Configurazione di APIC per l'amministrazione dei dispositivi con ISE e TACACS+

Sommario

Introduzione

Prerequisiti

- Requisiti
- Componenti usati

Configurazione

- Esempio di rete
- Procedura di autenticazione
- Configurazione APIC
- Configurazione di ISE

Verifica

Risoluzione dei problemi

Introduzione

In questo documento viene descritta la procedura per integrare APIC con ISE per l'autenticazione degli utenti amministratore con il protocollo TACACS+.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Application Policy Infrastructure Controller (APIC)
- Identity Services Engine (ISE)
- Protocollo TACACS

Componenti usati

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

- APIC versione 4.2(7u)
- Patch 1 per ISE versione 3.2

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.

Configurazione

Esempio di rete

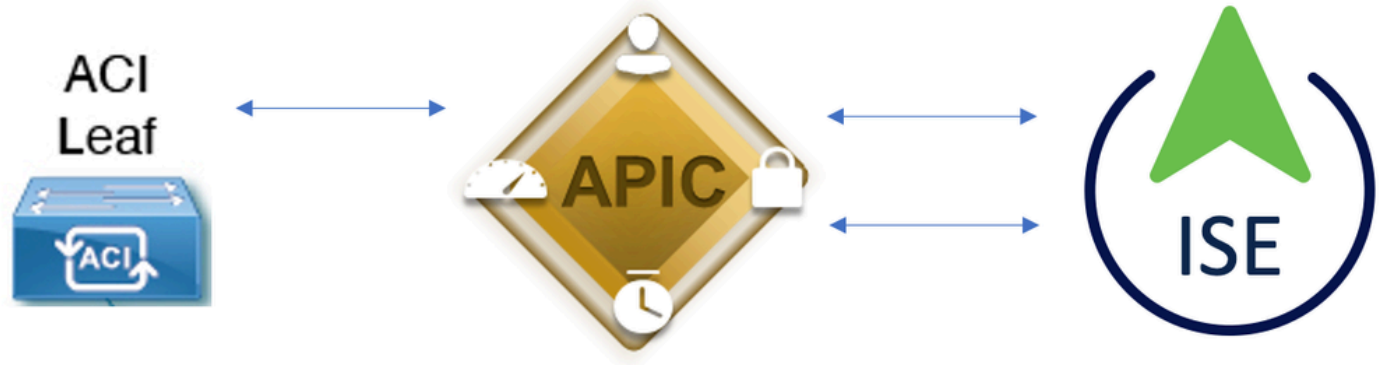


Diagramma integrazione

Procedura di autenticazione

Passaggio 1. Accedere all'applicazione APIC con le credenziali utente di amministratore.

Passaggio 2. Il processo di autenticazione attiva e ISE convalida le credenziali localmente o tramite Active Directory.

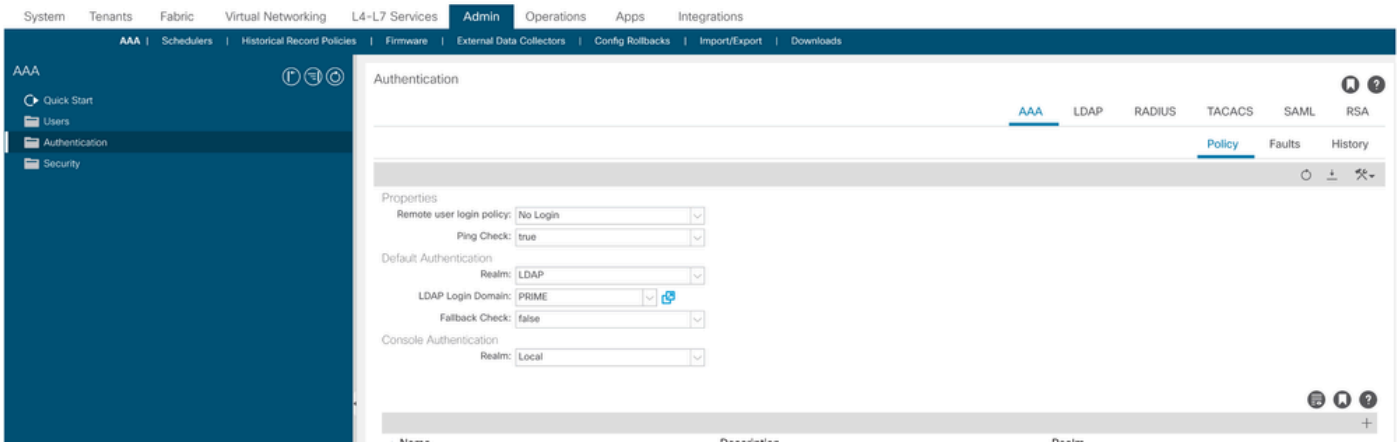
Passaggio 3. Una volta completata l'autenticazione, ISE invia un pacchetto di autorizzazioni per autorizzare l'accesso all'APIC.

Passaggio 4. ISE mostra un log live di autenticazione completato.

Nota: APIC replica la configurazione TACACS+ sugli switch foglia che fanno parte della struttura.

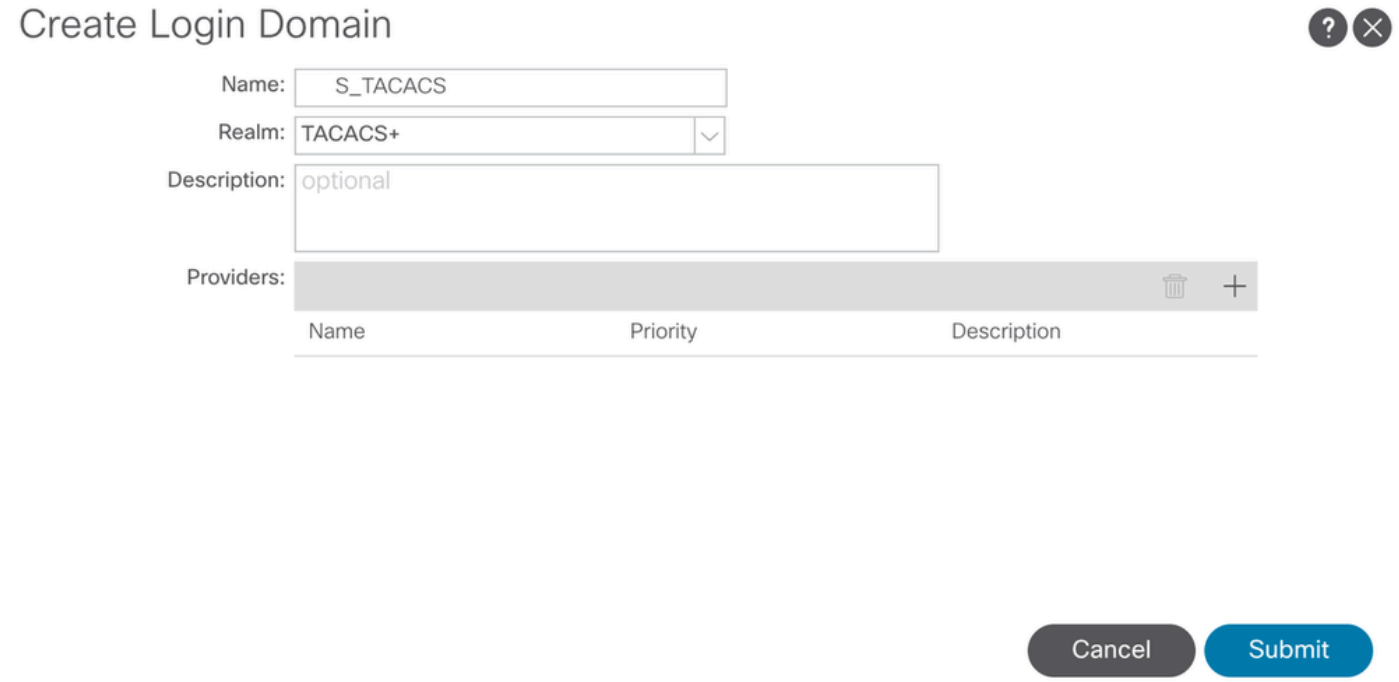
Configurazione APIC

Passaggio 1. Per creare un nuovo dominio di accesso, passare allAdmin > AAA > Authentication > AAA'icona e scegliere+tale icona.

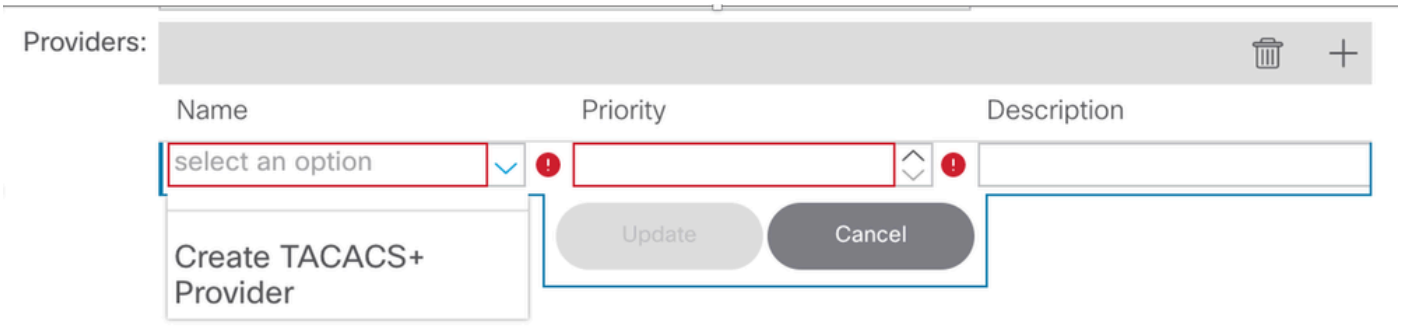


Configurazione dell'amministratore dell'accesso APIC

Passaggio 2. Definire un nome e un realm per il nuovo dominio di accesso e fare clic su+in Provider per creare un nuovo provider.



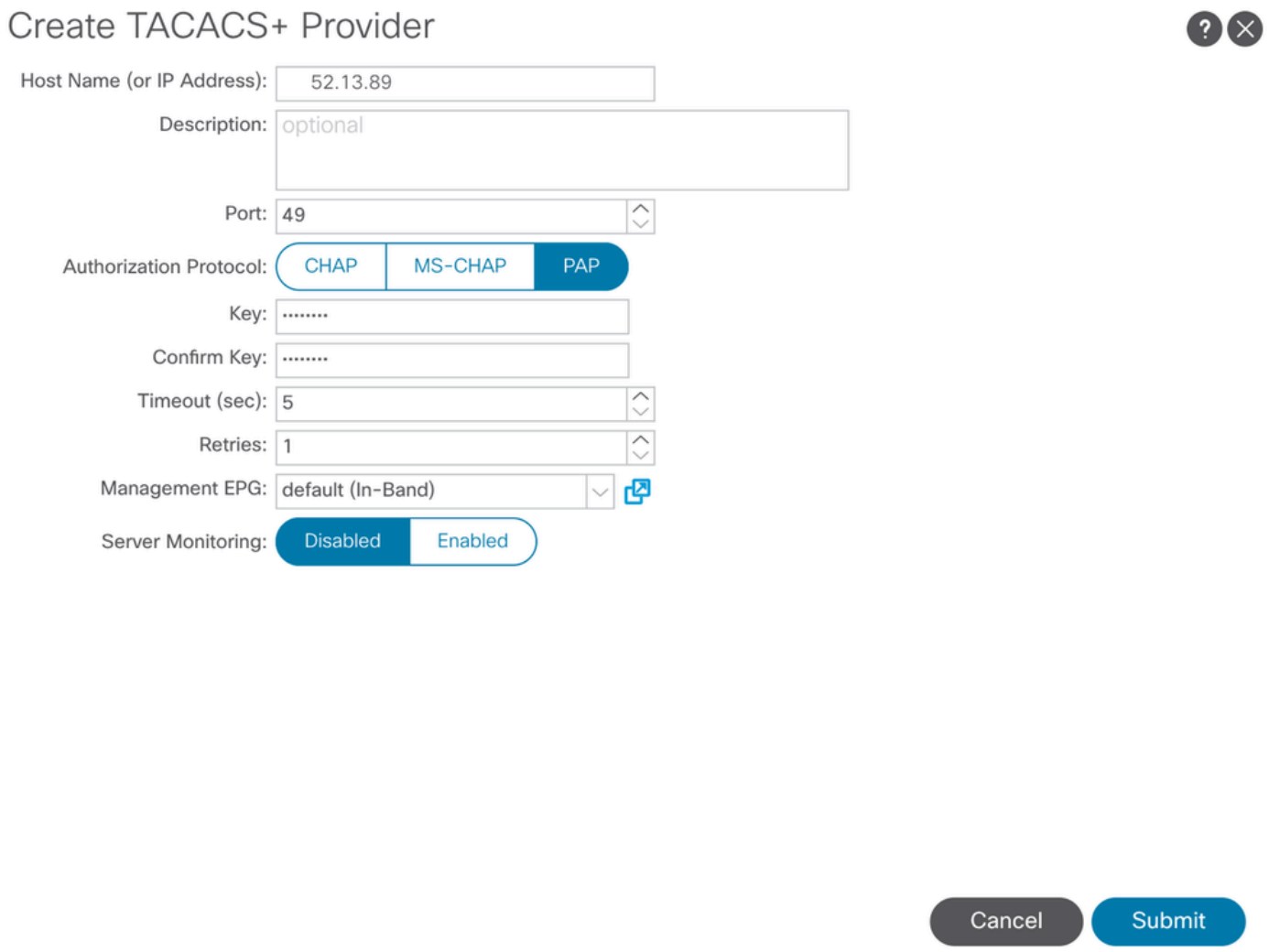
Amministratore accesso APIC



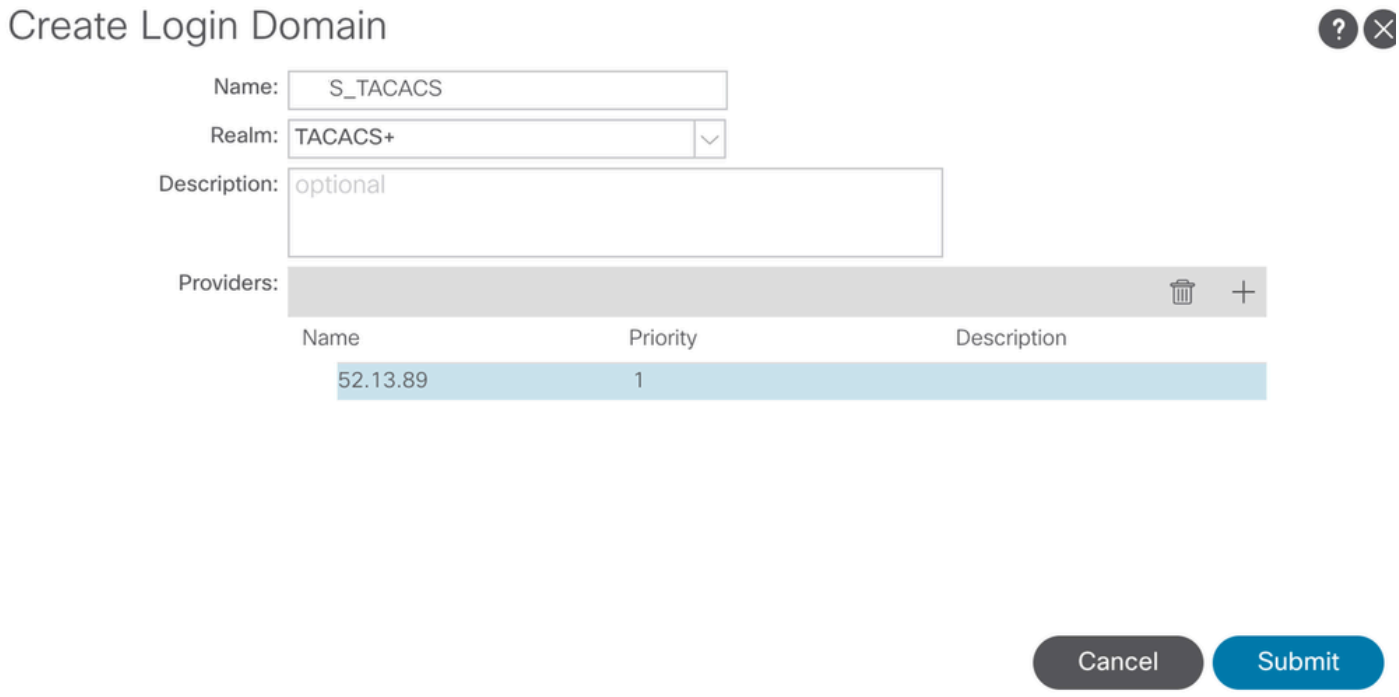
Provider TACACS APIC

Passaggio 3. Definire l'indirizzo IP o il nome host ISE, definire un segreto condiviso e scegliere il

gruppo di criteri endpoint di gestione (EPG). Fare clicSubmitper aggiungere il provider TACACS+ all'account admin.



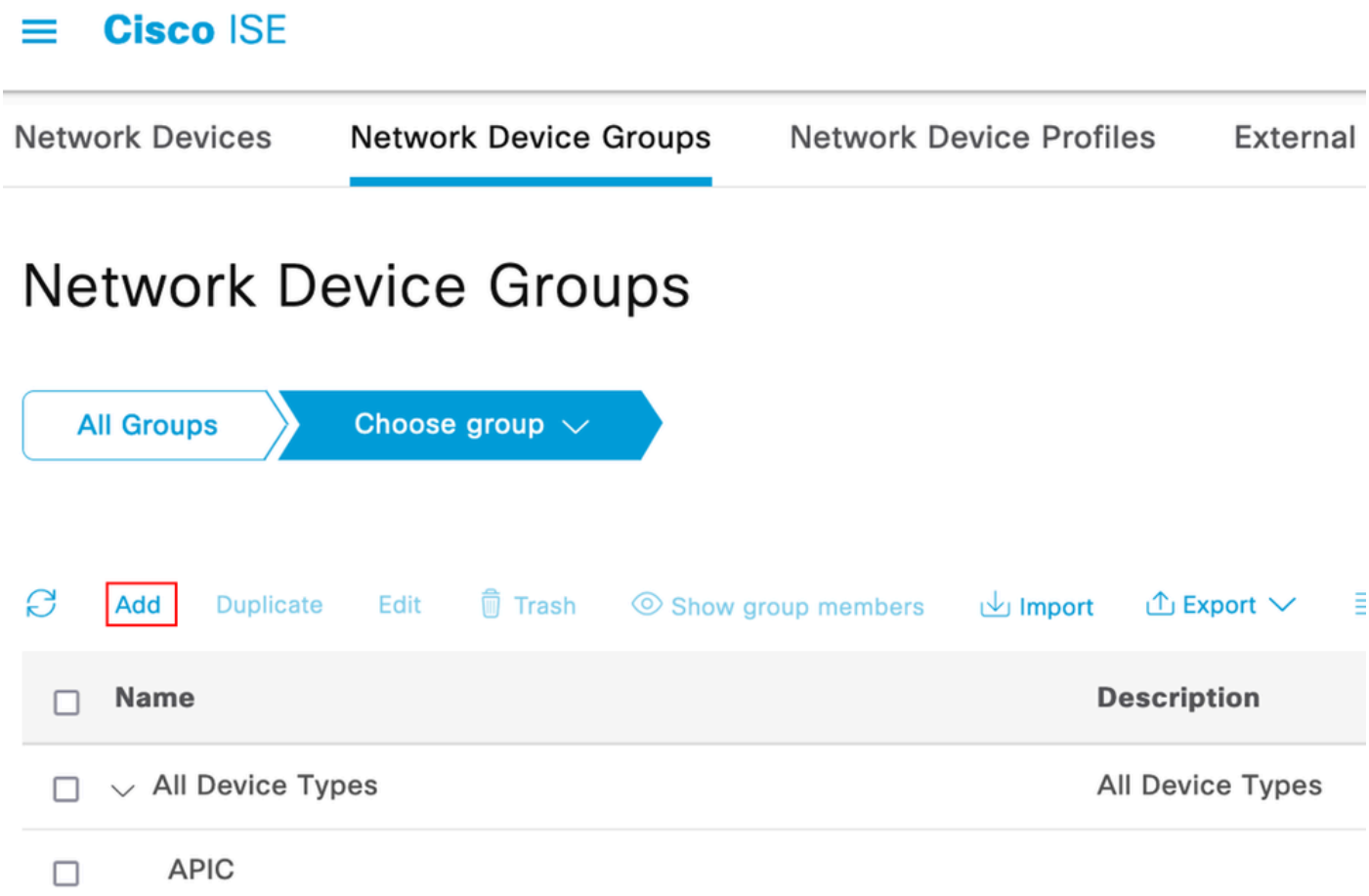
Impostazioni provider TACACS APIC



Visualizzazione provider TACACS

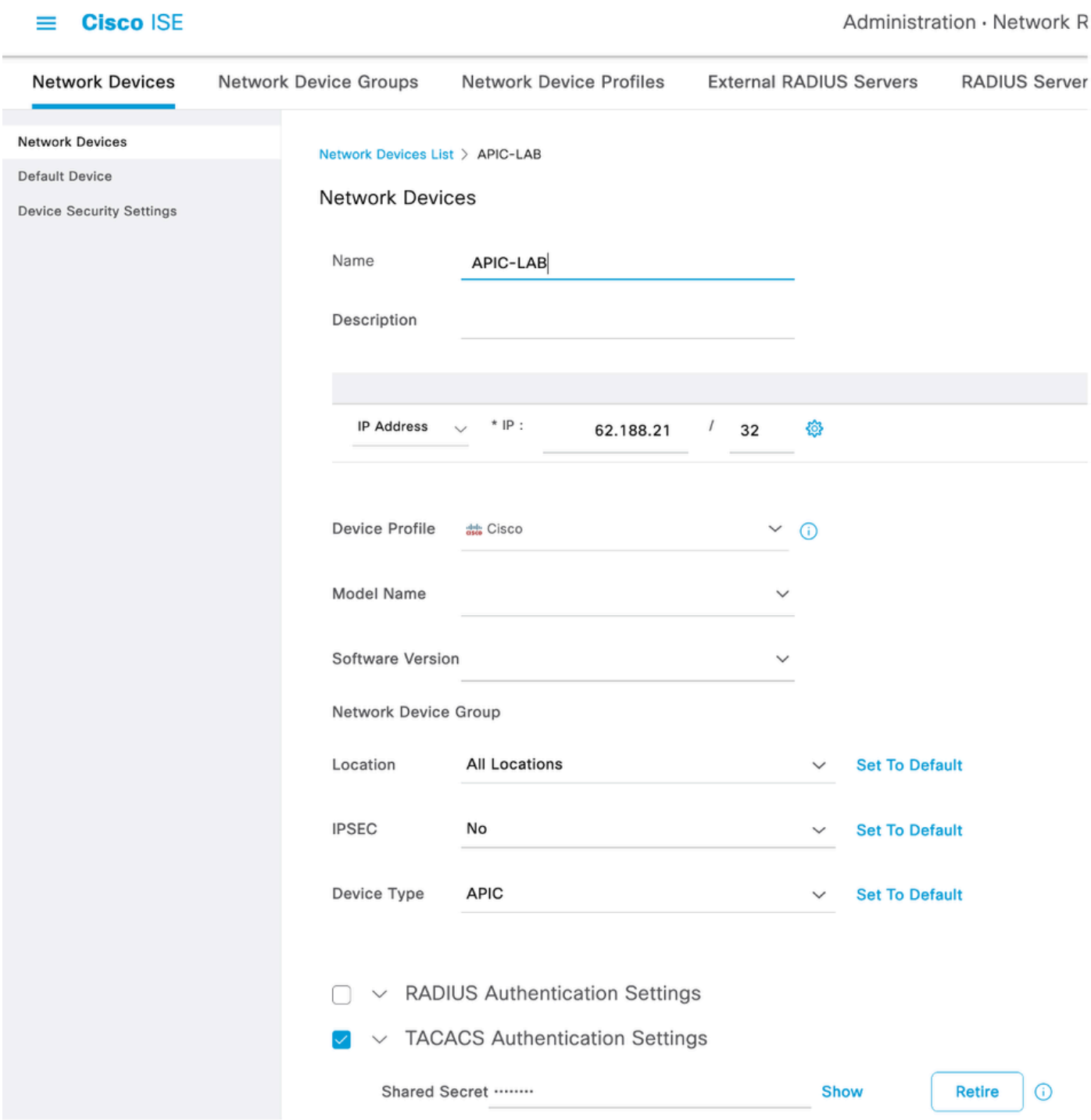
Configurazione di ISE

Passaggio 1. Passare a purtroppo>Amministrazione > Risorse di rete > Gruppi di dispositivi di rete. Creare un gruppo di dispositivi di rete in Tutti i tipi di dispositivi.



ISE Network Device Group

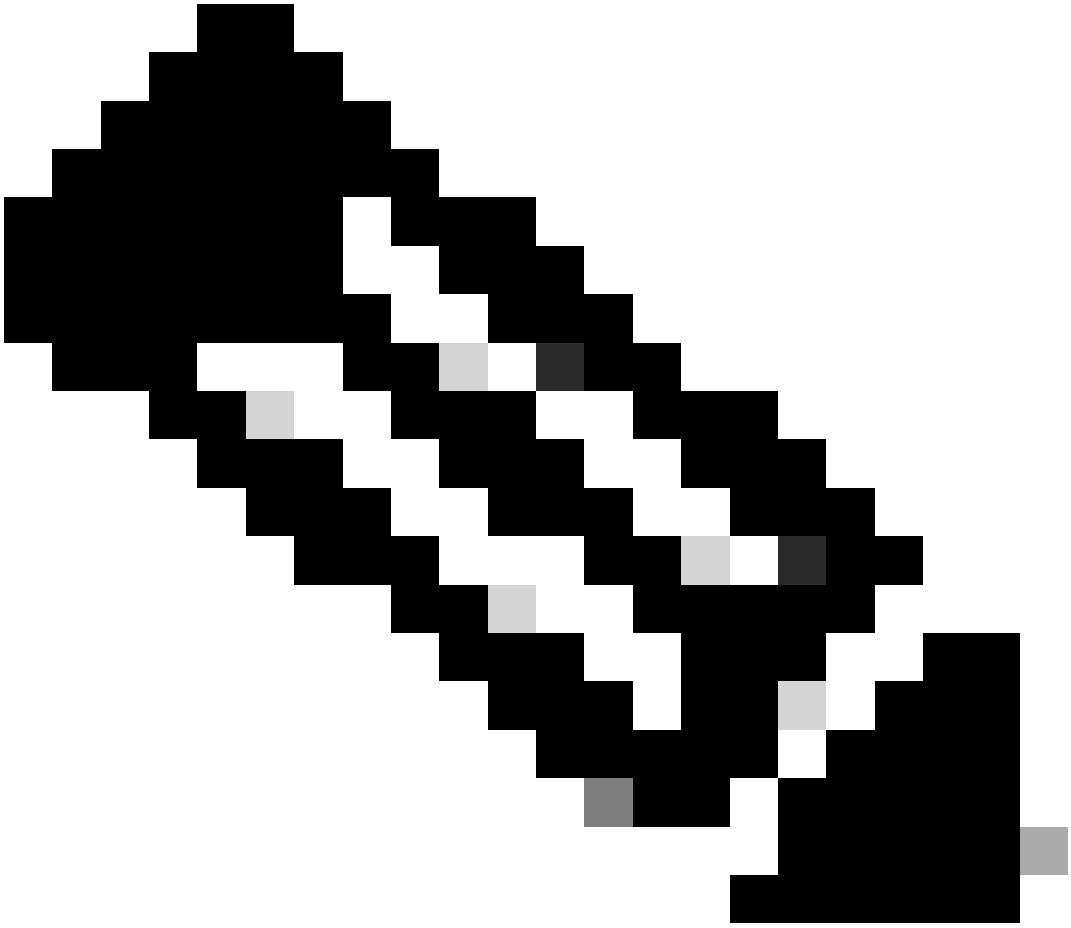
Passaggio 2. Passare aAdministration > Network Resources > Network Devices. SelezionareAdddefine APIC Name and IP address, scegliere APIC in Device Type and TACACS+ checkbox, quindi definire la password da usare nella configurazione del provider TACACS+ per APIC. Fare clic su .Submit



Ripetere i passaggi 1 e 2 per gli switch foglia.

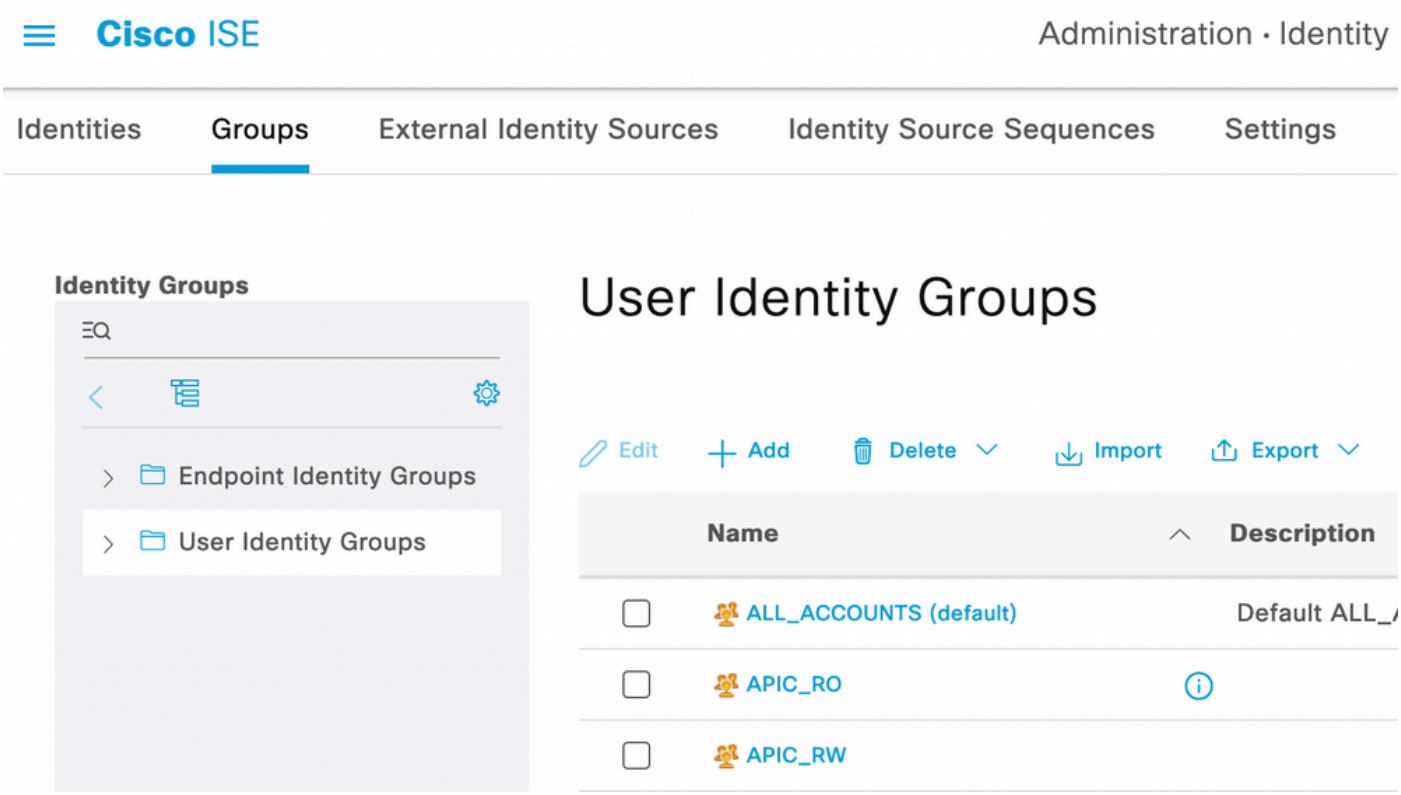
Passaggio 3. Per integrare ISE con Active Directory, seguire le istruzioni riportate sul collegamento;

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/217351-ad-integration-for-cisco-ise-gui-and-cli.html.



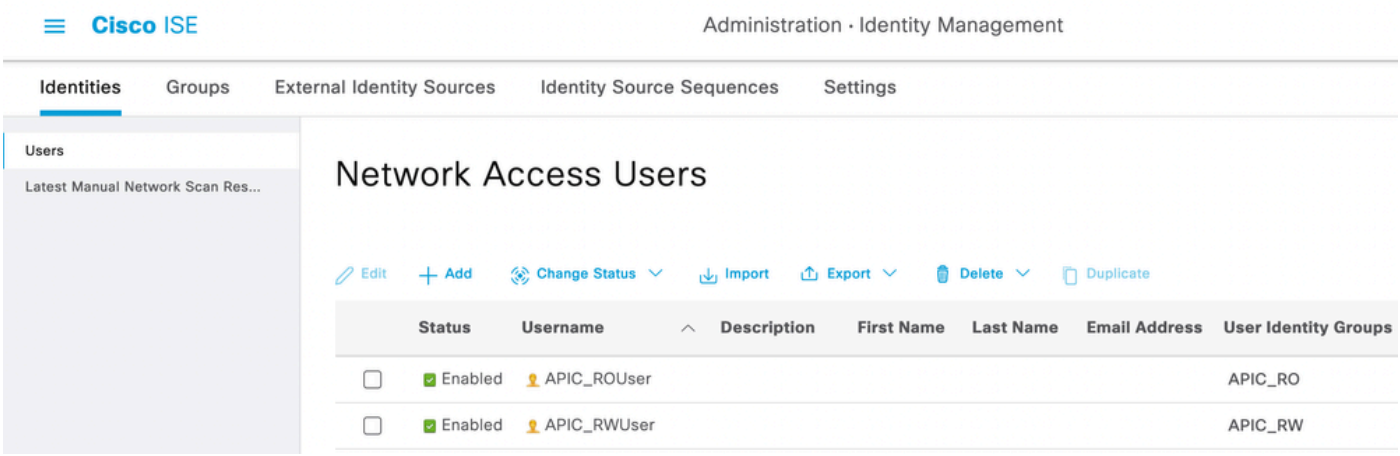
Nota: In questo documento sono inclusi sia gli utenti interni che i gruppi degli amministratori di Active Directory come origini di identità. Tuttavia, il test viene eseguito con l'origine di identità degli utenti interni. Il risultato è lo stesso per i gruppi AD.

Passaggio 4. (Facoltativo) Navigare su Outlook>Administration > Identity Management > Groups. SelezionateUser Identity Groups e fate clic su Add. Creare un gruppo per gli utenti Admin di sola lettura e gli utenti Admin.

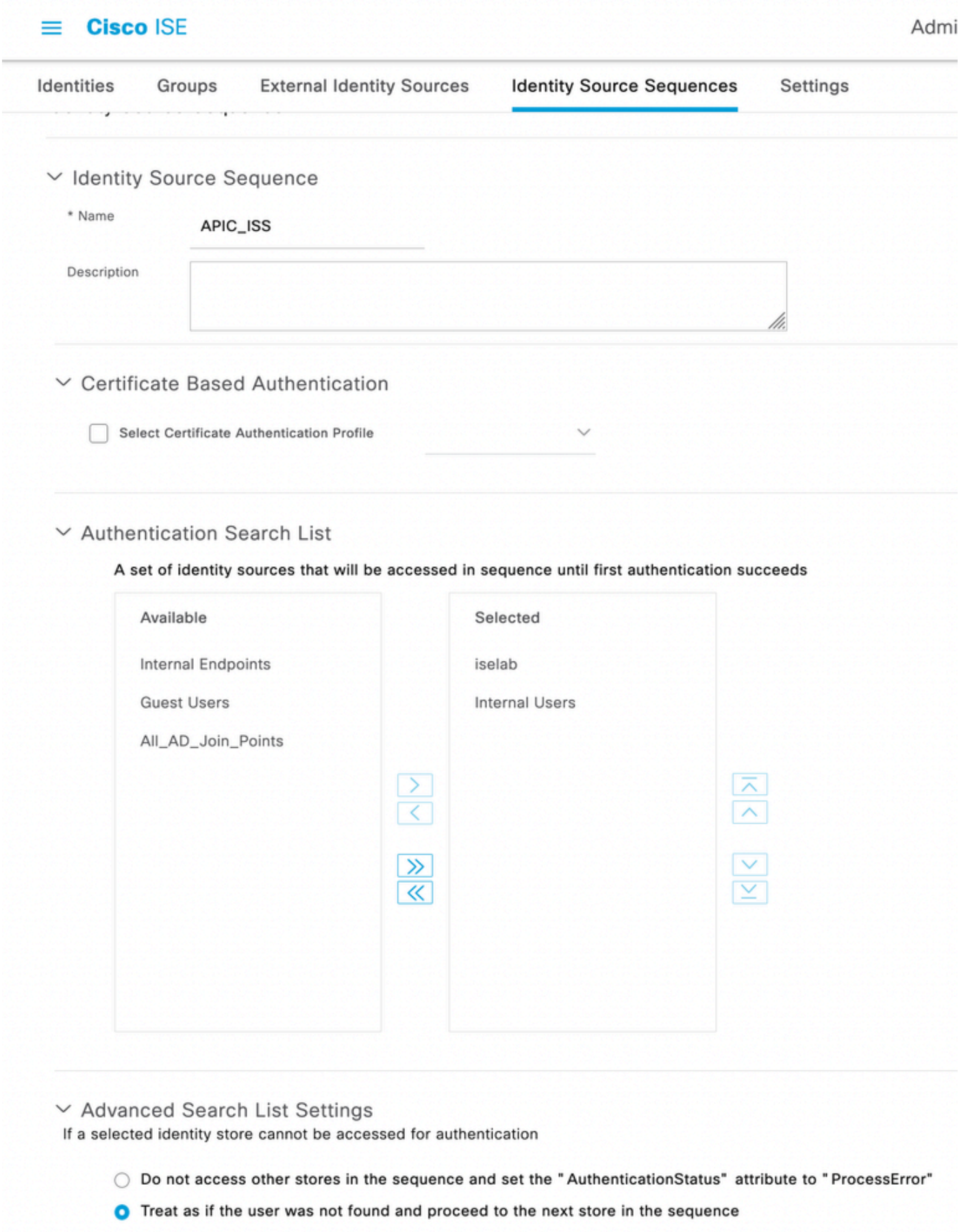


Gruppo di identità

Passaggio 5. (Facoltativo) Passare a >Outlook Administration > Identity Management > Identity.Fare clicAdde creare unRead Only Adminutente e unAdminutente. Assegnare ogni utente a ogni gruppo creato nel passaggio 4.



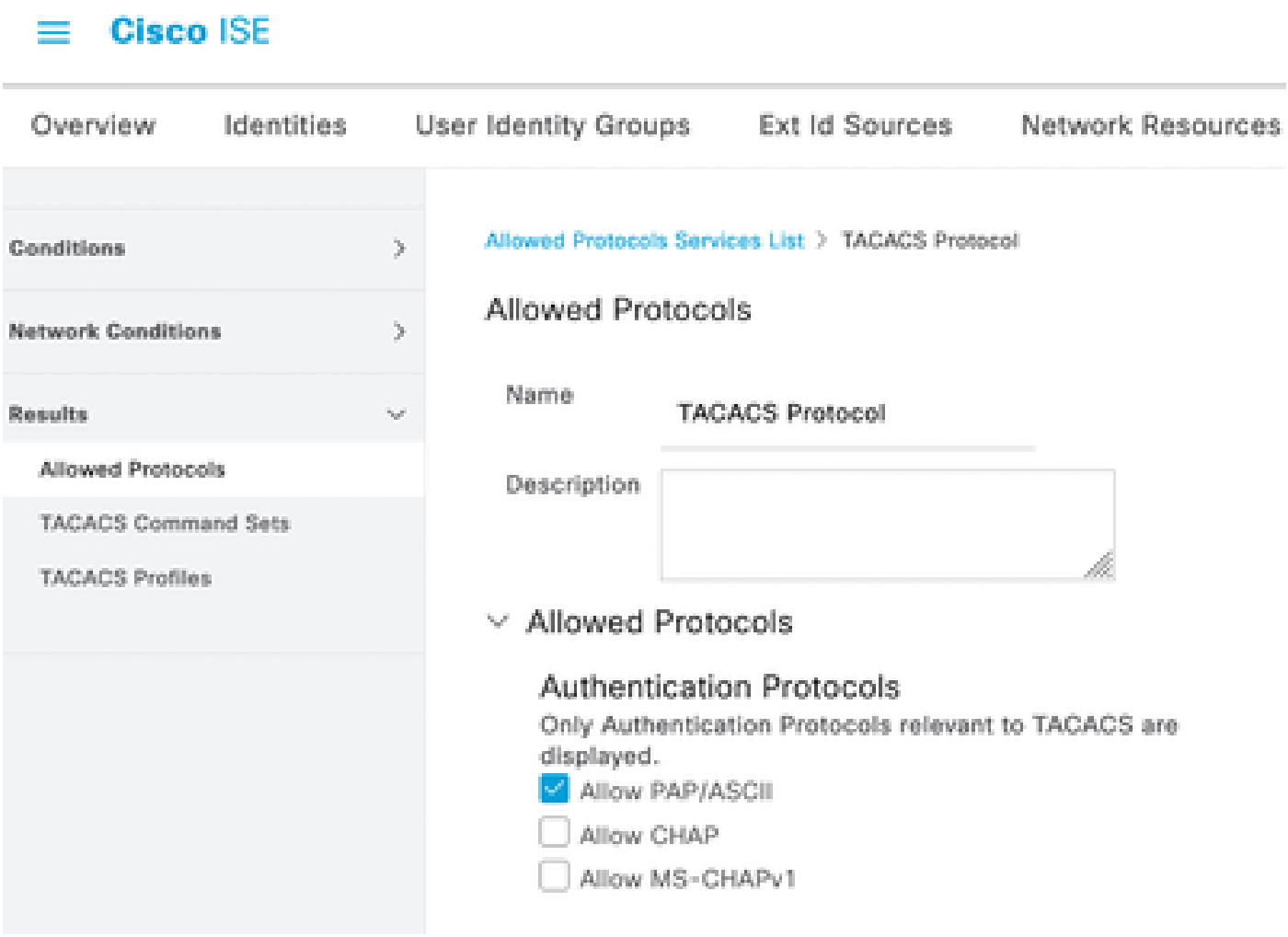
Passaggio 6. Navigare fino a Android>Administration > Identity Management > Identity Source Sequence. ScegliereAddDefinisci nome, quindi scegliereAD Join PointseInternal UsersOrigine identità dall'elenco. SelezionareTreat as if the user was not found and proceed to the next store in the sequencesottoAdvanced Search List Settingse fare clic suSave.



Sequenza origine identità

7. Passare a ☰>**Work Centers** > **Device Administration** > **Policy Elements** > **Results** > **Allowed Protocols**. Selezionare

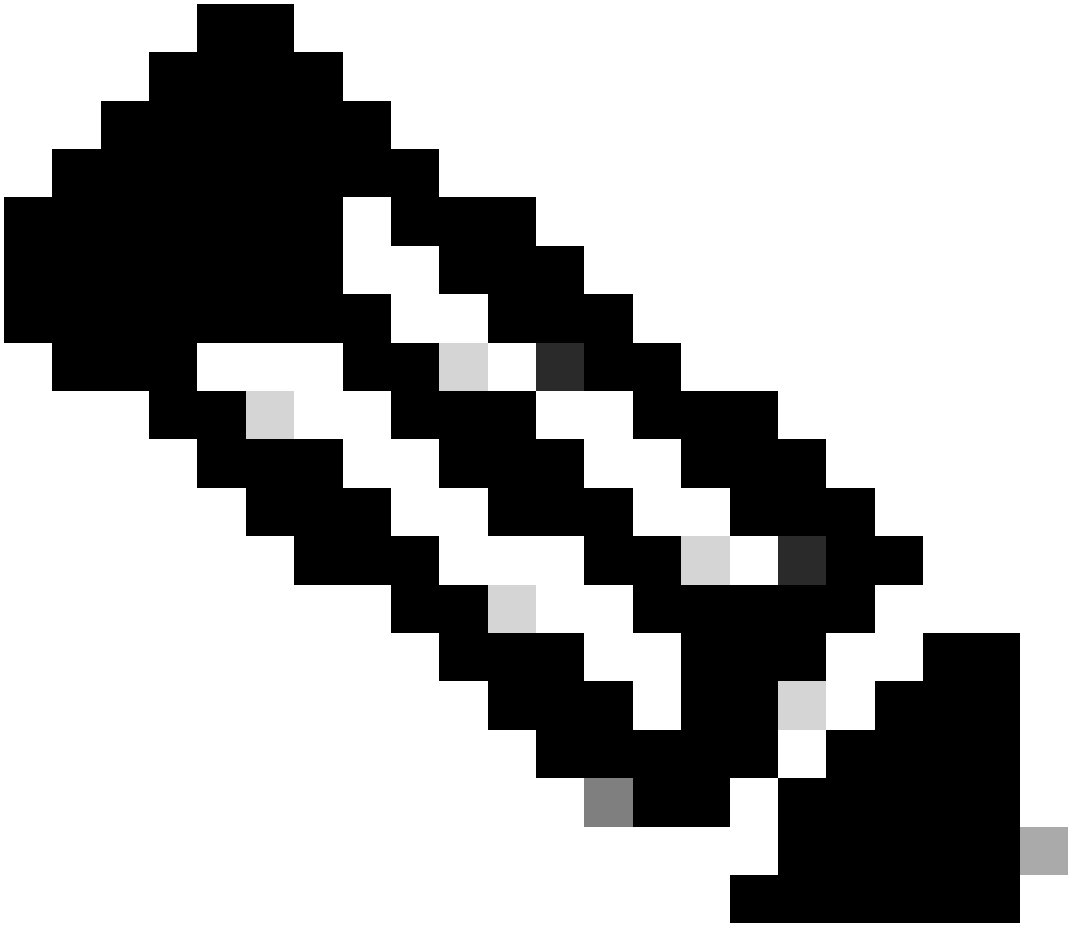
Aggiungi, definire un nome e deselezionare Consenti CHAP e Consenti MS-CHAPv1 dall'elenco dei protocolli di autenticazione. Selezionare Salva.



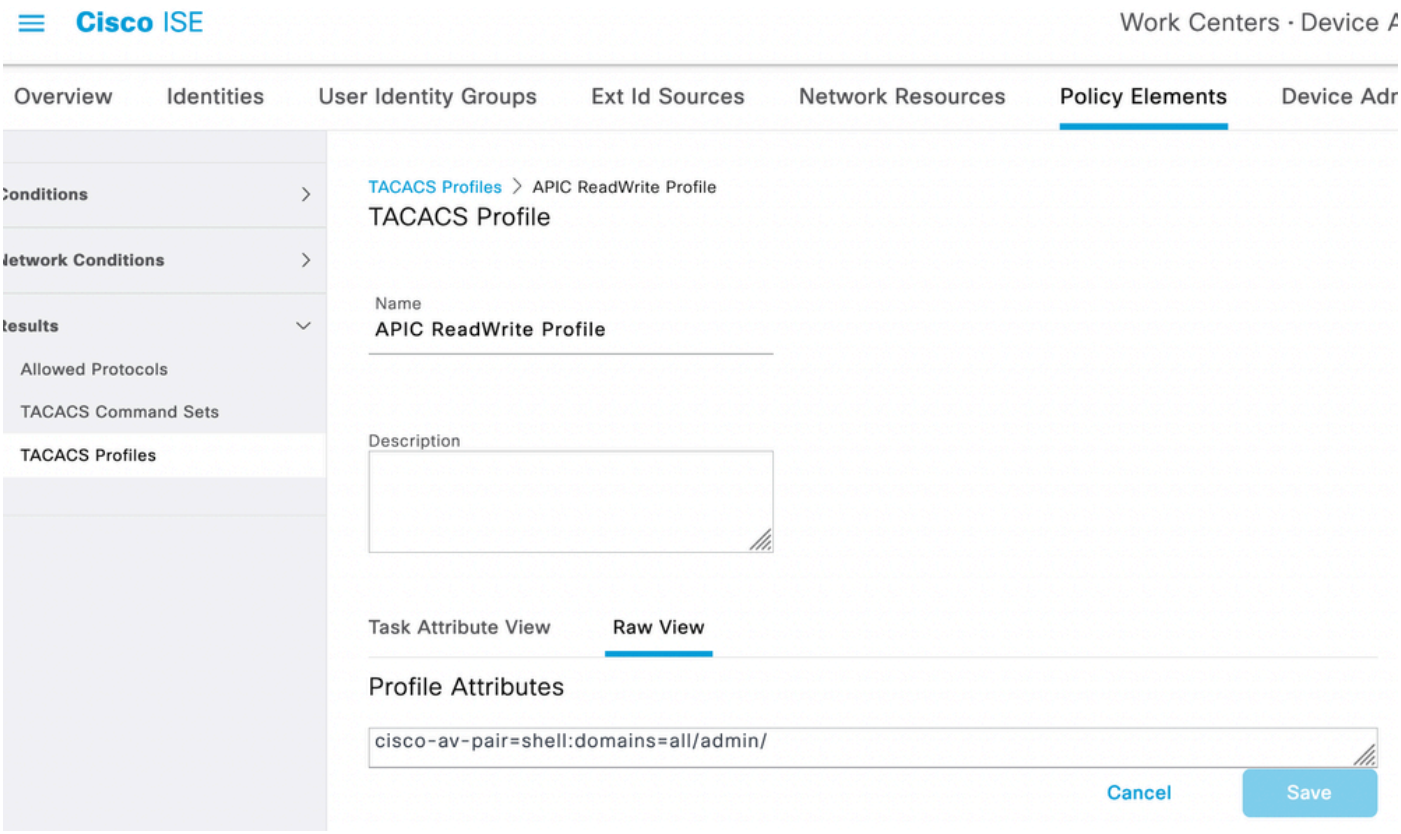
TACACS - Consenti protocollo

8. Navigare fino a>Aeroporto di AtlantaWork Centers > Device Administration > Policy Elements > Results > TACACS Profile. Fare clic suadde creare due profili in base agli attributi presenti nell'elenco inRaw View. Fare clic su .Save

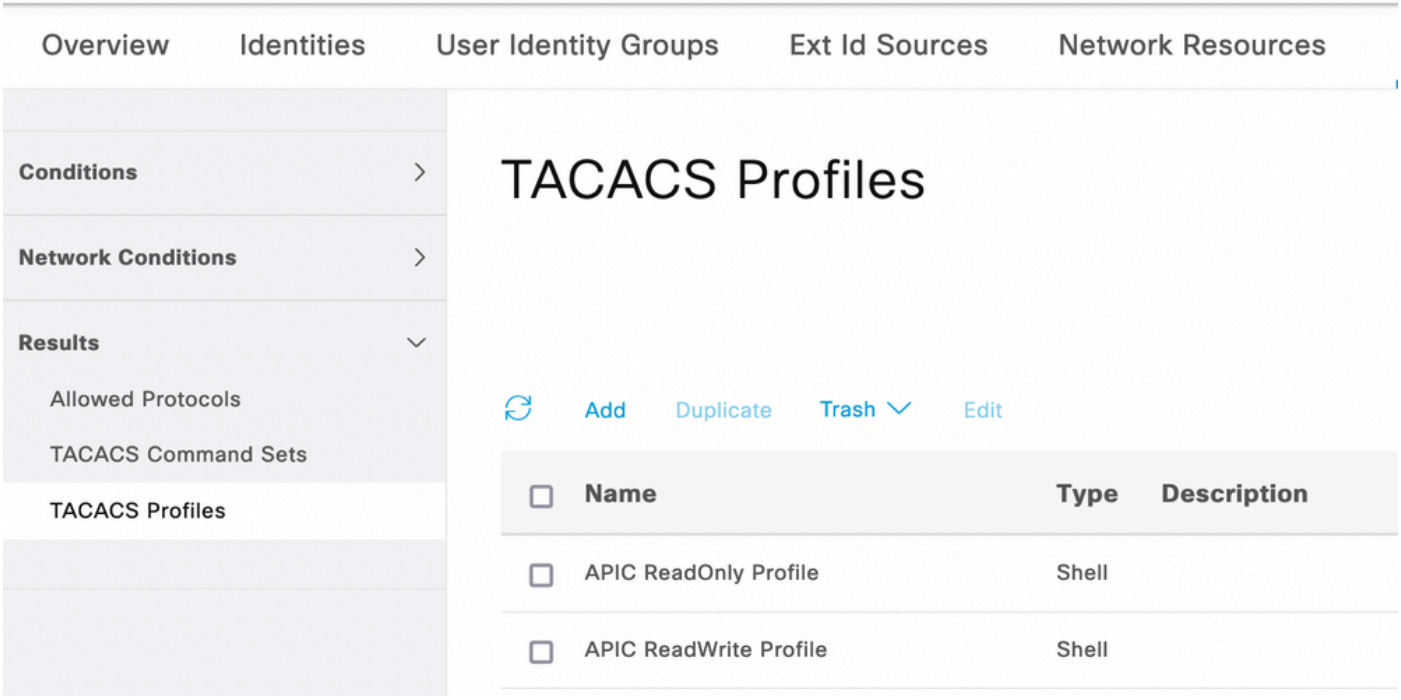
- Utente amministratore: cisco-av-pair=shell:domains=all/admin/
- Utente amministratore di sola lettura: cisco-av-pair=shell:domains=all//read-all



Nota: In caso di spazio o caratteri aggiuntivi, la fase di autorizzazione ha esito negativo.

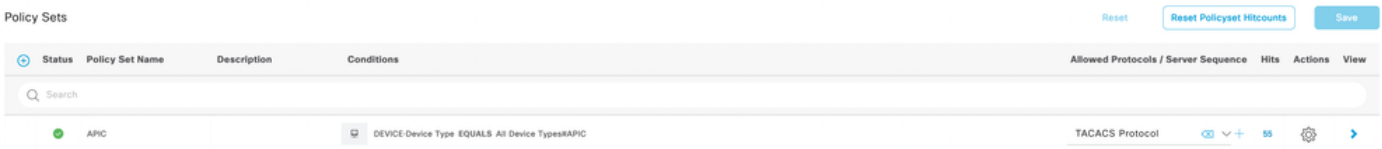


Profilo TACACS



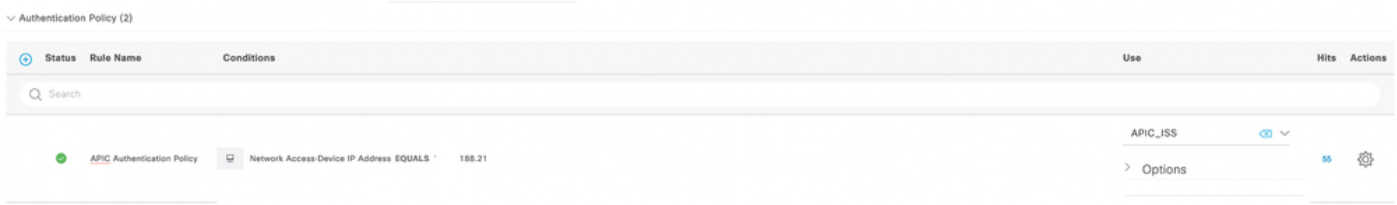
Profili Amministratore TACACS e Amministratore di sola lettura

Passaggio 9. Navigare fino a recentemente>Work Centers > Device Administration > Device Admin Policy Set. Creare un nuovo set di criteri, definire un nome e scegliere il tipo di dispositivoAPICcreato nel passaggio 1. ScegliereTACACS Protocolcreato nel passaggio 7. come protocollo consentito, quindi fare clic suSave.

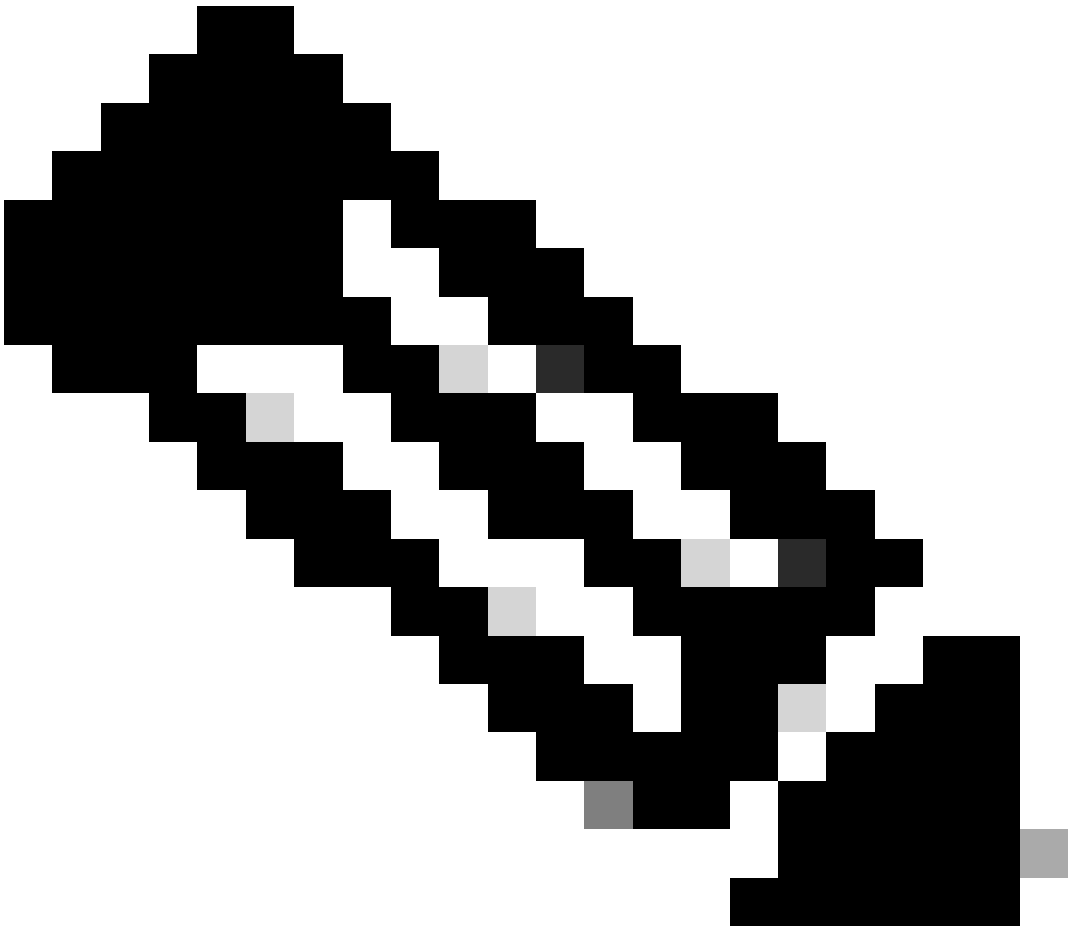


Set di criteri TACACS

Passaggio 10. In NuovoPolicy Setfare clic sulla freccia destra>e creare un criterio di autenticazione. Definite un nome e scegliete l'indirizzo IP del dispositivo come condizione. Scegliere quindi la sequenza di origine delle identità creata al passo 6.

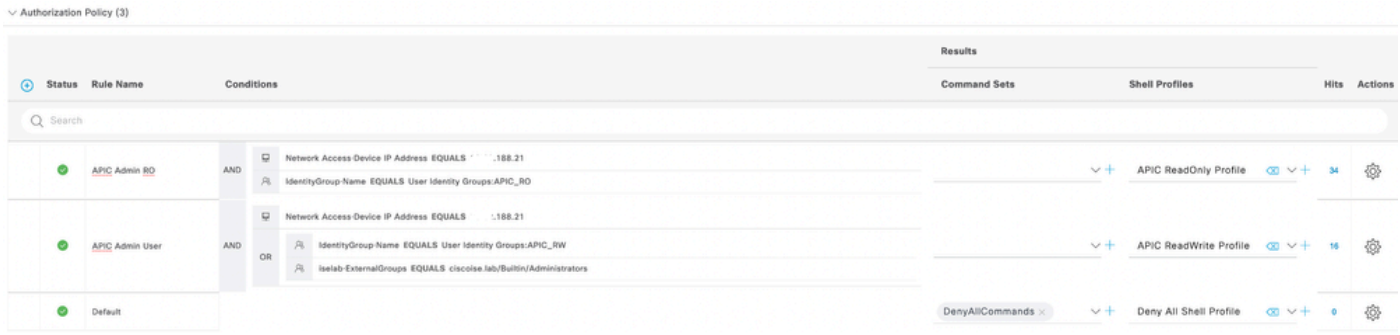


Criterio di autenticazione



Nota: La posizione o altri attributi possono essere utilizzati come condizione di autenticazione.

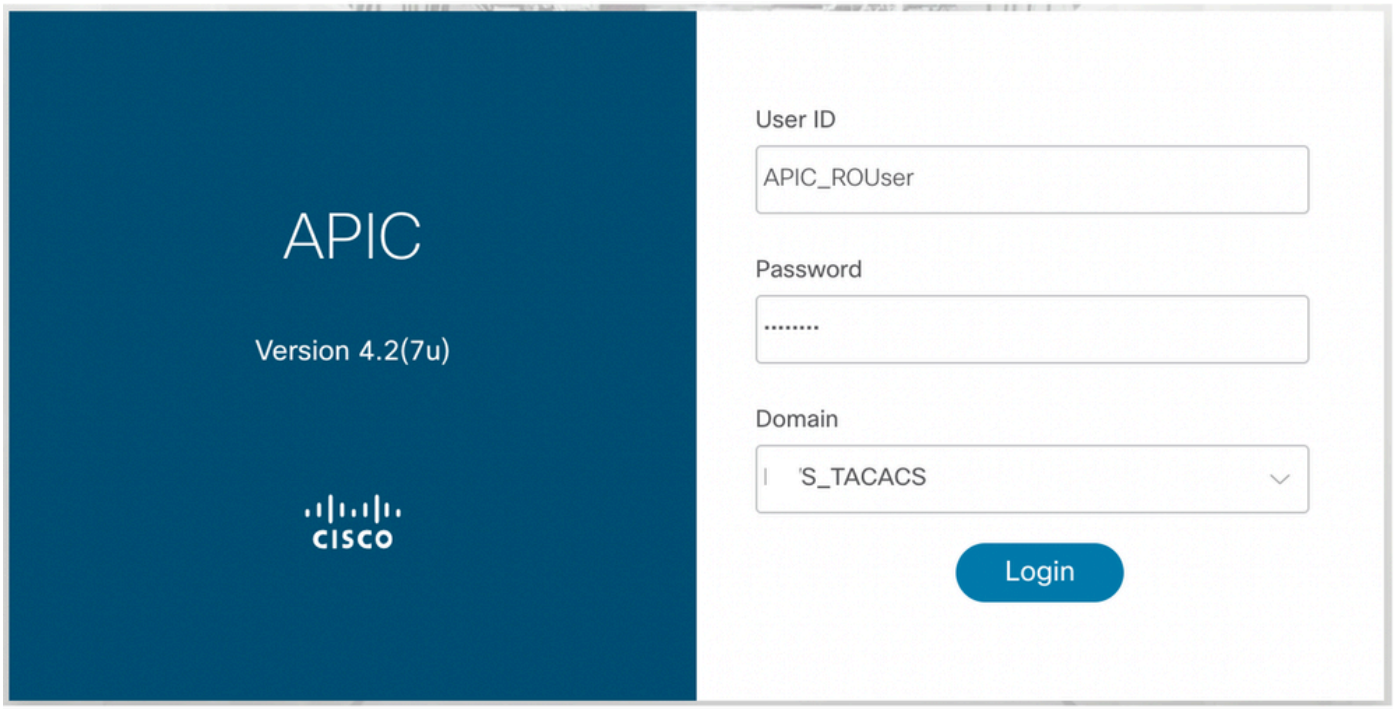
Passaggio 11. Creare un profilo di autorizzazione per ogni tipo di utente Amministratore, definire un nome e scegliere un utente interno e/o un gruppo di utenti AD come condizione. È possibile utilizzare condizioni aggiuntive, ad esempio APIC. Scegliere il profilo della shell appropriato in ogni criterio di autorizzazione e fare clic suSave.



Profilo di autorizzazione TACACS

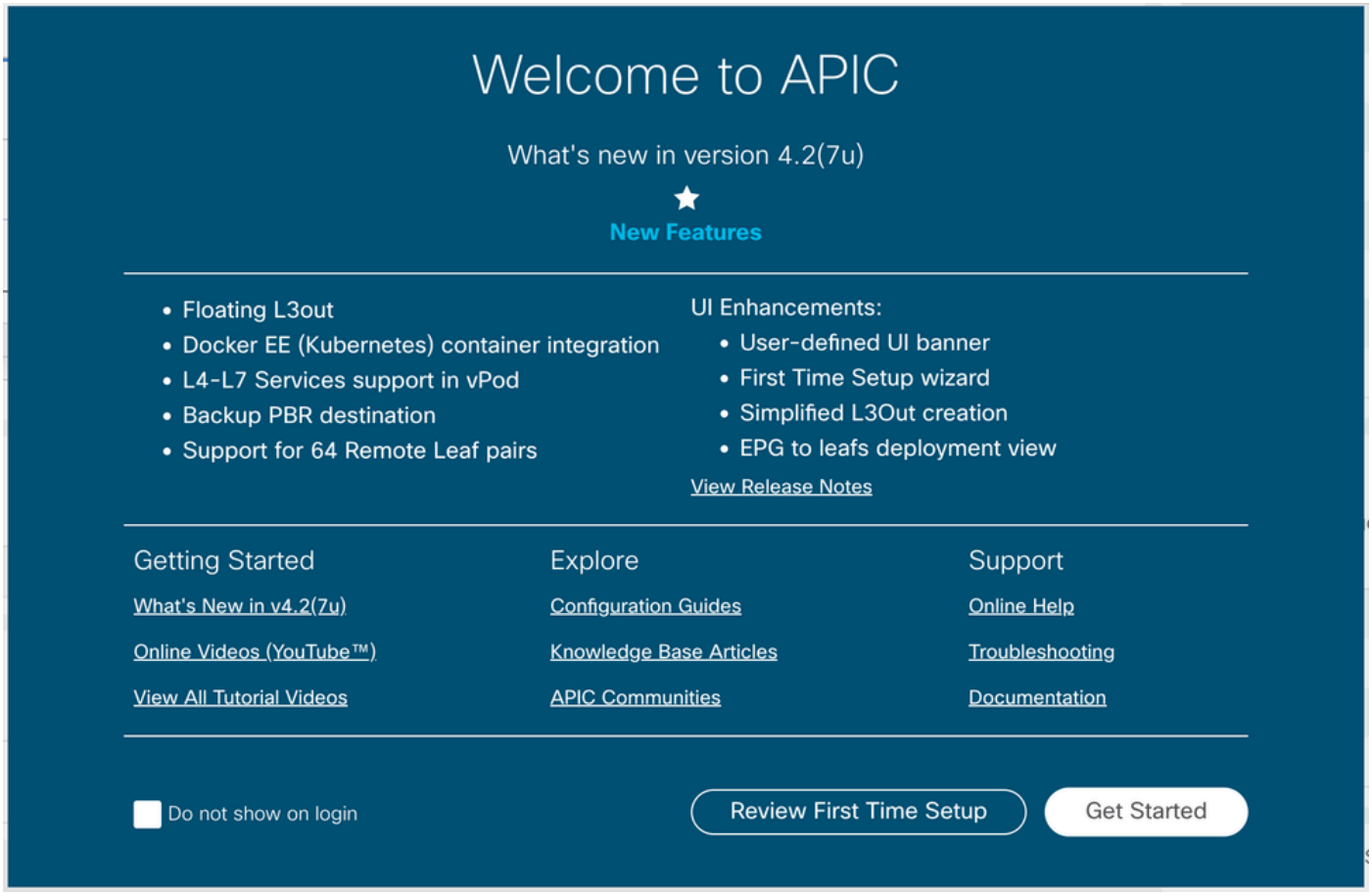
Verifica

Passaggio 1. Accedere all'interfaccia utente APIC con le credenziali User Admin. Selezionare l'opzione TACACS dall'elenco.



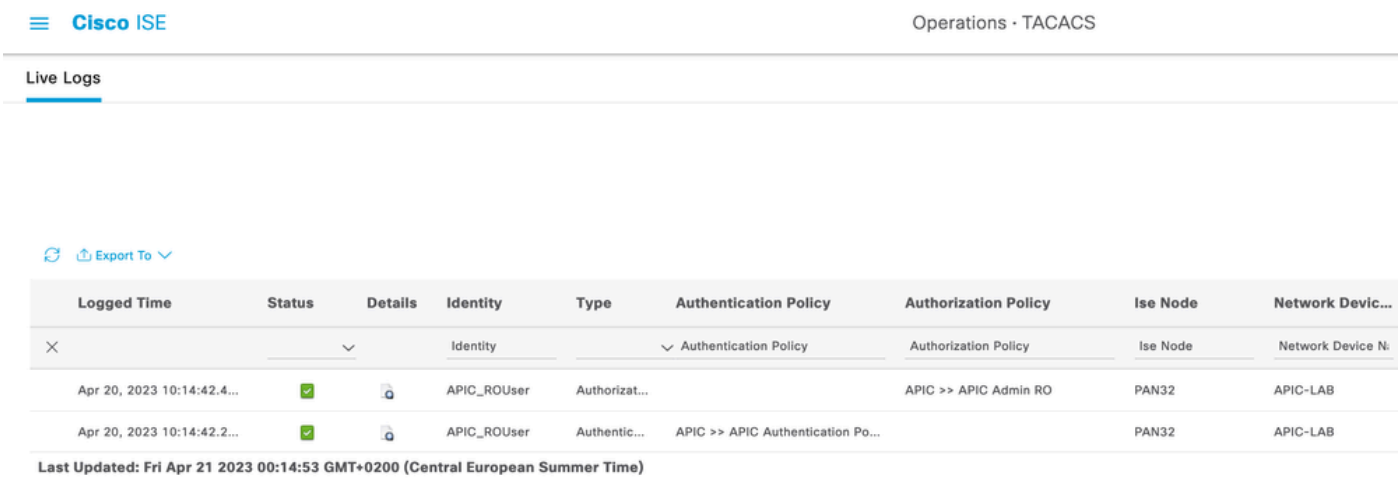
Log in APIC

Passaggio 2. Verificare l'accesso sull'interfaccia utente APIC e l'applicazione dei criteri appropriati ai log TACACS Live.



messaggio di benvenuto APIC

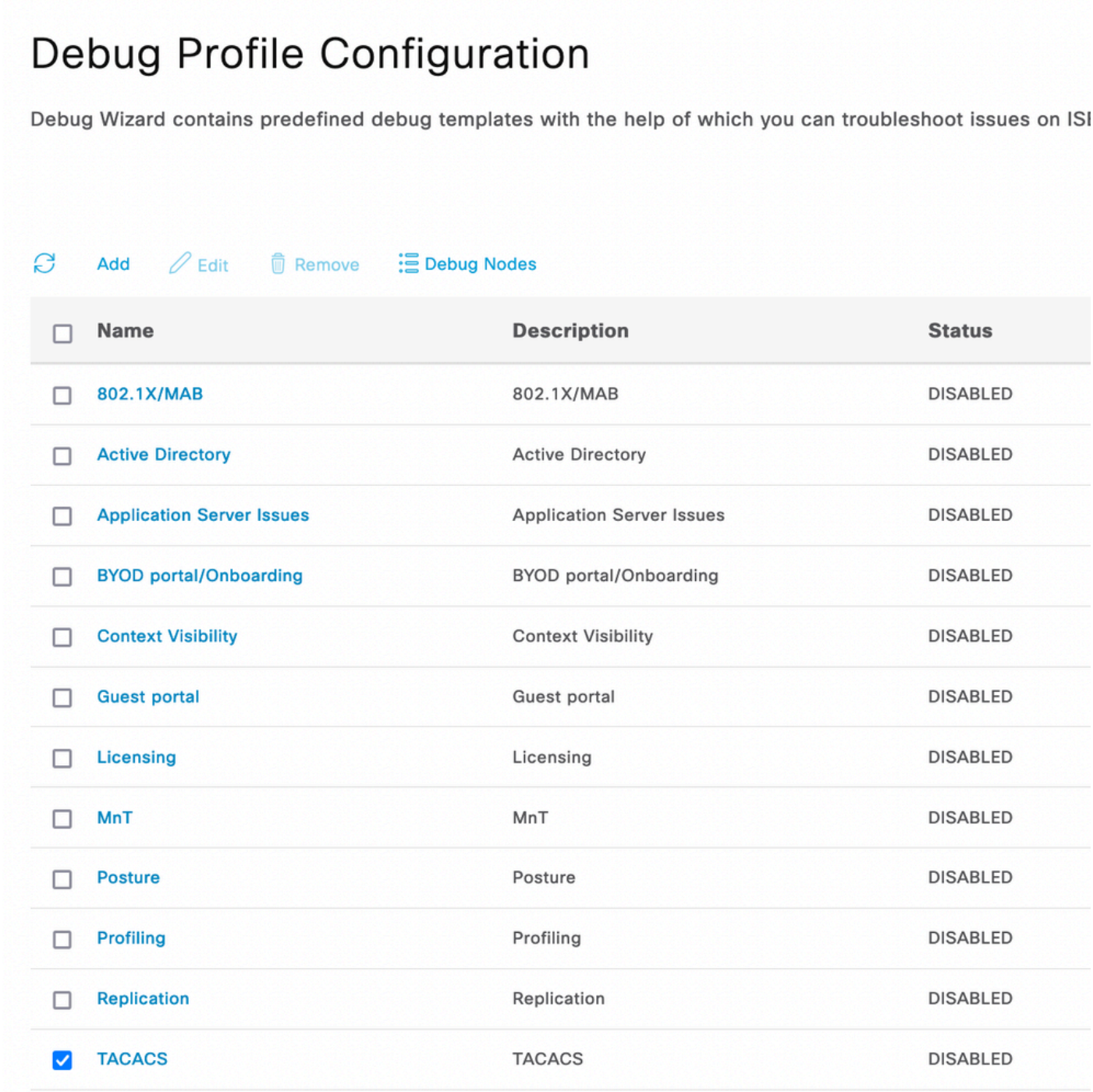
Ripetere i passaggi 1 e 2 per gli utenti Amministratore di sola lettura.



Log TACACS+ Live

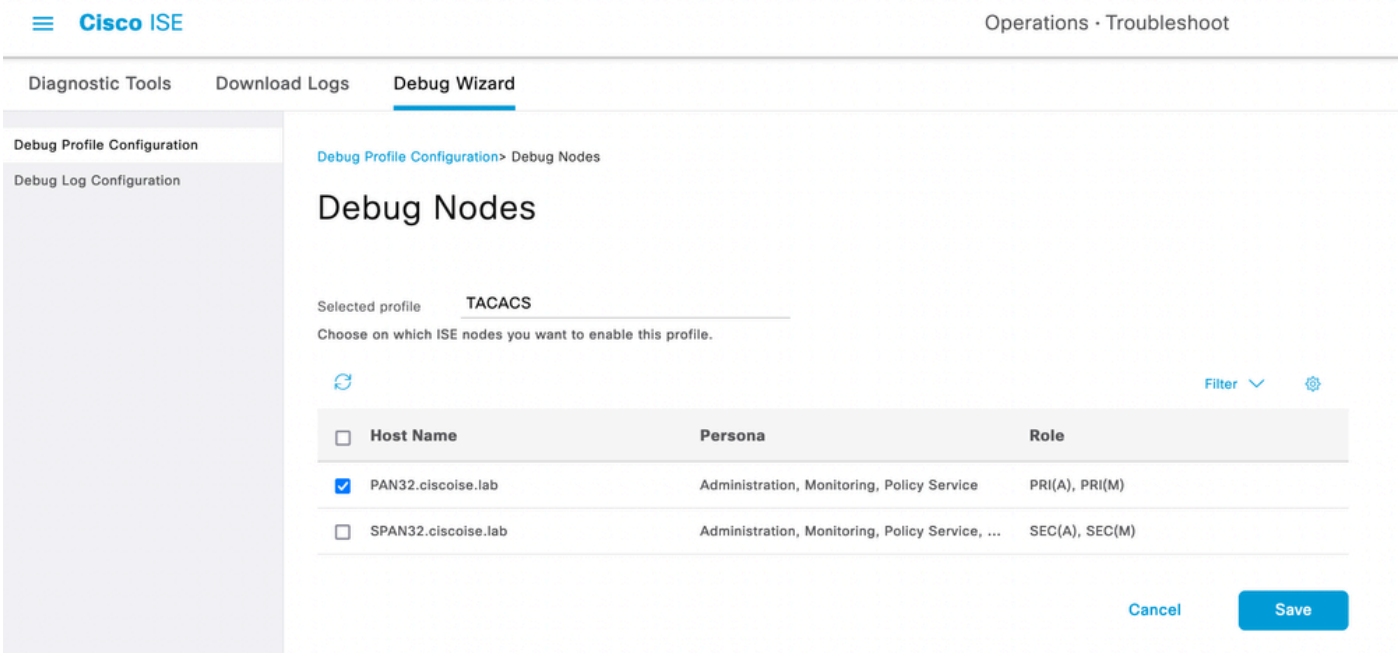
Risoluzione dei problemi

Passaggio 1. Navigare fino a Android>Operations > Troubleshoot > Debug Wizard. SelezionateTACACSe fate clic su Debug Nodes.



Configurazione profilo di debug

Passaggio 2. Scegliere il nodo che riceve il traffico e fare clic suSave.



Selezione nodi di debug

Passaggio 3. Eseguire un nuovo test e scaricare i log in Operations > Troubleshoot > Download logs come mostrato:

```
AcsLogs,2023-04-20 22:17:16,866,DEBUG,0x7f93cabc7700,cntx=0004699242,sesn=PAN32/469596415/70,CPMSessionI
```

Se nei debug non vengono visualizzate le informazioni di autenticazione e autorizzazione, verificare quanto segue:

1. Il servizio Amministrazione dispositivi è abilitato sul nodo ISE.
2. L'indirizzo IP ISE corretto è stato aggiunto alla configurazione APIC.
3. Se al centro si trova un firewall, verificare che la porta 49 (TACACS) sia autorizzata.

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).