

Configurazione dell'amministrazione dei dispositivi TACACS+ su Palo Alto con ISE

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Componenti usati](#)

[Esempio di rete](#)

[Flusso di autenticazione](#)

[Configurazione](#)

[Sezione 1: Configurazione di Palo Alto Firewall per TACACS+](#)

[Sezione 2: Configurazione TACACS+ su ISE](#)

[Verifica](#)

[Recensione ISE](#)

[Risoluzione dei problemi](#)

[TACACS Pacchetto di richiesta TACACS+ non valido - Possibile mancata corrispondenza dei segreti condivisi](#)

[Problema](#)

[Possibili cause](#)

[Soluzione](#)

Introduzione

Questo documento descrive la configurazione di TACACS+ su Palo Alto con Cisco ISE.

Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Protocollo Cisco ISE e TACACS+.
- Firewall di Palo Alto.

Componenti usati

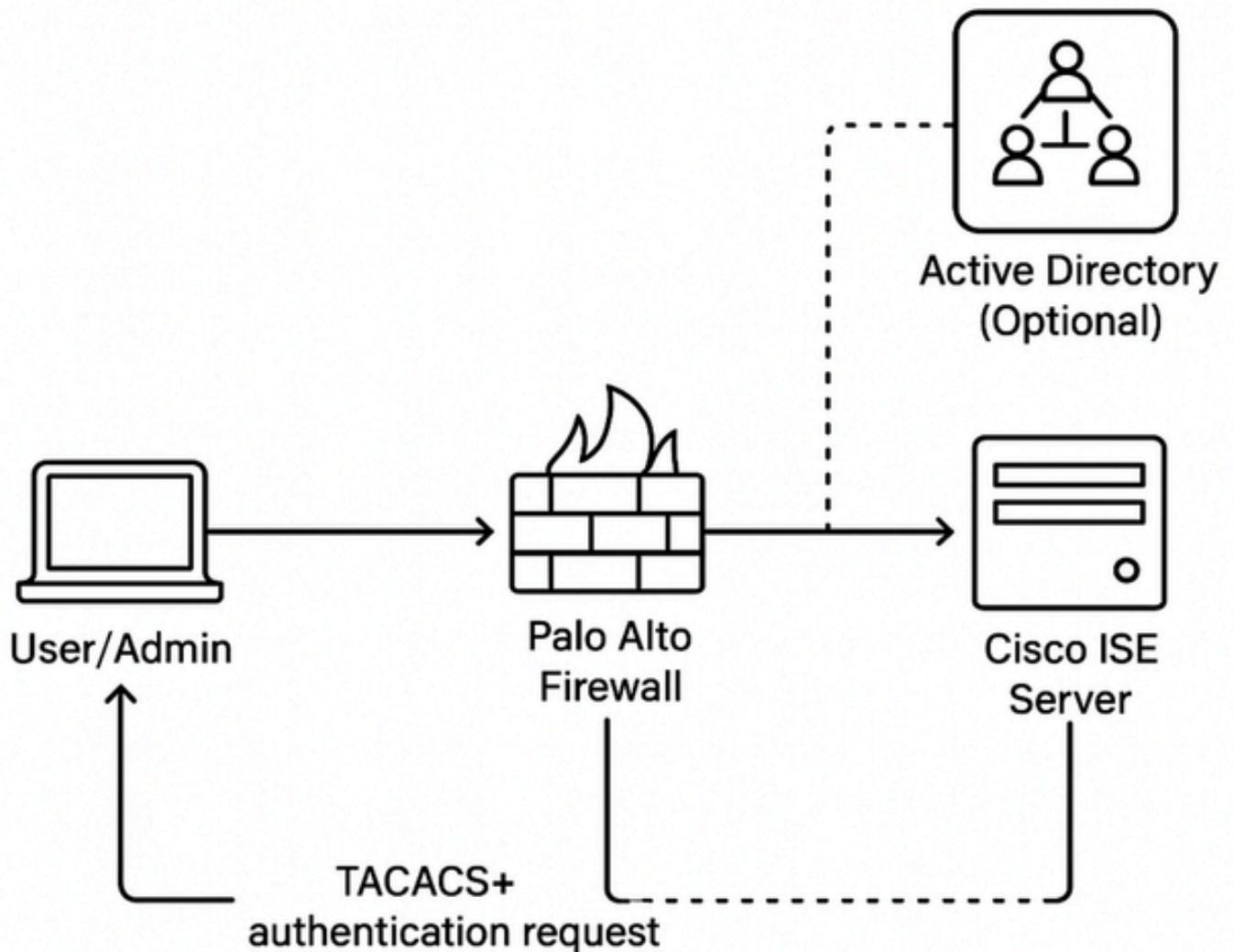
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esempio di rete



Flusso di autenticazione

1. L'amministratore accede al firewall di Palo Alto.
2. Palo Alto invia una richiesta di autenticazione TACACS+ a Cisco ISE.
3. Cisco ISE:
 - Se è integrato, AD viene interrogato per l'autenticazione e l'autorizzazione.
 - In assenza di Active Directory, vengono utilizzati gli archivi identità o i criteri locali.
 - Cisco ISE invia a Palo Alto una risposta di autorizzazione basata sulle policy configurate.
 - L'amministratore ottiene l'accesso con il livello di privilegi appropriato.

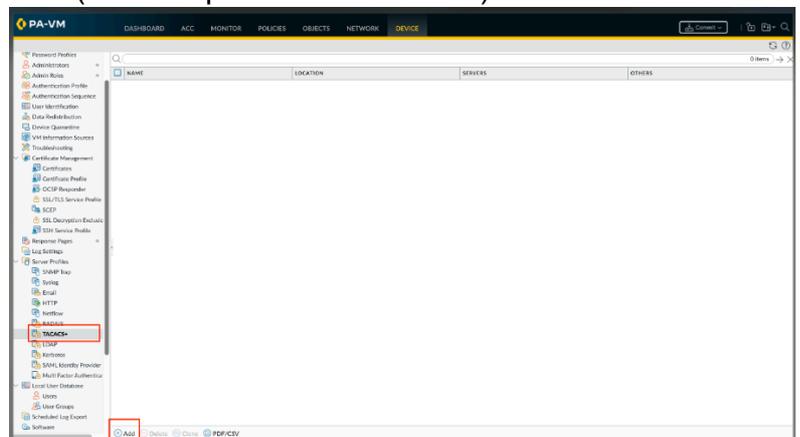
Configurazione

Sezione 1: configurazione di Palo Alto Firewall per TACACS+

Passaggio 1. Aggiungere un profilo server TACACS+.

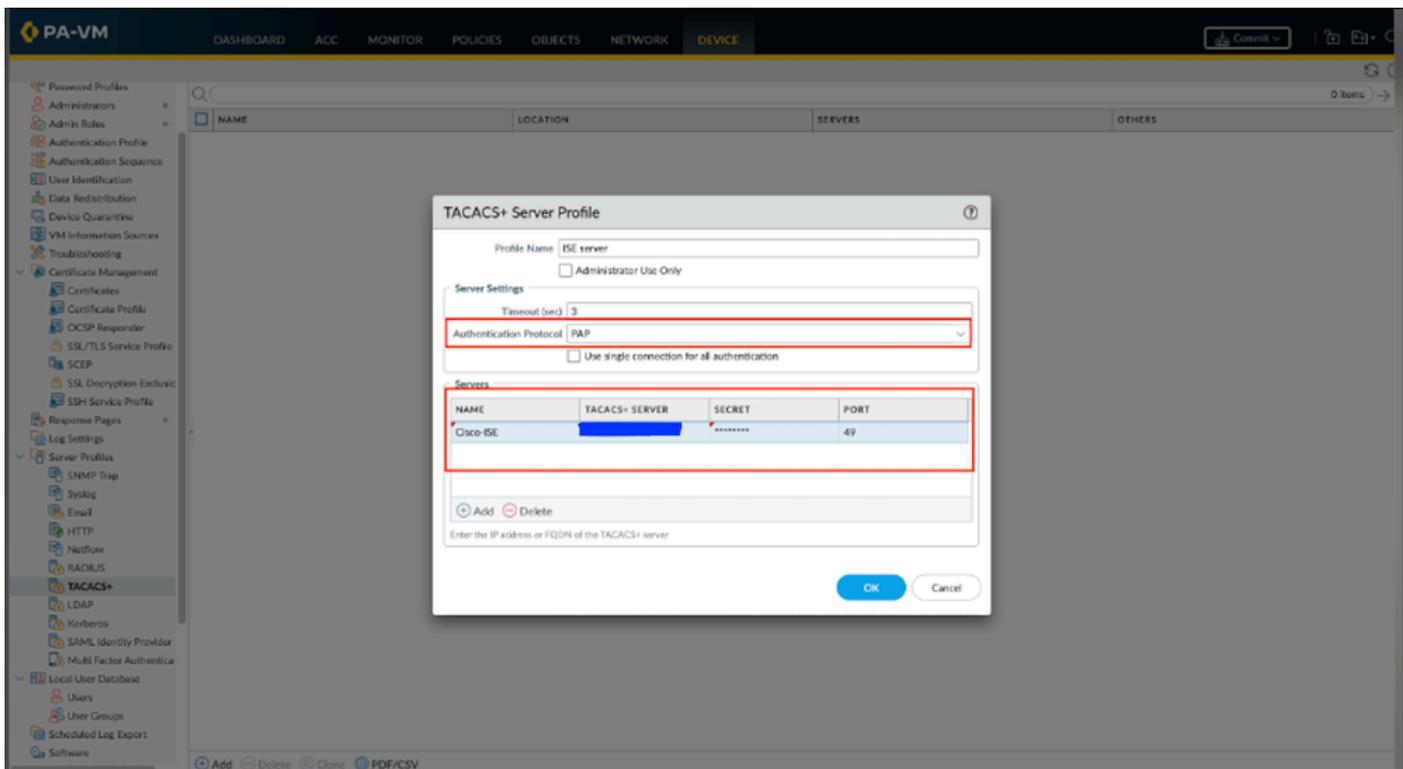
Il profilo definisce il modo in cui il firewall si connette al server TACACS+.

1. Selezionare Periferica > Profili server > TACACS+ o Panorama > Profili server > TACACS+ su Panorama e Aggiungere un profilo.
2. Immettere un Nome profilo per identificare il profilo del server.
3. (Facoltativo) Selezionare Solo uso amministratore per limitare l'accesso agli amministratori.
4. Immettere un intervallo di timeout in secondi dopo il quale si verifica il timeout di una richiesta di autenticazione (il valore predefinito è 3; intervallo compreso tra 1 e 20).
5. Selezionare il protocollo di autenticazione (il valore predefinito è CHAP) che il firewall utilizza



per autenticarsi sul server TACACS+.

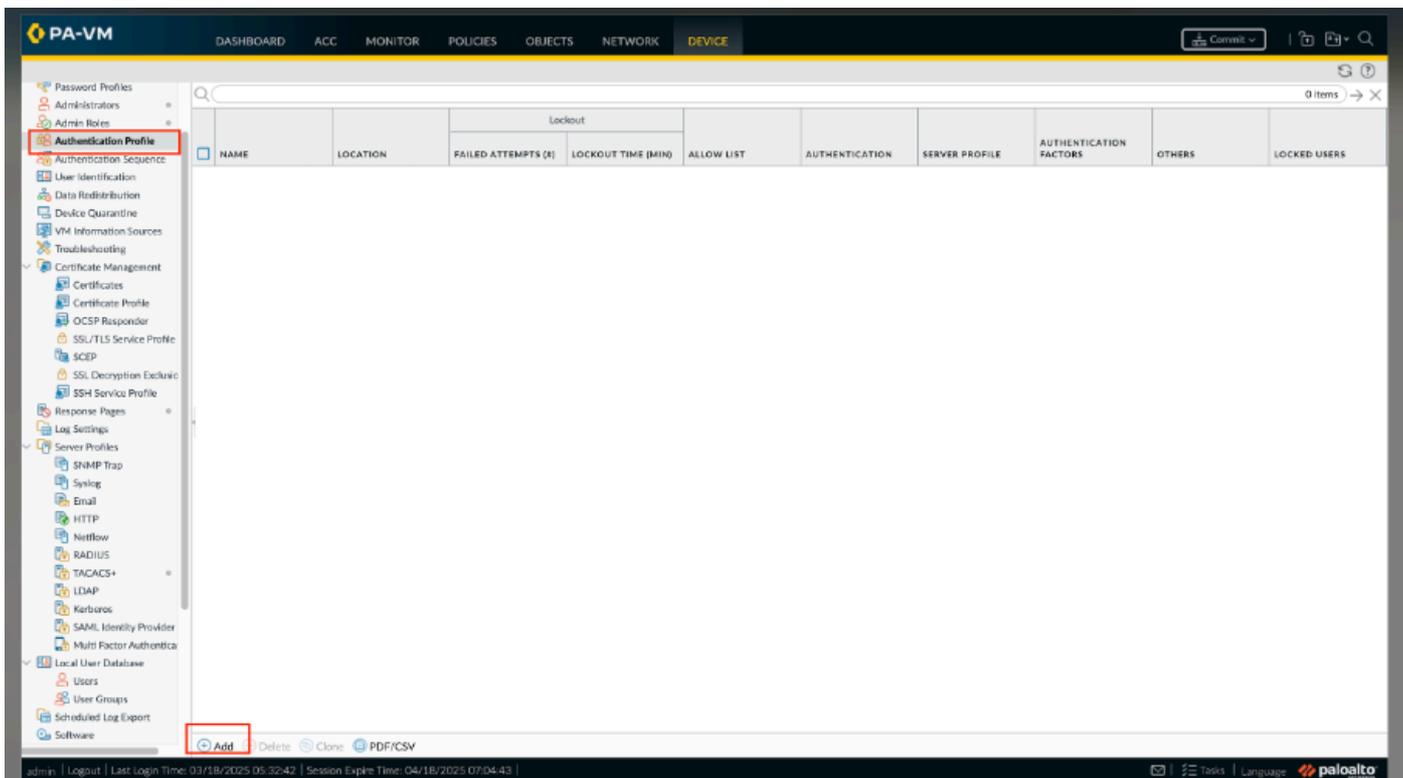
6. Aggiungere ciascun server TACACS+ ed eseguire i seguenti passaggi:
 1. Nome che identifica il server.
 2. Indirizzo IP o FQDN del server TACACS+. Se si utilizza un oggetto indirizzo FQDN per identificare il server e successivamente si modifica l'indirizzo, è necessario eseguire il commit della modifica affinché il nuovo indirizzo del server abbia effetto.
 3. Le opzioni Segreto e Conferma segreto consentono di crittografare nomi utente e password.
 4. La porta del server per le richieste di autenticazione (il valore predefinito è 49). Fare clic su OK per salvare il profilo del server.
7. Fare clic su OK per salvare il profilo del server.



Passaggio 2. Assegnare il profilo del server TACACS+ a un profilo di autenticazione.

Il profilo di autenticazione definisce le impostazioni di autenticazione comuni a un insieme di utenti.

1. Selezionare Periferica > Profilo di autenticazione e Aggiungi profilo.
 1. Immettere un nome per identificare il profilo
 2. Impostare Type su TACACS+.
 3. Selezionare il profilo del server configurato.
 4. Selezionare Recupera gruppo di utenti da TACACS+ per raccogliere le informazioni sui gruppi di utenti dalle VSA definite sul server TACACS+.



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

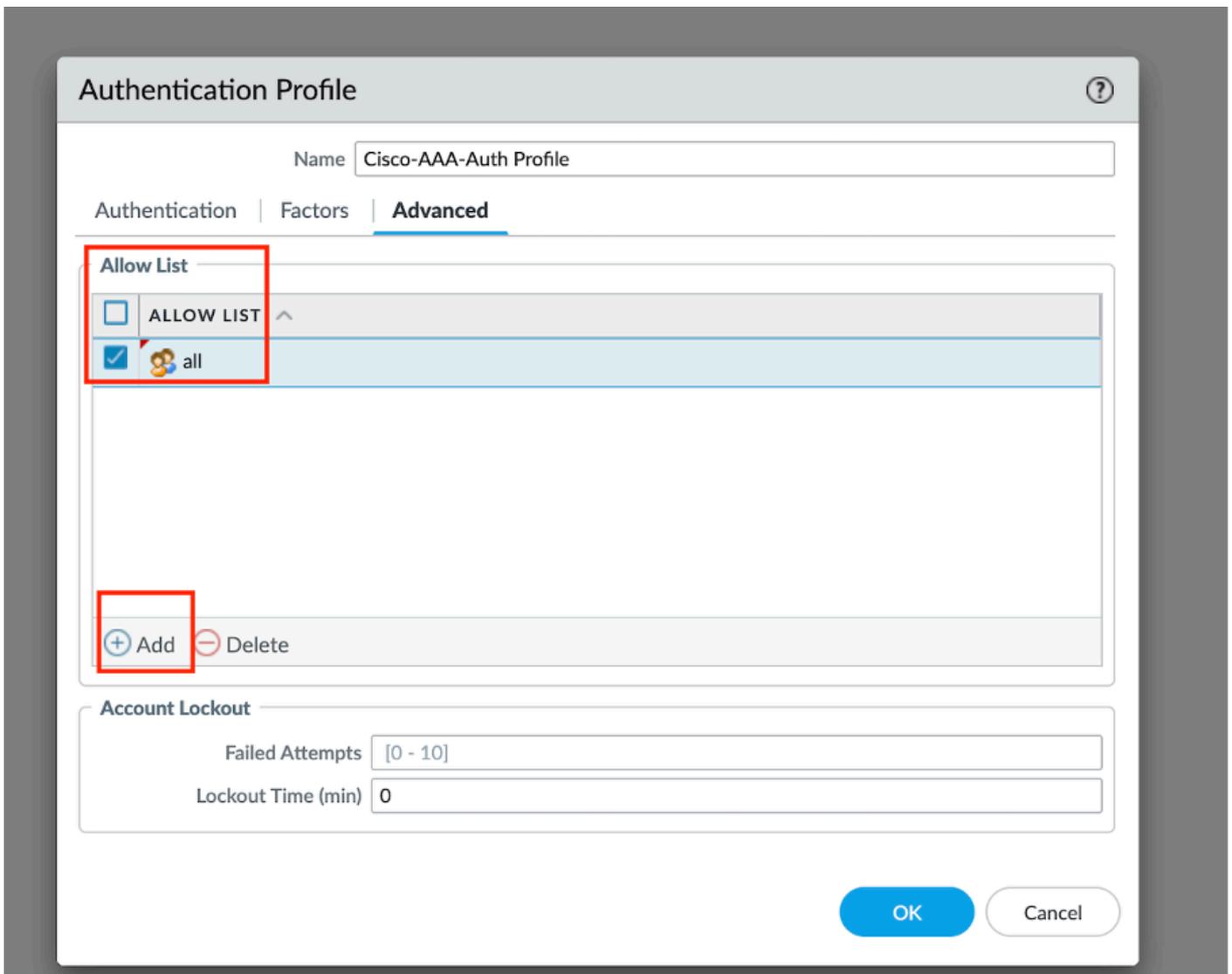
Kerberos Realm:

Kerberos Keytab: [X Import](#)

OK Cancel

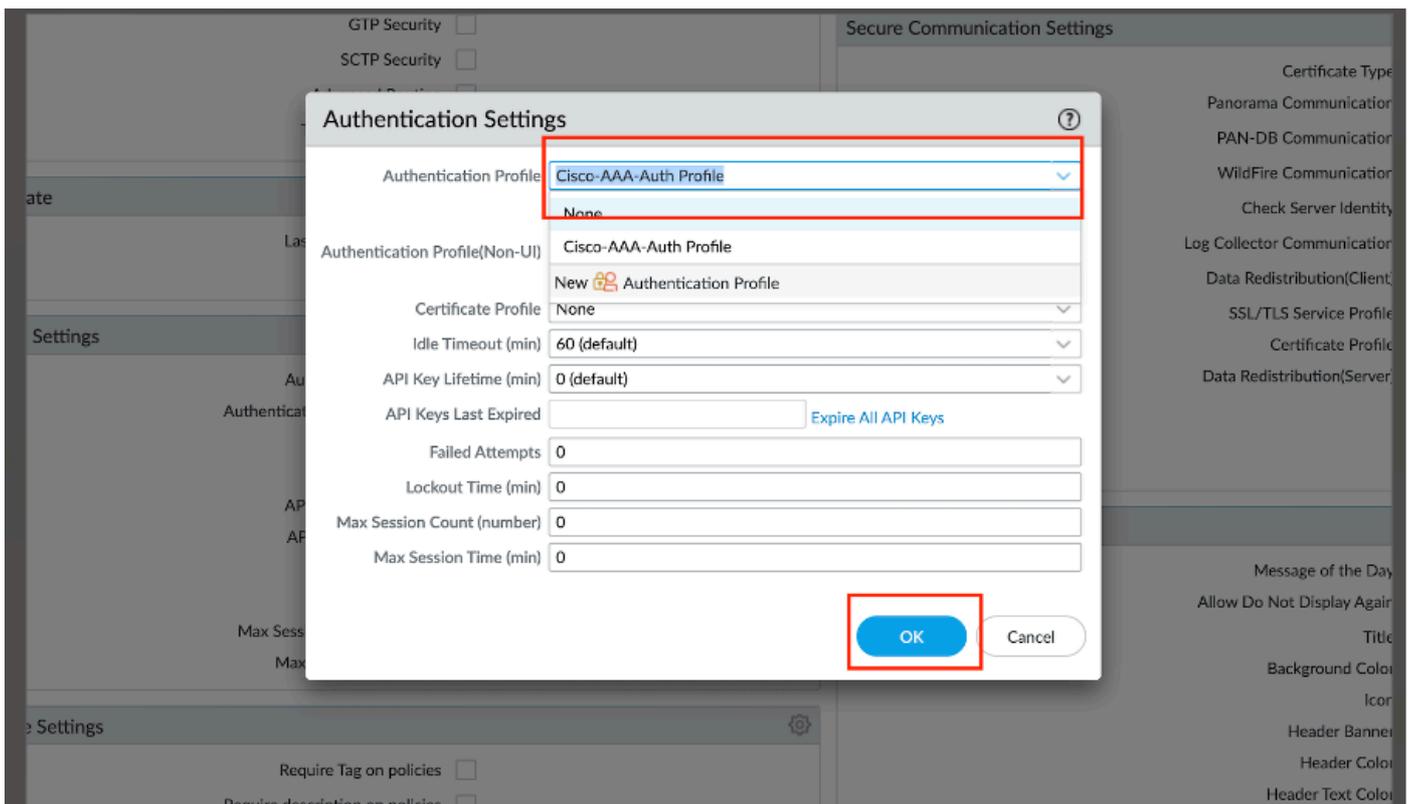
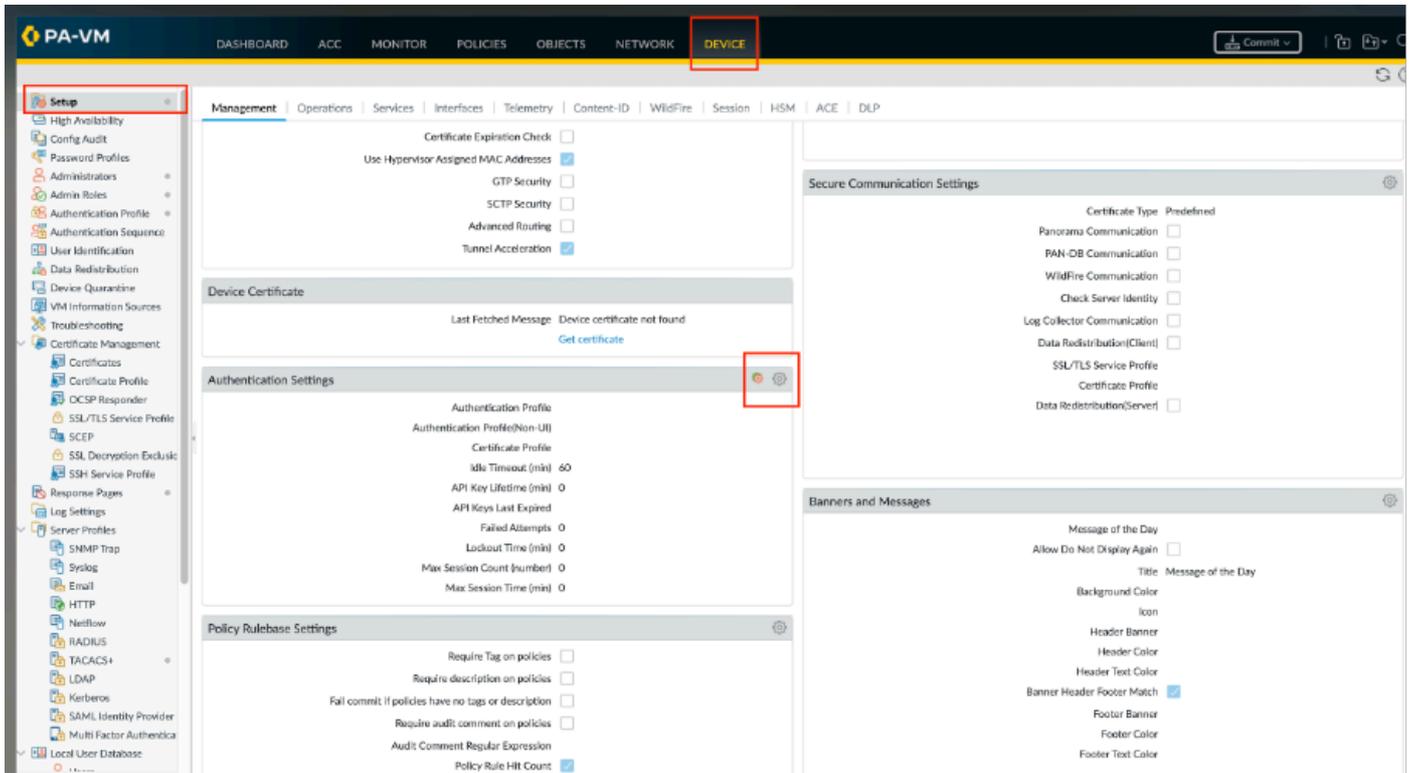
Il firewall corrisponde alle informazioni sui gruppi utilizzando i gruppi specificati nell'elenco Consenti del profilo di autenticazione.

1. Selezionare Avanzate e nell'elenco Consenti Aggiungere gli utenti e i gruppi che possono eseguire l'autenticazione con questo profilo di autenticazione.
2. Fare clic su OK per salvare il profilo di autenticazione.



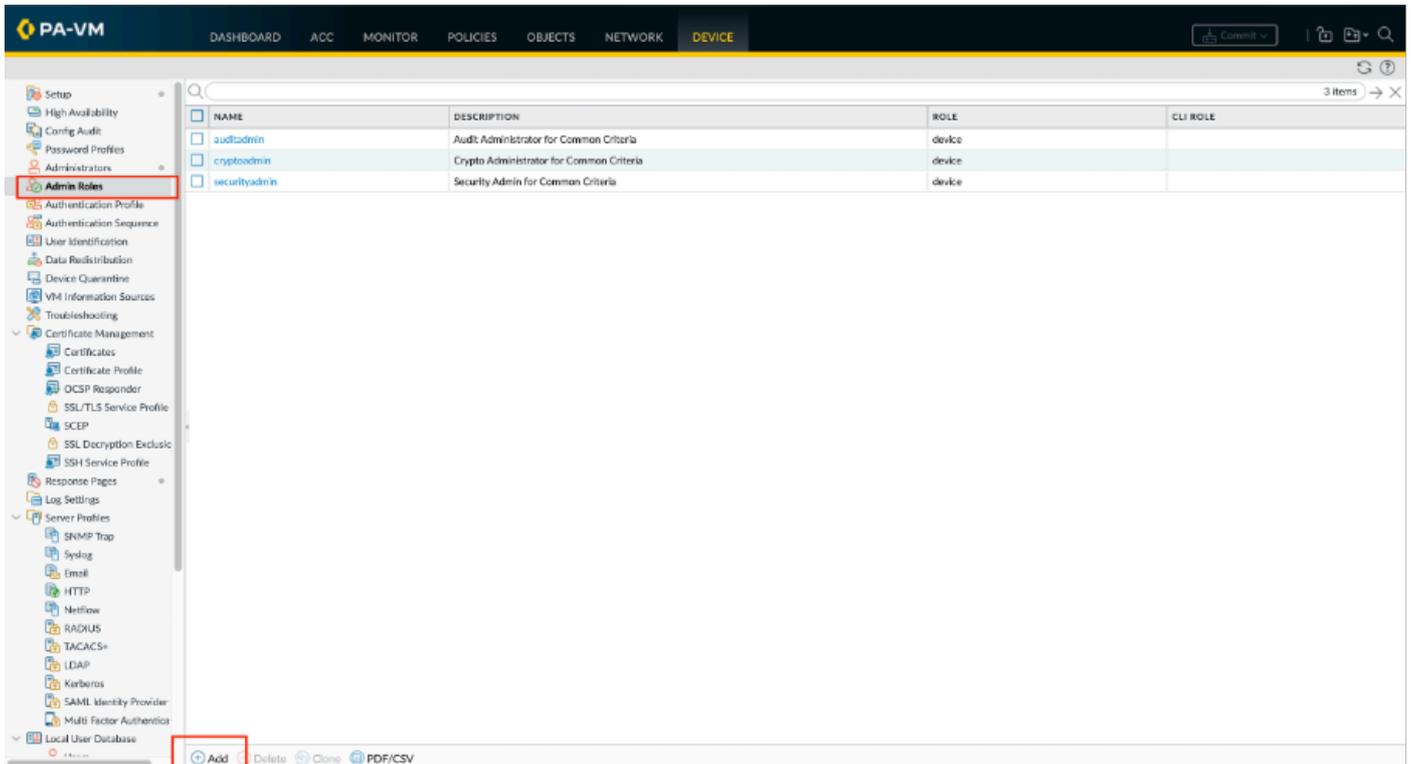
Passaggio 3. Configurare il firewall in modo che utilizzi il profilo di autenticazione per tutti gli amministratori.

1. Selezionare Periferica > Impostazione > Gestione e modificare le impostazioni di autenticazione.
2. Selezionare il profilo di autenticazione configurato e fare clic su OK.

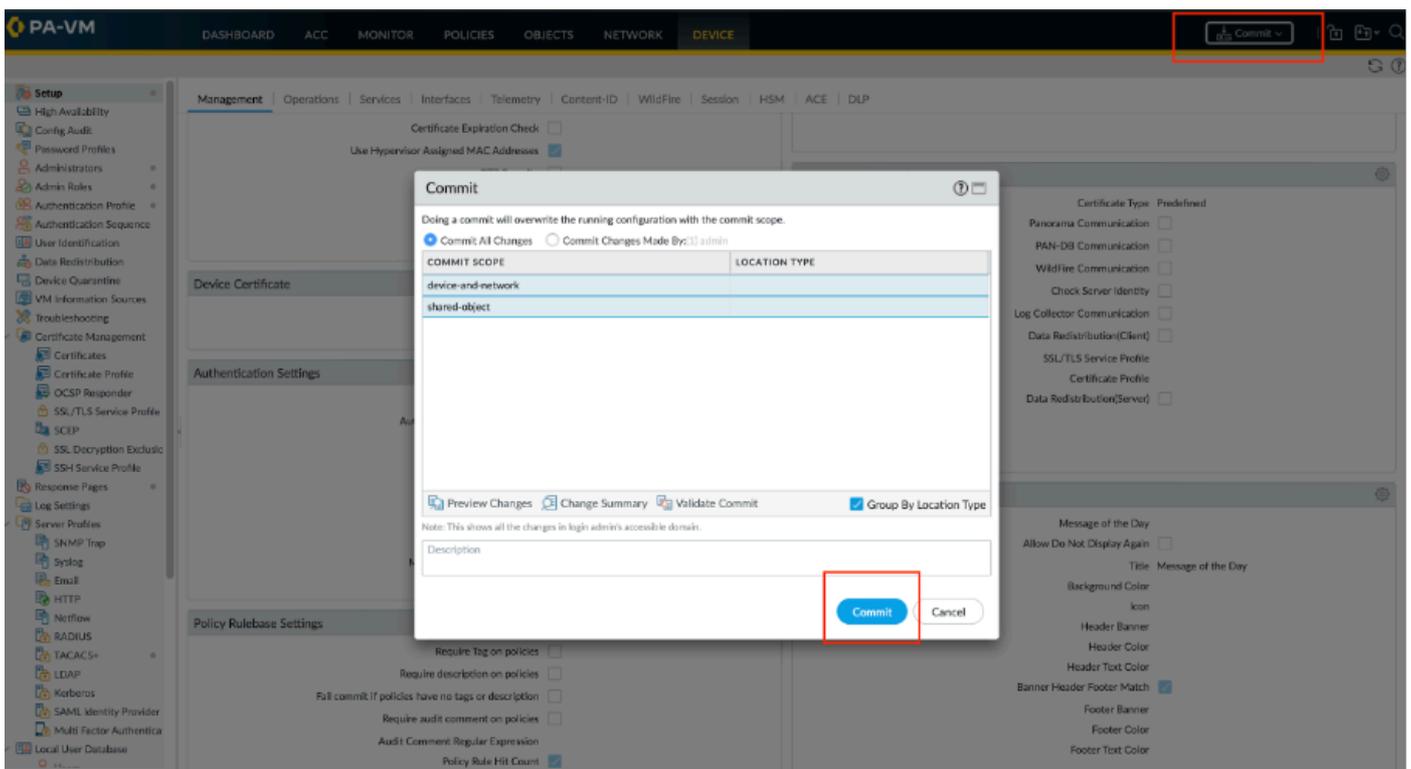


Passaggio 4. Configurare un profilo del ruolo di amministratore.

Selezionare Periferica > Ruoli amministrativi e fare clic su Aggiungi. Immettere un nome per identificare il ruolo.



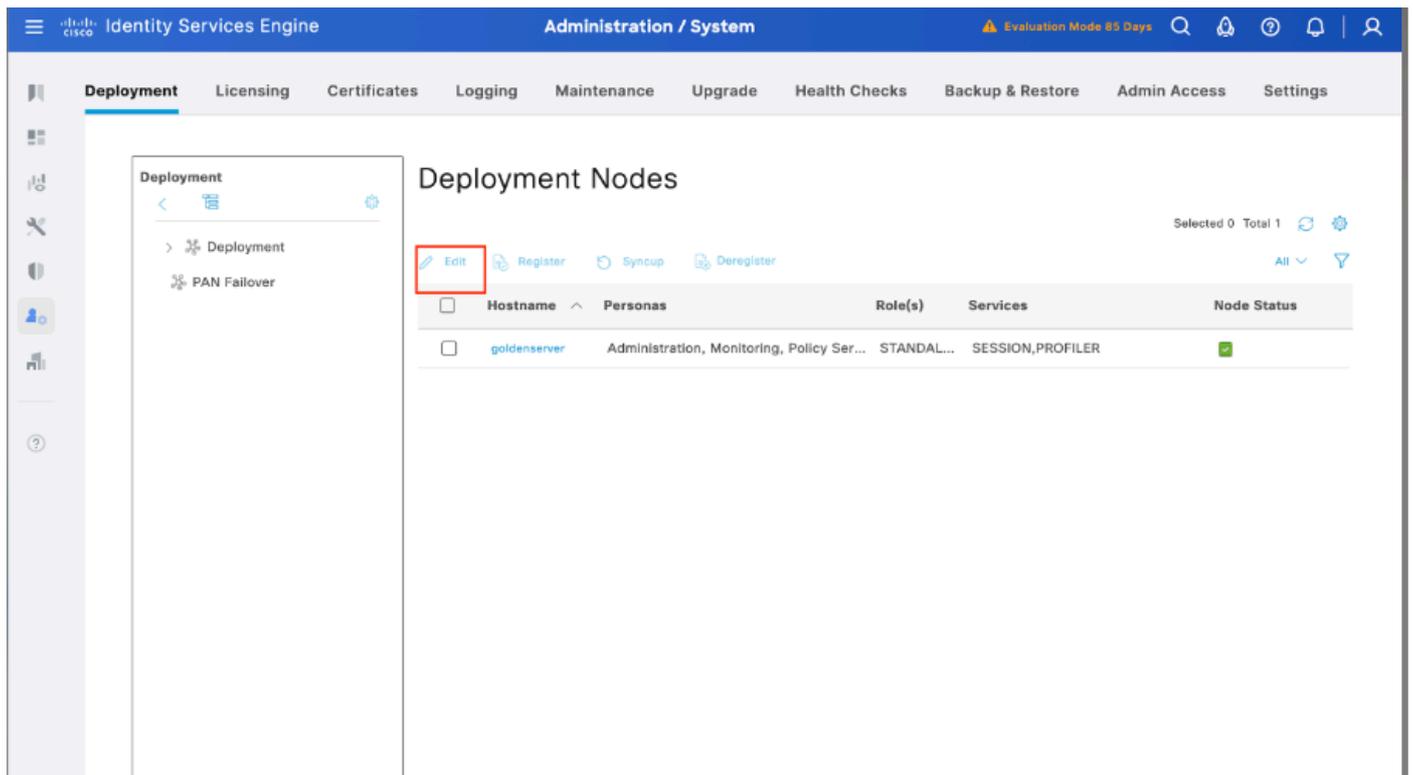
Passaggio 5. Eseguire il commit delle modifiche per attivarle sul firewall.



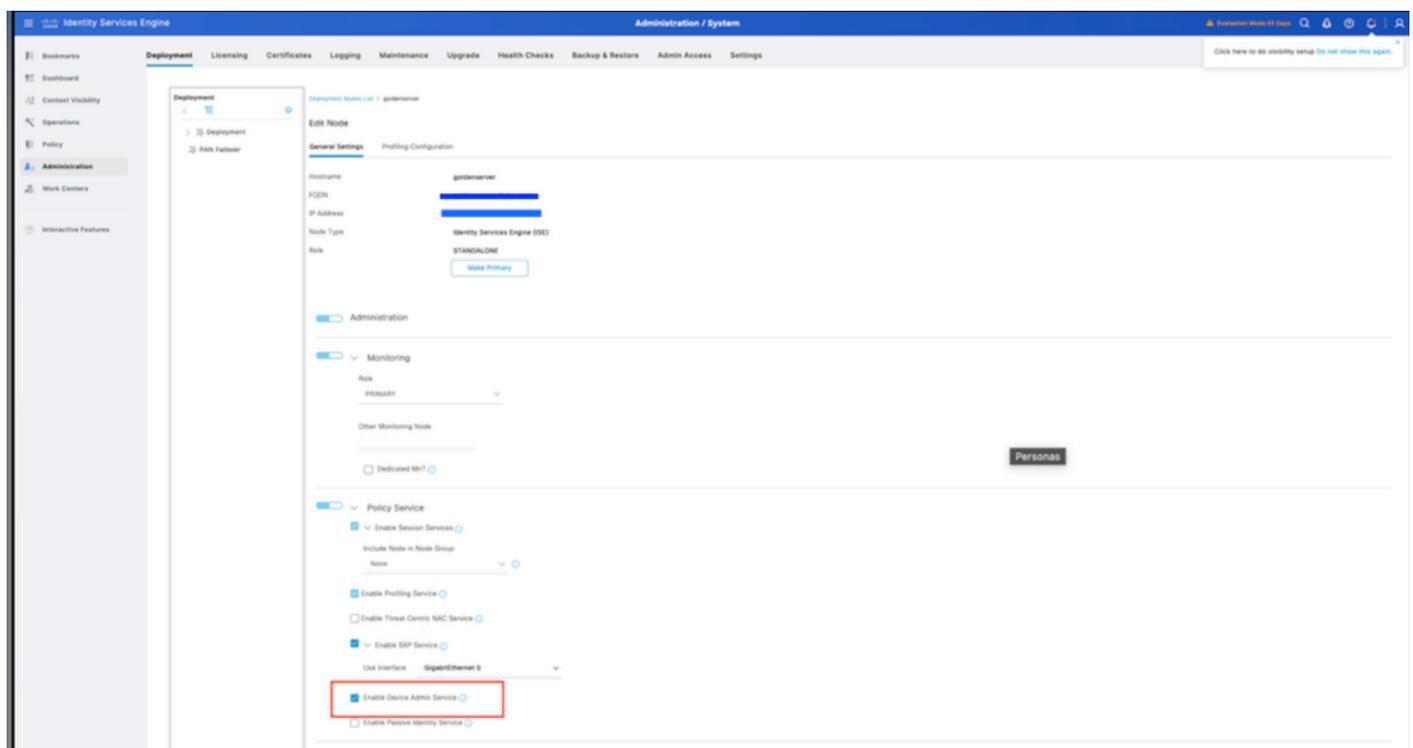
Sezione 2: Configurazione TACACS+ su ISE

Passaggio 1. Il passaggio iniziale consiste nel verificare se Cisco ISE dispone delle funzionalità necessarie per gestire l'autenticazione TACACS+. A tale scopo, verificare che nel nodo PSN (Policy Service Node) desiderato sia attivata la funzionalità Servizio amministrazione dispositivi. Selezionare Amministrazione > Sistema > Distribuzione, selezionare il nodo appropriato in cui ISE

elabora l'autenticazione TACACS+ e fare clic su Modifica per rivedere la configurazione.

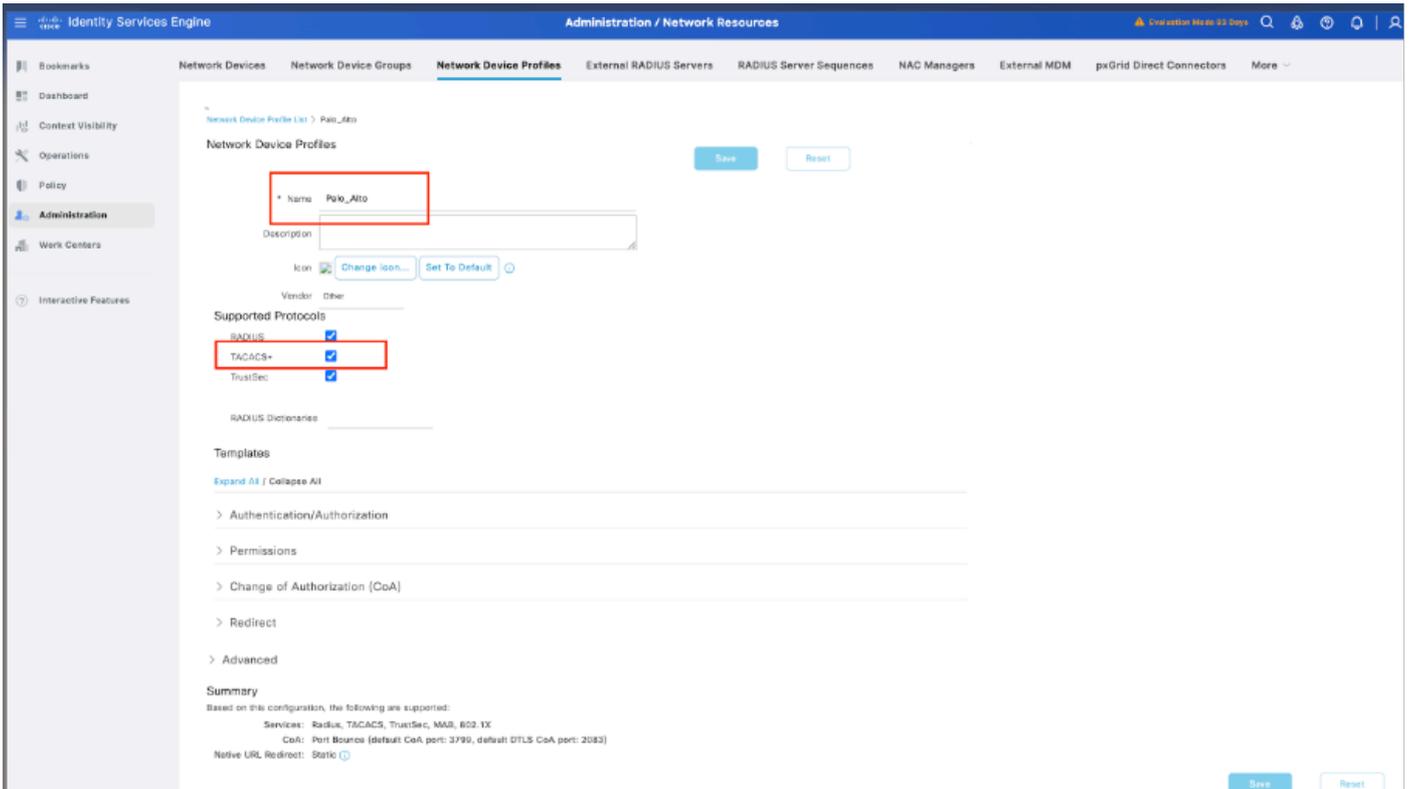


Passaggio 2. Scorrere verso il basso per individuare la funzionalità Servizio di amministrazione del dispositivo. Notare che l'abilitazione di questa funzionalità richiede che la persona del servizio criteri sia attiva sul nodo, insieme alle licenze TACACS+ disponibili nella distribuzione. Selezionare la casella di controllo per abilitare la funzionalità, quindi salvare la configurazione.



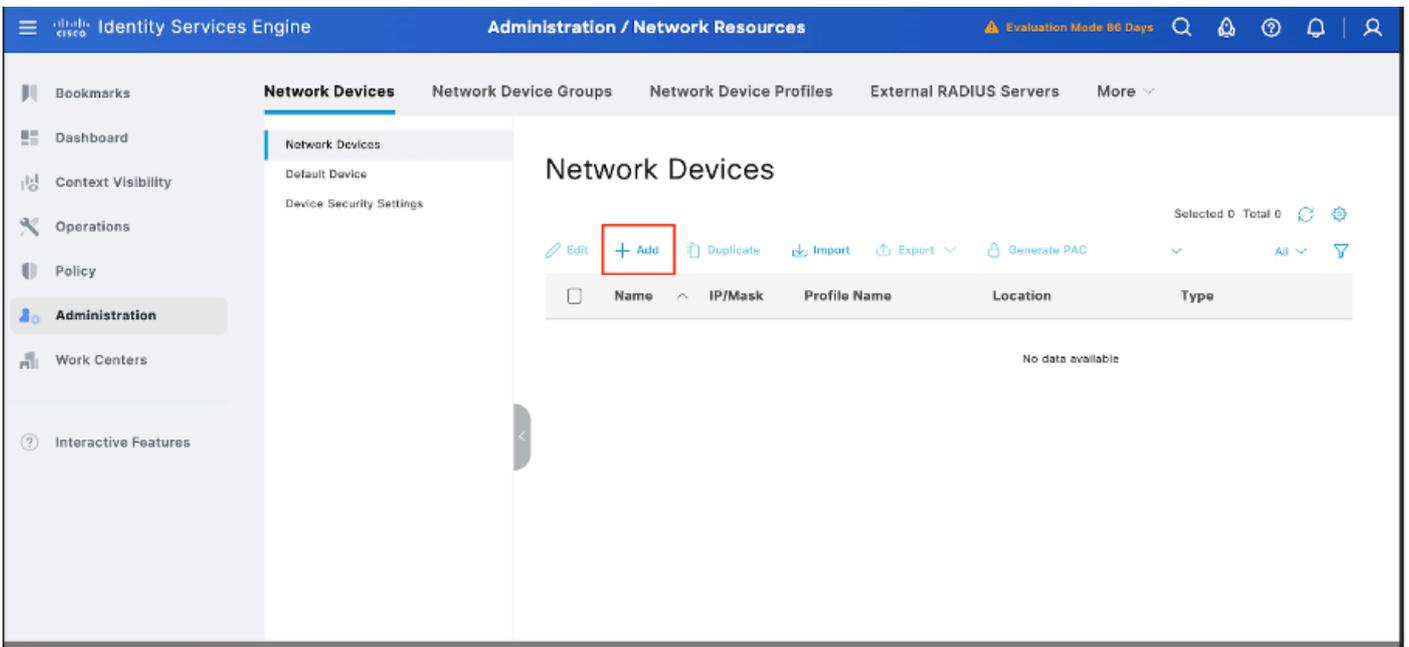
Passaggio 3. Configurare Palo Alto Network Device Profile per Cisco ISE.

Selezionare Amministrazione > Risorse di rete > Profilo dispositivo di rete. Fare clic su Add (Aggiungi) e specificare il nome (Palo Alto) e abilitare TACACS+ nei protocolli supportati.



Passaggio 4. Aggiungere Palo Alto come dispositivo di rete.

1. Selezionare Amministrazione > Risorse di rete > Dispositivi di rete > +Aggiungi.



2. Fare clic su Add (Aggiungi) e inserire i seguenti dettagli:

Nome: Palo-Alto

Indirizzo IP: <IP di Palo-Alto>

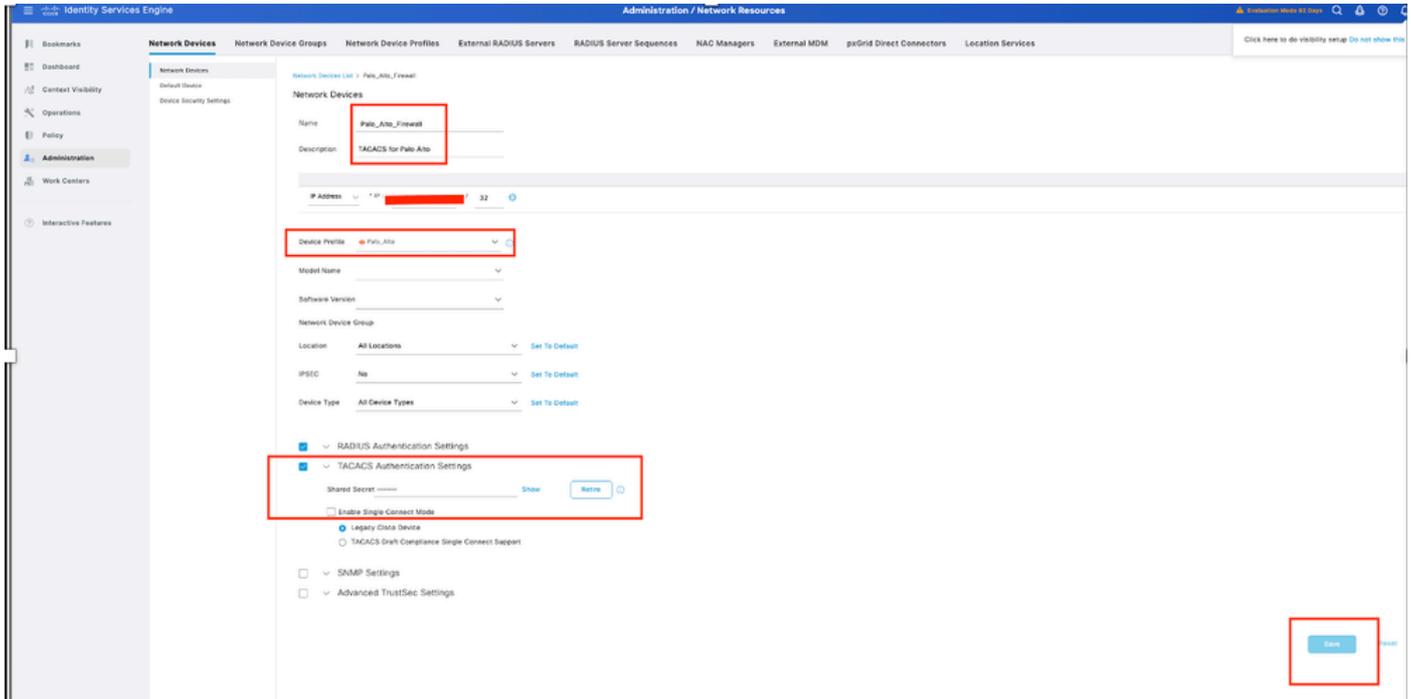
Profilo dispositivo di rete: selezionare Palo Alto

Impostazioni autenticazione TACACS:

Abilita autenticazione TACACS+

Immettere il segreto condiviso (deve corrispondere alla configurazione di Palo Alto)

Fare clic su Save (Salva).



Passaggio 5. Creazione dei gruppi di identità degli utenti.

Passare a Centri di lavoro > Amministrazione dispositivi > Gruppi di identità utente, quindi fare clic su Aggiungi e specificare il nome del gruppo di utenti.

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 EQ

- 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 Name
<input type="checkbox"/> Enabled		divz	

Identity Services Engine Work Centers / Device Administration Evaluation Mode 84 Days

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

Users

Network Access User > divz@net

* Username **divz@net**

Status **Enabled**

Account Name Size

Email

Passwords

Password Type: Internal Users

Password Linting: With Capital Never Expires

* Login Password: **** Re-Enter Password: ****

Enable Password:

User Information

First Name:

Last Name:

Account Options

Description:

Change password on next sign:

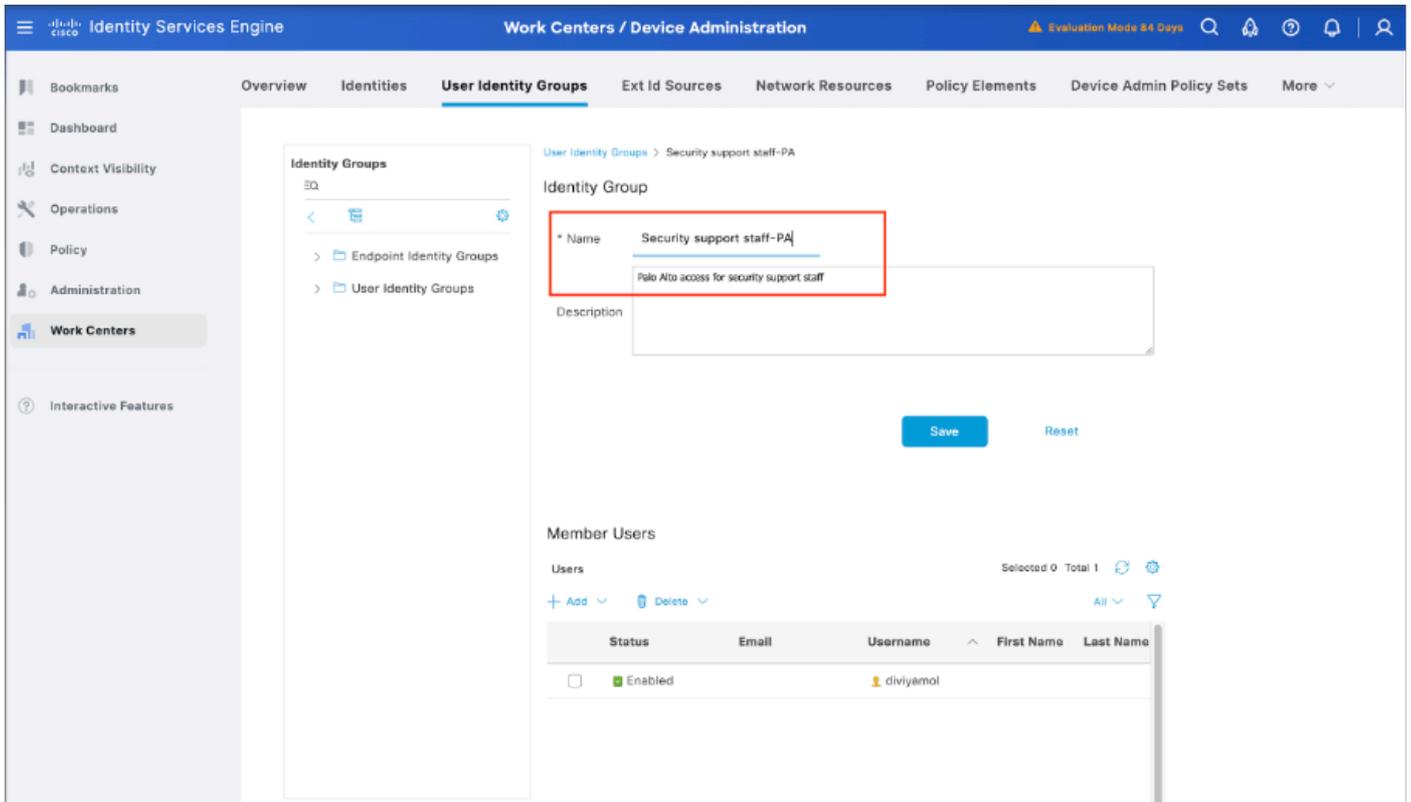
Account Disable Policy

Enable account if date exceeds: 2023-03-19 0000-00-00

User Groups

Security support idMP PA

Save Reset



Passaggio 6. Configurare Un Profilo TACACS.

La fase successiva è la configurazione di un profilo TACACS, che consente di configurare impostazioni quali il livello di privilegio e le impostazioni di timeout. Selezionare Work Center > Device Administration > Policy Elements > Results > TACACS Profiles (Centri di lavoro > Amministrazione dispositivi > Elementi criteri > Risultati > Profili TACACS).

Fare clic su Add per creare un nuovo profilo TACACS. Assegnare un nome valido al profilo.

The screenshot shows the 'Policy Elements' configuration page in Identity Services Engine. The breadcrumb trail is 'TACACS Profiles > New TACACS Profile'. The profile name is 'PaloAlto_Security_Support'. Under 'Common Tasks', 'Default Privilege' is set to 0 and 'Maximum Privilege' is set to 15. The 'Custom Attributes' table is empty. A 'Mandatory' attribute is being added with the name 'PaloAlto_Admin_Role' and the value 'Support'. The 'Save' button is highlighted.

The screenshot shows the configuration page for a TACACS Profile named 'PaloAlto_Engineers_Profile'. The profile name is 'PaloAlto_Engineers_Profile'. Under 'Common Tasks', 'Default Privilege' is set to 0 and 'Maximum Privilege' is set to 15. The 'Custom Attributes' table is empty. A 'Mandatory' attribute is being added with the name 'PaloAlto_Admin_Roles' and the value 'securtyadm'. The 'Save' button is highlighted.

Passaggio 6. Configurare i set di comandi TACACS.

A questo punto è possibile configurare i comandi che gli utenti possono utilizzare. Poiché è

possibile concedere a entrambi questi casi il livello di privilegio 15, che consente l'accesso a tutti i comandi disponibili, utilizzare i set di comandi TACACS per limitare i comandi da utilizzare.

Selezionare Work Center > Device Administration > Policy Elements > Results > TACACS Command Sets (Centri di lavoro > Amministrazione dispositivi > Elementi criteri > Risultati > Set di comandi TACACS). Fare clic su Add per creare un nuovo set di comandi TACACS e assegnargli il nome PermitAllCommands. Applicare questo set di comandi TACACS per il supporto della sicurezza.

L'unica cosa che è necessario configurare in questo set di comandi TACACS è selezionare la casella di controllo Permit qualsiasi comando non elencato di seguito.

The screenshot displays the Cisco Identity Services Engine (ISE) interface for configuring a TACACS Command Set. The breadcrumb navigation path is: Work Centers / Device Administration > Policy Elements > Results > TACACS Command Sets. The 'Name' field is set to 'PermitAllCommands'. The 'Commands' section has the checkbox 'Permit any command that is not listed below' checked. The 'Save' button is highlighted.

Identity Services Engine Work Centers / Device Administration Evaluation Mode 82 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

Click here to do visibility setup Do not show this again.

Conditions > TACACS Command Sets > PermitAllCommands
Command Set

Network Conditions >

Results > Name: PermitAllCommands

Allowed Protocols

TACACS Command Sets Description

Commands

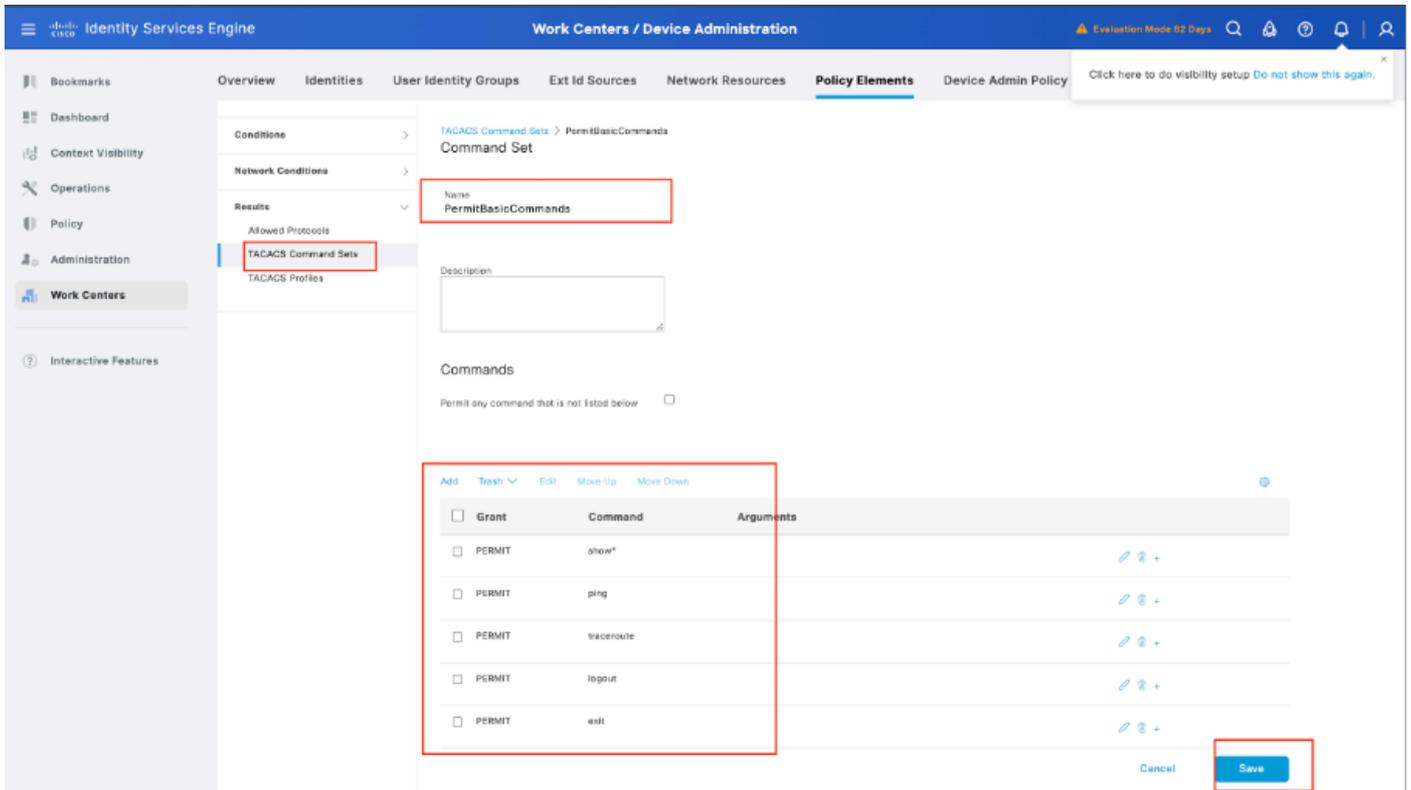
Permit any command that is not listed below

Add Trash Edit Move Up Move Down

Grant	Command	Arguments
<input type="checkbox"/>		

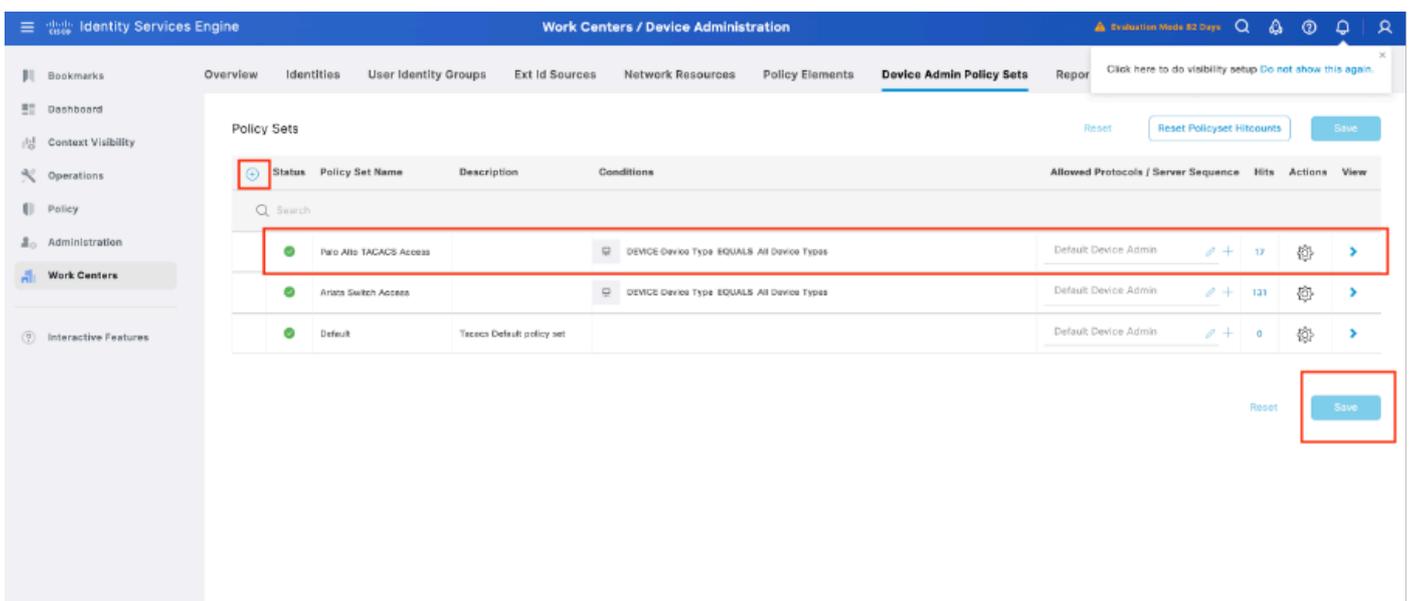
No data found.

Cancel Save



Passaggio 7. Creare un set di criteri di amministrazione dei dispositivi da utilizzare per Palo Alto, Navigare nel menu Centri di lavoro > Amministrazione dispositivi > Set di criteri di amministrazione dei dispositivi, Fare clic sull'icona Aggiungi +.

Passaggio 8. Assegnare un nome al nuovo set di criteri, aggiungere le condizioni in base alle caratteristiche delle autenticazioni TACACS+ in corso dal firewall di Palo Alto e selezionare Protocolli autorizzati > Amministratore di dispositivo predefinito. Salvare la configurazione.



Passaggio 9. Selezionare nell'opzione > view, quindi nella sezione Authentication Policy (Criteri di autenticazione) selezionare l'origine identità esterna utilizzata da Cisco ISE per eseguire la query del nome utente e delle credenziali per l'autenticazione sul firewall di Palo Alto. Nell'esempio, le credenziali corrispondono a Internal Users memorizzato in ISE.

Identity Services Engine Work Centers / Device Administration

Policy Sets -> Palo Alto TACACS Access

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)

Status	Rule Name	Conditions	Use	Hits	Actions
●	PaloAlto_Authz Policy	Network Access-Device IP Address EQUALS [REDACTED]	Internal Users > Options	17	⚙️
●	Default		Internal Users > Options	0	⚙️

Authorization Policy - Local Exceptions
Authorization Policy - Global Exceptions
Authorization Policy(3)

Reset Save

Passaggio 10. Scorrere verso il basso fino alla sezione Criteri di autorizzazione fino al criterio Predefinito, selezionare l'icona dell'ingranaggio, quindi inserire una regola.

Identity Services Engine Work Centers / Device Administration

Policy Sets -> Palo Alto TACACS Access

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

Authorization Policy(3)

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

Reset Save

Passaggio 11. Assegnare un nome alla nuova regola di autorizzazione, aggiungere le condizioni relative all'utente già autenticato come appartenenza al gruppo e, nella sezione Profili shell, aggiungere il profilo TACACS configurato in precedenza e salvare la configurazione.

Verifica

Recensione ISE

Passaggio 1. Verificare che il servizio TACACS+ sia in esecuzione e che sia possibile archivarlo:

- GUI: Verificare se il nodo è elencato con il servizio DEVICE ADMIN in Amministrazione -> Sistema -> Distribuzione.
- CLI: Eseguire il comando show ports | includere 49 per confermare che la porta TCP contiene connessioni che appartengono a TACACS+

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

Passaggio 2. Confermare la presenza di log attivi relativi ai tentativi di autenticazione TACACS+: è possibile controllare questa condizione nel menu Operations (Operazioni) -> TACACS (TAC) -> Live logs (Registri attivi).

A seconda del motivo dell'errore, è possibile modificare la configurazione o risolvere la causa dell'errore.

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Devic...
Mar 22, 2025 06:54:38.8...	●	[REDACTED]	diviyamol	Authentic...	Palo Alto TACACS Access >> P...		goldenserver	Palo_Alto_Firewall
Mar 22, 2025 06:54:17.5...	●	[REDACTED]	diviyamol	Authentic...	Palo Alto TACACS Access >> P...		goldenserver	Palo_Alto_Firewall
Mar 22, 2025 06:49:42.0...	●	[REDACTED]	divi	Authorizat...		Palo Alto TADACS Access >> P...	goldenserver	Palo_Alto_Firewall
Mar 22, 2025 06:49:41.9...	●	[REDACTED]	divi	Authentic...	Palo Alto TACACS Access >> P...		goldenserver	Palo_Alto_Firewall
Mar 22, 2025 06:49:28.2...	●	[REDACTED]	diviyamol	Authorizat...		Palo Alto TADACS Access >> P...	goldenserver	Palo_Alto_Firewall
Mar 22, 2025 06:49:28.1...	●	[REDACTED]	diviyamol	Authentic...	Palo Alto TACACS Access >> P...		goldenserver	Palo_Alto_Firewall

Passaggio 3. Se non viene visualizzato alcun log in tempo reale, procedere con l'acquisizione di un pacchetto. Passare al menu Operazioni > Risoluzione dei problemi > Strumenti diagnostici > Strumenti generali > Dump TCP, selezionare Aggiungi.

Operations / Troubleshoot

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 Valid...
- Posture Troubleshooting
- Agentless Posture Troublesho...
- EndPoint Debug
- TCP Dump**
- Session Trace Tests

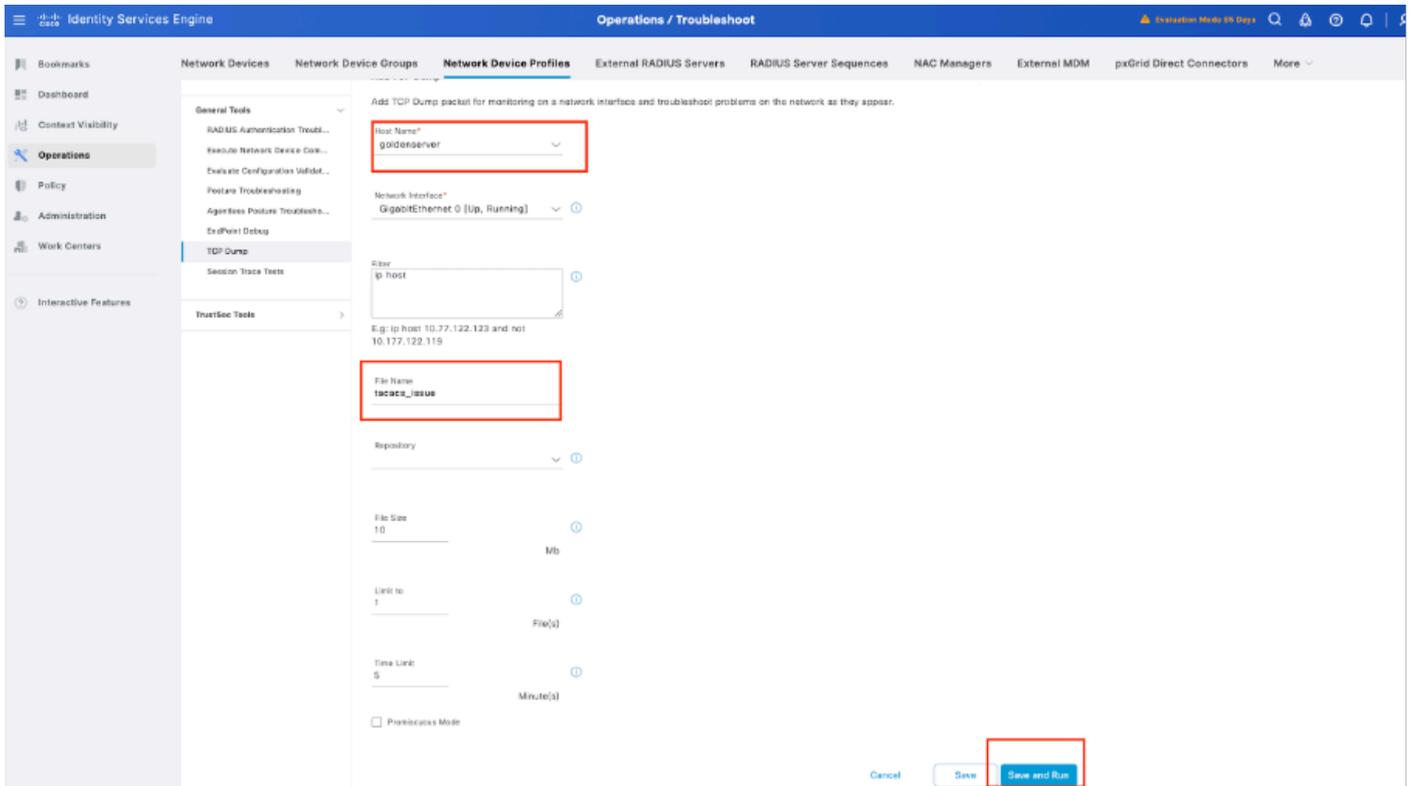
TCP Dump

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

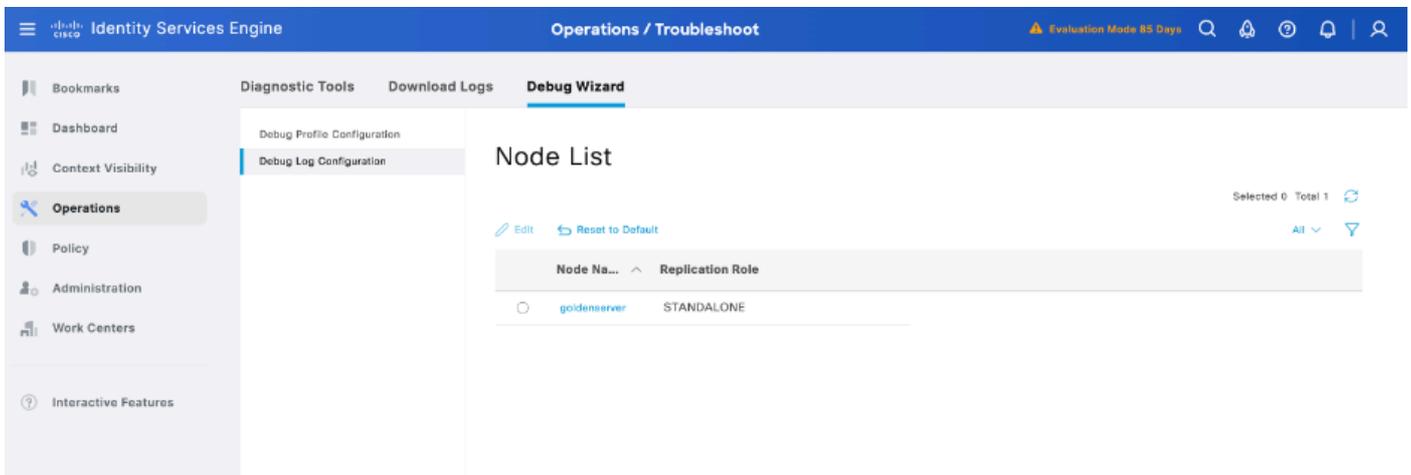
Row/Page 0 << 0 / 0 >> Go

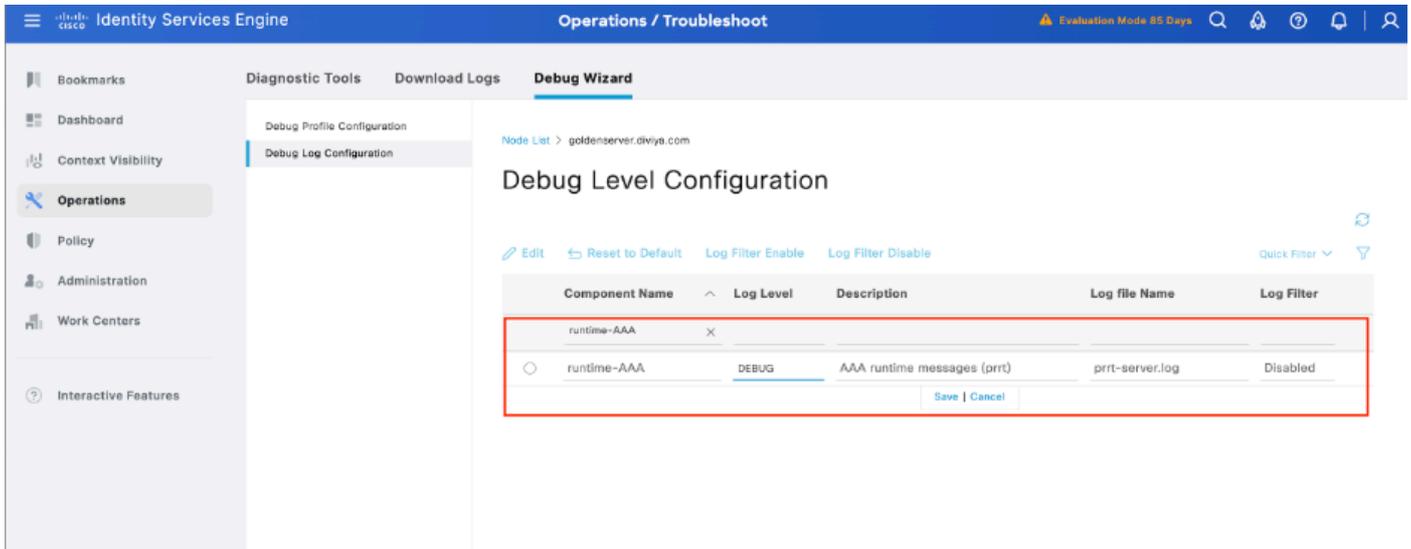
Add Edit Trash Start Stop Download

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



Passaggio 4. Abilitare il componente runtime-AAA nel debug all'interno del PSN da cui viene eseguita l'autenticazione in Operazioni > Risoluzione dei problemi > Procedura guidata debug > Configurazione del log di debug, selezionare il nodo PSN, quindi selezionare avanti nel pulsante Modifica.





Identificare il componente runtime-AAA, impostarne il livello di log per eseguire il debug, riprodurre il problema e analizzare i log per ulteriori informazioni.

Risoluzione dei problemi

TACACS Pacchetto di richiesta TACACS+ non valido - Possibile mancata corrispondenza dei segreti condivisi

Problema

L'autenticazione TACACS+ tra Cisco ISE e il firewall di Palo Alto (o un dispositivo di rete) non riesce con il messaggio di errore:

"Pacchetto di richiesta TACACS+ non valido. Probabilmente i segreti condivisi non corrispondono"

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	

In questo modo si evitano tentativi di accesso di amministrazione riusciti e il controllo dell'accesso ai dispositivi può essere compromesso dall'autenticazione centralizzata.

Possibili cause

- Mancata corrispondenza nel segreto condiviso configurato su Cisco ISE e sul firewall o sul dispositivo di rete di Palo Alto.
- Configurazione errata del server TACACS+ sul dispositivo (ad esempio, indirizzo IP, porta o protocollo errato).

Soluzione

Per questo problema esistono diverse soluzioni possibili:

1. Verificare il segreto condiviso:

- Su Cisco ISE:
Passare a Amministrazione > Risorse di rete > Dispositivi di rete, selezionare il dispositivo interessato e confermare il segreto condiviso.
- Sul firewall di Palo Alto:
Selezionare Device > Server Profiles > TACACS+ (Dispositivo > Profili server > TACACS+) e verificare che il segreto condiviso corrisponda esattamente, includendo maiuscole e minuscole e caratteri speciali.

2. Controllare le impostazioni del server TACACS+:

- Verificare che l'indirizzo IP e la porta corretti (l'impostazione predefinita è 49) di Cisco ISE siano configurati nel profilo TACACS+ del firewall.
- Confermare che il tipo di protocollo è TACACS+ (non RADIUS).

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).