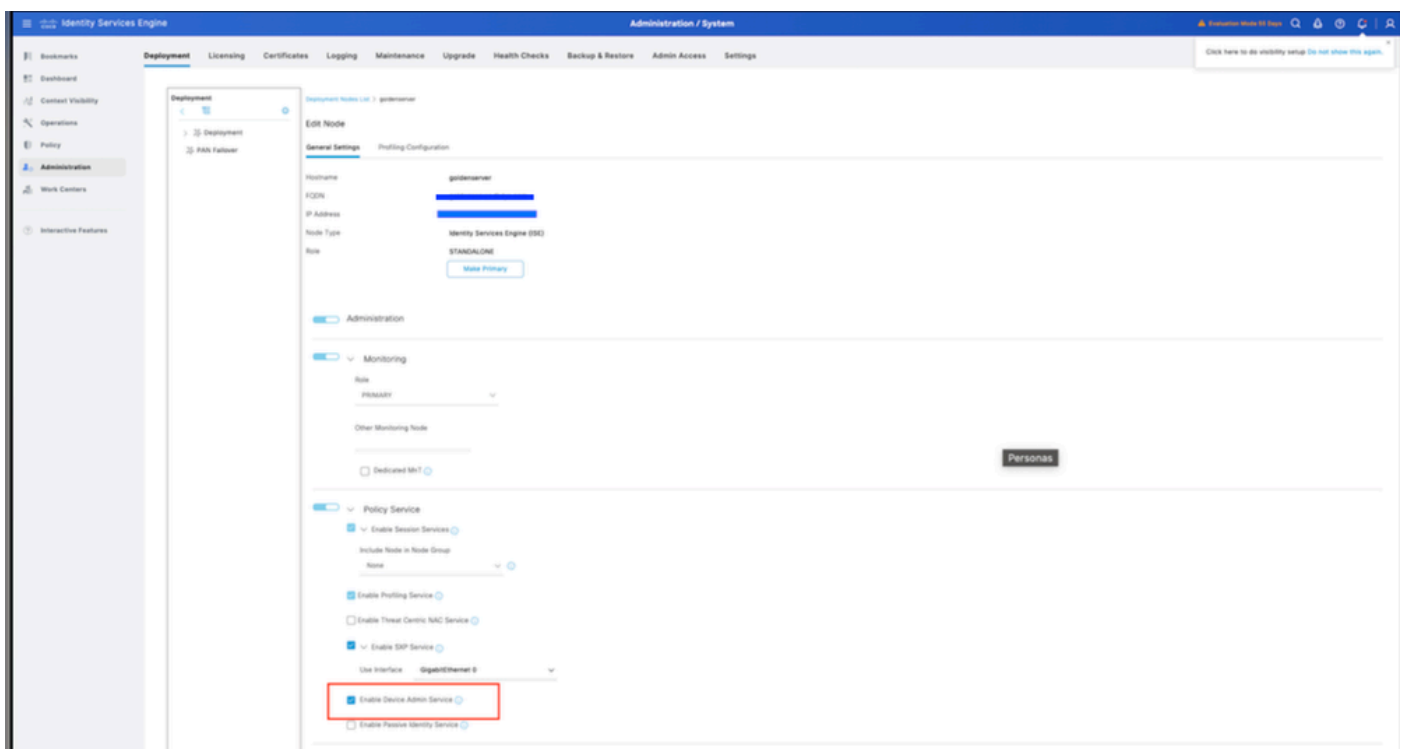


ISE ىل ع TACACS+ نيوكت 2 مسقلا

ةمزاللا تاردقلا Cisco ISE ىدل ناك اذا ام ققحتلا ي في ةيلوالا ةوطخل لثمتت 1 ةوطخل اذقعل (PSN) "جهنلا ةمدخ" ةزيم نيكمت نم دكأت ،كلذب مايقلل . TACACS+ ةقداصم ةجل اعمل شح ةبسانملا ةدقعل ددحو ،رشنلا > ماظنلا > ةرادلا ىل لقتنا . ةبولطملا جهنلا ةمدخ هب صاخلا نيوكتلا ةعجارمل ريحت قوف رقناو ، TACACS+ ةقداصم ةجل اعمل ISE موقي



هذه نيكمت نأ طحال .ةزهجال ةرادا ةمدخ ةزيم عقوم ديدحتل لفسأل ريرمتلاب مق 2. ةوطخل صيخارت بناج ىلا ،ةدقعل ىلع اطشن ةسايسلا ةمدخ صخش نوكي نأ بلطتي ةزيملا نيوكتل ظفحا م ث ،ةزيملا نيكمتل رايتخالا ةناخ دح .رشنلا يف ةحاتملا TACACS+



Palo Alto Network ل Cisco ISE زاخ فيرعت فلم نيوكتب مق 3. ةوطخل

مسالا ةفاضل قوف رقنا .ةكبشلا زاخ فيرعت فلم > ةكبشلا دراوم > ةرادا ىلا لقتنا (Palo Alto) ةمدوملا تالوكوتوربلا نمض TACACS+ نيكمتب مقو

Identity Services Engine Administration / Network Resources

Network Device Profiles

Name: Palo_Alto

Description:

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

Vendor: Other

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

ةكبش زاهجك Palo Alto ةفاضإ 4. ةوطخل

ةفاضإ+ > ةكبشلل ةزهجأ > ةكبشلل دراوم > ةرادإ ىلإ لقنتنا 1.

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				

ةيئاتل لىصافتلا لخدأو ةفاضإ قوف رقنا 2:

وتلأ ولاب :مسال

IP: <palo-alto IP> ناونع

وتلأ ولاب ددح :ةكبشلل زاهج فيرعت فلم

TACACS: ةقداصم تادادع

TACACS+ ةقداصم نيكم ت

(وتلأ ولاب نيوكت قباطي نأ بجي) "كرتشم لا رسل" لخدا

ظفح قوف رقنا

The screenshot displays the 'Administration / Network Resources' page in the Identity Services Engine. The 'Network Devices' tab is active, showing a list of devices. The 'Palo_Alto_Firewall' device is selected, and its configuration is shown. The 'Device Profile' is set to 'Palo_Alto'. The 'TACACS Authentication Settings' section is expanded, showing a 'Shared Secret' field with a 'Show' button and a 'Save' button. The 'Save' button is highlighted with a red box.

مدختسمل ةي وه تاعومجم ءاشنإ 5. ةوطخل

مسا ددحو ةفاضإ رقنا م ث ،مدختسمل ةي وه تاعومجم > زاهال ةرادإ > لمعل زكارم ىلإ لقتنا
نم مدختسمل ةعومجم

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 Name

☐ 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 Device > divznet

Network Access User

* Username divznet

Status Enabled

Account Name divz

Email

Passwords

Password Type Internal Users

Password Lifespan

With Capitalization Never Expires

Password

Re-Enter Password

* Login Password

Enable Password

Generate Password

User Information

First Name

Last Name

Account Options

Description

Change password on next login

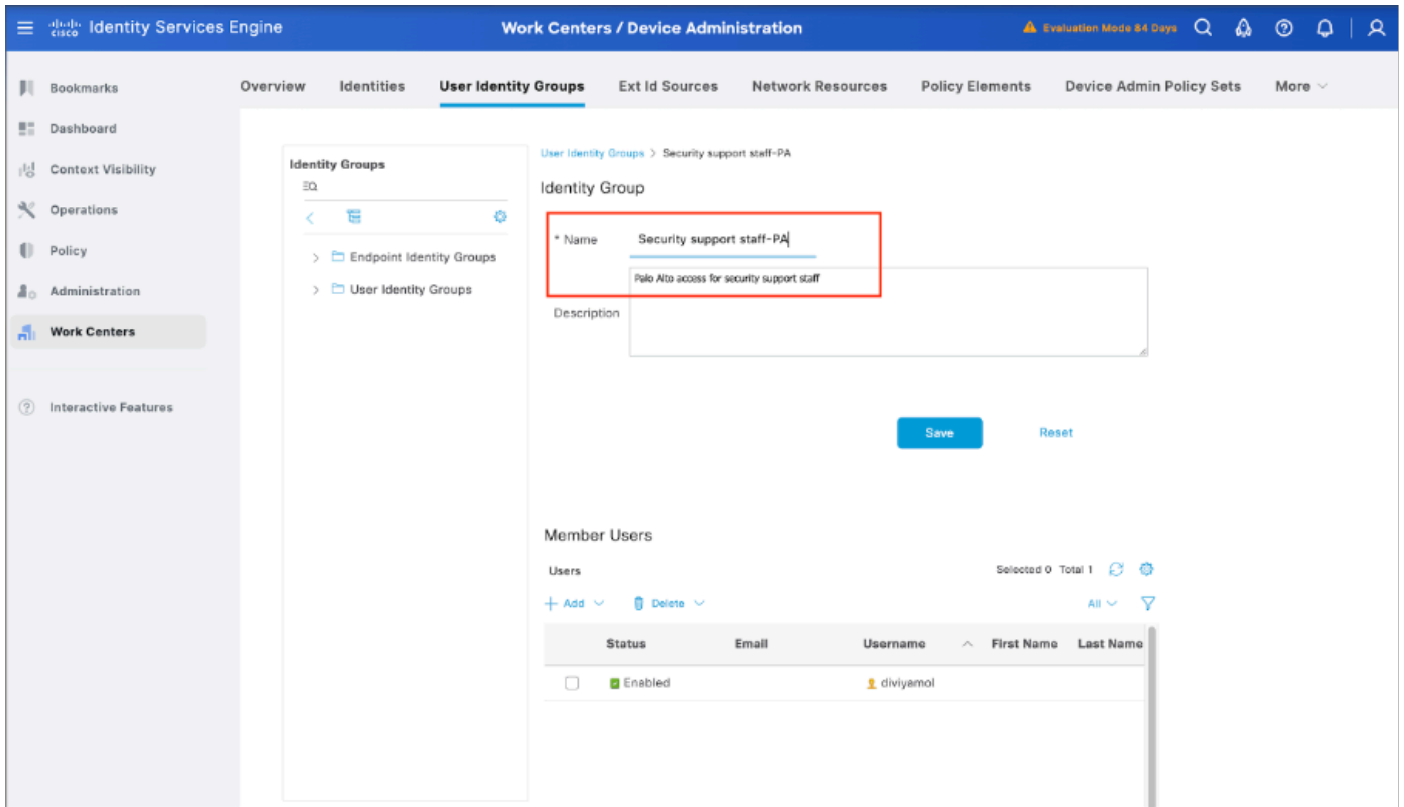
Account Disable Policy

Disable account if date exceeds 2023-03-19

User Groups

Security support staff PK

Save Reset



TACACS فيرعت فلم نيوكت 6. ةوطخل

لثم تادادعإ نيوكت هي ف كنكمي يذل ناكملا وهو TACACS فيصوت up يلاتال لكشي
 -> جهنل رصانع -> ةزهألأ ةرادإ > لمعل زكارم يلا لقتنا .ةلهمل تادادعإو زايتمالا يوتسم
 TACACS فيرعت تافلما -> جئاتنلا

مساب فيرعتال فلم ةيمستب مق .ديج TACACS فيرعت فلم عاشنال ةفاضإ يلع رقنا
 ديج .

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 Trash Edit

Type	Name	Value
Mandatory	PaloAlto_Admin_Role	Support

No data found.

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 Trash Edit

Type	Name	Value
Mandatory	PaloAlto_Admin_Roles	securhythm

No data found.

Cancel Save

TACACS رماو اتاعومجم نيوكت 6. ةوطخل

عيطتسي تنأ نأ امب .اهم ادختساب ني مدختسم ل حومسم ل رماوالا نيوكتل تقولا ناح ، نآل

رفوتي رمأ لك إلى ذفنم يطيغي يأ 15، وتسم زايتم الالاح لامعتسا اذه نم الالك تحنم،
تلمعتسا تنك عيظتسي رمأ يأ دحي نأ عومجم رمأ TACACS تلمعتسا

TACACS. رمأوا تاعومجم -> جئاتنل > عسايسل رصانع > زاهجلا ةرادا > لمعلل زكارم إلى لقتنا
PermitAllCommands اهتيمستو ةديج TACACS رمأوا عومجم عاشنل ةفاضل قوف رقنا
نامأل معدل هذه TACACS رمأوا عومجم قيبت

عبرملا ديدحت وه هذه TACACS رمأوا عومجم يف هنيوكت إلى جاتحت يذلل ديحولل ايشل
هاندا جردم ريغ رمأ يأب حامسلل

Identity Services Engine Work Centers / Device Administration

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy

Conditions > TACACS Command Sets > PermitAllCommands
Command Set

Name: PermitAllCommands

Description:

Commands

Permit any command that is not listed below ☒

Add Trash Edit Move Up Move Down

Grant	Command	Arguments
No data found.		

Cancel Save

Identity Services Engine Work Centers / Device Administration

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy

Conditions > TACACS Command Sets > PermitBasicCommands
Command Set

Name: PermitBasicCommands

Description:

Commands

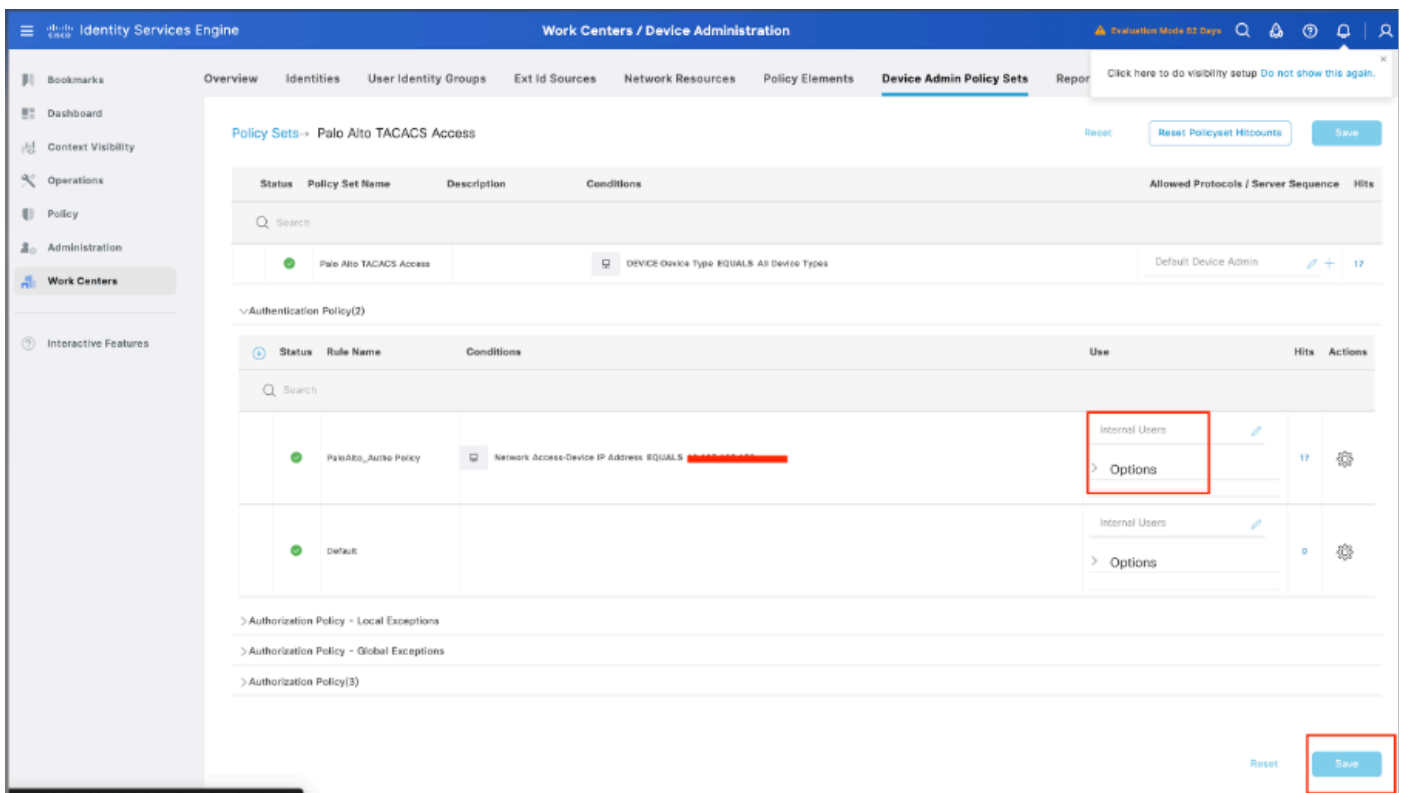
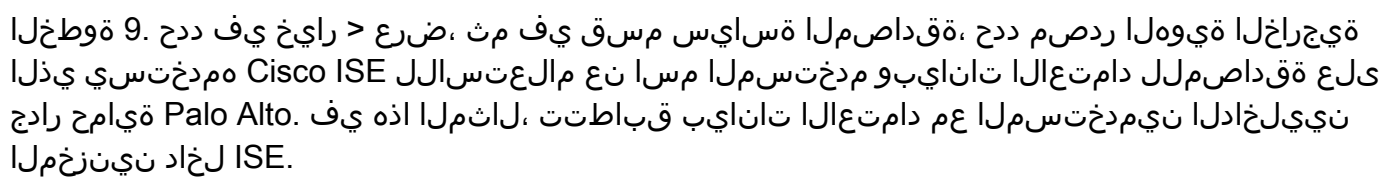
Permit any command that is not listed below ☐

Add Trash Edit Move Up Move Down

Grant	Command	Arguments
☐	PERMIT	show*
☐	PERMIT	ping
☐	PERMIT	traceroute
☐	PERMIT	logout
☐	PERMIT	exit

Cancel Save

قد اصم صئاصخل اقفو طورش ةفاضإو، هذه ةديدل جهنل ةعومجم ةيمستب مق 8. ةوطخل زاهل لوؤسم > اهب حومسم تالوكوتوربك ددح مث ، Palo Alto ةيامح رادج نم ةيرال TACACS+ .كب صاخل نيوكتل ظفح. يضارتال



جهنللا ىتح لىوختلا جهن ىمسمل مسقلا ىتح لفسأل رىرمتلاب مق 10. ةوطخلال هالعا ءءاوةءاق لالءاب مق مء ءاءءالا ءنوقى ءءو ءىضارئالا

مءءءسملاب ءقلءءءملا ءورشلل فضاء ءءءءل لىوختلا ءءاق ءىمسءب مق 11. ةوطخلال فلم فضاء Shell فىرءءءافلم مسق فىو ءءوءءم ءىوؤءءك لءفلاب هءقءاصم ءمء ىءلا فىرءءءافلم ءافءا ءقءسم هءىوؤءب ءمق ىءلا TACACS فىرءءءافلم

ءءصلا نم ققءءءلا

ءءءء ISE

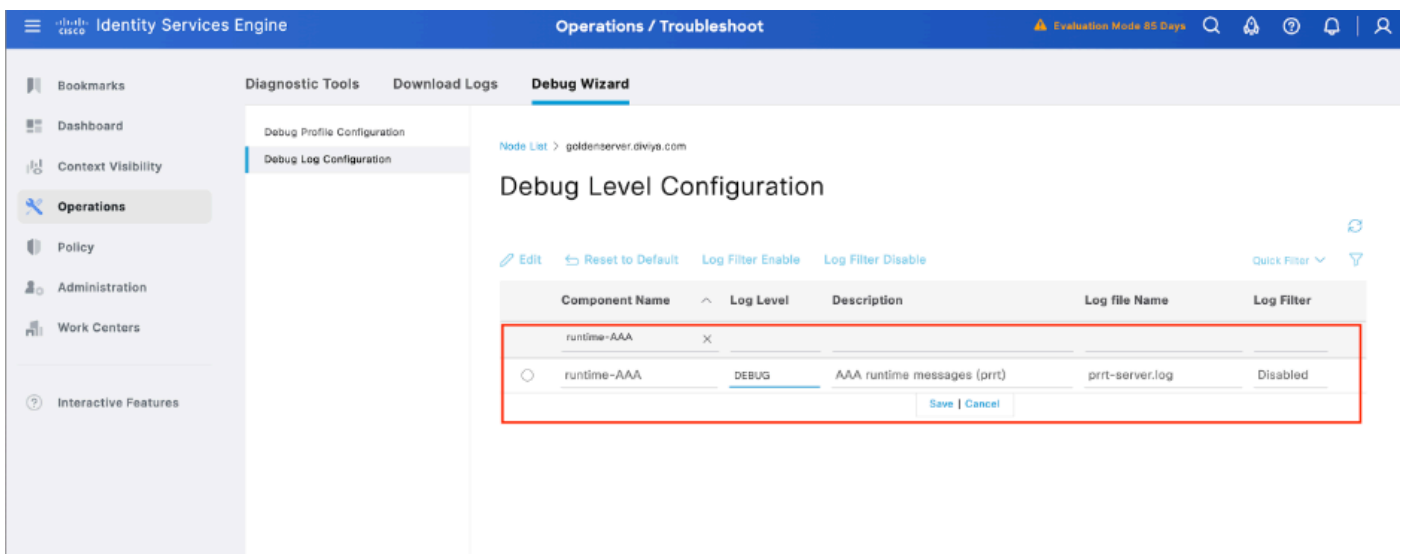
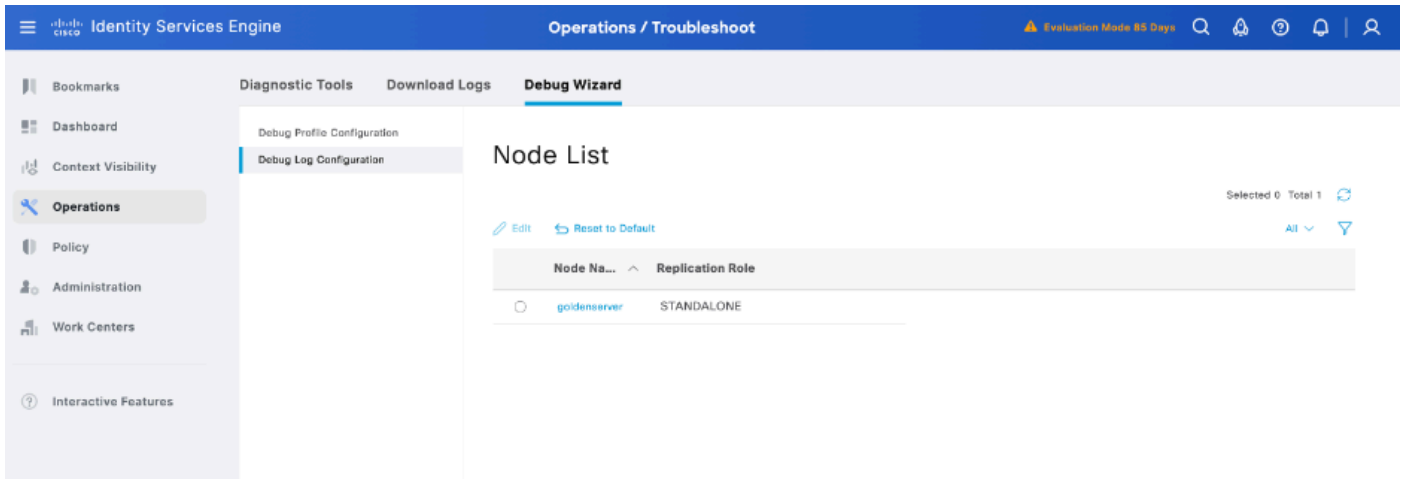
ىلى ام ءاءى نكمىو ءىغءءءلا ءىق TACACS+ ءءءءءا ءءا ءءار 1. ةوطخلال

- ءءا ءءا -> ءءاءال فى ءءءءال زاء ءوؤسم ءم ءءءءملا ءءءءل ءءل ناك ءءا ءءارم GUI: رءءءل
- CLI: ءءم فى ءالاءءءا ءوءو ءىءءل 49 نمؤءءى | show ports رملال لىغءءب مق TACACS+ ءلى ءىءءء

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

ءه ءاءى نكمى : TACACS+ ءقءاصم بقلءءء ءرءابم ءالءس ءانه ءءا ءءا ءءا 2. ةوطخلال Live ءالءس -> TACACS ءءءاقال ءالءم فى

لشفلل ببس ءءلاءم وأ نىوؤءلا ءبؤ ءنكمى لشفلل ببس ببس ءلء



حيحصت ىل ع هب صاخال لىجستل لىوتسم نىي عتب مقو، AAA لىغشتل ت قو نوكم ددح قىقحتل نم دىزمل تالچسل لىلحتو، لكشم لاشن اءاعاو، اءاخال

اهحال صاوا اءاخال فاشكتسا

رىغ كرتشم لارسلال نوكت دق - ءحال ص رىغ TACACS+ بل ط ءم زح: TACACS
ءق باطام

ءلكشم ل

ءلاس ر عم (ءكبش زاهج ا و) Palo Alto ءىامح راءحو Cisco ISE نىب TACACS+ ءقءاصم لشفى
اأخال:

"ءق باطام رىغ كرتشم لارسلال نوكت دق - ءحال ص رىغ TACACS+ بل ط ءم زح"

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	

في مكدحتل الى ع رثؤي نأ نكمي و عجانل اة رادلل لوخدل ليجست تالواحم عنم الى يدؤي اذهو
ةيزكرمل اة قداصم لال خ نم زاهج الى ل لوصول

ةلمتحم ال بابسأل

- Palo اةي امح رادج و Cisco ISE الى ع هنيوكت مت يذل كرتشم ال رسل ي قفاوت مدع ةلا ح
ة. كبش زاهج وأ Alto
- وأ ذفنم ال وأ حيحص ريغ IP ناوع لثم) زاهج الى ع حيحص ريغ TACACS+ مداخ نيوكت
(لوكتو و ربل).

الحل

ةضقلا هذهل ةلمتحملا تارارقلا نم ديدعلا كانهو

1. كرتشملا رسلال نم ققحتلا:

- Cisco ISE ىلع:
رسلال ىلع دكأ م ث ، رثأتملا زاهجلا ددحو ، ةكبشلل ةزهجأ > ةكبشلل دراوم > ةرادإ ىلإ لقتنا
كرتشملا.
- Palo Alto ةيامح رادج ىف:
رسلال ةملك قباطت نم دكأتو ، TACACS+ > مداخلل فيرعت تافلم > زاهجلا ىلإ لقتنا
ةصاخلا فرحألاو ةلاحلا كلذ ىف امب ، امامت ةكرتشملا.

2. TACACS+ مداخل تادادعإ ددح:

- فلم ىف Cisco ISE ل (49 وه ىضارتفالا) حىحصلا ذفنملاو IP ناونع نىوكت نم دكأت
ةيامحلا رادجل TACACS+ فيرعت.
- (RADIUS سىلو) TACACS+ وه لوكوتوربلا عون نأ نم دكأت.

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا