Configurazione dell'autenticazione ISE Radius per Secure Firewall Chassis Manager (FCM)

Sommario

Introduzione

In questo documento viene descritto il processo di configurazione dell'accesso con Autorizzazione/Autenticazione Radius per Secure Firewall Chassis Manager con ISE.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Secure Firewall Chassis Manager (FCM)
- Cisco Identity Services Engine (ISE)
- Autenticazione Radius

Componenti usati

- Cisco Firepower 4110 Security Appliance FXOS v2.12
- Patch 4 di Cisco Identity Services Engine (ISE) v3.2

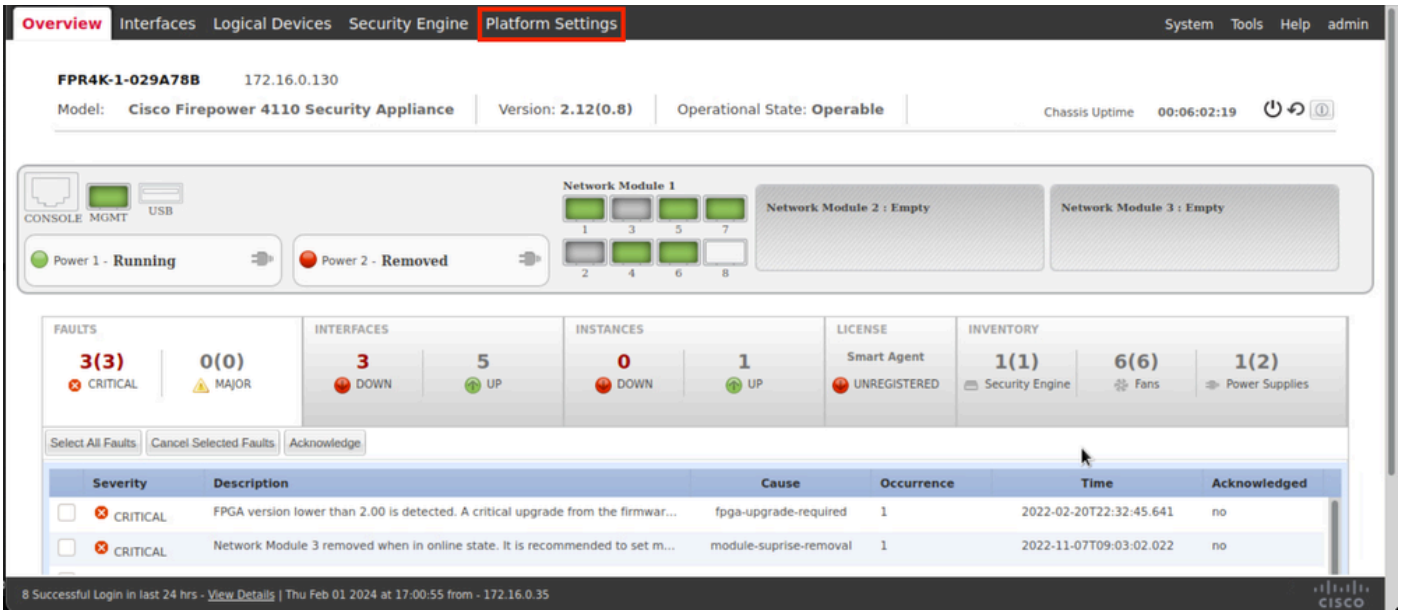
  Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

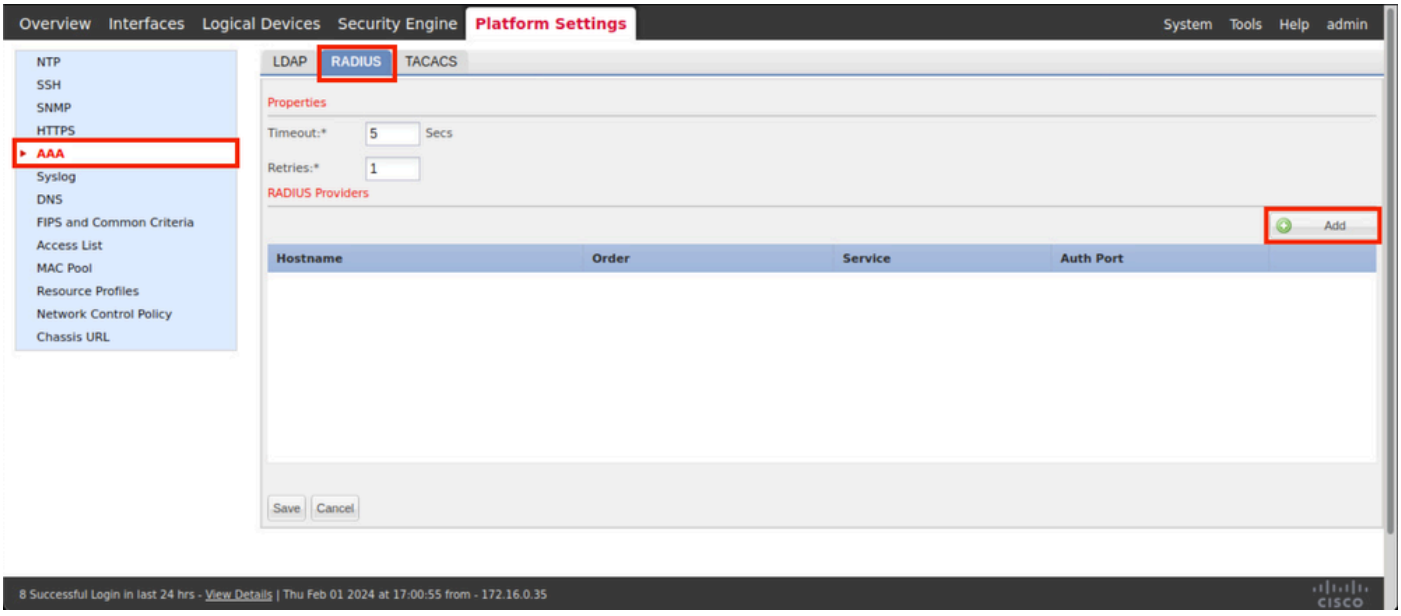
Configurazioni

Secure Firewall Chassis Manager

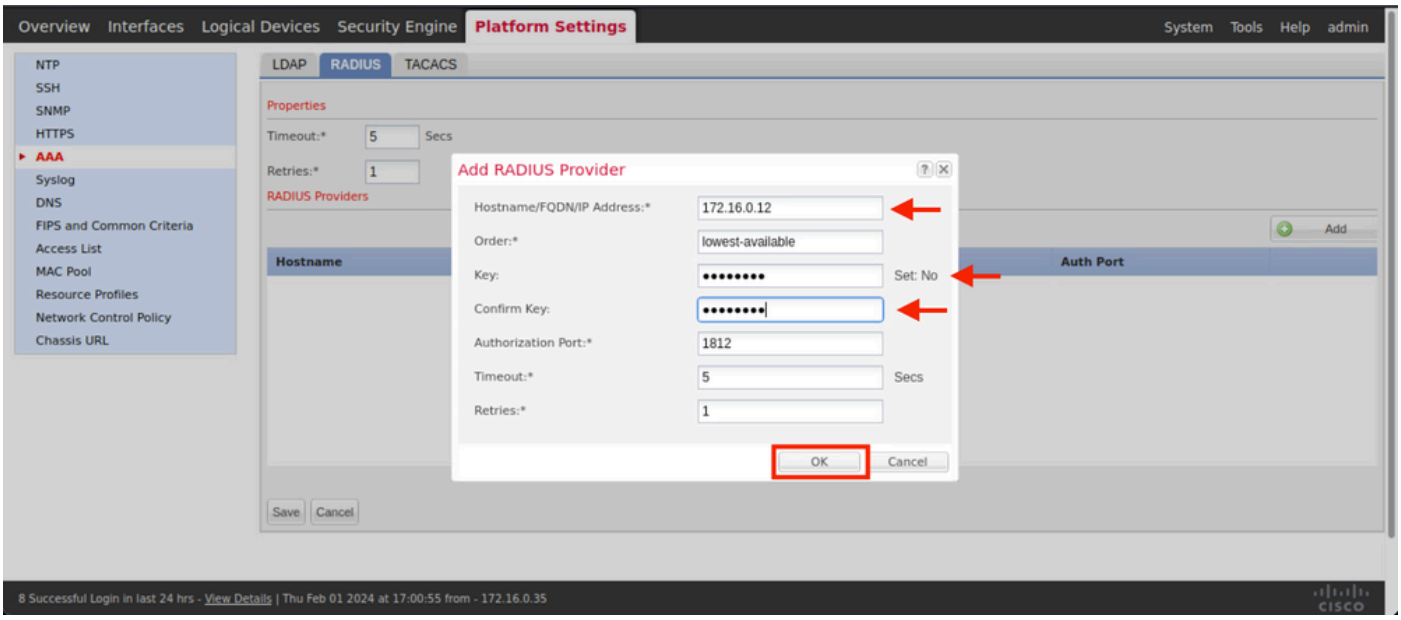
Passaggio 1. Accedere all'interfaccia utente di Firepower Chassis Manager.
Passaggio 2. Passa a Impostazioni piattaforma



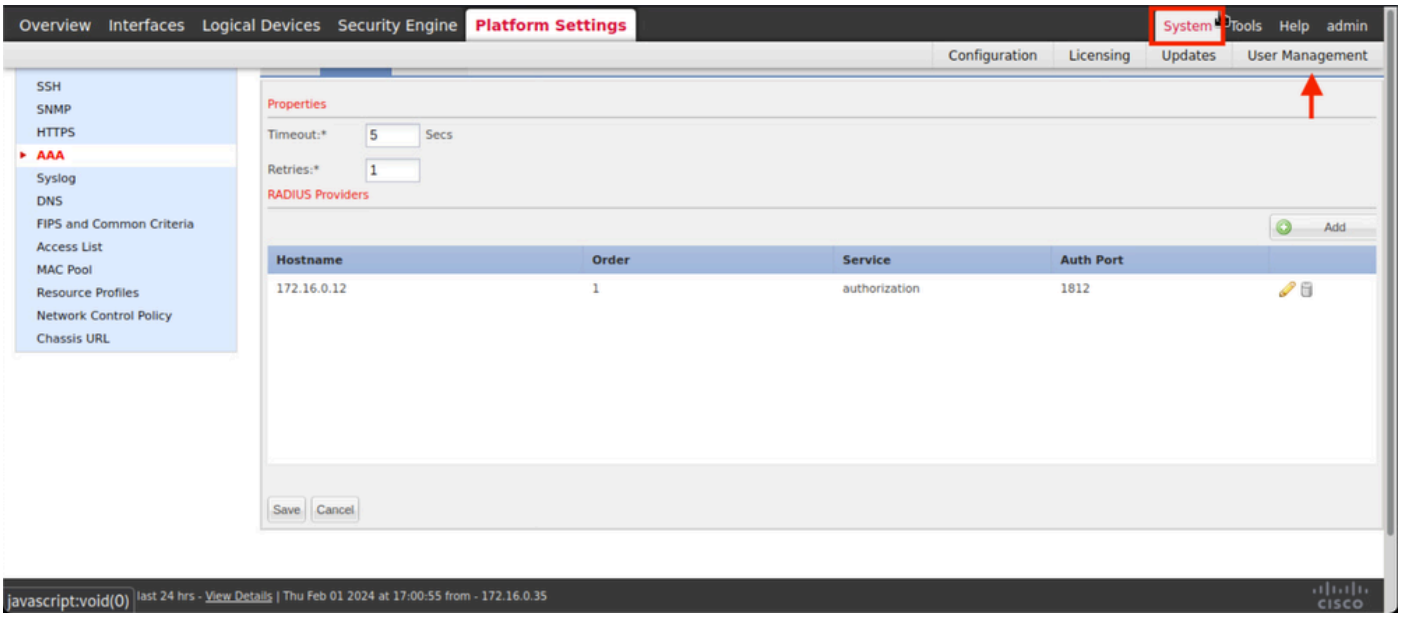
Passaggio 3. Dal menu a sinistra, fare clic su AAA. Selezionare Raggio e Aggiungere un nuovo provider RADIUS.



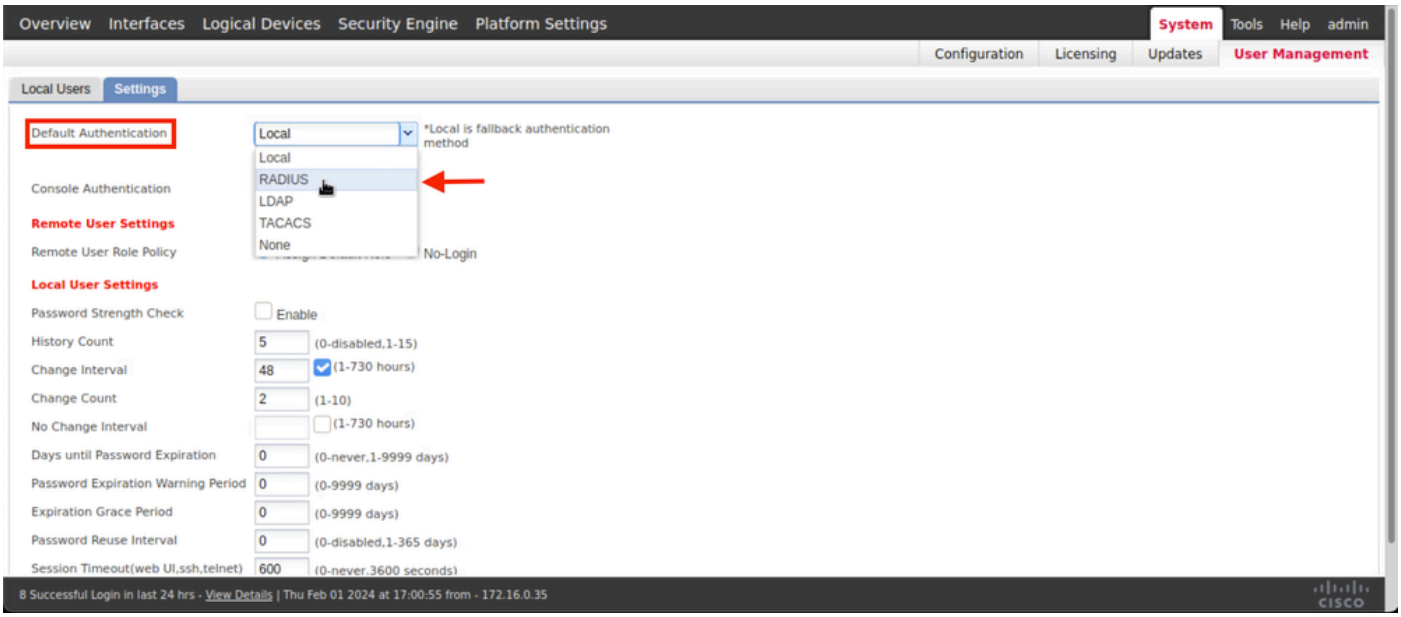
Passaggio 4. Inserite nel menu del prompt le informazioni richieste dal provider Radius. Fare clic su OK.

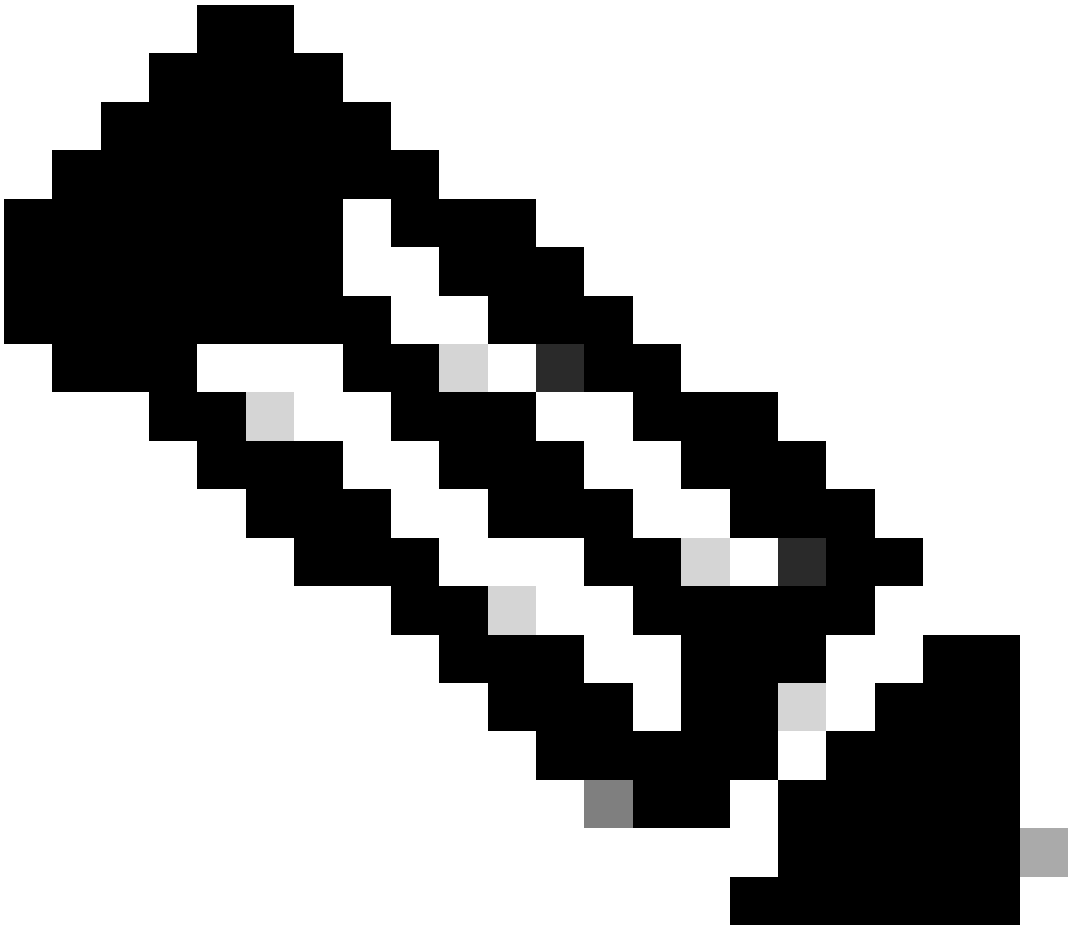


Passaggio 5. Selezionare Sistema > Gestione utente



Passaggio 6. Fare clic sulla scheda Settings (Impostazioni) e impostare Default Authentication (Autenticazione predefinita) dal menu a discesa su Radius, quindi scorrere verso il basso e salvare la configurazione.



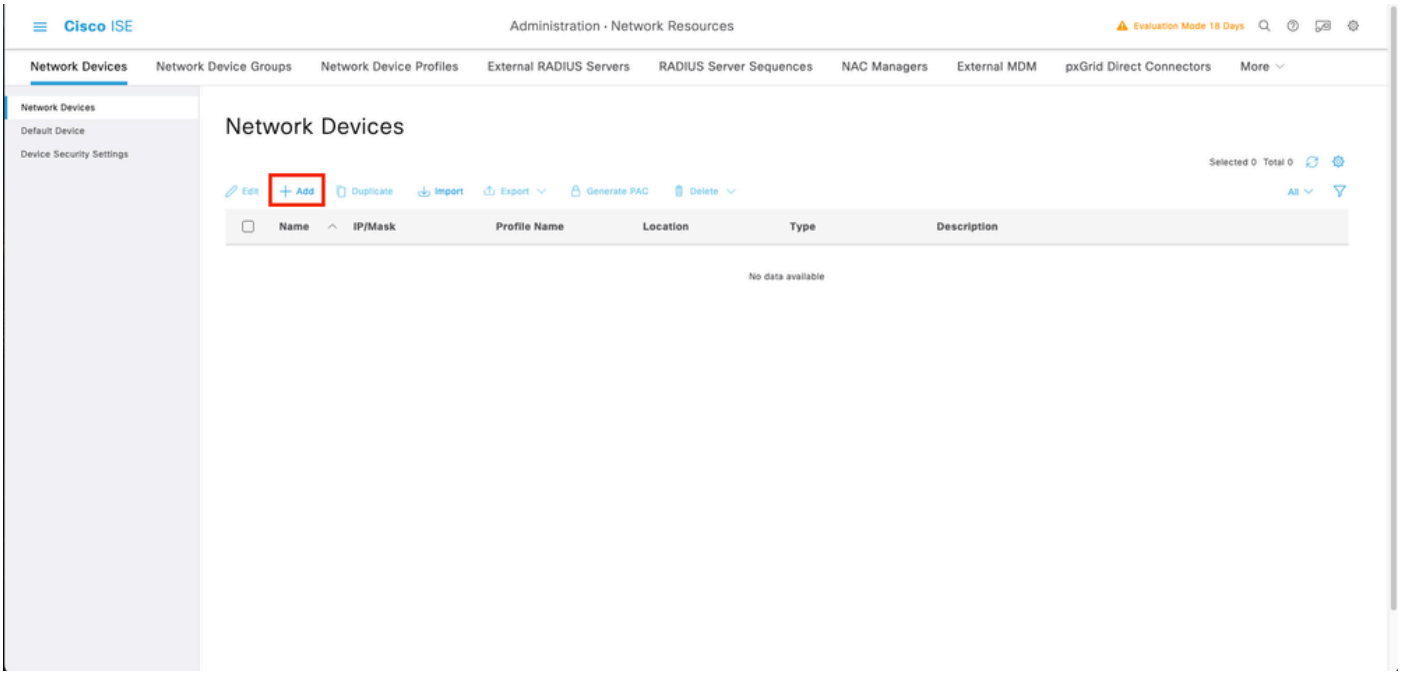


Nota: a questo punto, la configurazione di FCM è terminata.

Identity Service Engine

Passaggio 1. Aggiungere un nuovo dispositivo di rete.

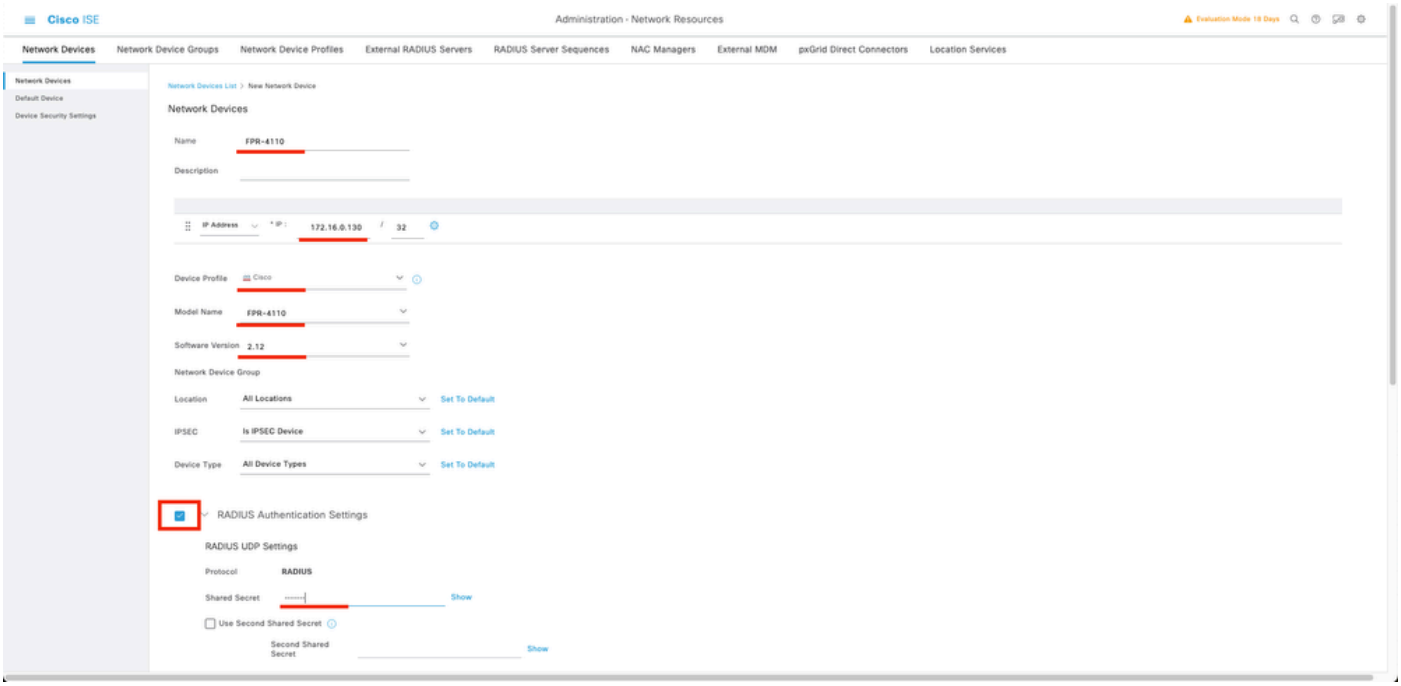
Spostarsi sull'icona del hamburger=situata nell'angolo superiore sinistro > Amministrazione > Risorse di rete > Dispositivi di rete > +Aggiungi.



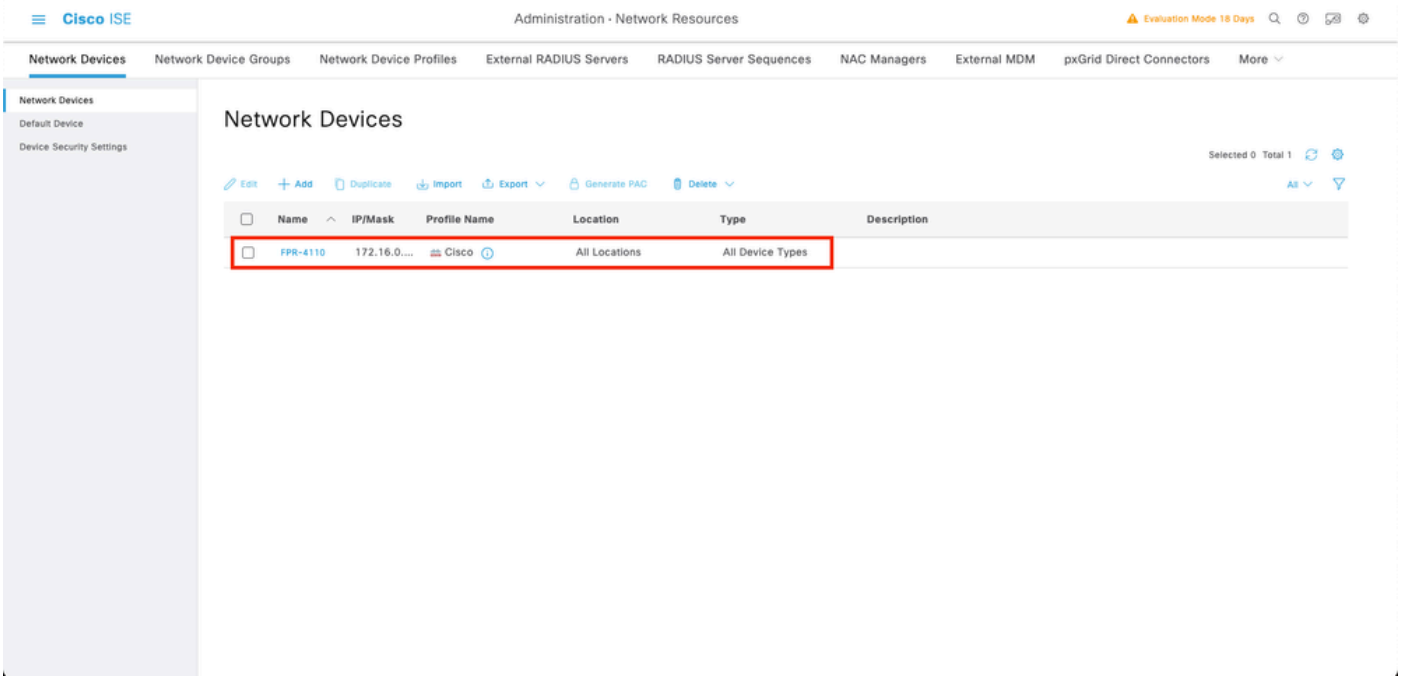
Passaggio 2. Specificare i parametri richiesti per le informazioni sui nuovi dispositivi di rete.

2.1 Selezionare la casella di controllo RADIUS
2.2 Configurare la stessa chiave segreta condivisa della configurazione Radius di FCM.

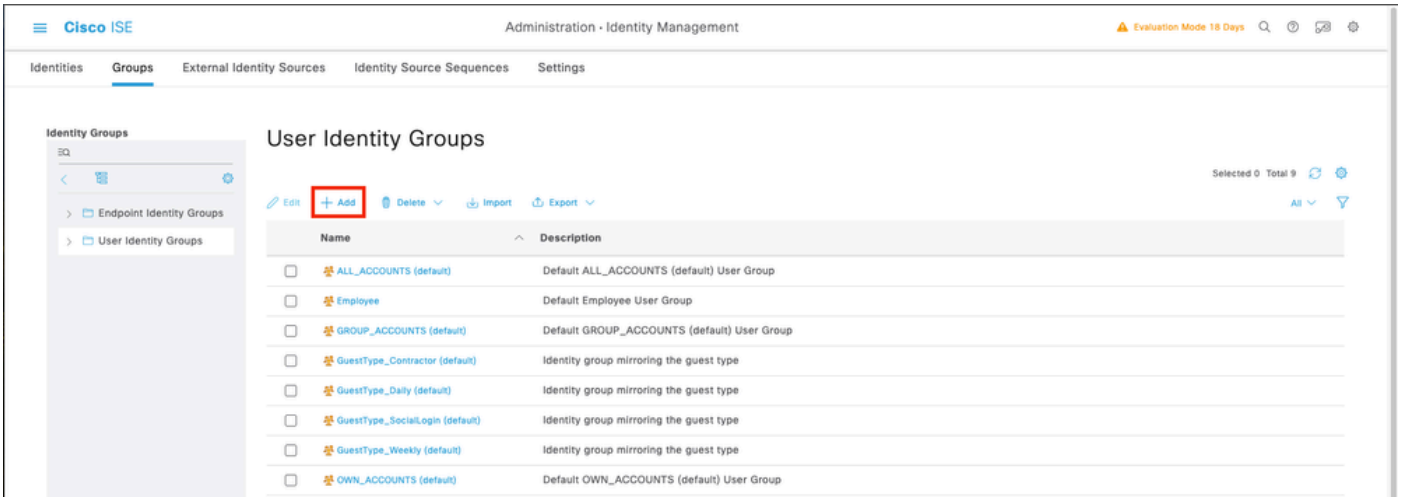
2.1 Scorrere verso il basso e fare clic su Submit (Invia).



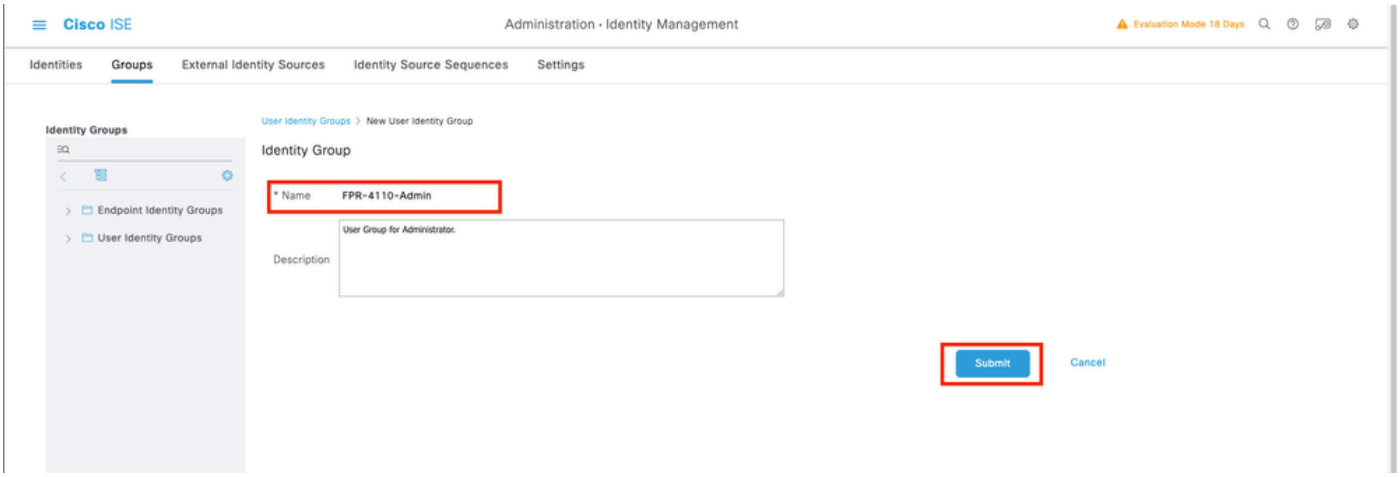
Passaggio 3. Verificare che la nuova periferica sia visualizzata in Periferiche di rete.



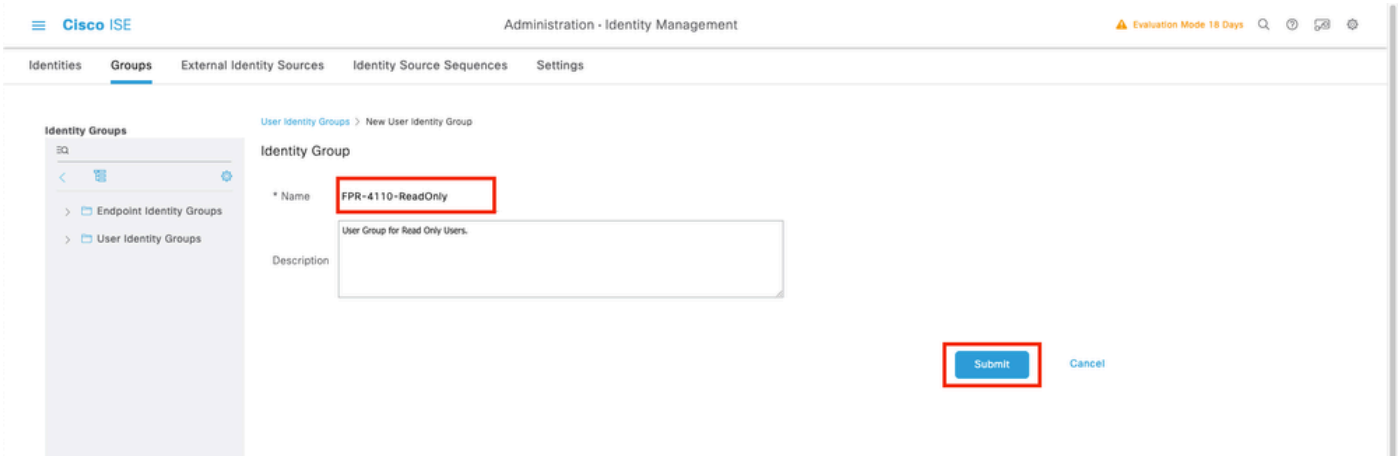
Passaggio 4. Creare i gruppi di identità utente richiesti. Passare all'icona del hamburger che si trova nell'angolo superiore sinistro > Amministrazione > Gestione delle identità > Gruppi > Gruppi identità utente > + Aggiungi



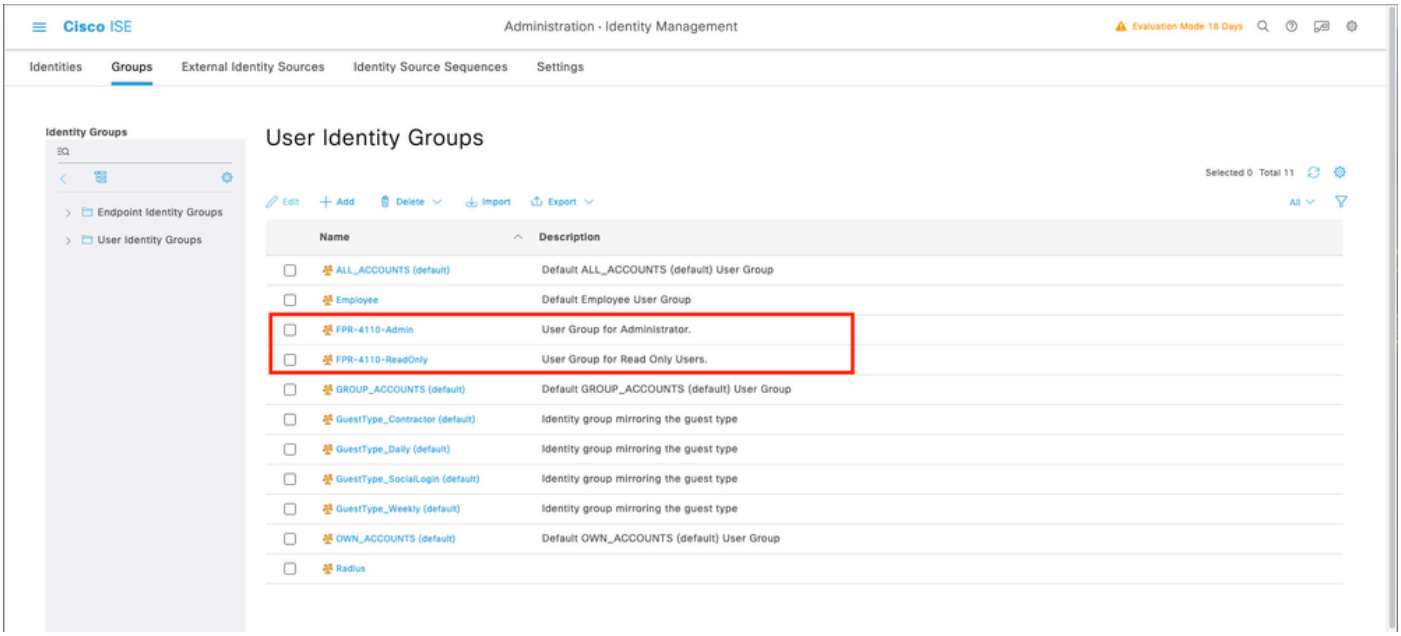
Passaggio 5. Per salvare la configurazione, impostare un nome per il gruppo di identità dell'utente amministratore e fare clic su Invia.



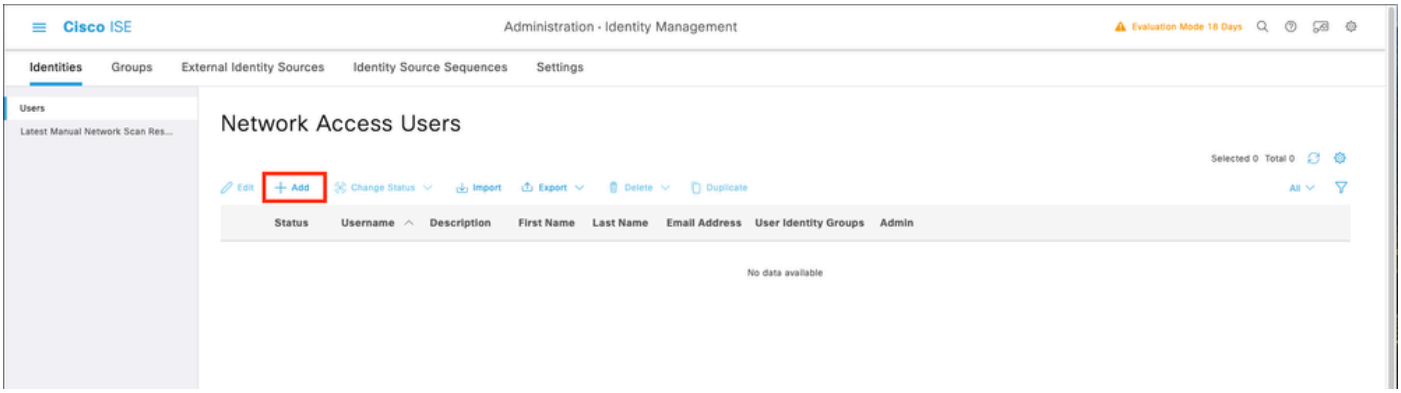
5.1 Ripetere la stessa procedura per gli utenti di sola lettura.



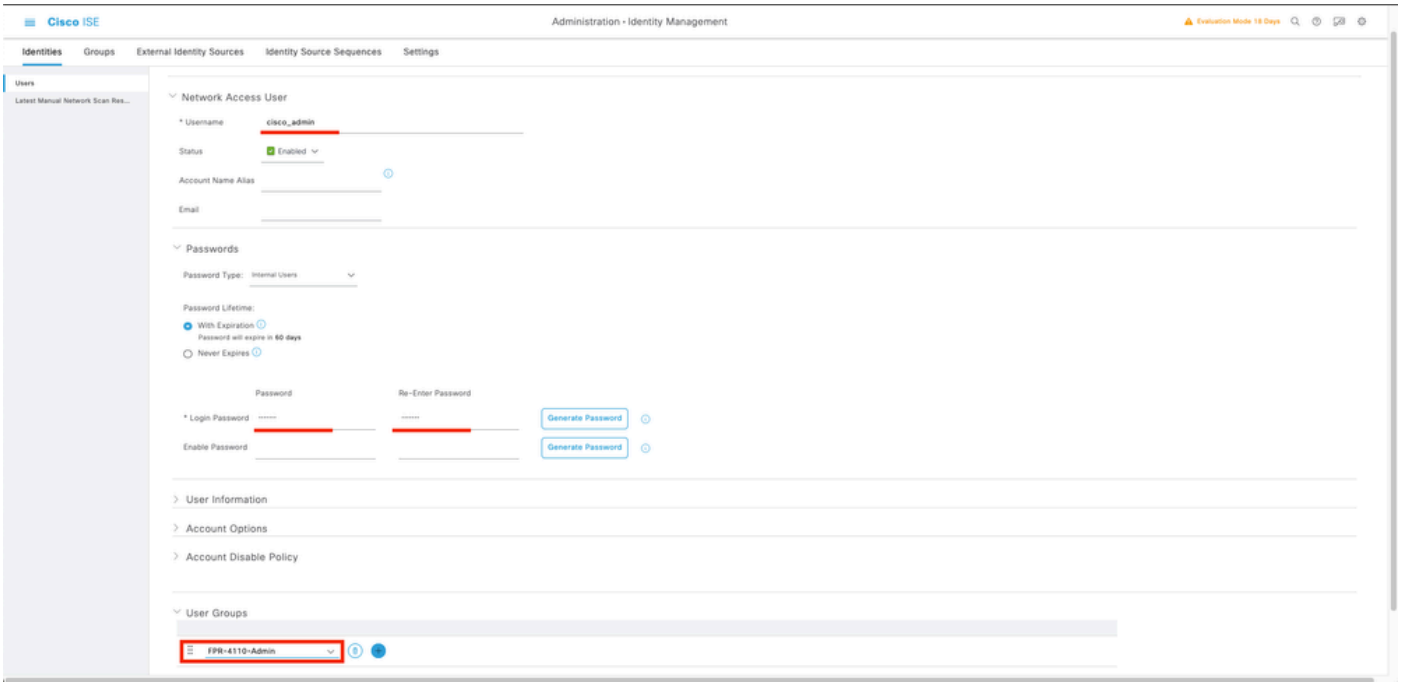
Passaggio 6. Verificare che i nuovi gruppi di utenti siano visualizzati in Gruppi identità utente.



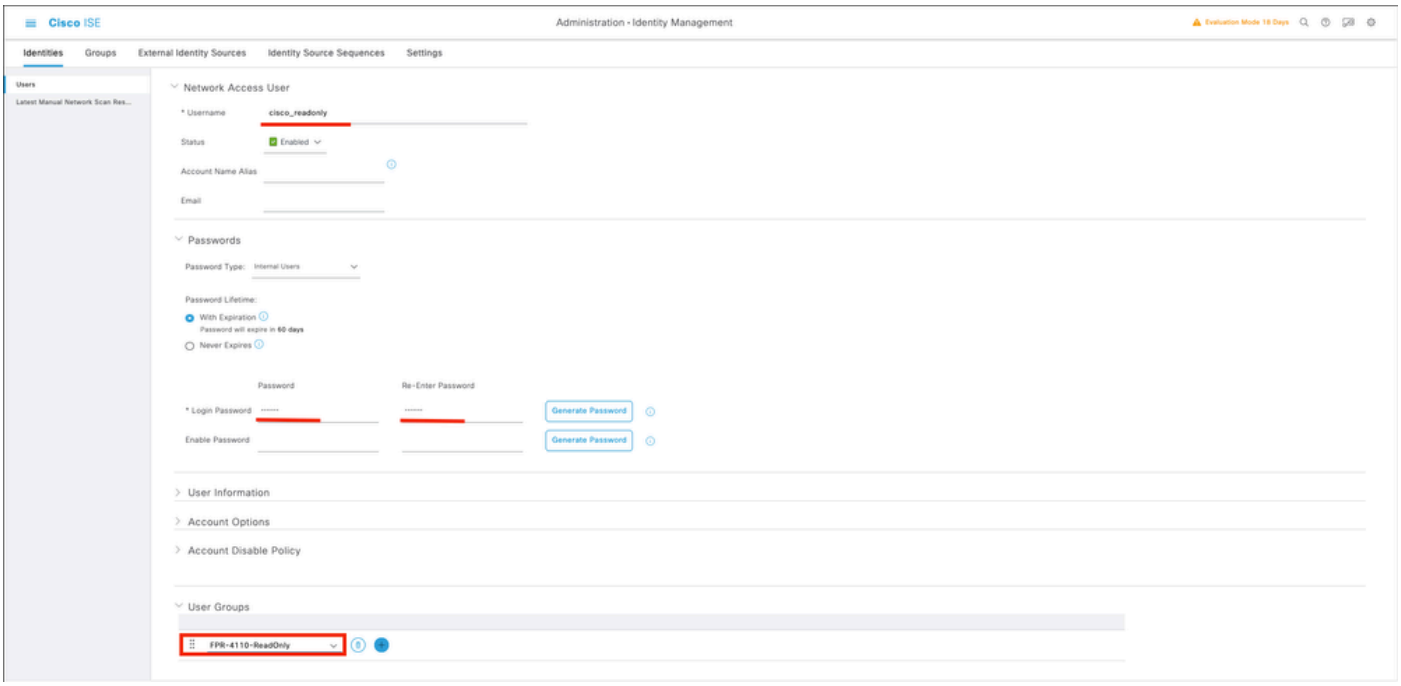
Passaggio 7. Creare gli utenti locali e aggiungerli al gruppo corrispondente. Passare all'icona del hamburger +++ > Amministrazione > Gestione delle identità > Identità > + Aggiungi.



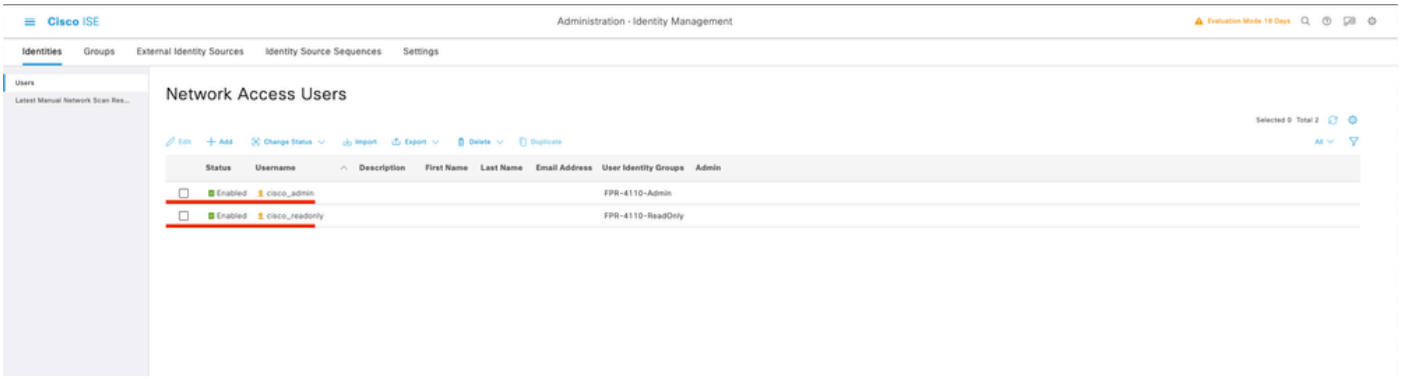
7.1 Aggiungere l'utente con diritti di amministratore. Impostare un nome e una password e assegnarli a FPR-4110-Admin, scorrere verso il basso e fare clic su Submit (Invia) per salvare le modifiche.



7.2 Aggiungere l'utente con diritti di sola lettura. Impostare un nome e una password e assegnarli a FPR-4110-ReadOnly, scorrere verso il basso e fare clic su Submit (Invia) per salvare le modifiche.



7.3 Verificare che gli utenti si trovino in Utenti accesso alla rete.



Passaggio 8. Creare il profilo di autorizzazione per l'utente Admin.

Lo chassis FXOS include i seguenti ruoli utente:

- Amministratore: accesso completo in lettura e scrittura all'intero sistema. All'account amministratore predefinito viene assegnato questo ruolo per impostazione predefinita e non può essere modificato.
- Sola lettura - Accesso in sola lettura alla configurazione del sistema senza privilegi per la modifica dello stato del sistema.
- Operazioni: accesso in lettura e scrittura alla configurazione NTP, alla configurazione di Smart Call Home per Smart Licensing e ai registri di sistema, inclusi i server syslog e i relativi errori. Accesso in lettura al resto del sistema.
- AAA: accesso in lettura e scrittura a utenti, ruoli e configurazione AAA. Accesso in lettura al resto del sistema

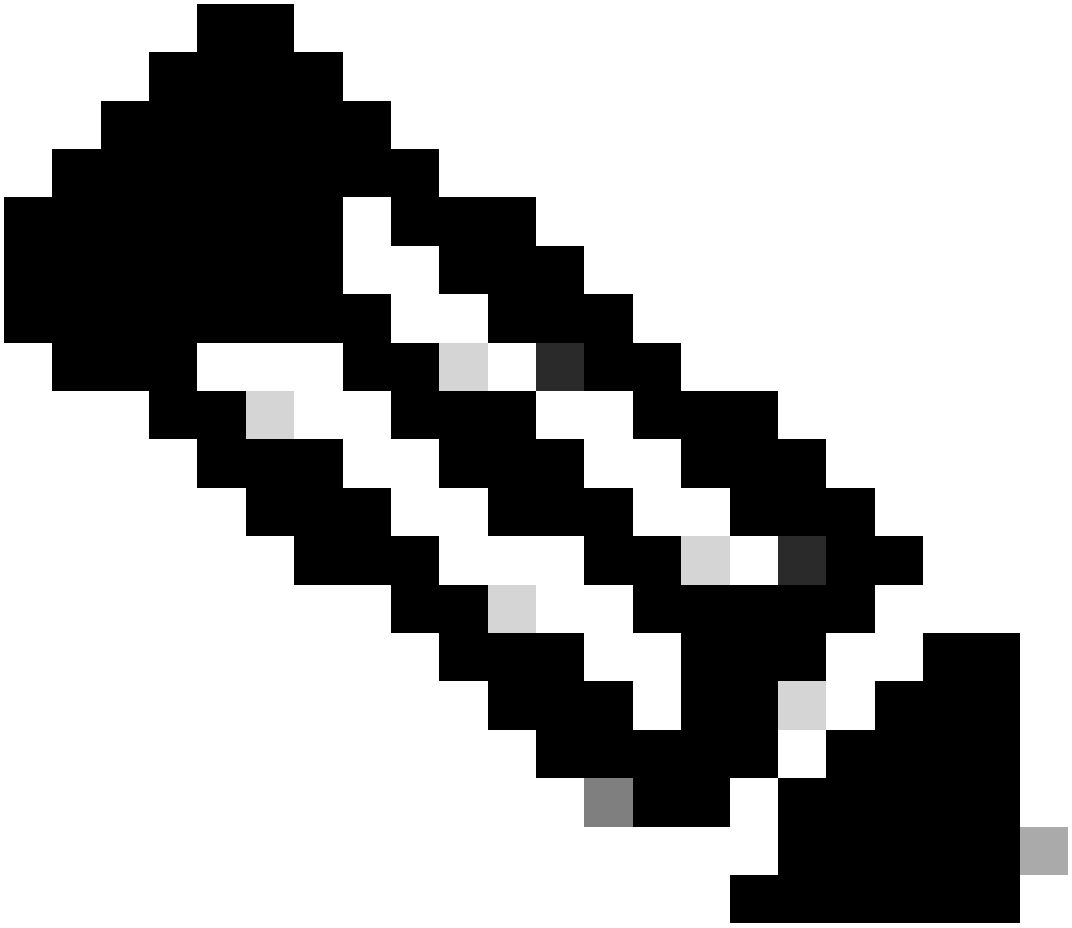
Attributi per ogni ruolo:

cisco-av-pair=shell:roles="admin"

cisco-av-pair=shell:roles="aaa"

cisco-av-pair=shell:roles="operazioni"

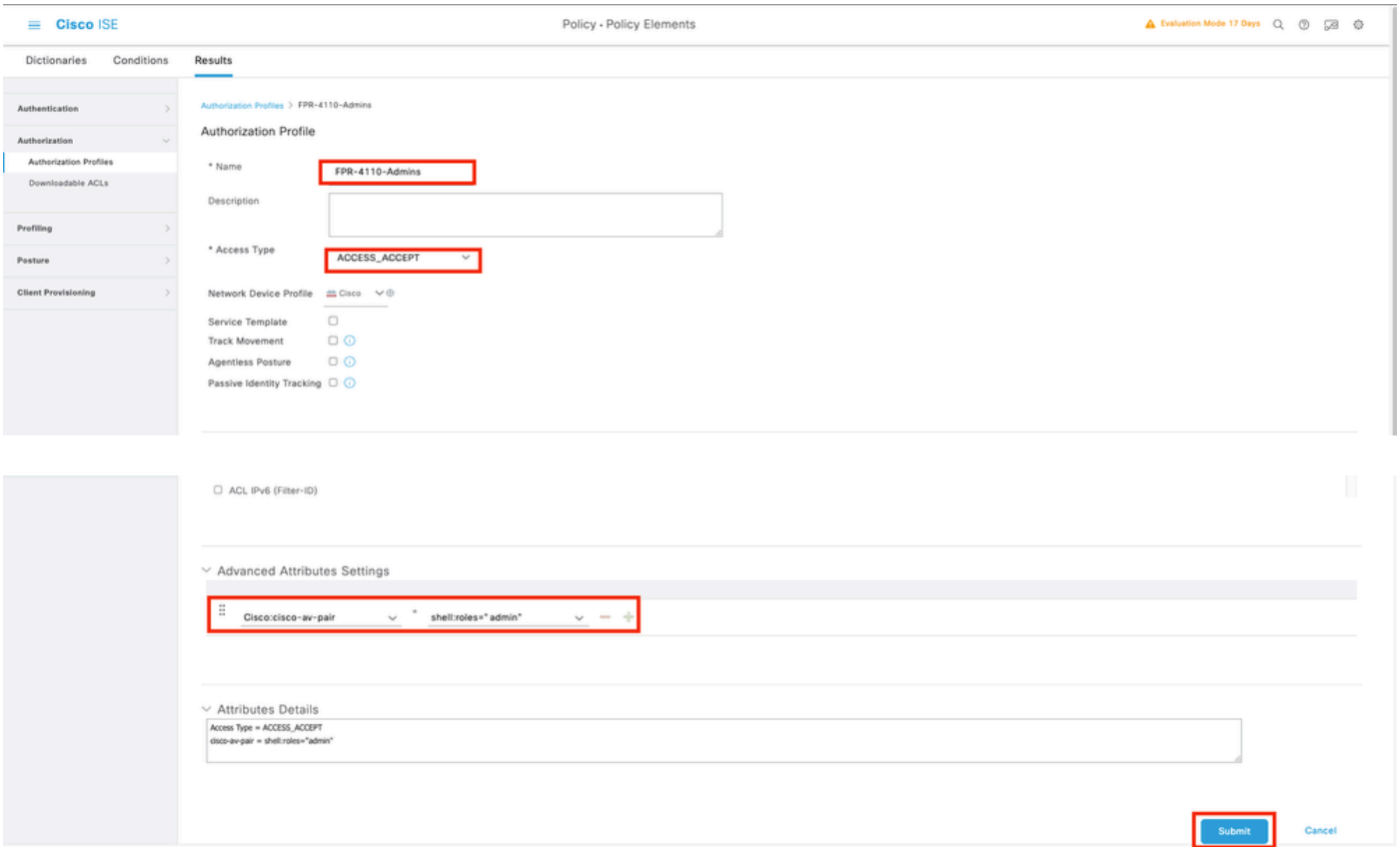
cisco-av-pair=shell:roles="sola lettura"



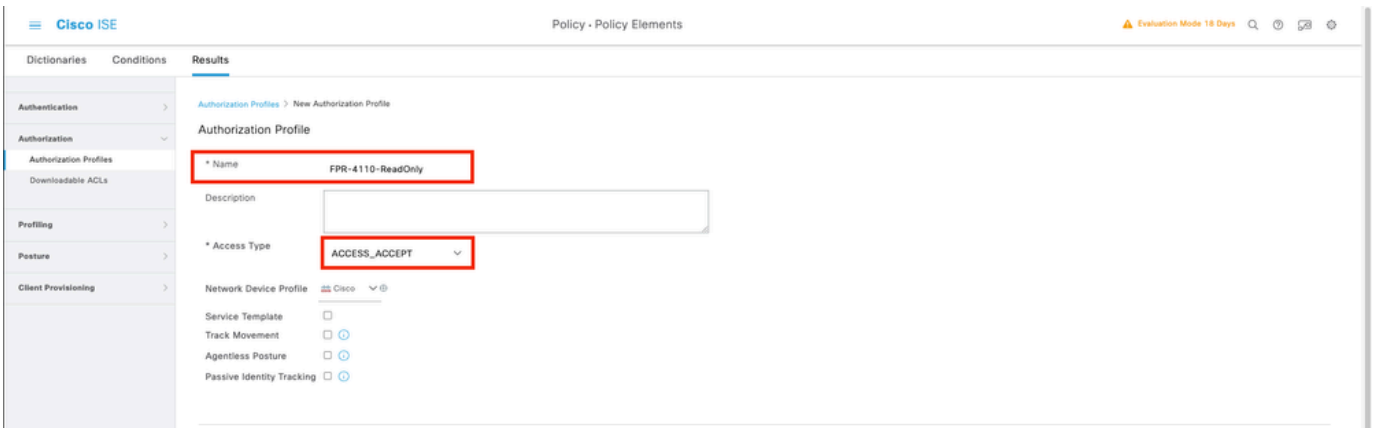
Nota: questa documentazione definisce solo gli attributi admin e read-only.

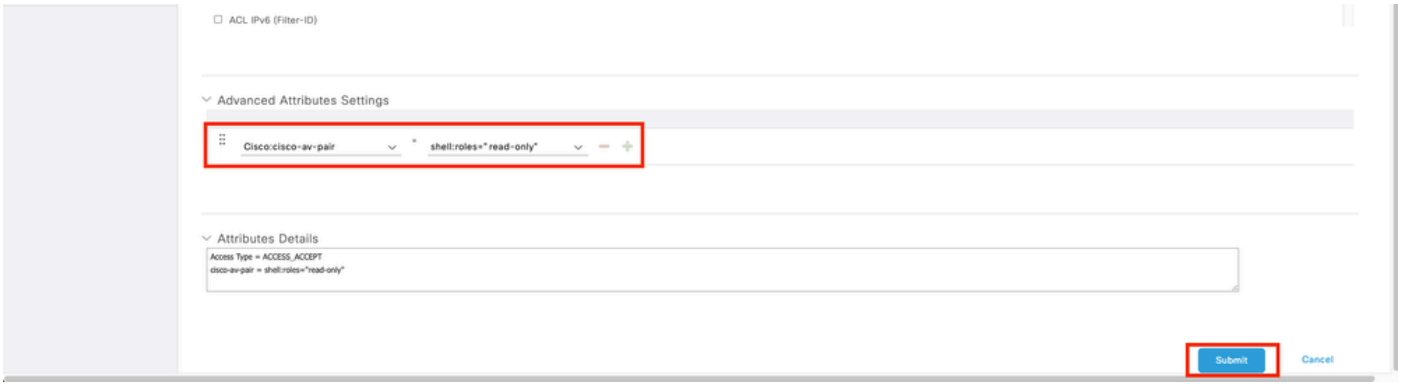
Passare a icona hamburger=> Criteri > Elementi criteri > Risultati > Autorizzazione > Profili di autorizzazione > +Aggiungi.

Definire un nome per il profilo di autorizzazione, lasciare il tipo di accesso impostato su ACCESS_ACCEPT e in Impostazioni avanzate attributi aggiungere cisco-av-pair=shell:roles="admin" con e fare clic su Submit.



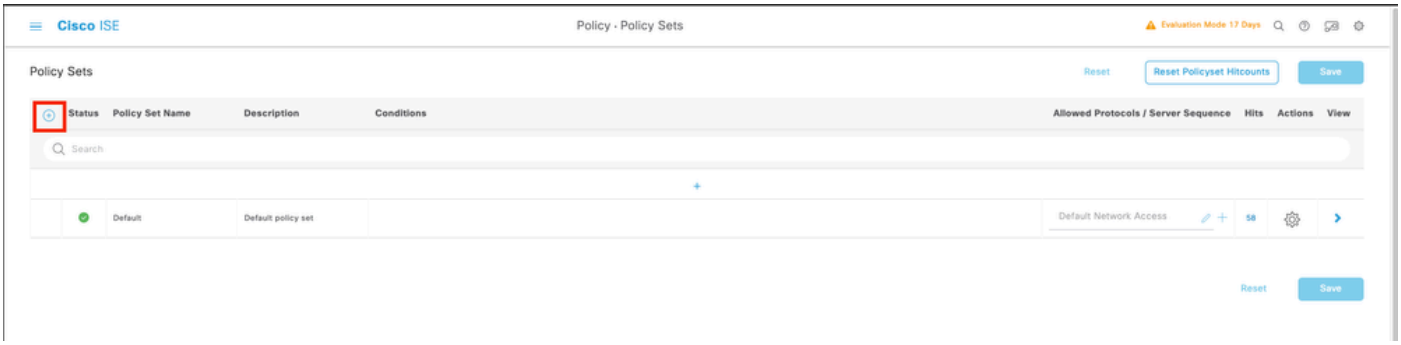
8.1 Ripetere il passaggio precedente per creare il profilo di autorizzazione per l'utente di sola lettura. Creare la classe Radius con il valore read-only in alternativa a Administrator.





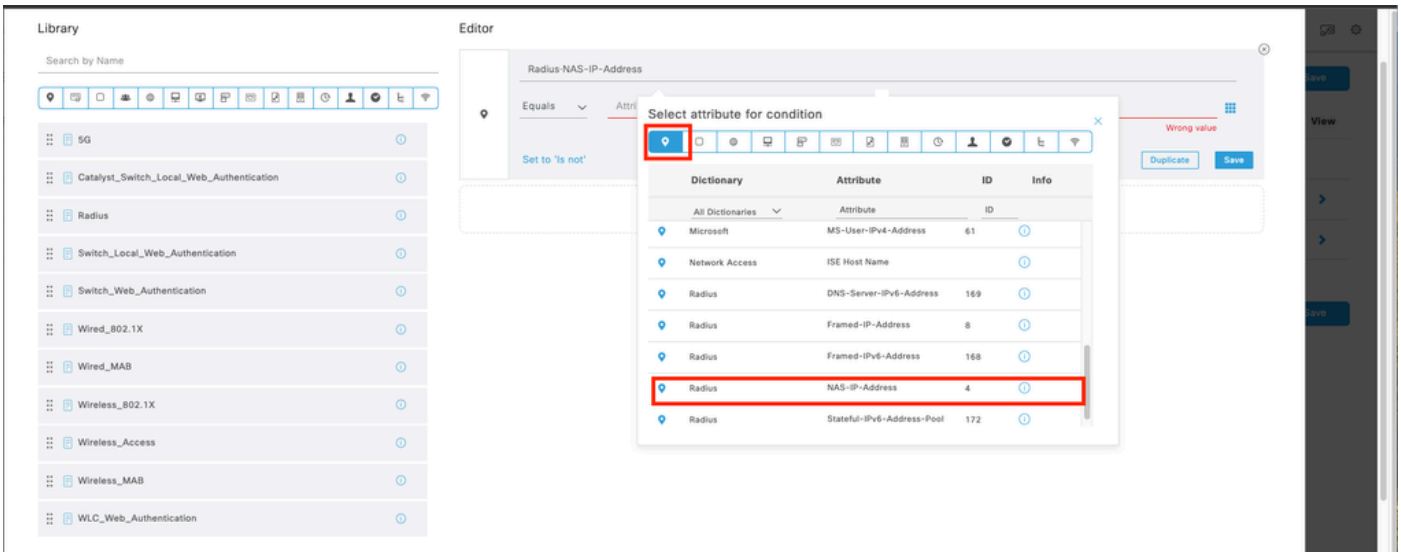
Passaggio 9.Creare un set di criteri corrispondente all'indirizzo IP del CCP. In questo modo si impedisce ad altre periferiche di concedere l'accesso agli utenti.

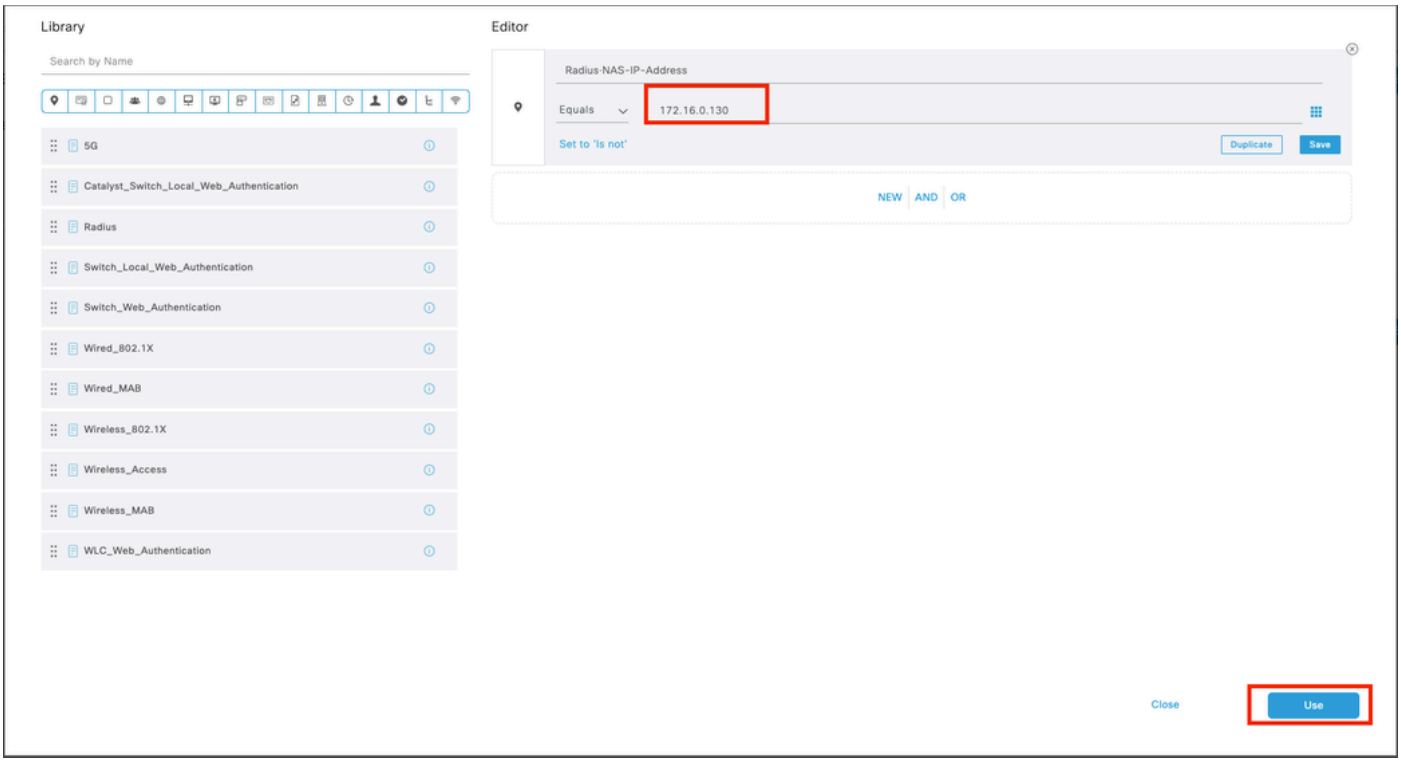
Passare a=> Criteri > Set di criteri >Aggiungi icona nell'angolo superiore sinistro.



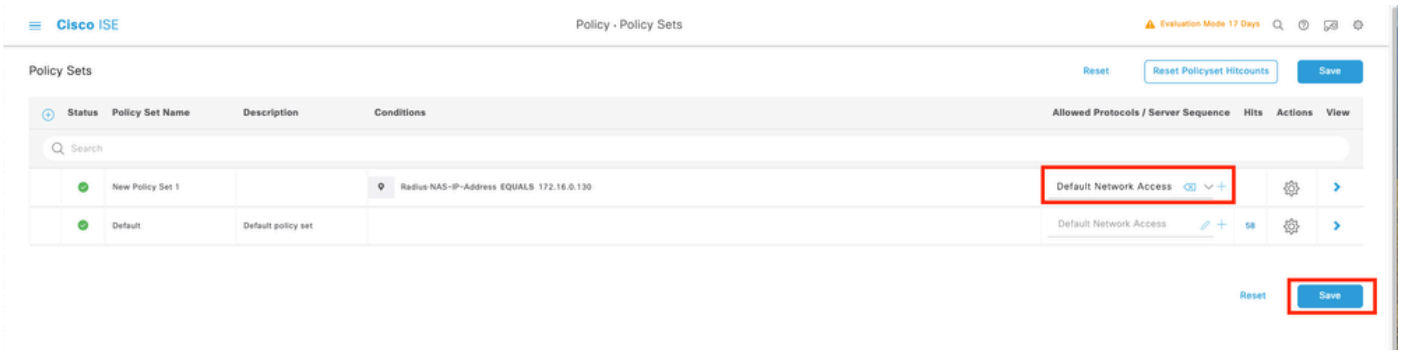
9.1 Una nuova riga viene posizionata in cima ai set di criteri. Fare clic sull'icona Aggiungi per configurare una nuova condizione.

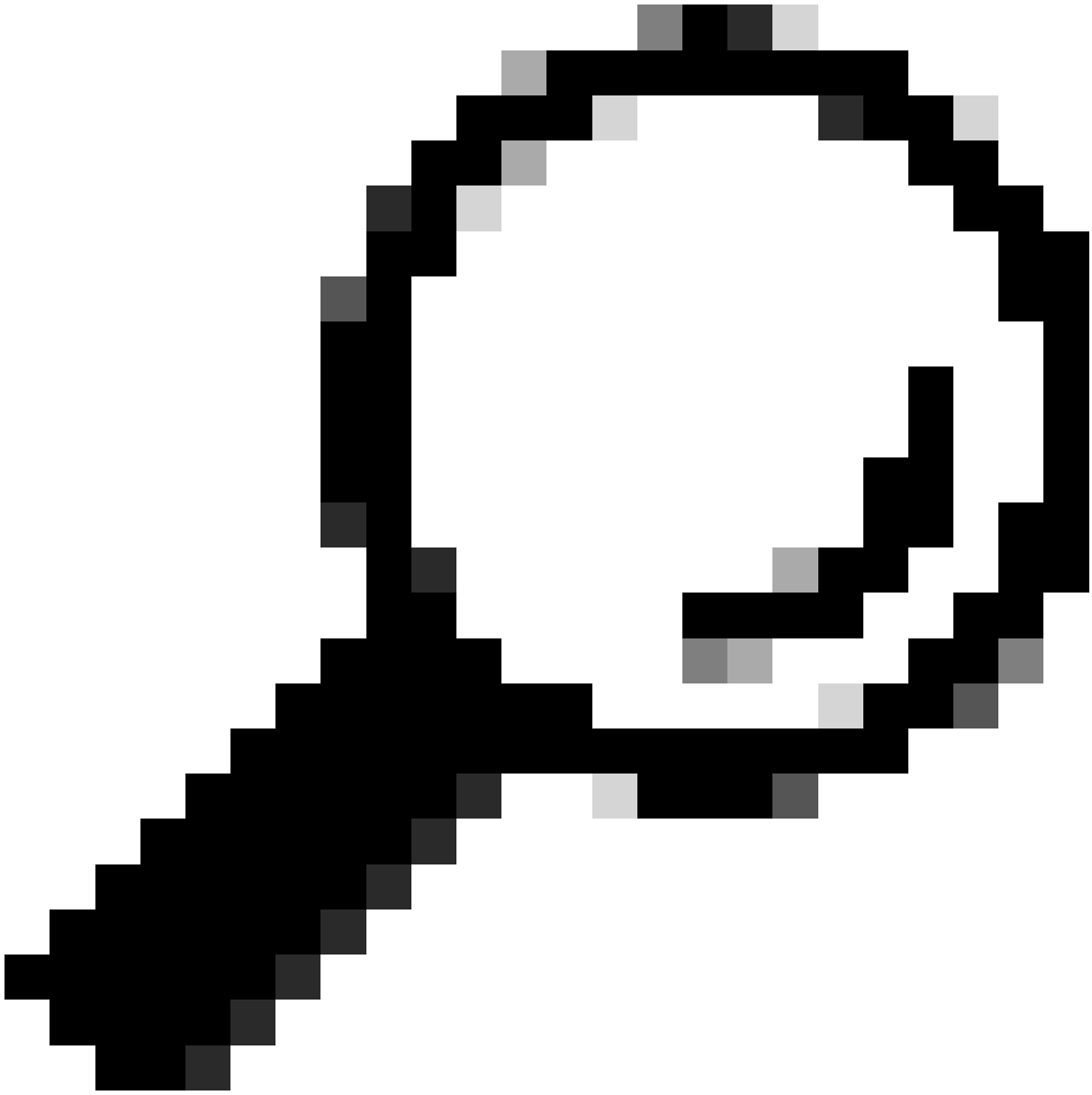
9.2 Aggiungere una condizione superiore per l'attributo NAS-IP-Addressdi RADIUS corrispondente all'indirizzo IP di FCM, quindi fare clic su Usa.





9.3 Al termine, fare clic su Save (Salva).





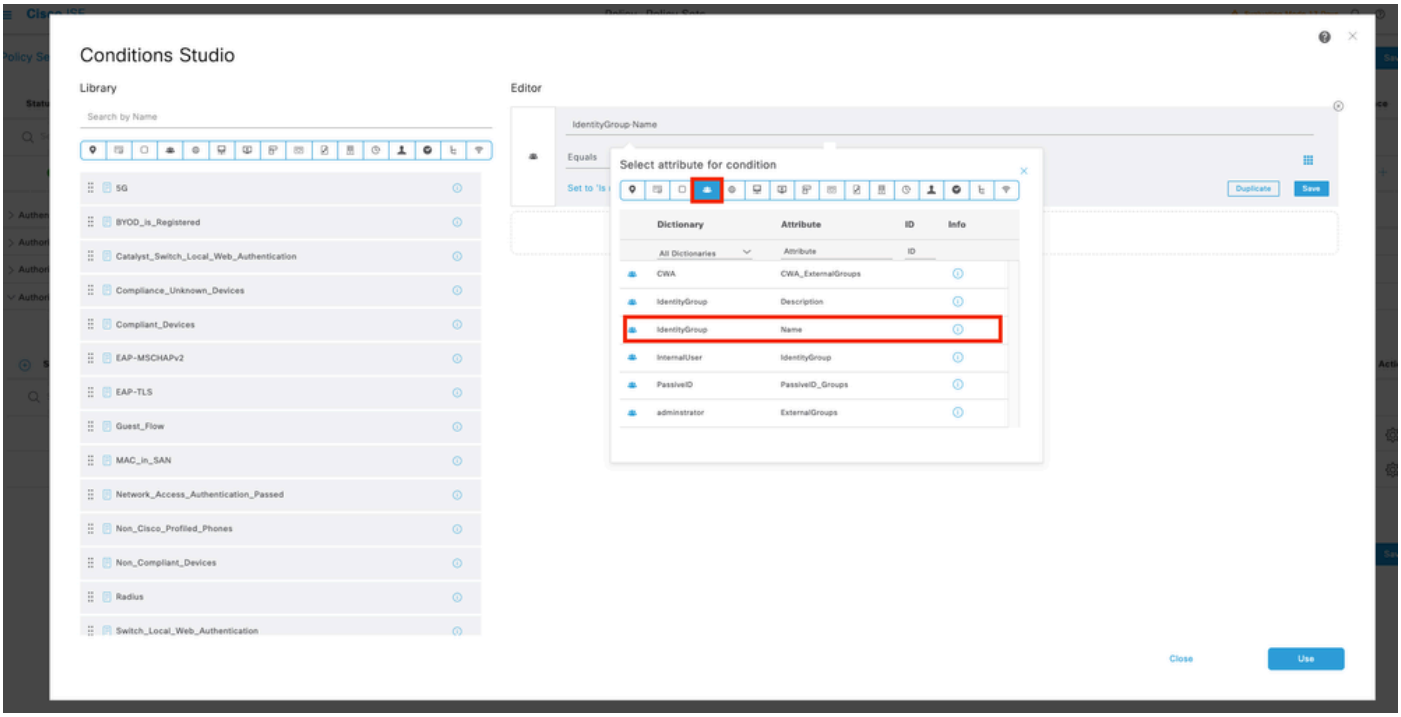
Suggerimento: per questo esercizio è stato consentito l'utilizzo dell'elenco Protocolli di accesso alla rete predefiniti. È possibile creare un nuovo elenco e restringerlo in base alle esigenze.

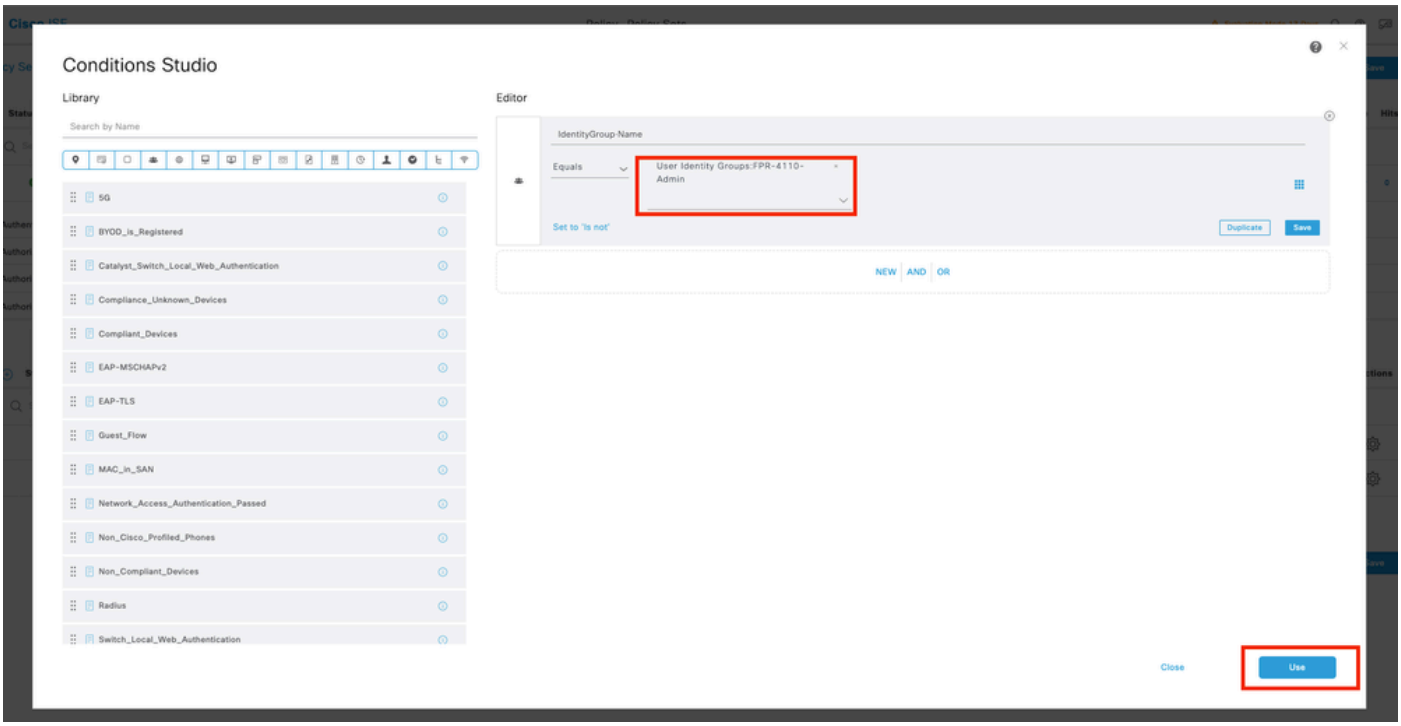
Passaggio 10. Visualizzare il nuovo set di criteri facendo clic sull'icona **>** situata alla fine della riga.

10.1 Espandere il menu Criteri di autorizzazione e fare clic su in (+) per aggiungere una nuova

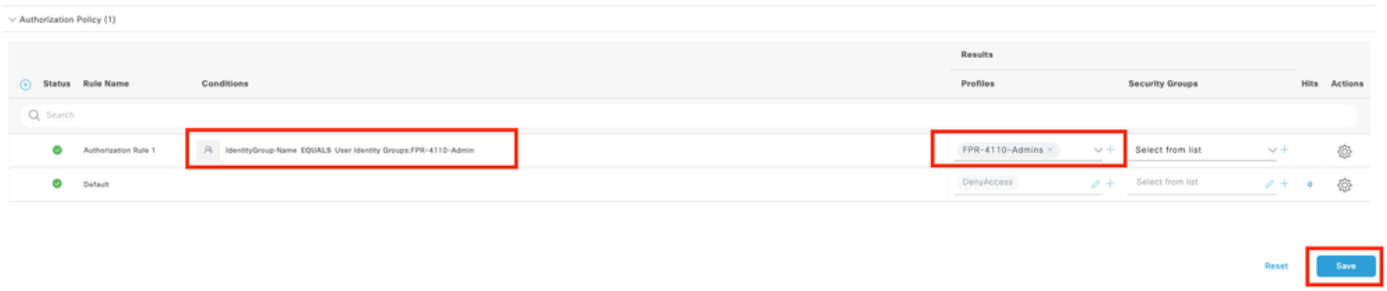
condizione.

10.2 Impostare le condizioni in modo che corrispondano al DictionaryIdentity Group con AttributeName uguale a User Identity Groups: FPR-4110-Admins(il nome del gruppo creato nel passaggio 7) e fare clic su Use.





Passaggio 10.3 Verificare che la nuova condizione sia configurata nel criterio di autorizzazione, quindi aggiungere un profilo utente in Profili.



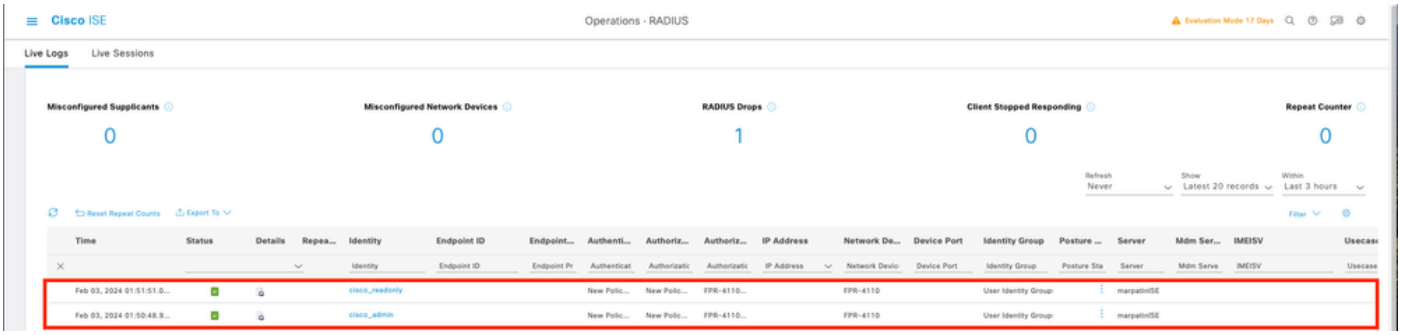
Passaggio 11. Ripetere lo stesso processo al passaggio 9 per gli utenti di sola lettura e fare clic su Salva.

Verifica

1. Tentare di accedere all'interfaccia utente grafica di FCM utilizzando le nuove credenziali Radius

2. Passare all'icona hamburger=> Operazioni > Raggio > Log attivi.

3. Le informazioni visualizzate indicano se un utente ha eseguito correttamente il login.



4. Convalidare il ruolo degli utenti registrati dalla CLI di Secure Firewall Chassis.

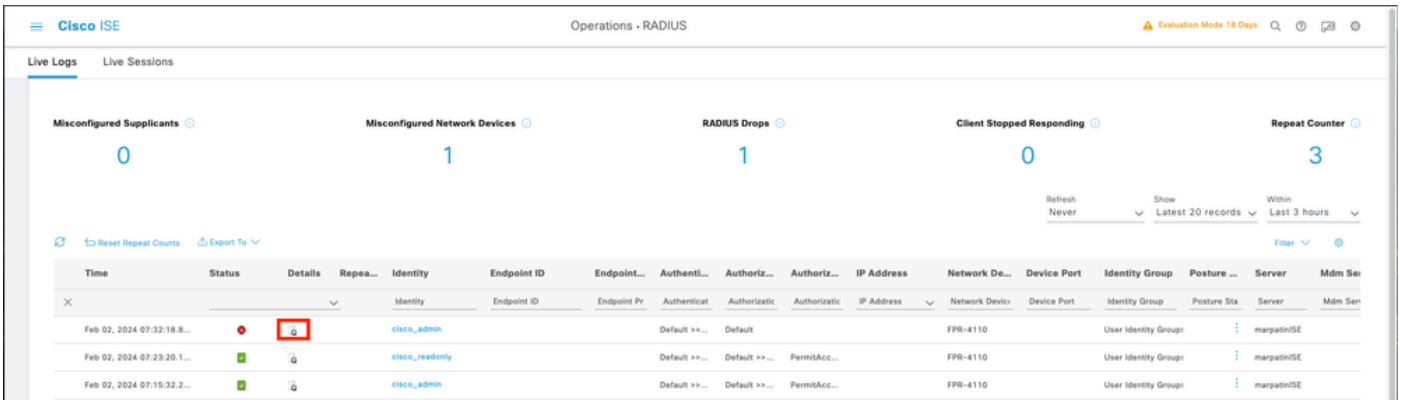
```
FPR4K-1-029A78B# scope se
security         server           service-profile

FPR4K-1-029A78B# scope security
FPR4K-1-029A78B /security # show remote-user detail
Remote User cisco_admin:
    Description:
    User Roles:
        Name: admin
        Name: read-only
FPR4K-1-029A78B /security #
```

Risoluzione dei problemi

1. Dalla GUI di ISE, passare all'icona hamburger= > Operazioni > Raggio > Log attivi.

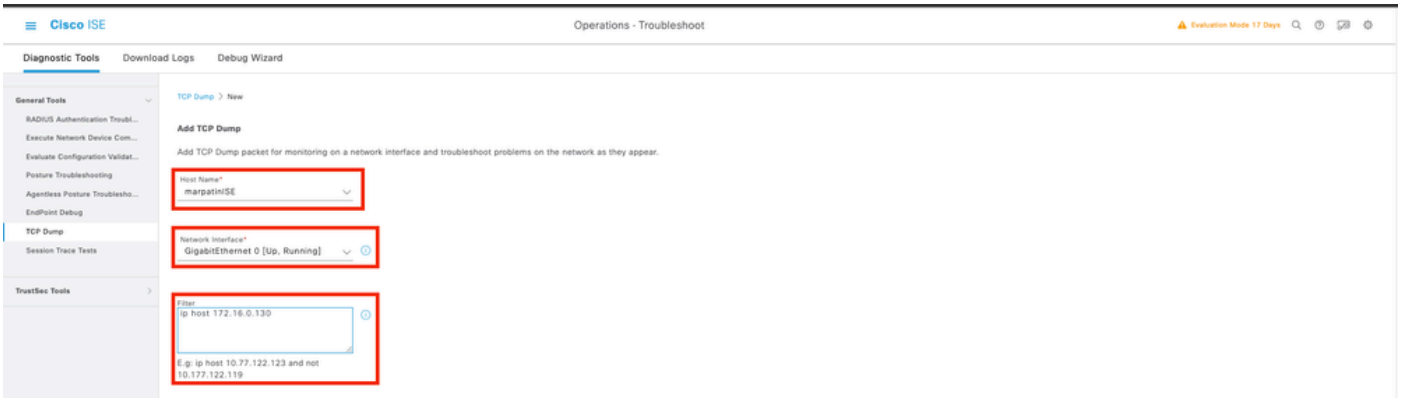
1.1 Convalidare se la richiesta della sessione di log sta raggiungendo il nodo ISE.
1.2 Per l'esame dello stato non riuscito, vedere i dettagli della sessione.



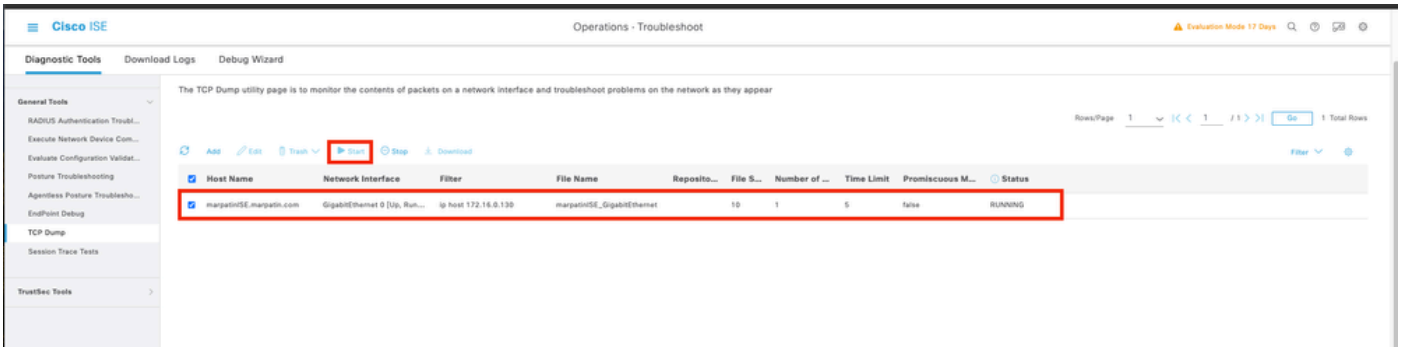
2. Per le richieste non visualizzate nei log Radius Live , verificare se la richiesta UDP sta raggiungendo il nodo ISE tramite un'acquisizione di pacchetti.

Selezionare l'icona del burger=> Operazioni > Risoluzione dei problemi > Strumenti diagnostici > Dump TCP. Aggiungere una nuova acquisizione e scaricare il file sul computer locale per verificare se i pacchetti UDP stanno arrivando al nodo ISE.

2.1 Inserire le informazioni richieste, scorrere verso il basso e fare clic su Salva.



2.2 Selezionare e avviare la cattura.



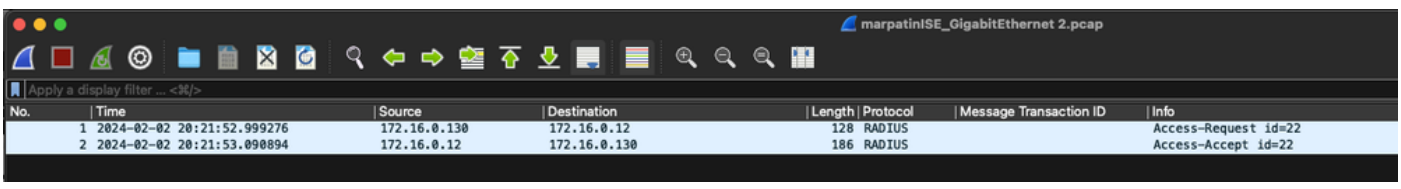
2.3 Tentativo di accedere allo chassis Secure Firewall mentre l'acquisizione ISE è in esecuzione

2.4 Arrestare il dump TCP in ISE e scaricare il file su un computer locale.

2.5 Controllare l'output del traffico.

Output previsto:

Pacchetto n. 1. Richiesta dal Secure Firewall al server ISE tramite la porta 1812 (RADIUS)
Pacchetto n. 2. Risposta del server ISE che accetta la richiesta iniziale.



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).