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

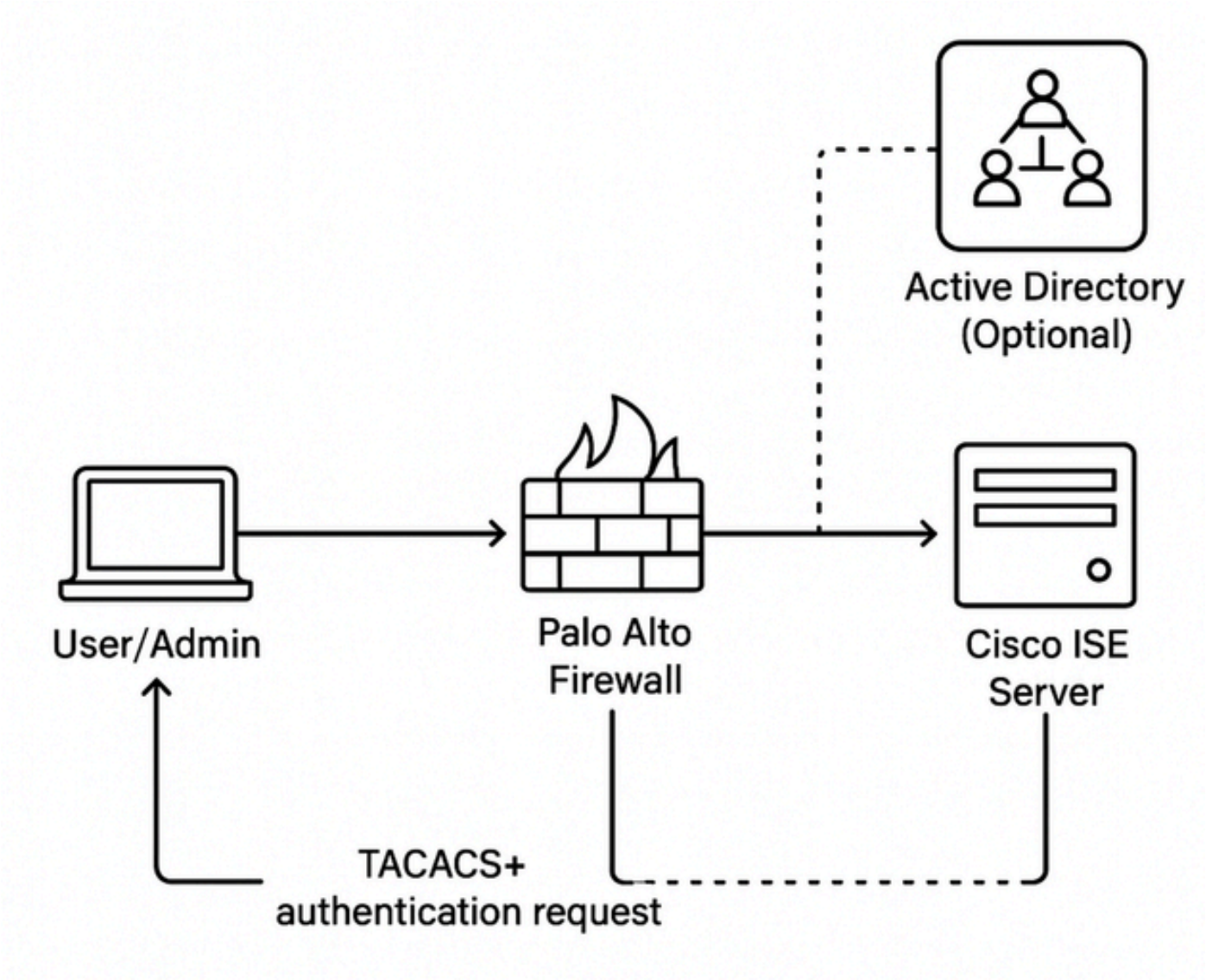
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- 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.

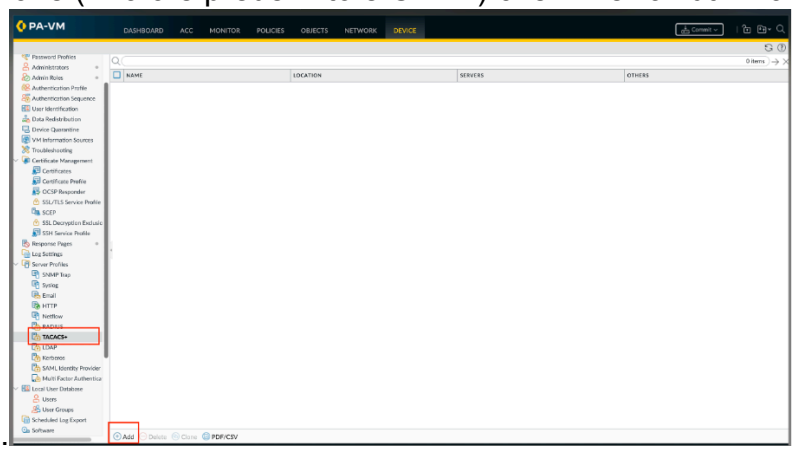
Configurazione

Sezione 1: configurazione di Palo Alto Firewall per TACACS+

Passaggio 1. Aggiungere un profilo server TACACS+.

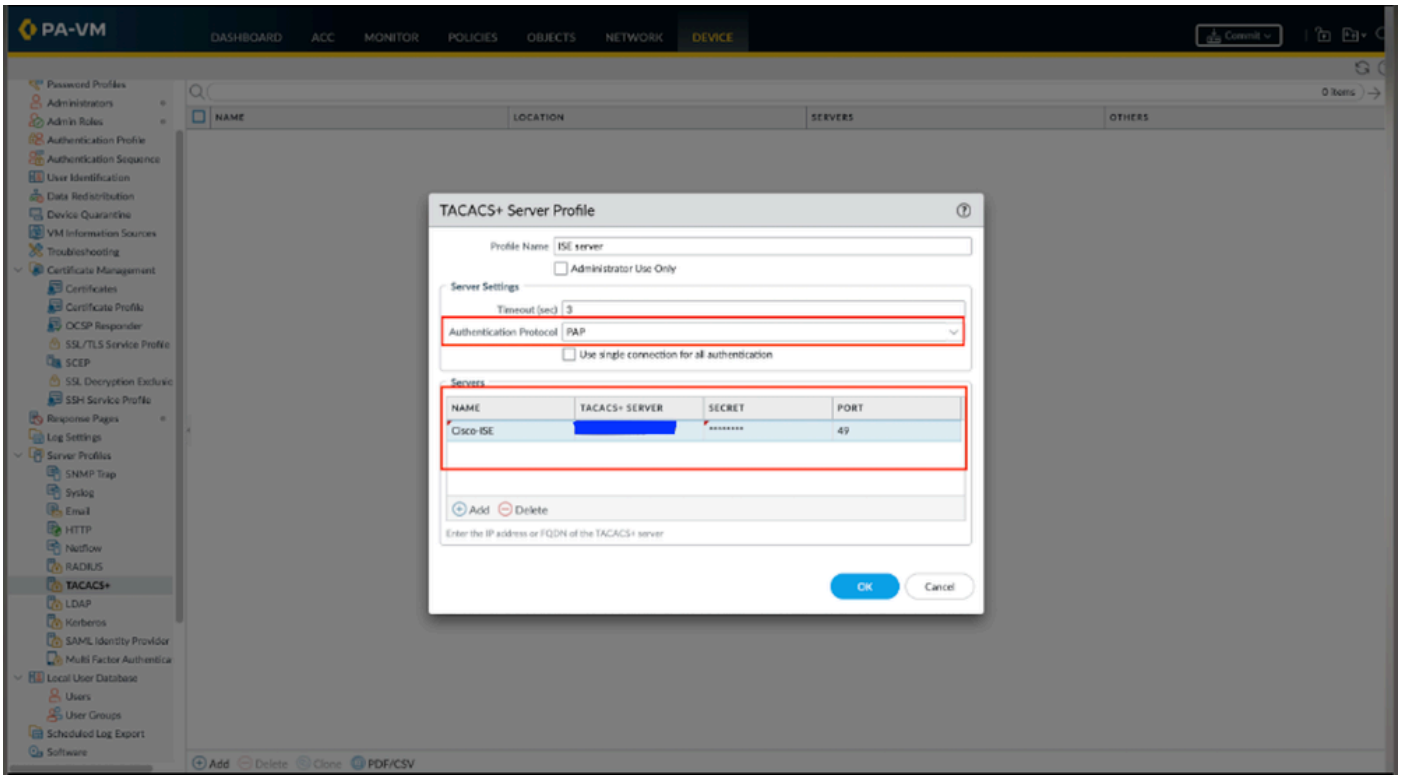
Il profilo definisce il modo in cui il firewall si connette al server TACACS+.

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.

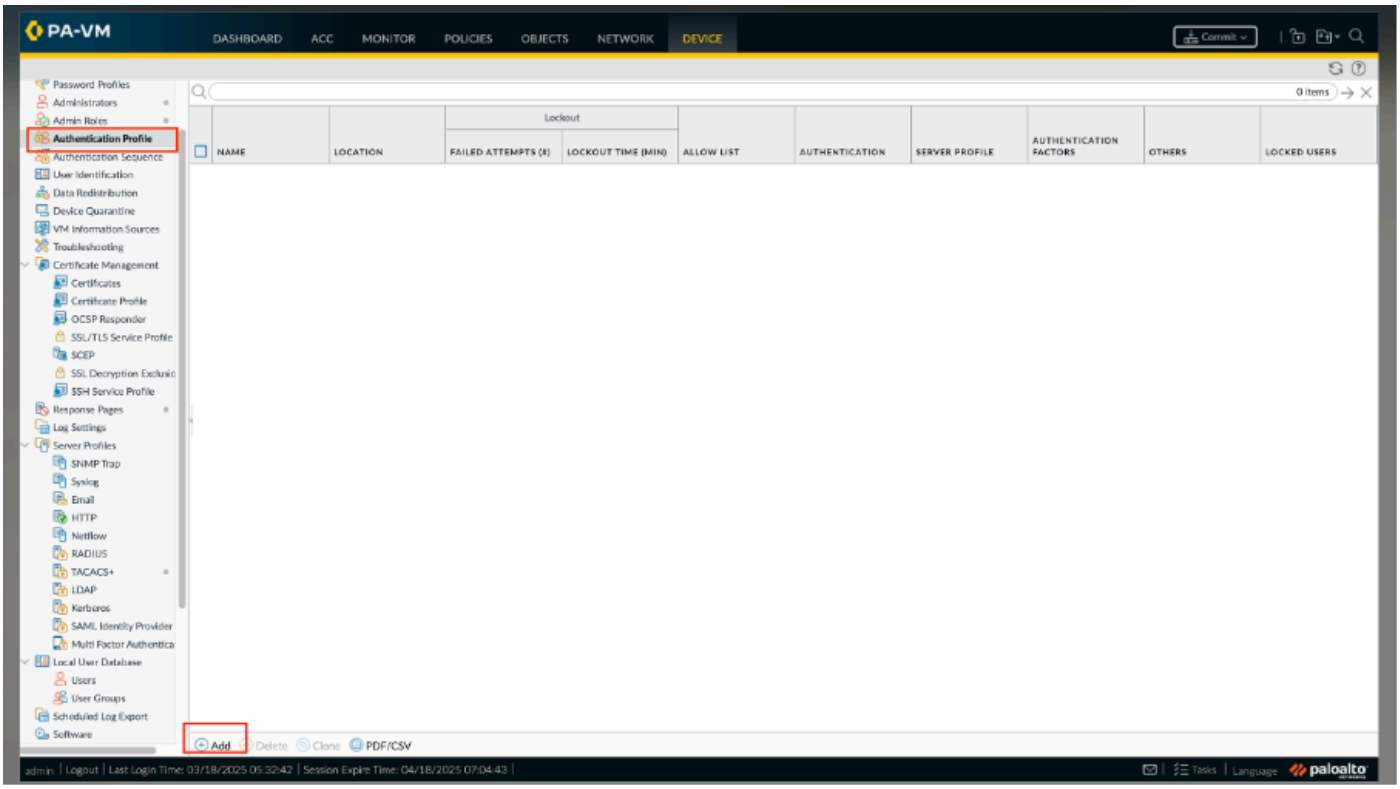
7. Fare clic su OK per salvare il profilo del server.

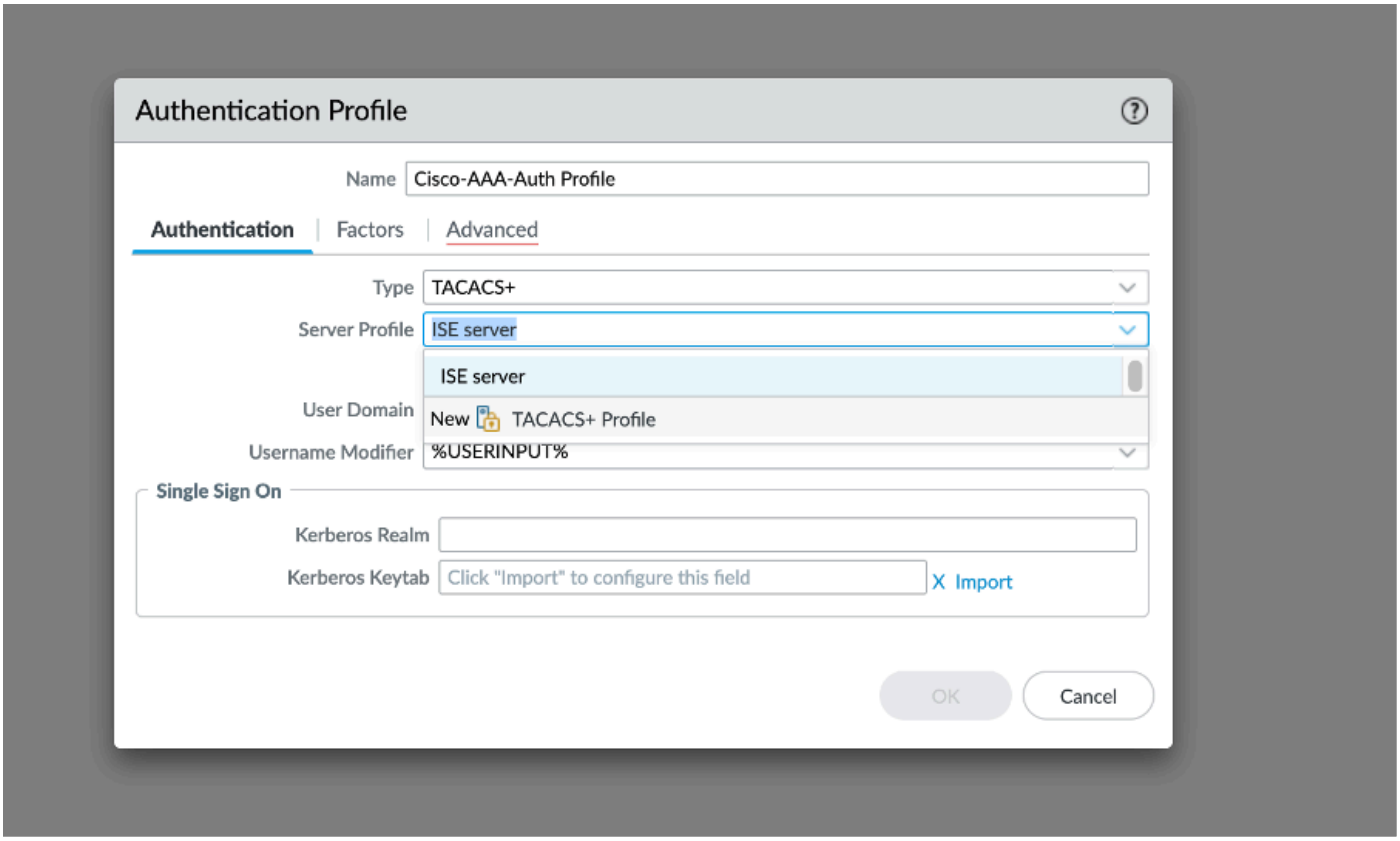


Passaggio 2. Assegnare il profilo del server TACACS+ a un profilo di autenticazione.

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

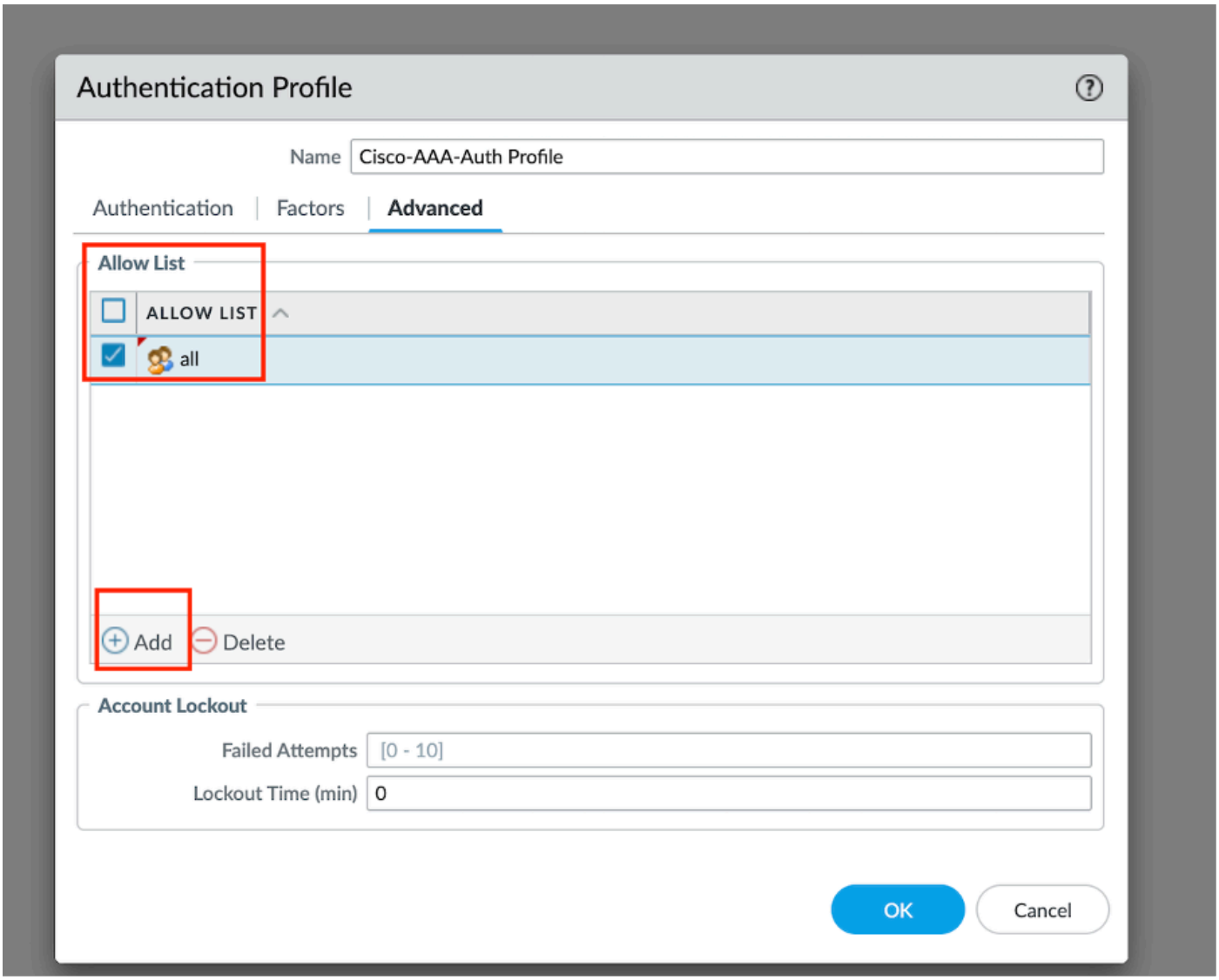
1. Selezionare Periferica > Profilo di autenticazione e Aggiungi profilo.
    1. Immettere un nome per identificare il profilo
    2. Impostare Type su TACACS+.
    3. Selezionare il profilo del server configurato.
    4. Selezionare Recupera gruppo di utenti da TACACS+ per raccogliere le informazioni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





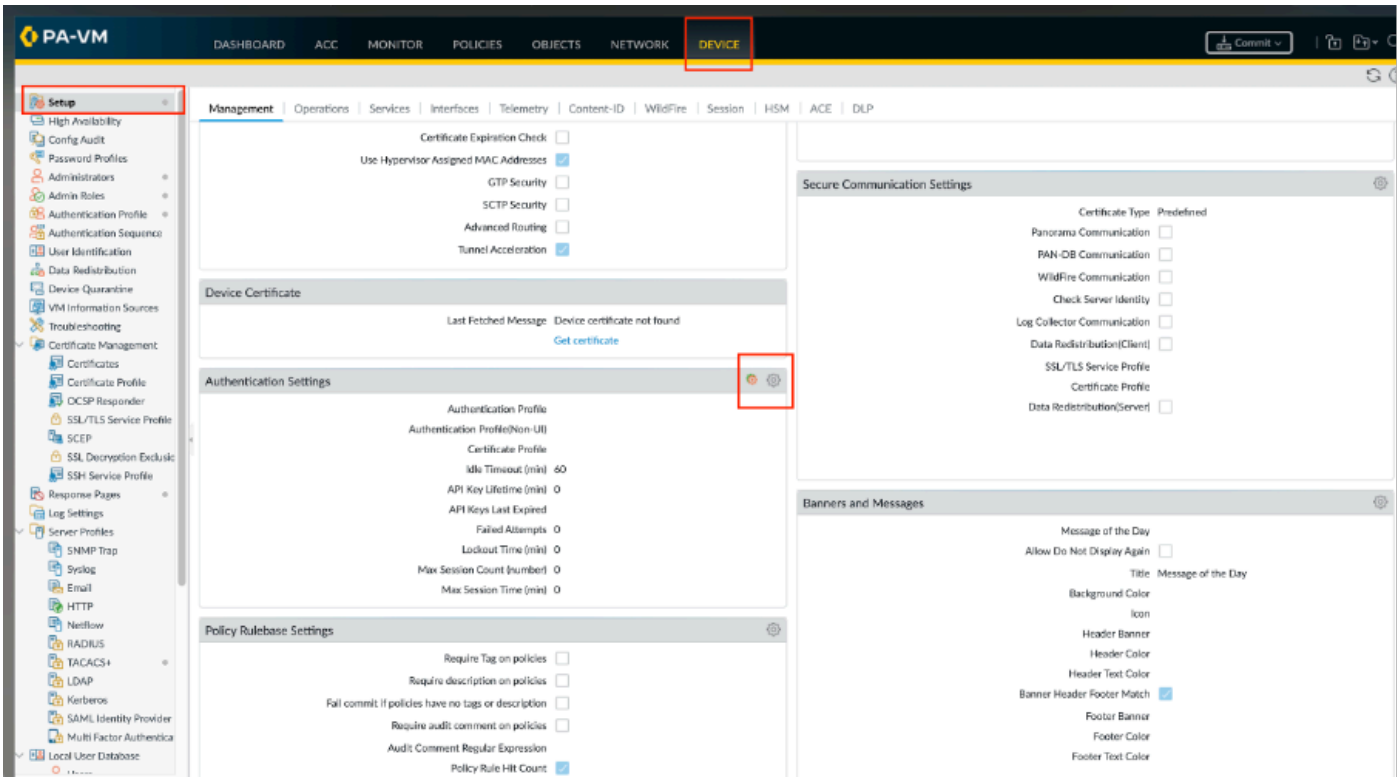
Il firewall corrisponde alle informazioni sui gruppi utilizzando i gruppi specificati nell'elenco Consenti del profilo di autenticazione.

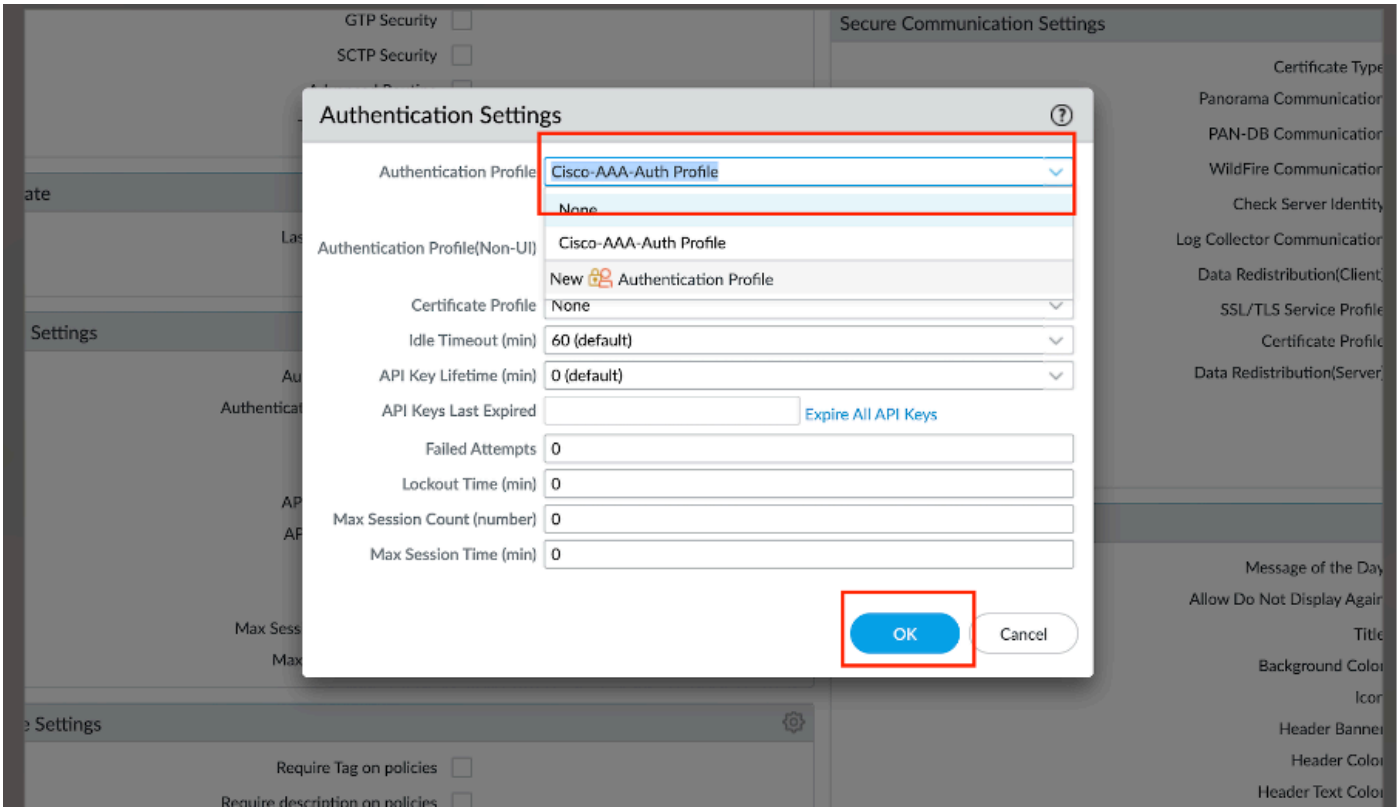
1. Selezionare Avanzate e nell'elenco Consenti Aggiungere gli utenti e i gruppi che possono eseguire l'autenticazione con questo profilo di autenticazione.
2. Fare clic su OK per salvare il profilo di autenticazione.



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

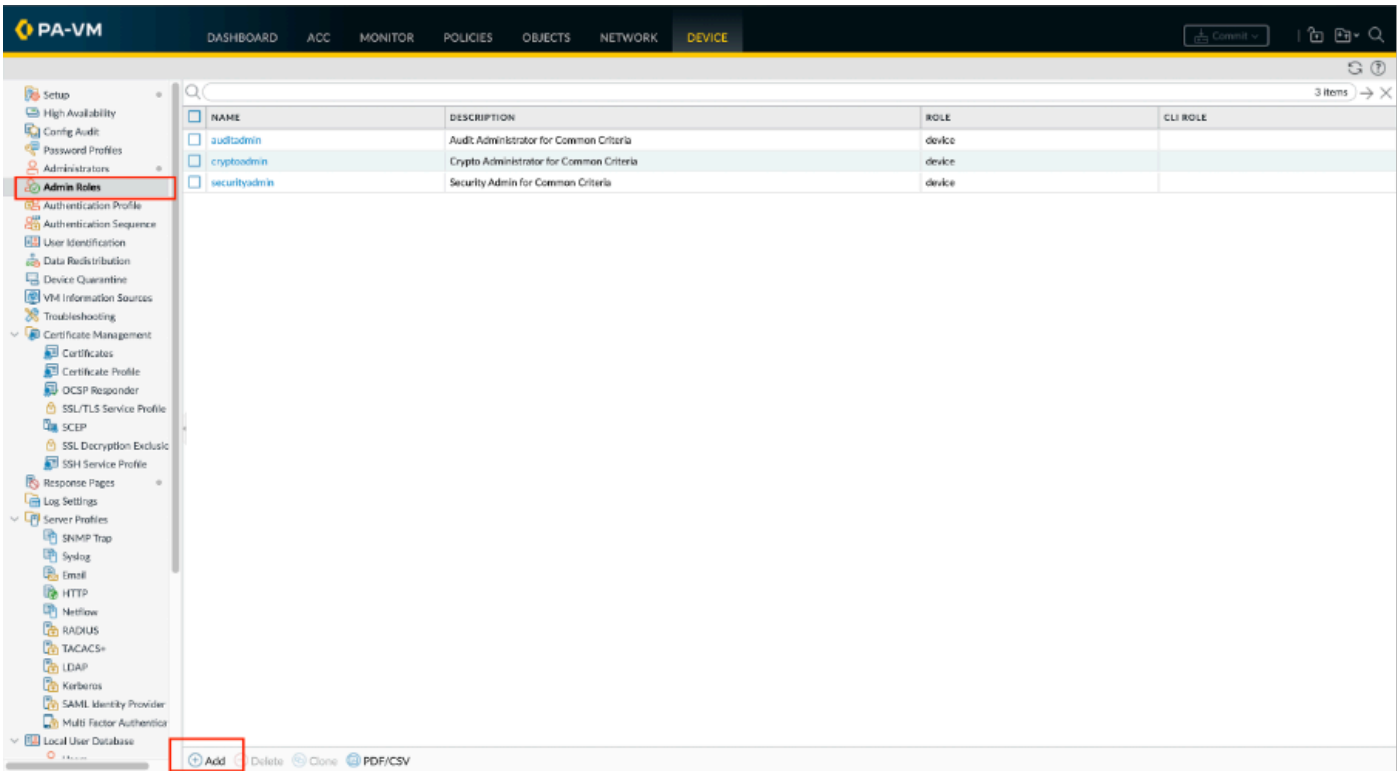
1. Selezionare Periferica > Impostazione > Gestione e modificare le impostazioni di autenticazione.
2. Selezionare il profilo di autenticazione configurato e fare clic su OK.



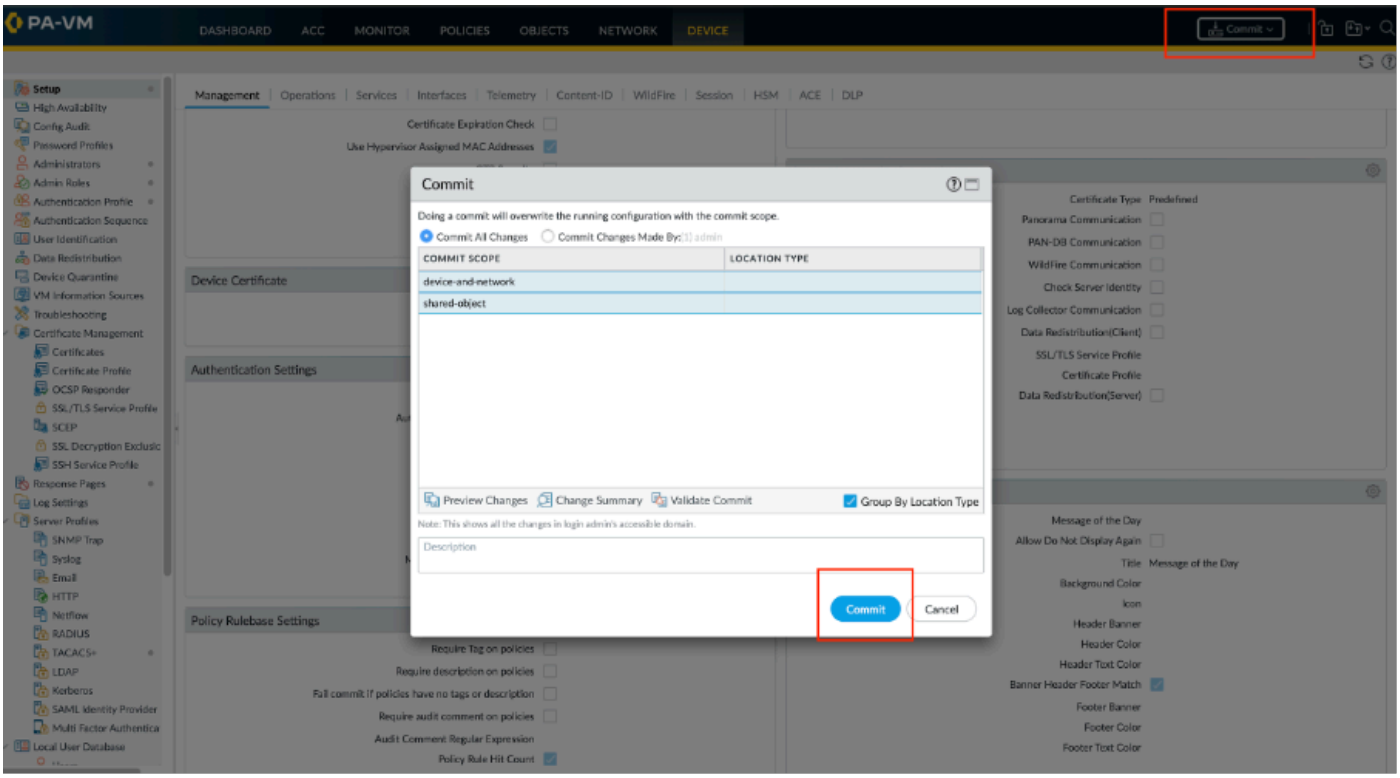


Passaggio 4. Configurare un profilo del ruolo di amministratore.

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



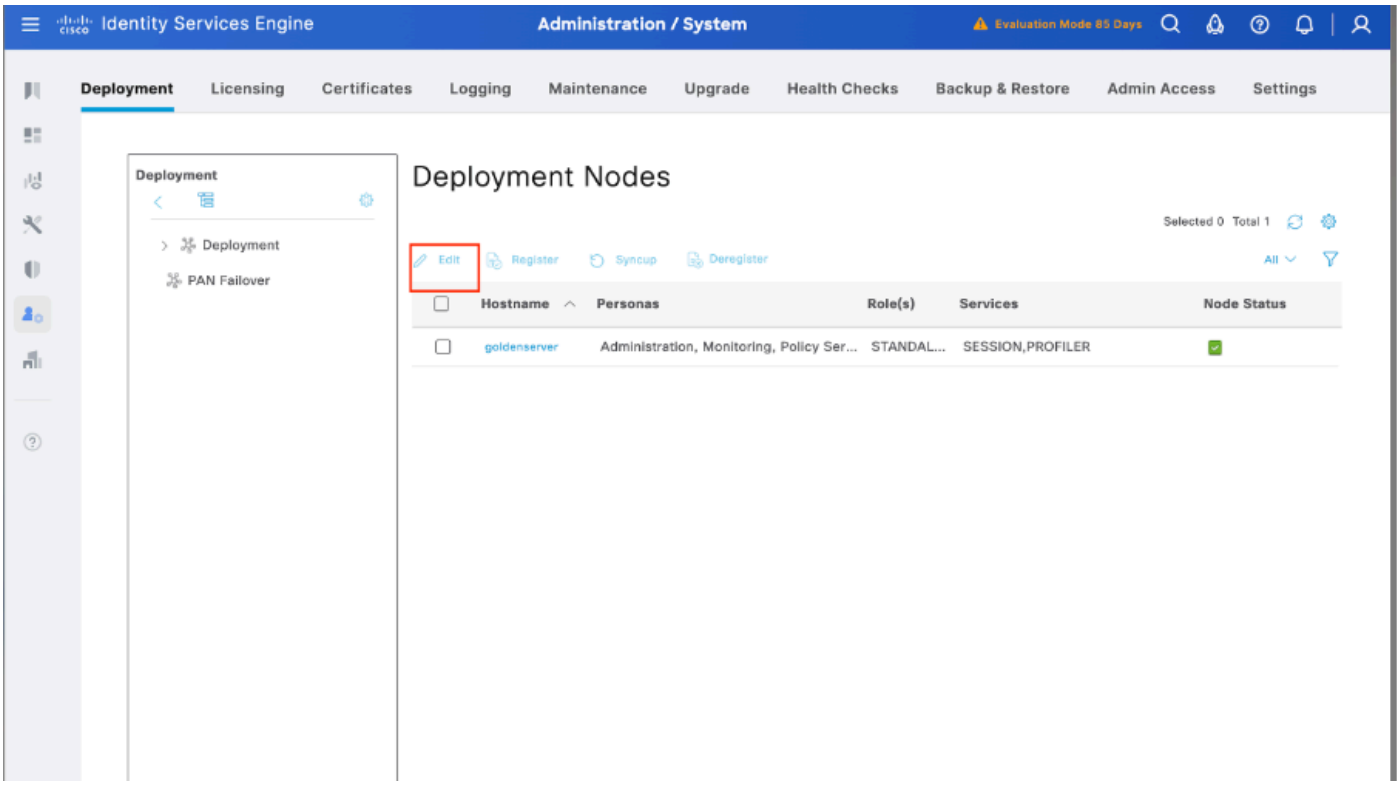
Passaggio 5. Eseguire il commit delle modifiche per attivarle sul firewall.



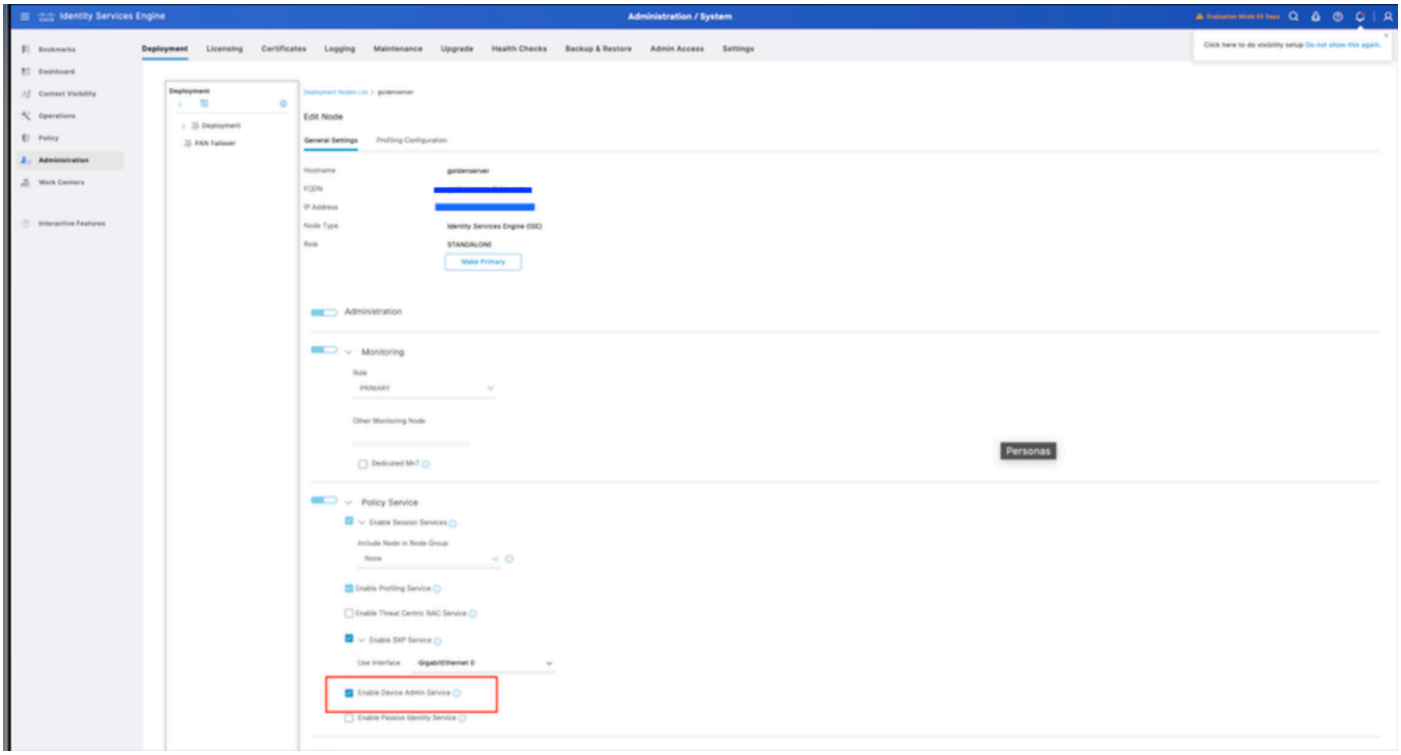
Sezione 2: Configurazione TACACS+ su ISE

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.

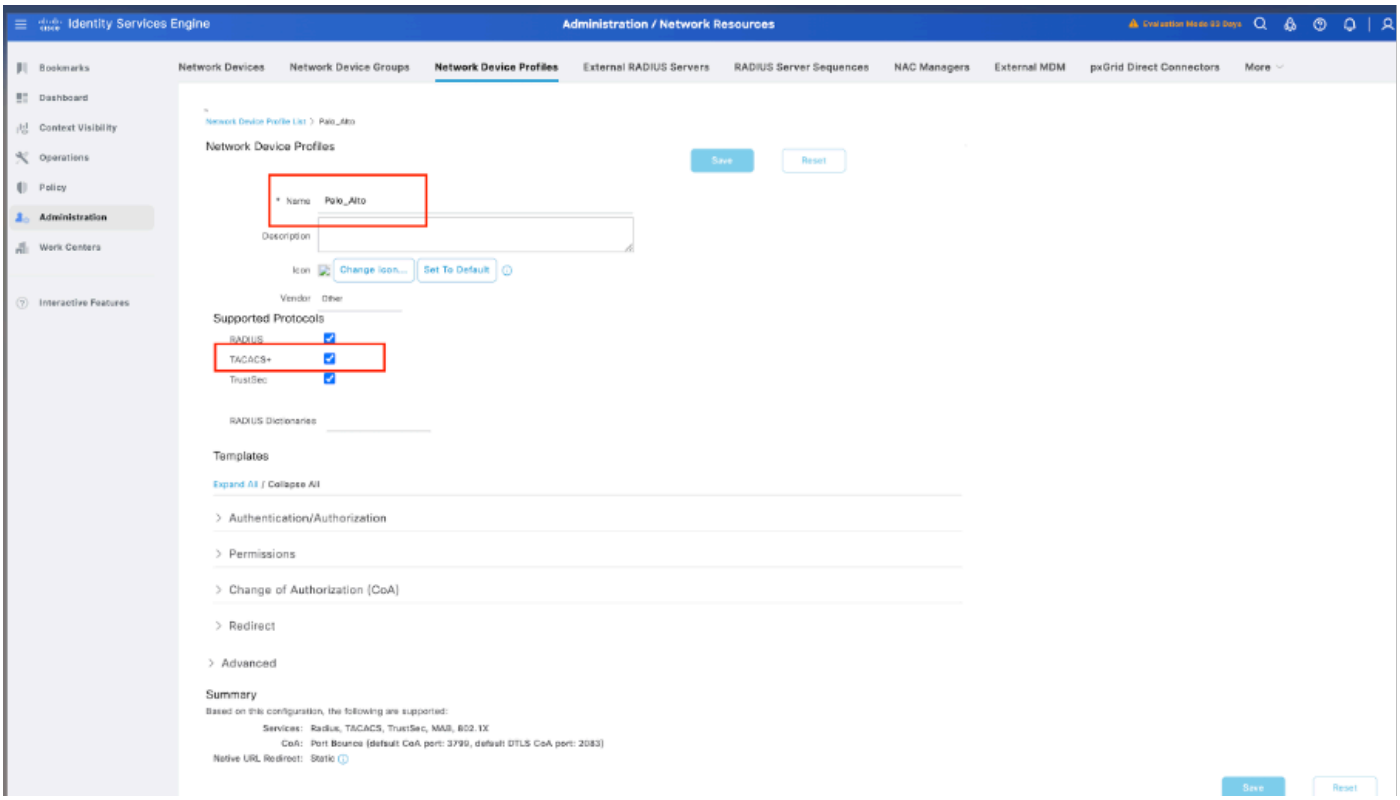


Passaggio 2. Scorrere verso il basso per individuare la funzionalità Servizio di amministrazione del dispositivo. Notare che l'abilitazione di questa funzionalità richiede che la persona del servizio criteri sia attiva sul nodo, insieme alle licenze TACACS+ disponibili nella distribuzione. Selezionare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



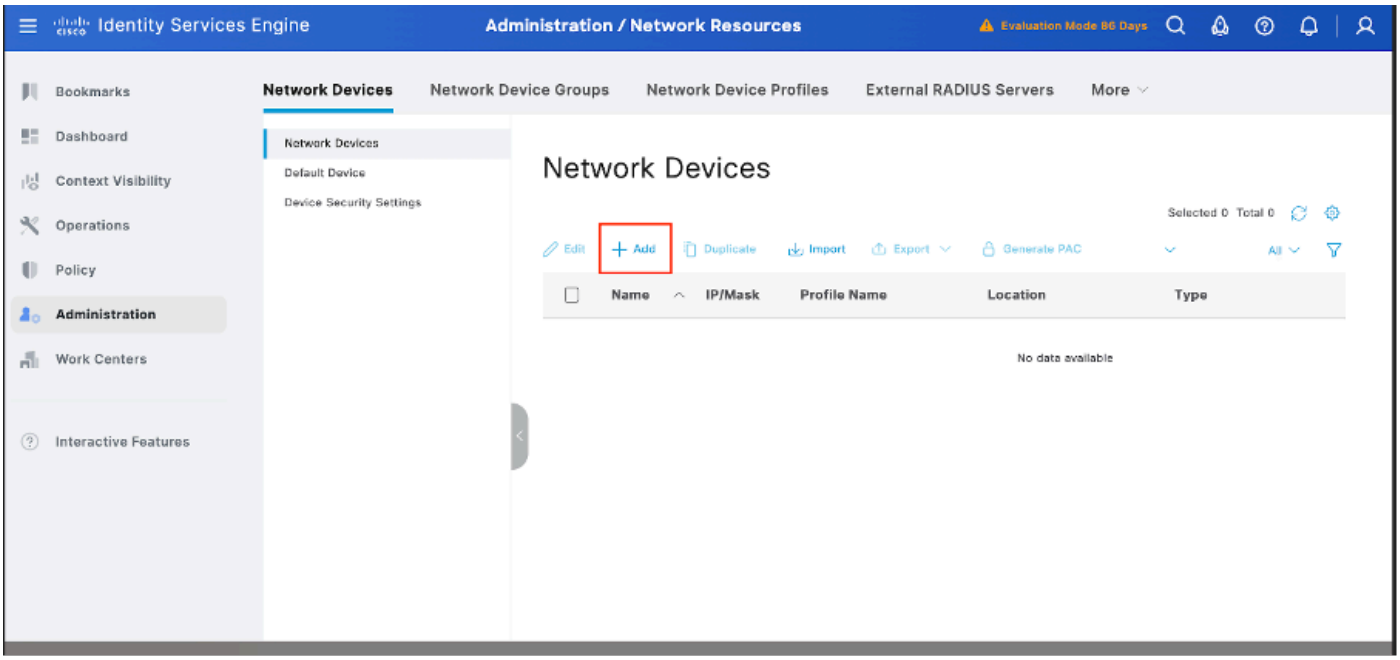
Passaggio 3. Configurare Palo Alto Network Device Profile per Cisco ISE.

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>

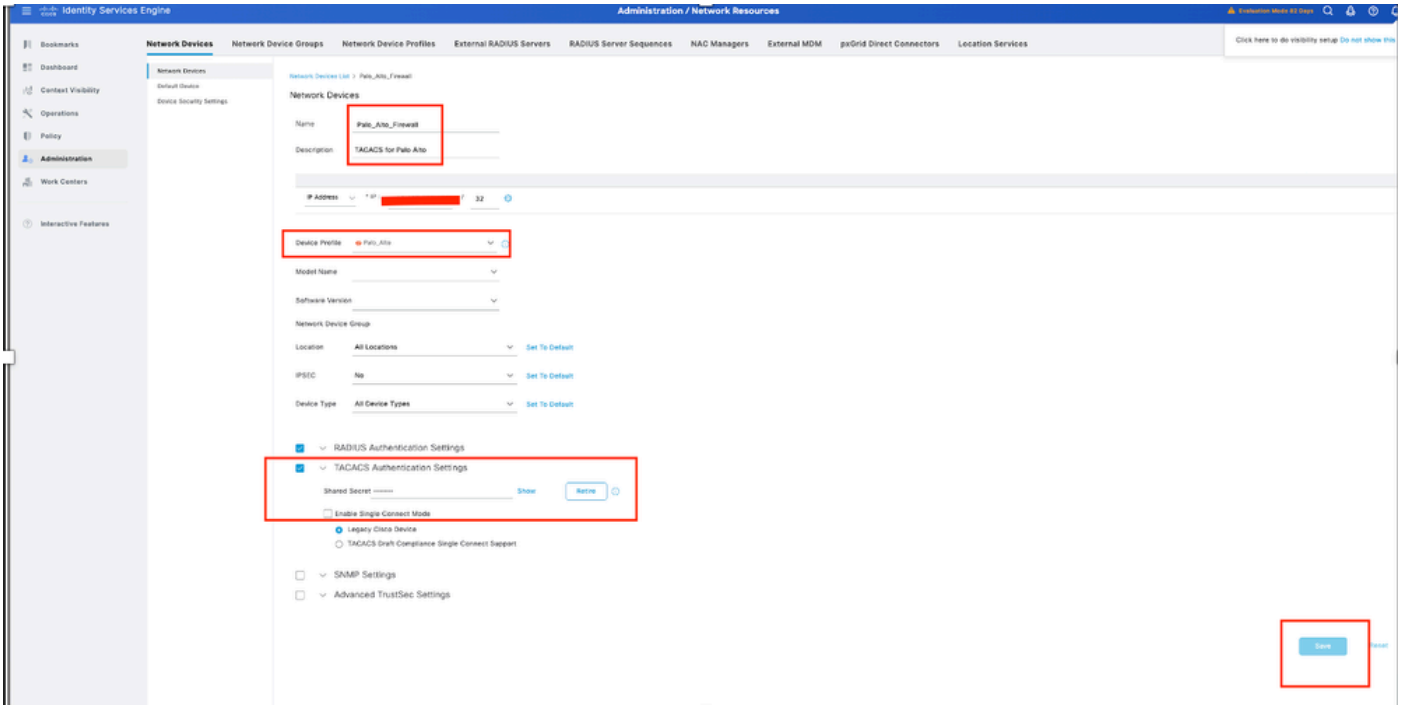
Profilo dispositivo di rete: selezionare Palo Alto

Impostazioni autenticazione TACACS:

Abilita autenticazione TACACS+

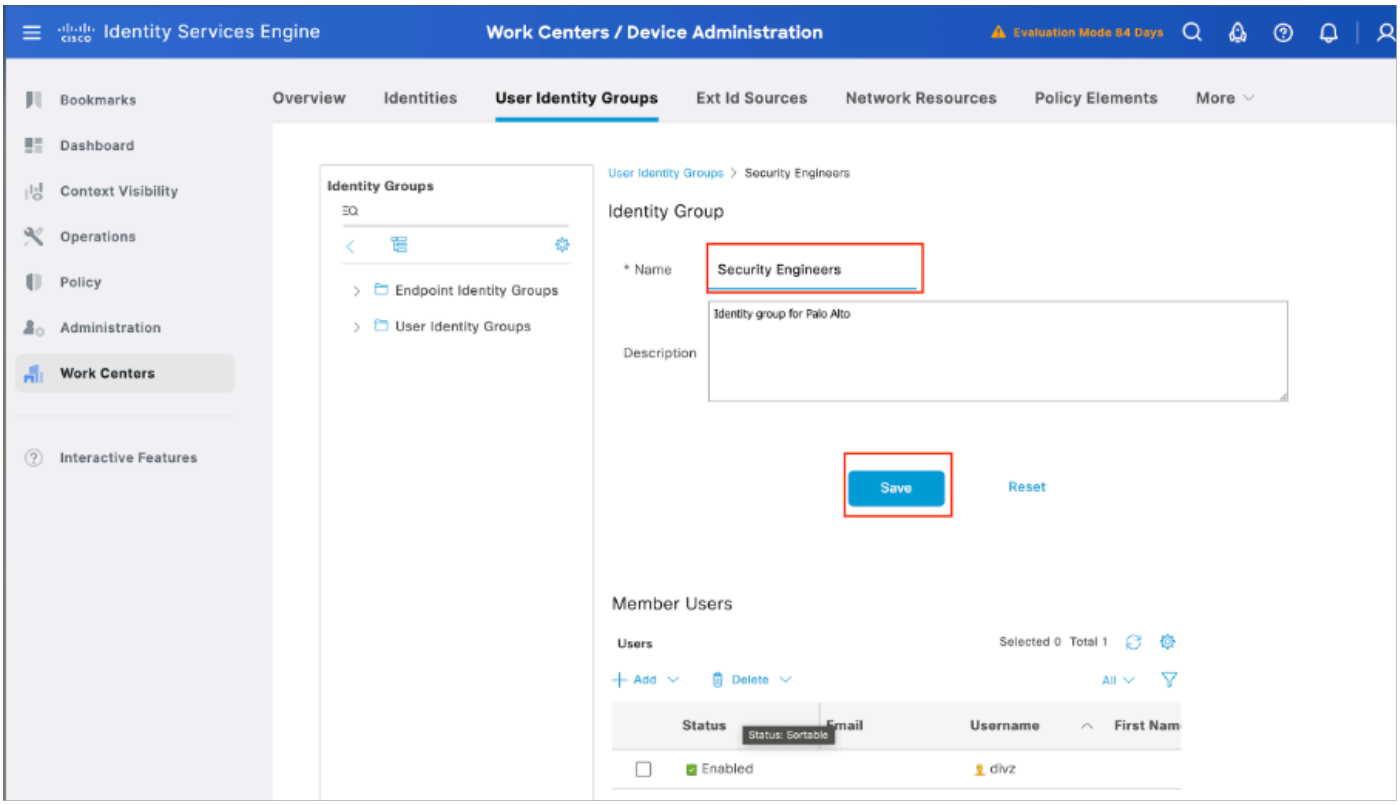
Immettere il segreto condiviso (deve corrispondere alla configurazione di Palo Alto)

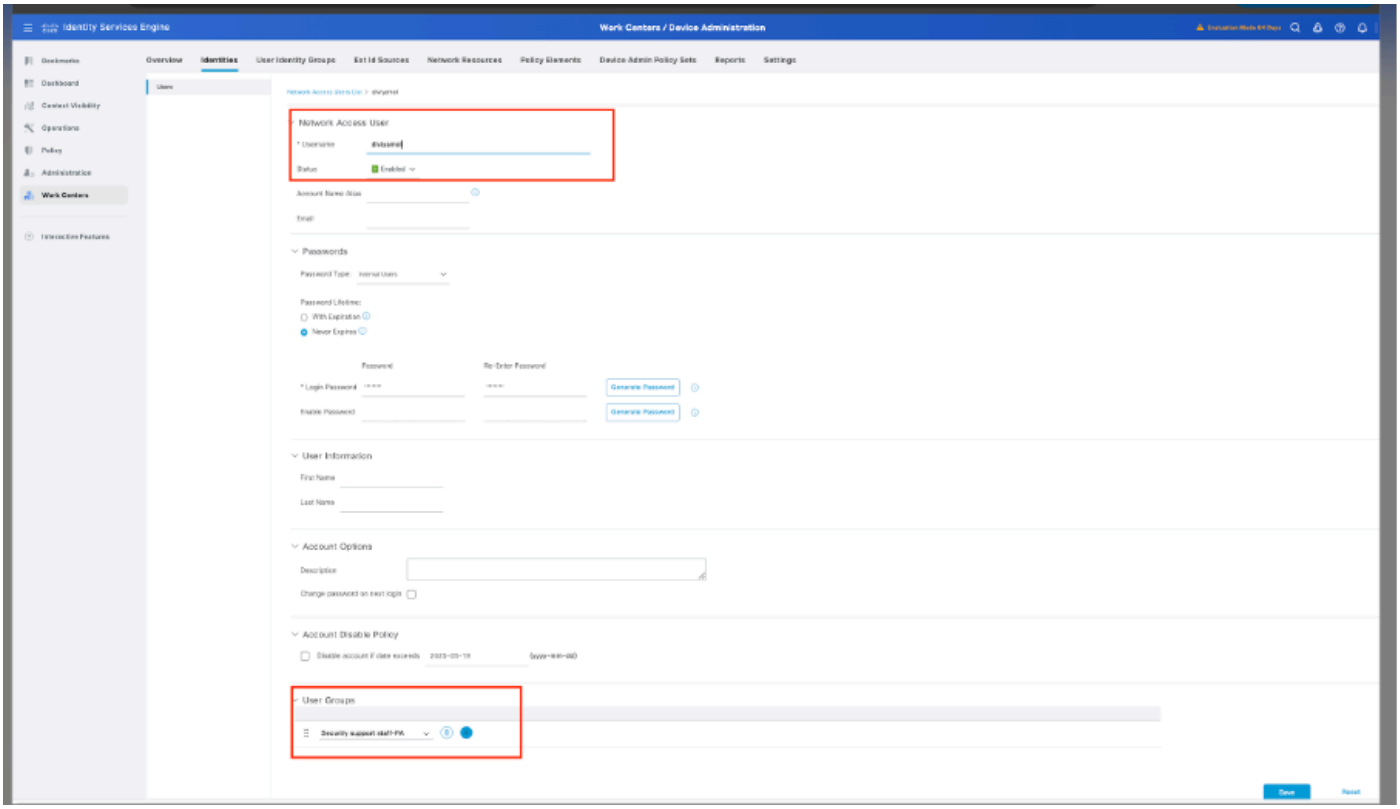
Fare clic su Save (Salva).

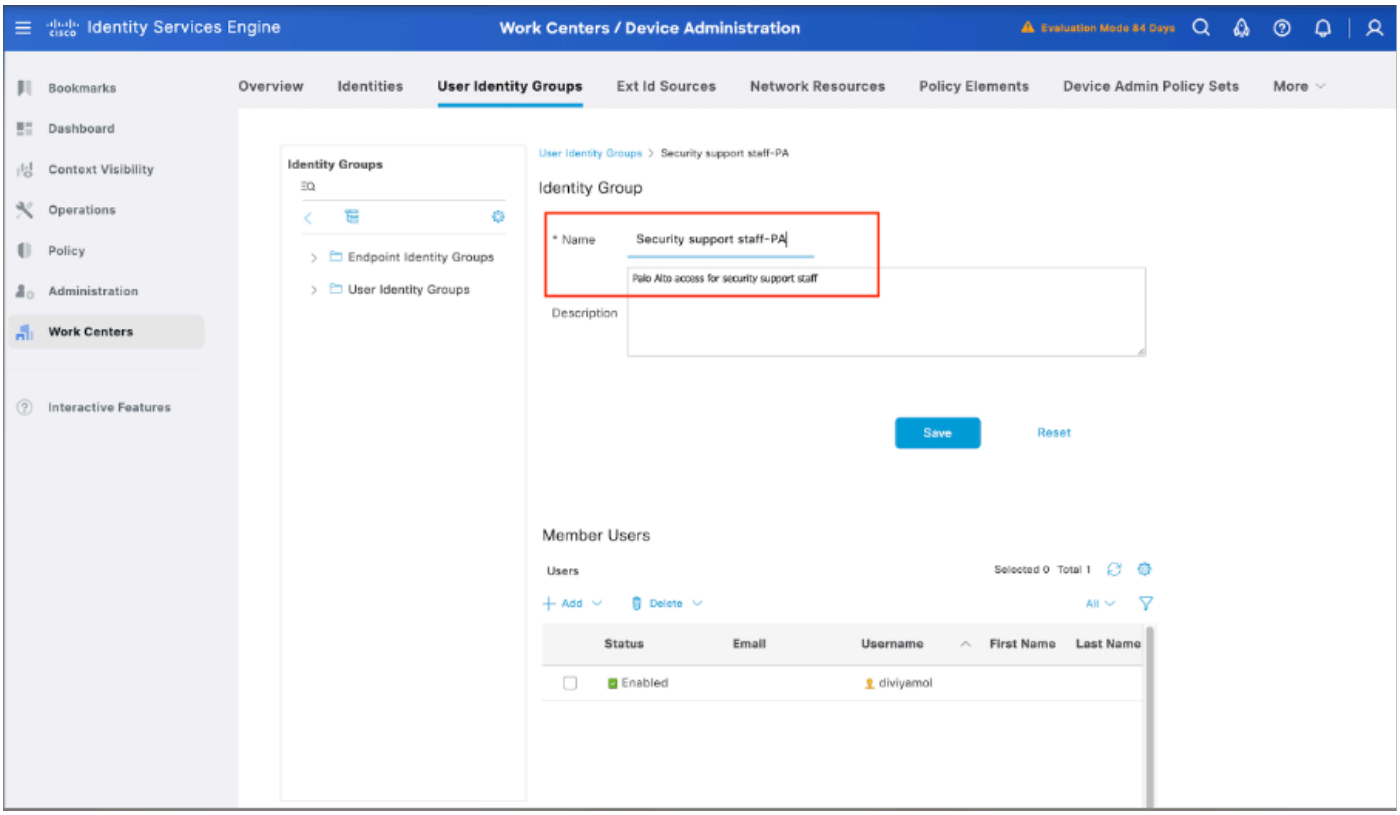


Passaggio 5. Creazione dei gruppi di identità degli utenti.

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
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

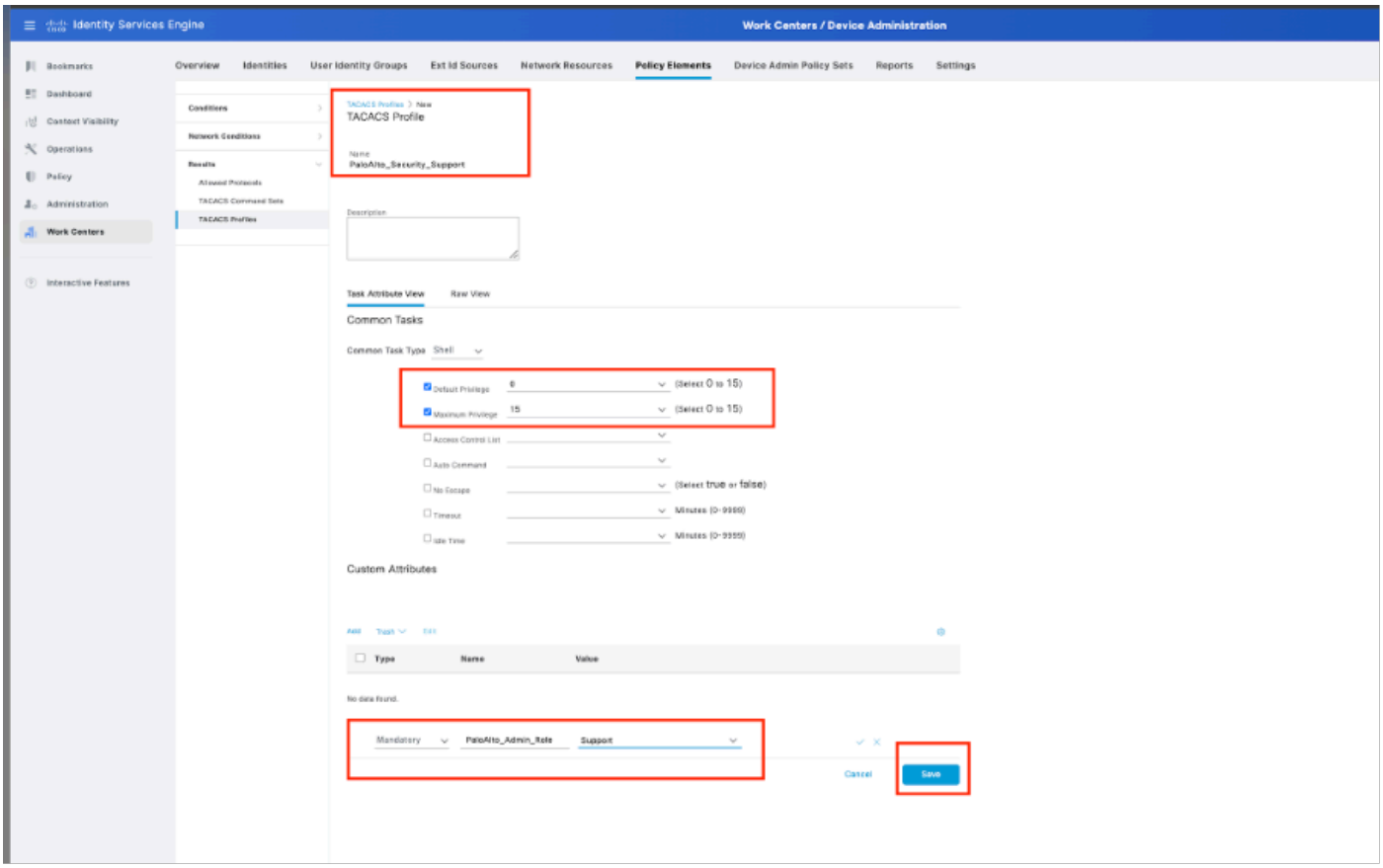

Identity Services Engine
Work Centers / Device Administration
Network Access User
Passwords
User Information
Account Options
Account Disable Policy
User Groups

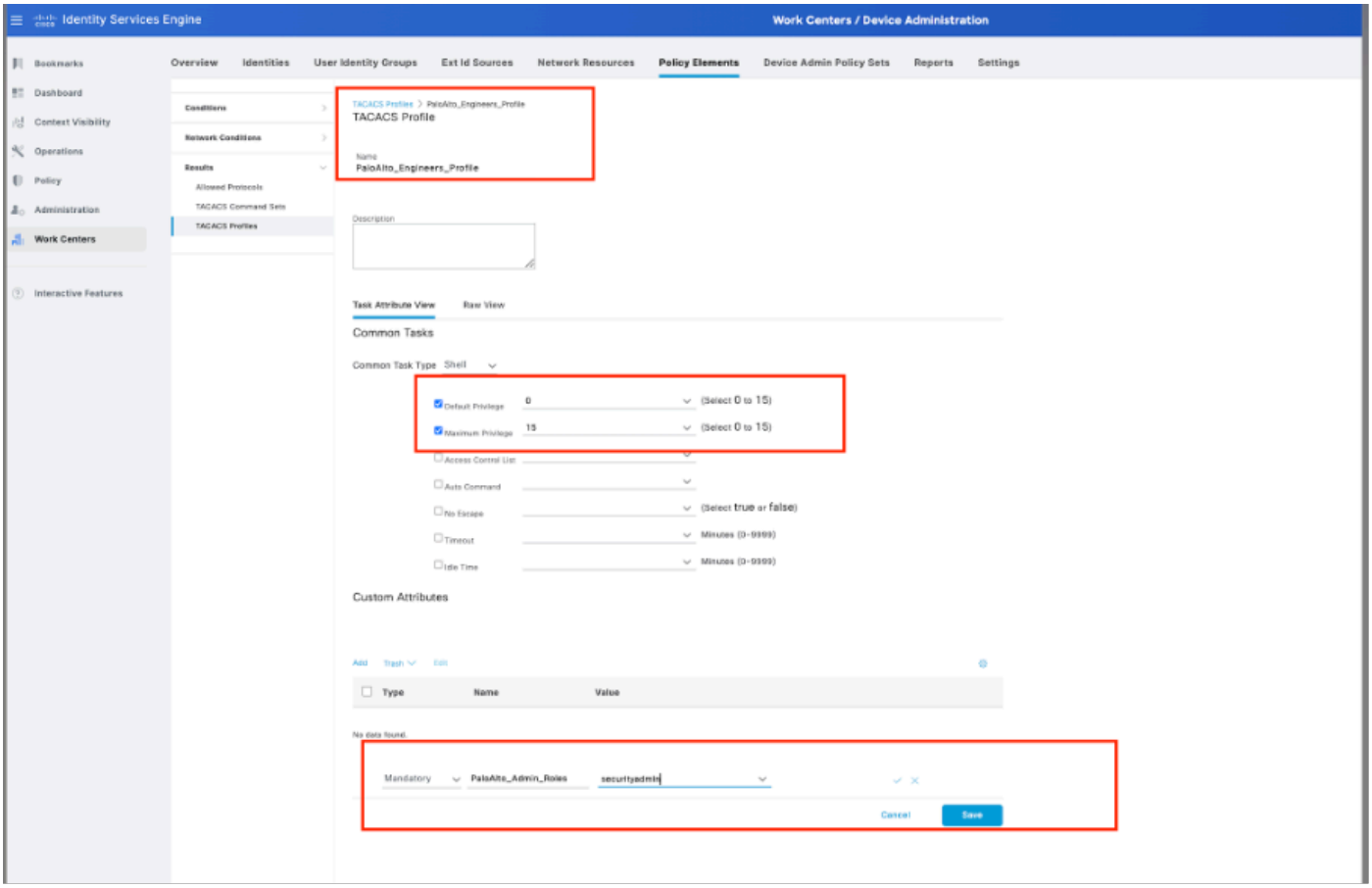


Passaggio 6. Configurare Un Profilo TACACS.

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.





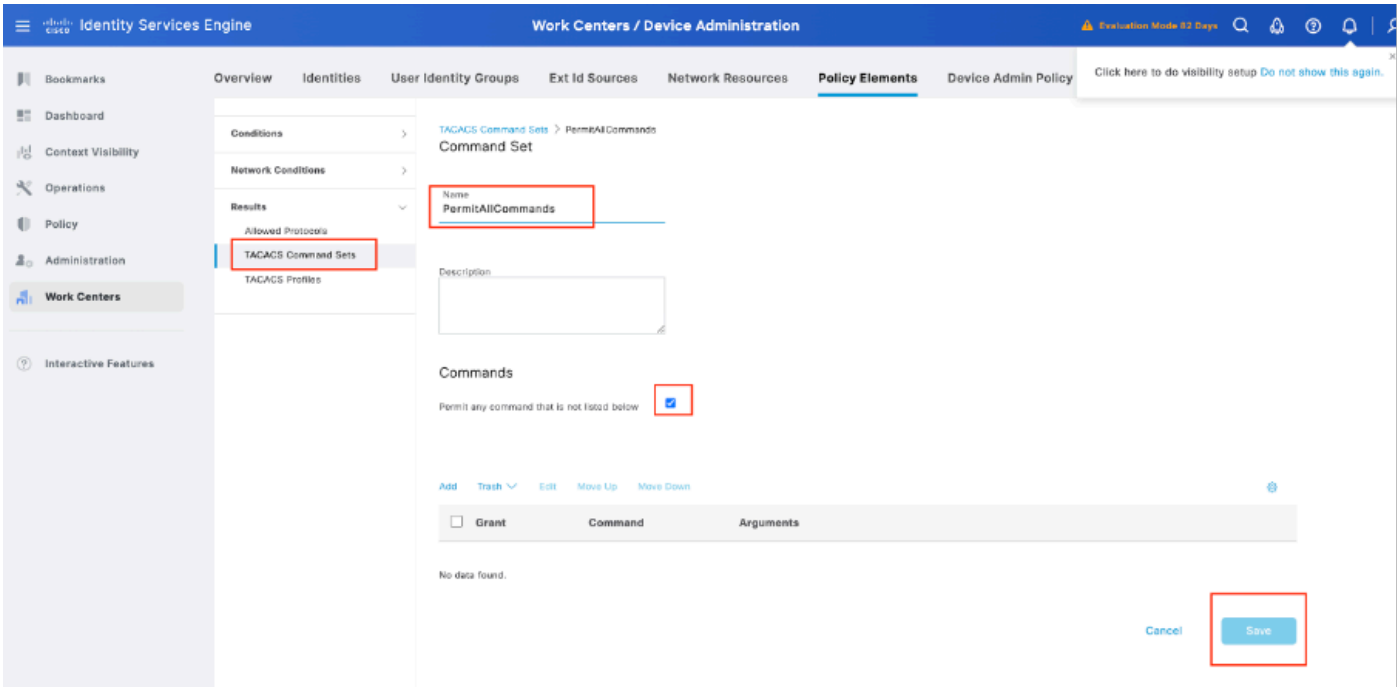
Passaggio 6. Configurare i set di comandi TACACS.

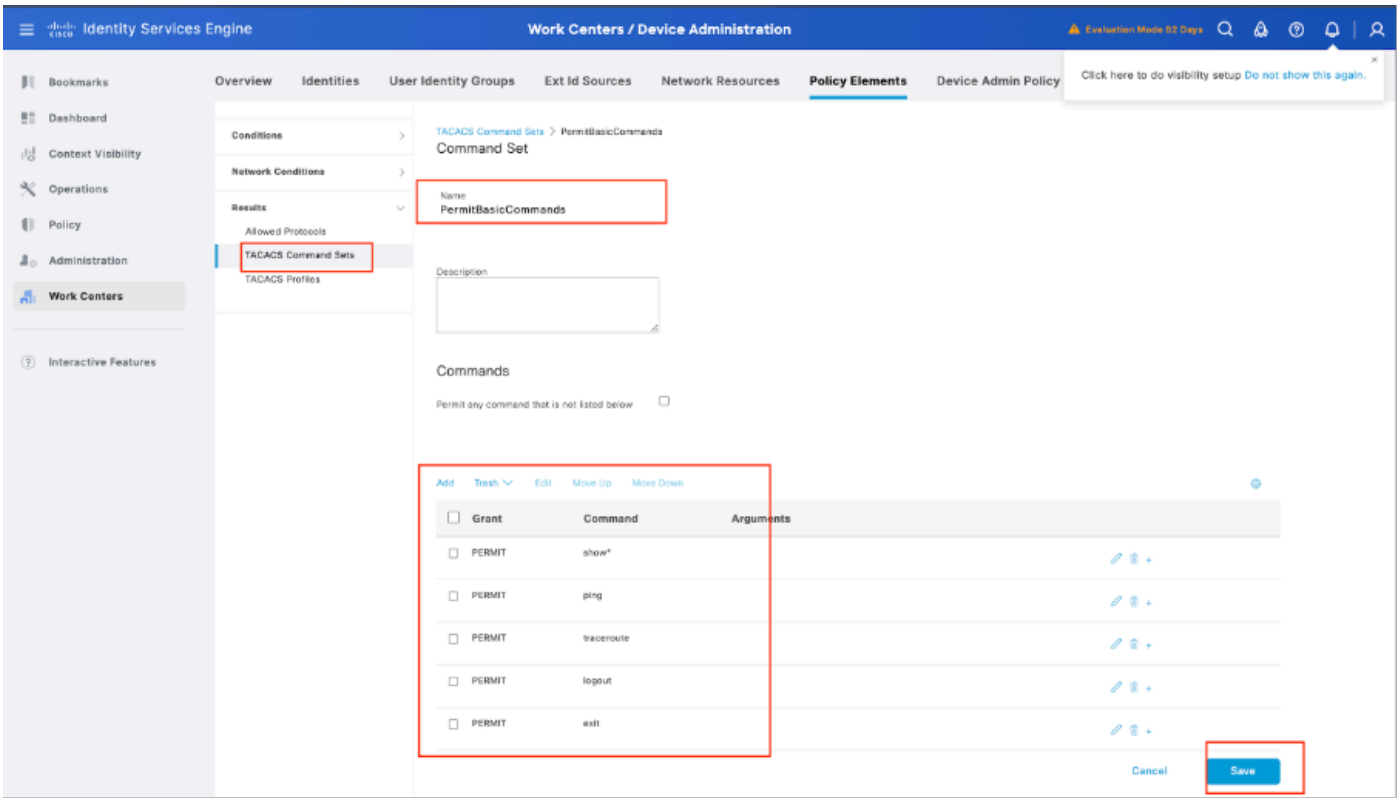
A questo punto è possibile configurare i comandi che gli utenti possono utilizzare. Poiché è

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.

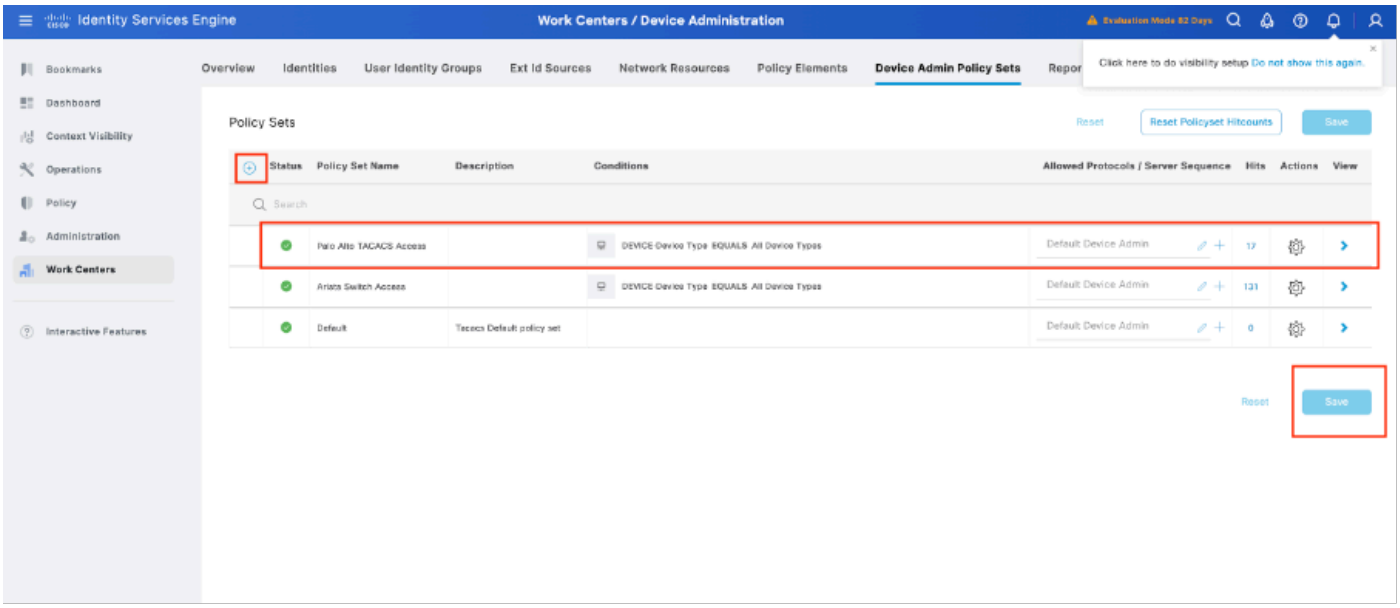
L'unica cosa che è necessario configurare in questo set di comandi TACACS è selezionare la casella di controllo Permit qualsiasi comando non elencato di seguito.



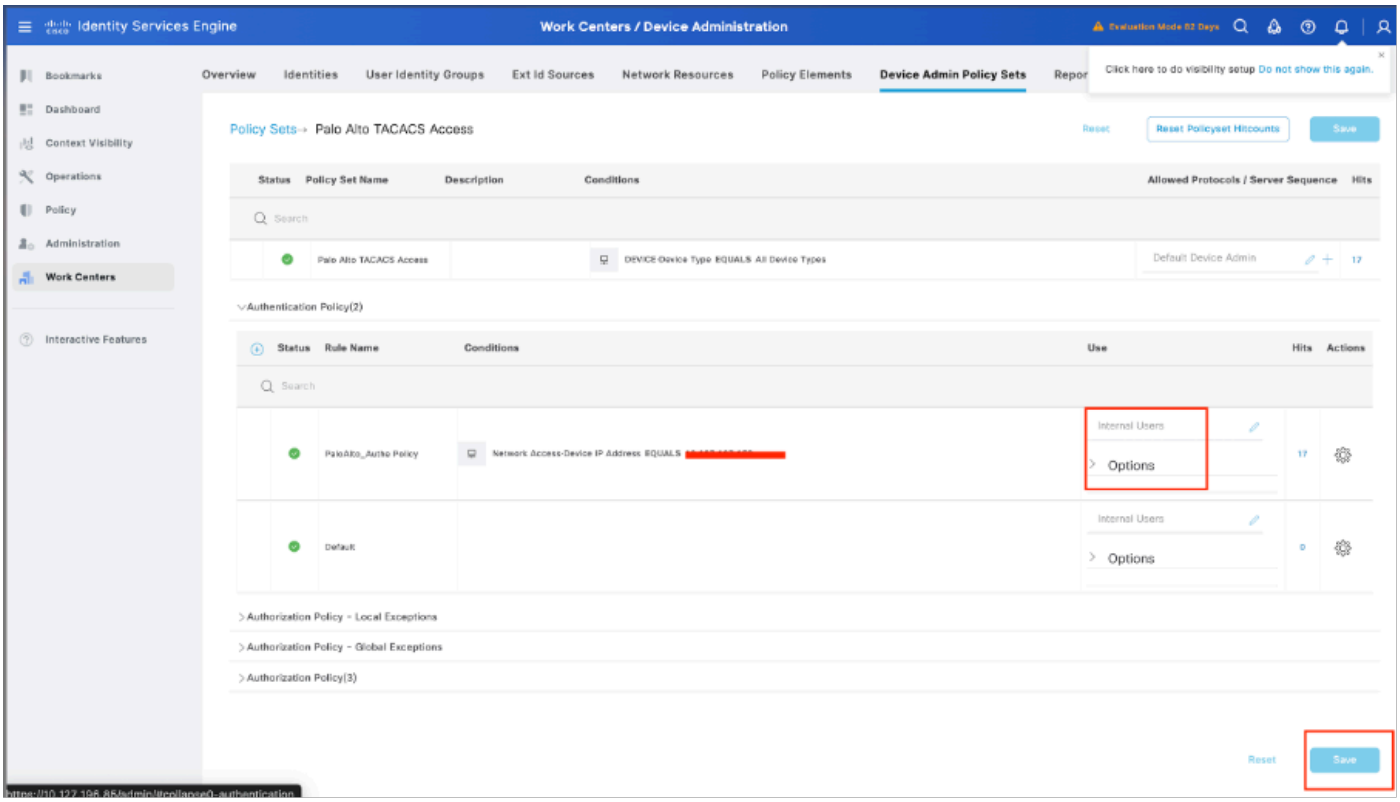


Passaggio 7. Creare un set di criteri di amministrazione dei dispositivi da utilizzare per Palo Alto, Navigare nel menu Centri di lavoro > Amministrazione dispositivi > Set di criteri di amministrazione dei dispositivi, Fare clic sull'icona Aggiungi +.

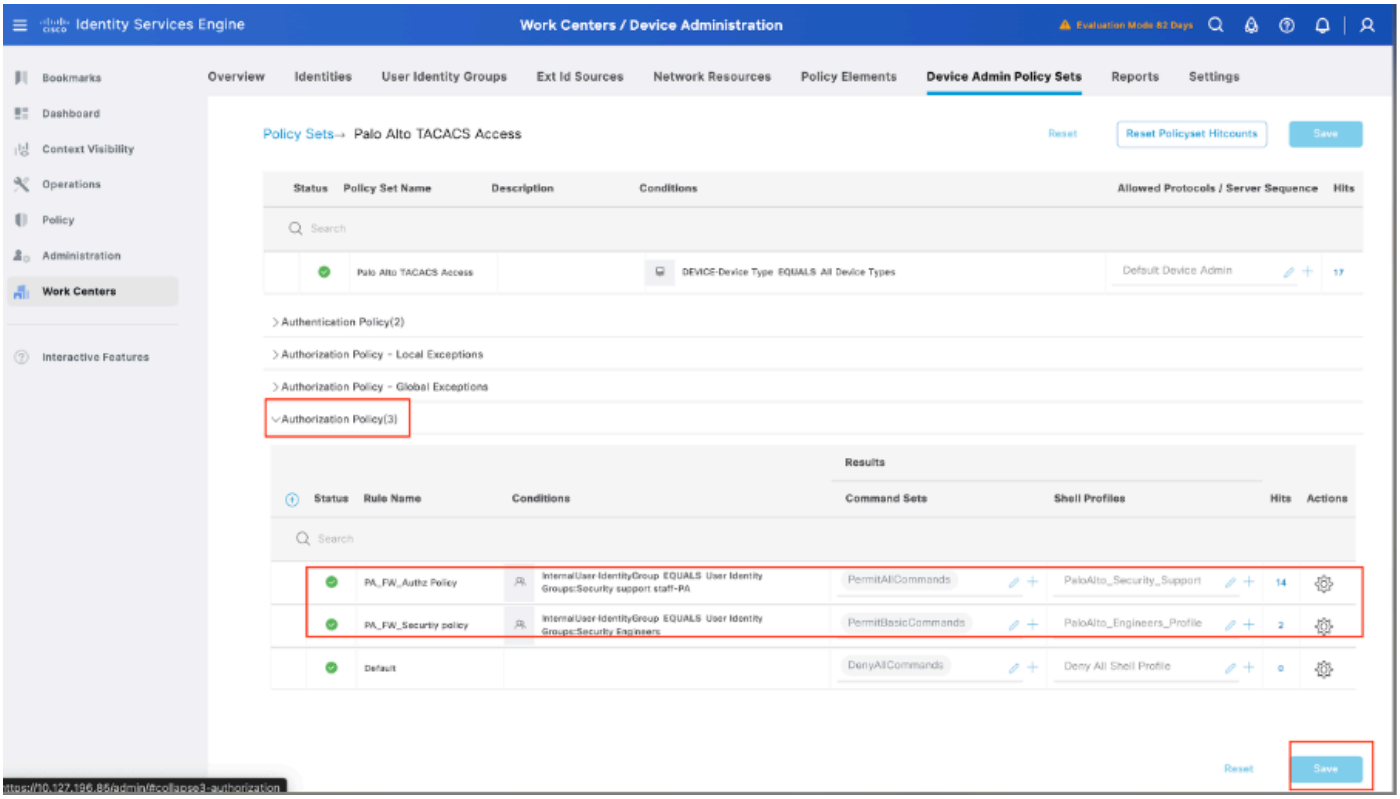
Passaggio 8. Assegnare un nome al nuovo set di criteri, aggiungere le condizioni in base alle caratteristiche delle autenticazioni TACACS+ in corso dal firewall di Palo Alto e selezionare Protocolli autorizzati > Amministratore di dispositivo predefinito. Salvare la configurazione.



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.



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.



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

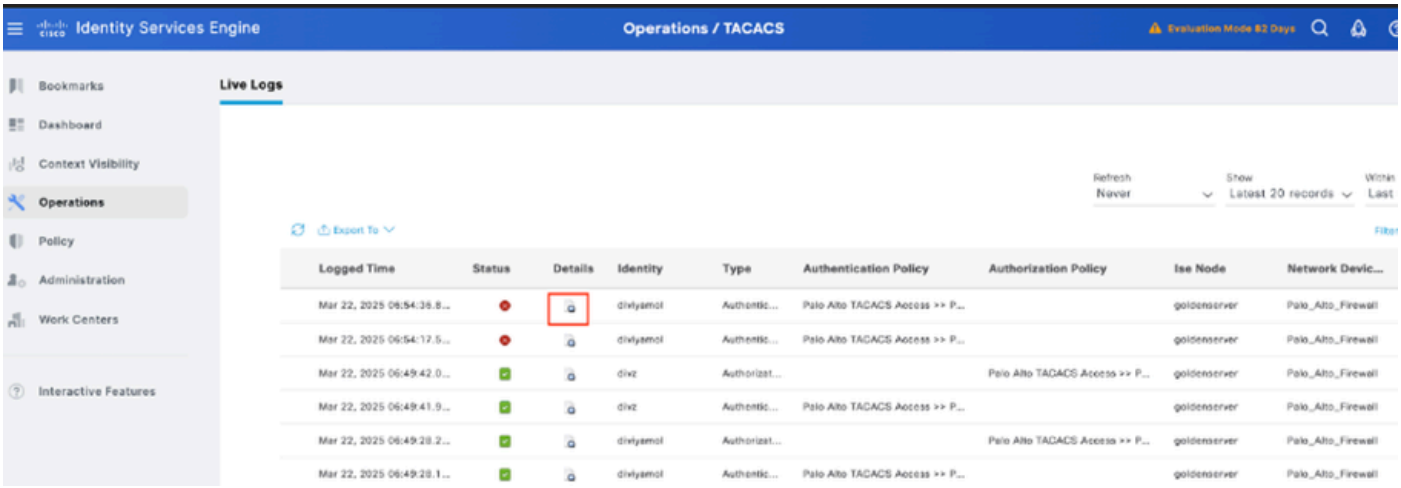
Passaggio 1. Verificare che il servizio TACACS+ sia in esecuzione e che sia possibile archiviarlo:

- 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+

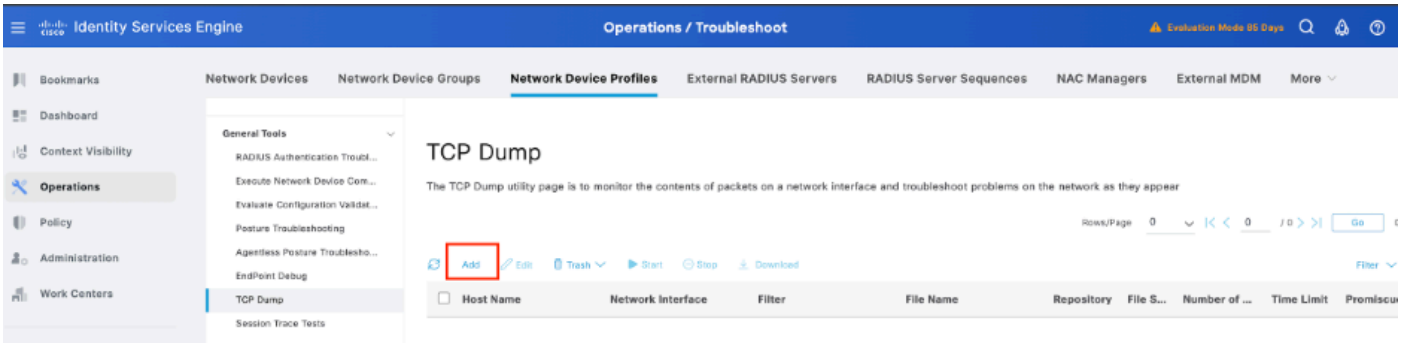
```
goldenserver/admin#show ports | include 49
tcp: [redacted]
```

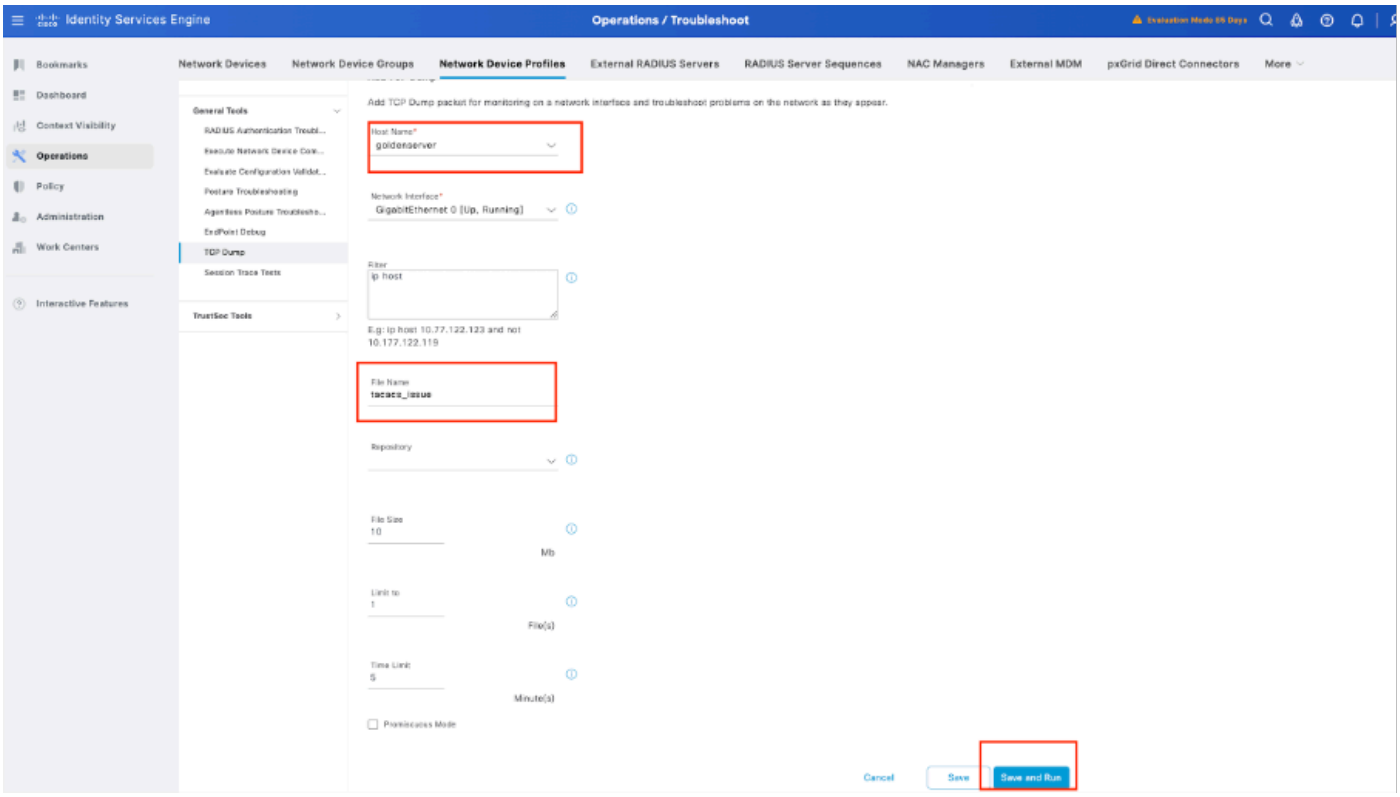
Passaggio 2. Confermare la presenza di log attivi relativi ai tentativi di autenticazione TACACS+: è possibile controllare questa condizione nel menu Operations (Operazioni) -> TACACS (TAC) -> Live logs (Registri attivi).

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

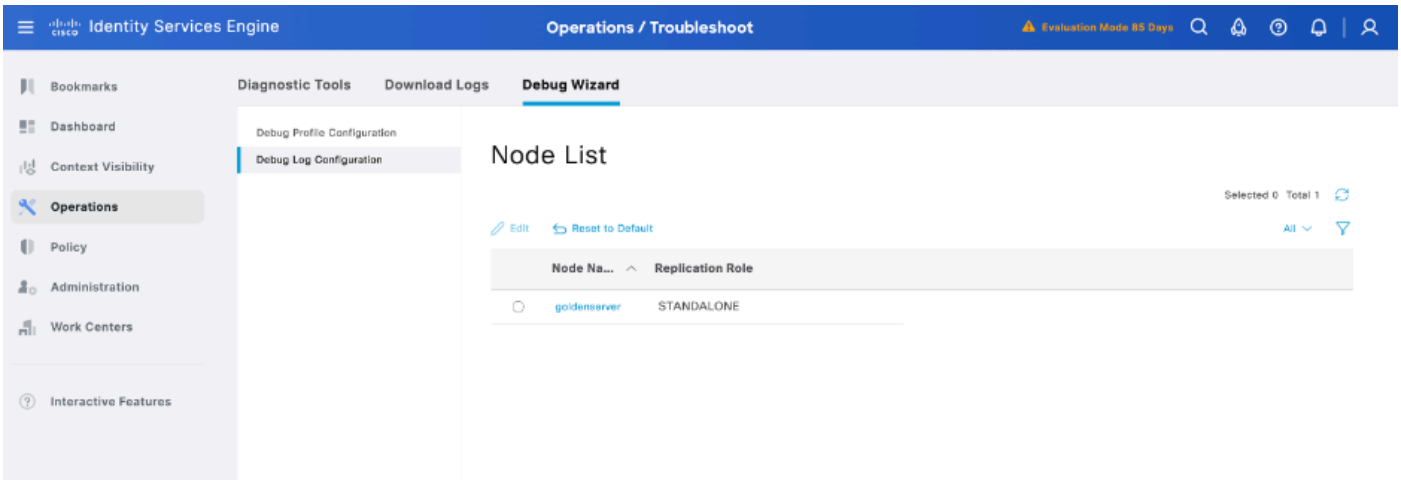


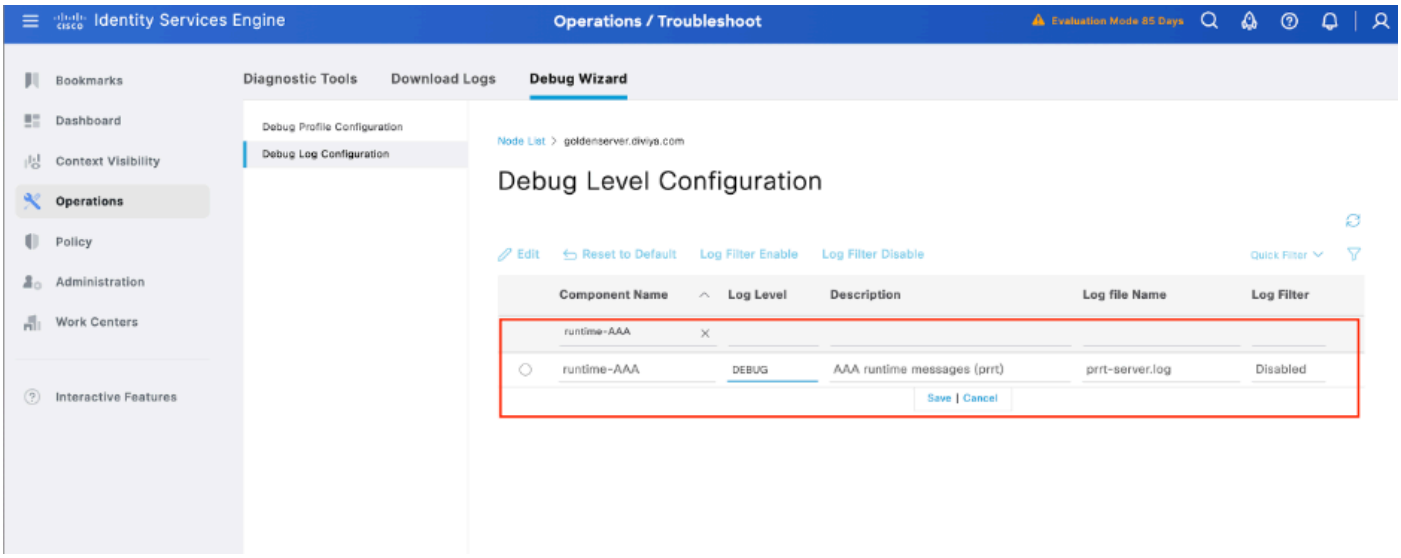
Passaggio 3. Se non viene visualizzato alcun log in tempo reale, procedere con l'acquisizione di un pacchetto. Passare al menu Operazioni > Risoluzione dei problemi > Strumenti diagnostici > Strumenti generali > Dump TCP , selezionare Aggiungi.





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.





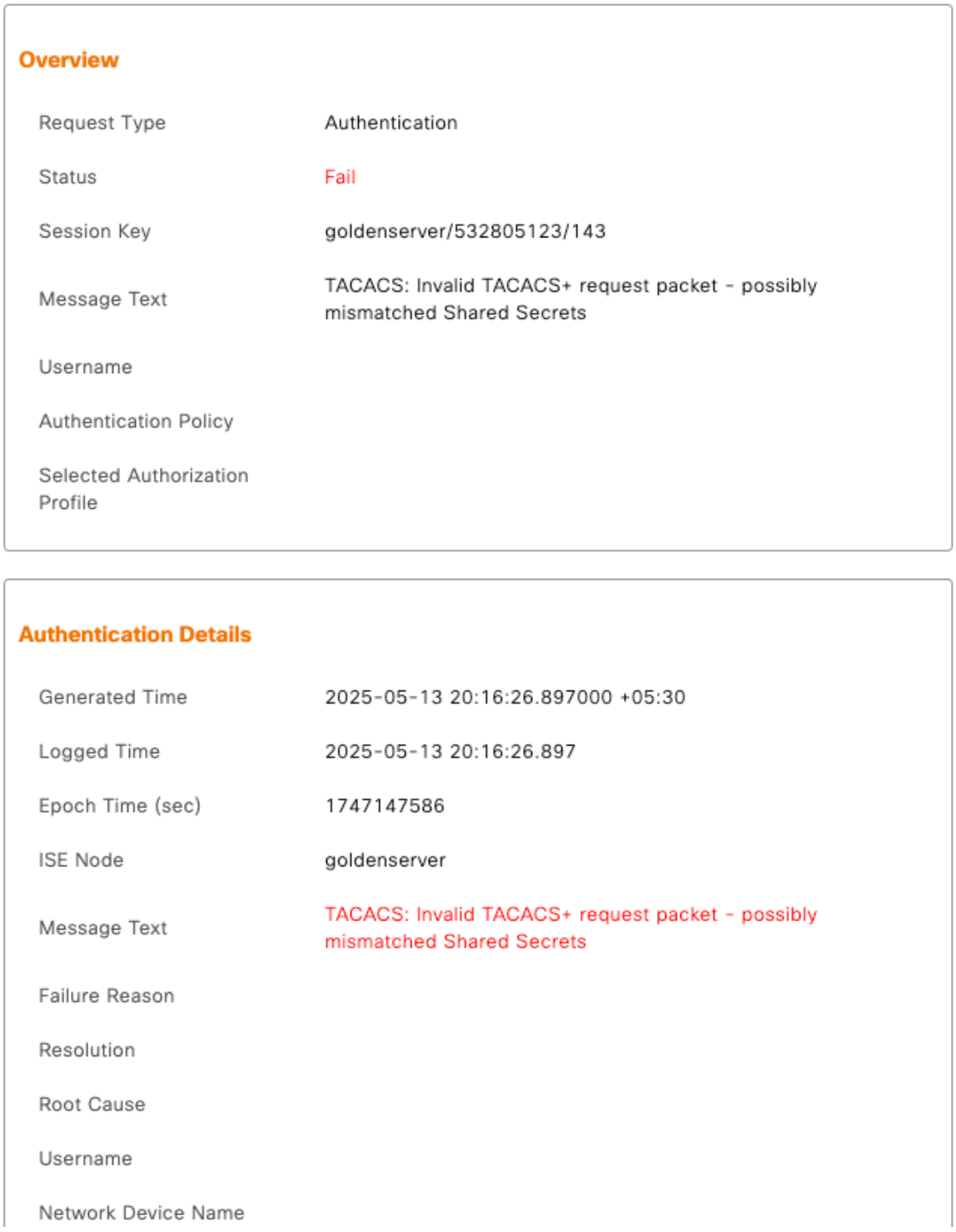
Identificare il componente runtime-AAA, impostarne il livello di log per eseguire il debug, riprodurre il problema e analizzare i log per ulteriori informazioni.

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).