Configurazione dell'autenticazione esterna FMC e FTD con ISE come server RADIUS

Sommario

Introduzione

Questo documento descrive un esempio di configurazione dell'autenticazione esterna per Secure Firewall Management Center e Firewall Threat Defense.

Prerequisiti

Requisiti

È consigliabile conoscere i seguenti argomenti:

- Configurazione iniziale di Cisco Secure Firewall Management Center tramite GUI e/o shell.
- Configurazione dei criteri di autenticazione e autorizzazione su ISE.
- Conoscenze base di RADIUS.

Componenti usati

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

- vFMC 7.2.5
- FTD 7.2.5
- ISE 3.2.2

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.

Premesse

Quando si abilita l'autenticazione esterna per gli utenti amministrativi e di gestione del sistema Secure Firewall, il dispositivo verifica le credenziali dell'utente con un server LDAP (Lightweight Directory Access Protocol) o RADIUS come specificato in un oggetto di autenticazione esterno.

Gli oggetti di autenticazione esterna possono essere utilizzati dai dispositivi FMC e FTD. È possibile condividere lo stesso oggetto tra diversi tipi di accessorio/dispositivo oppure creare oggetti distinti.

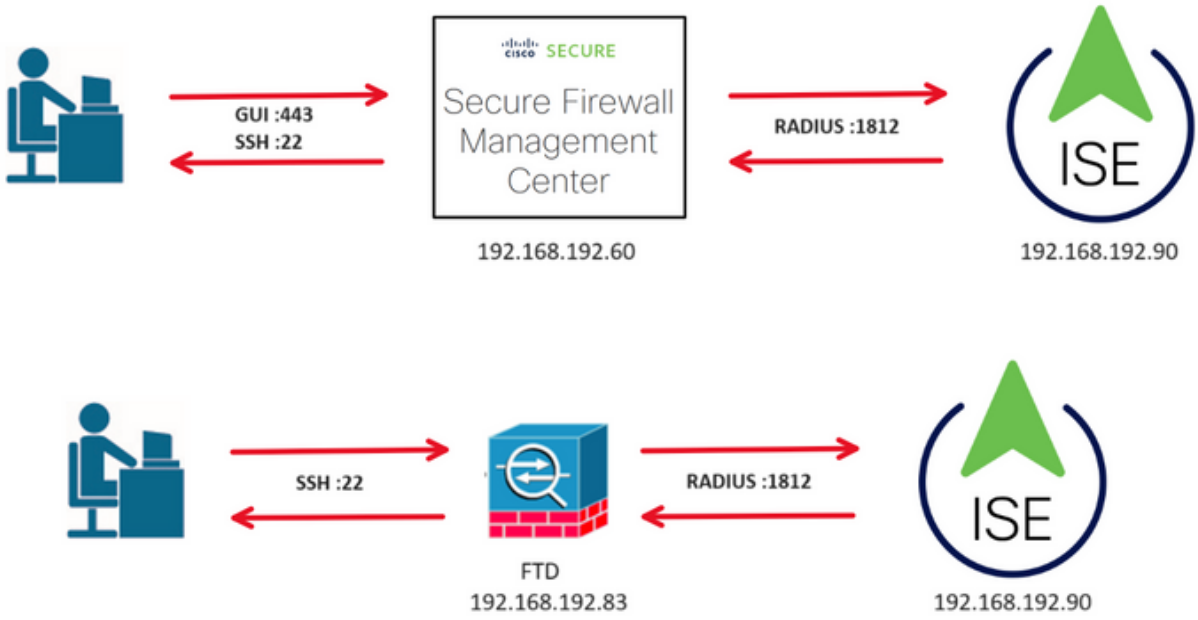
Autenticazione esterna per FMC

È possibile configurare più oggetti di autenticazione esterna per l'accesso all'interfaccia Web. È possibile utilizzare un solo oggetto di autenticazione esterno per l'accesso alla CLI o alla shell.

Autenticazione esterna per FTD

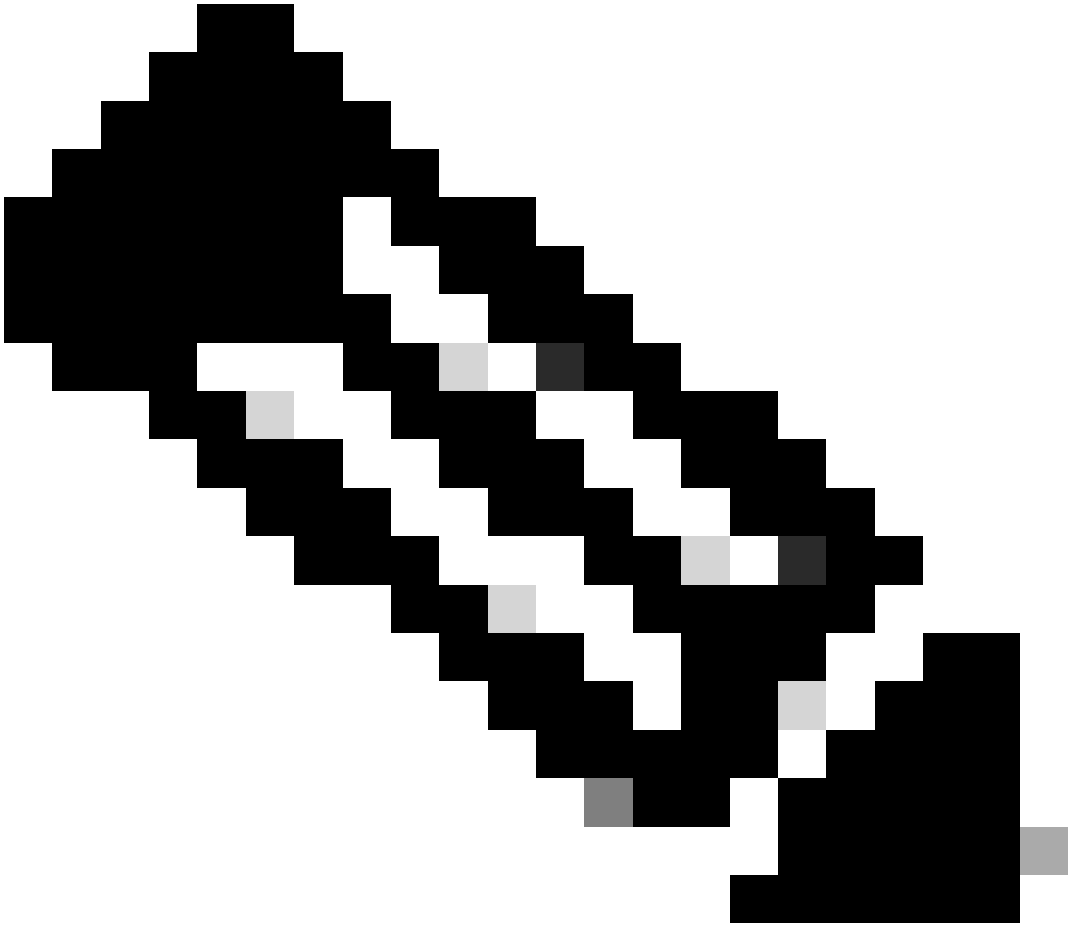
Per l'FTD, è possibile attivare un solo oggetto di autenticazione esterna.

Topologia della rete



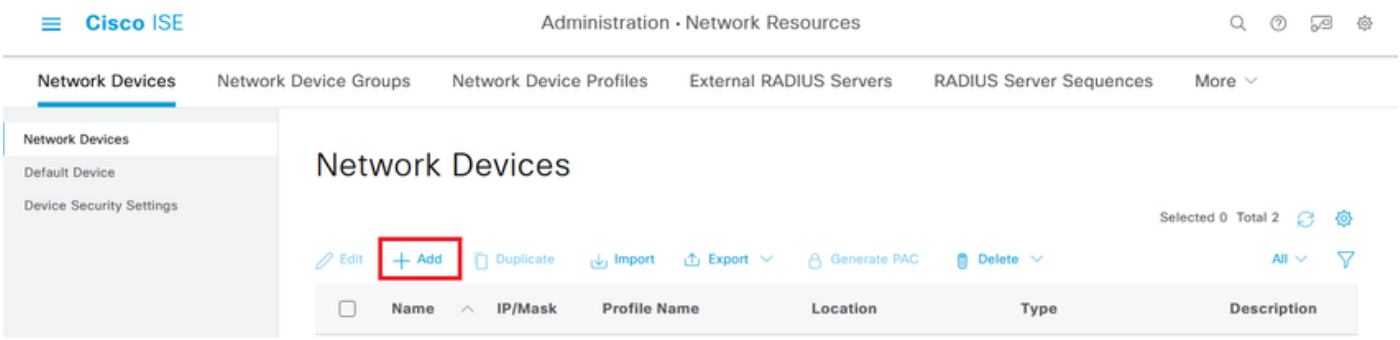
Configurazione

Configurazione di ISE



Nota: esistono diversi modi per configurare l'autenticazione ISE e i criteri di autorizzazione per i dispositivi di accesso alla rete (NAD), ad esempio FMC. L'esempio descritto in questo documento è un punto di riferimento in cui vengono creati due profili (uno con diritti di amministratore e l'altro di sola lettura) che possono essere adattati in modo da soddisfare le linee di base per l'accesso alla rete. In ISE è possibile definire uno o più criteri di autorizzazione che restituiscono al CCP i valori degli attributi RADIUS che vengono quindi mappati a un gruppo di utenti locale definito nella configurazione dei criteri di sistema del CCP.

Passaggio 1. Aggiungere un nuovo dispositivo di rete. Passare all'icona del hamburger situata nell'angolo superiore sinistro >Amministrazione > Risorse di rete > Dispositivi di rete > +Aggiungi.

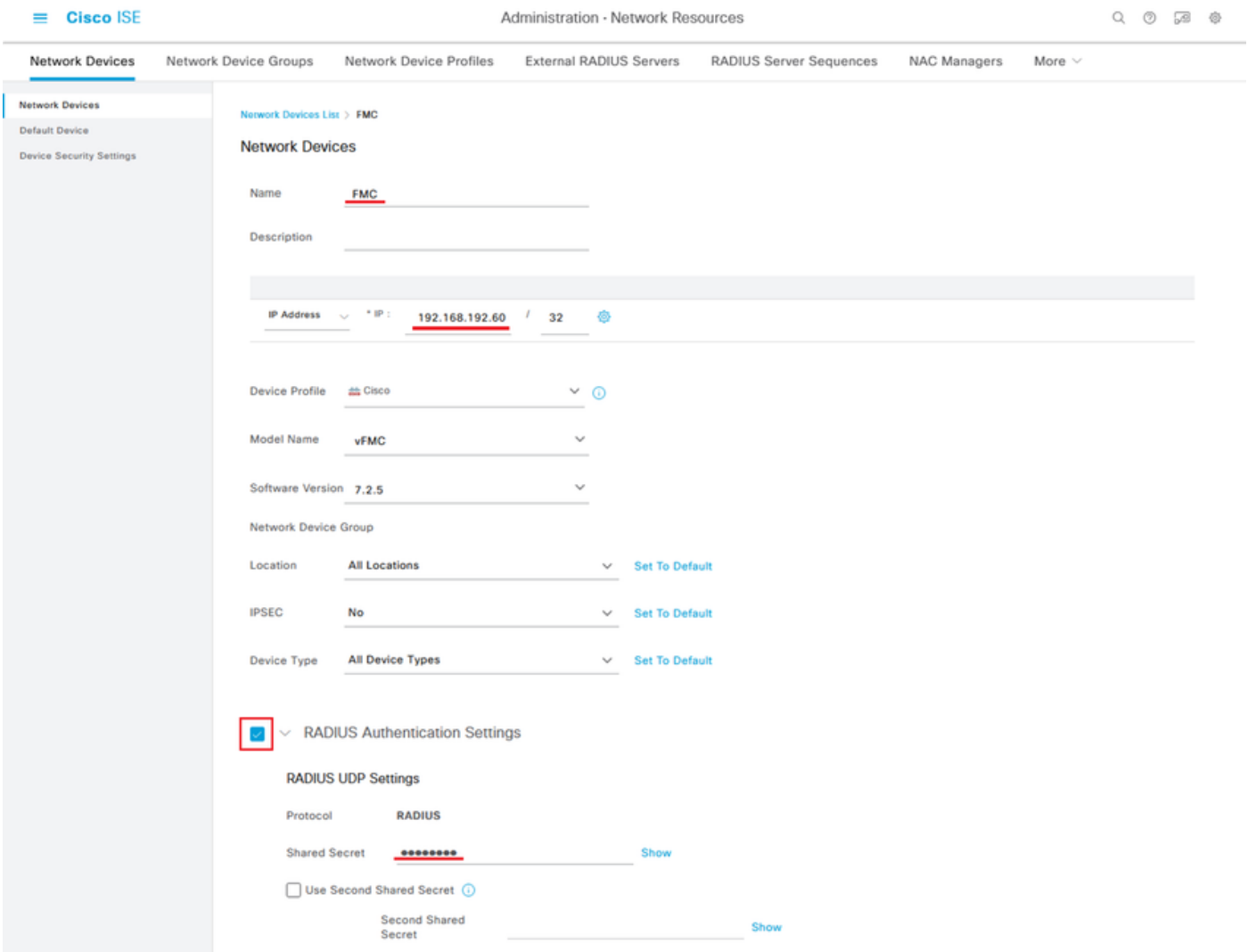


Passaggio 2. Assegnare un nome all'oggetto dispositivo di rete e inserire l'indirizzo IP del CCP.

Selezionare la casella di controllo RADIUS e definire un segreto condiviso.

La stessa chiave deve essere utilizzata successivamente per configurare il CCP.

Al termine, fare clic su Salva.

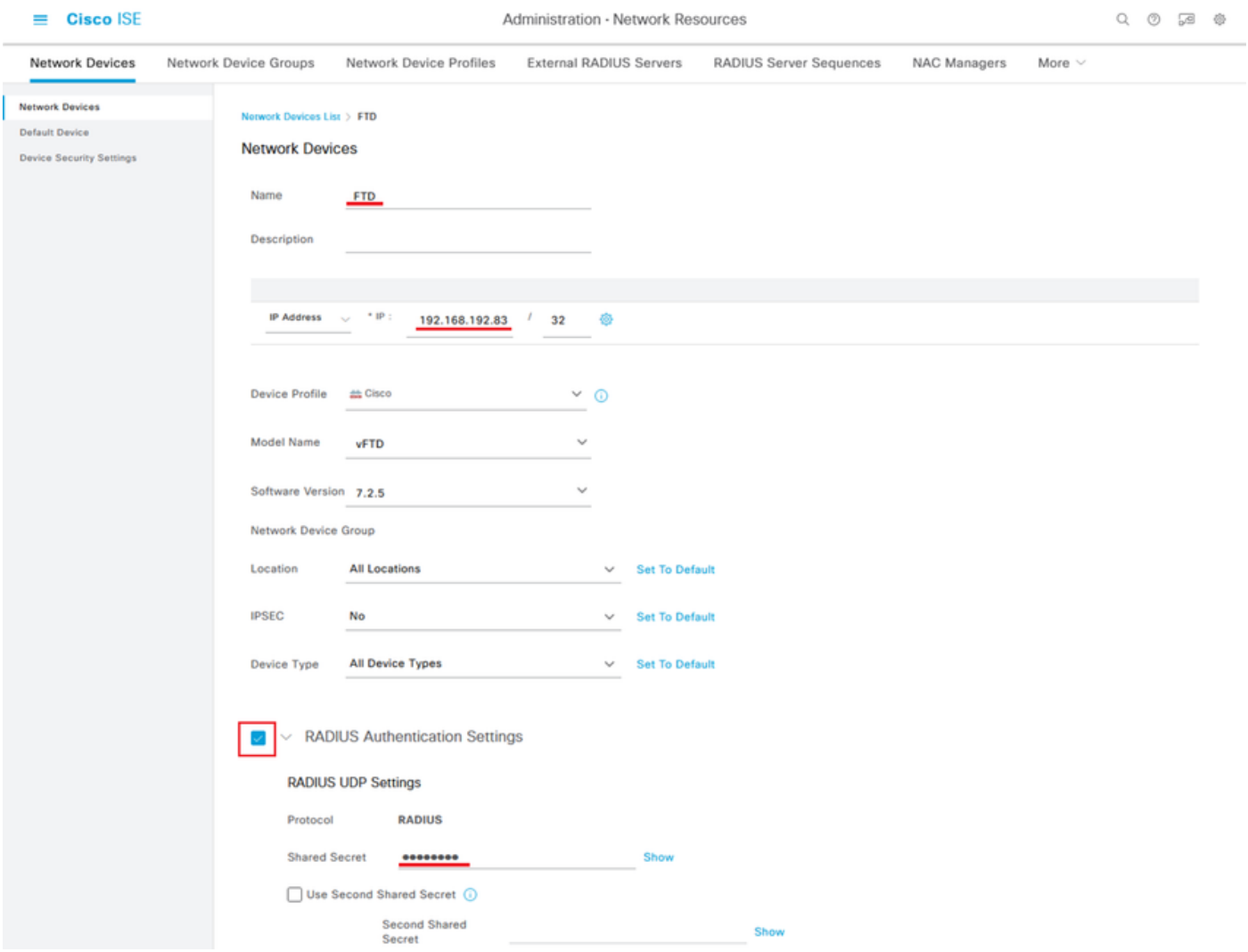


Passaggio 2.1. Ripetete la stessa procedura per aggiungere l'FTD.

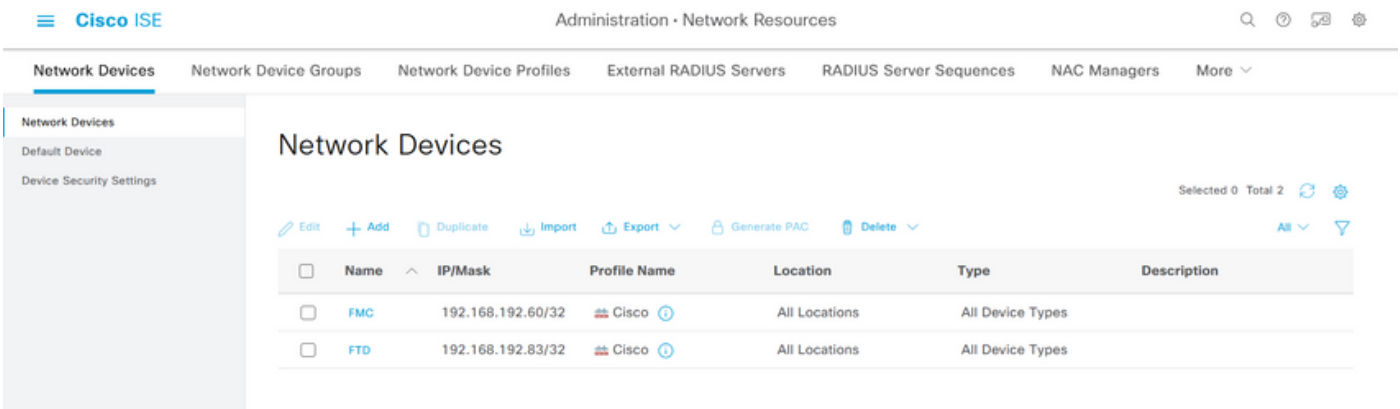
Assegnare un Nome all'oggetto dispositivo di rete e inserire l'indirizzo IP FTD.

Selezionare la casella di controllo RADIUS e definire un segreto condiviso.

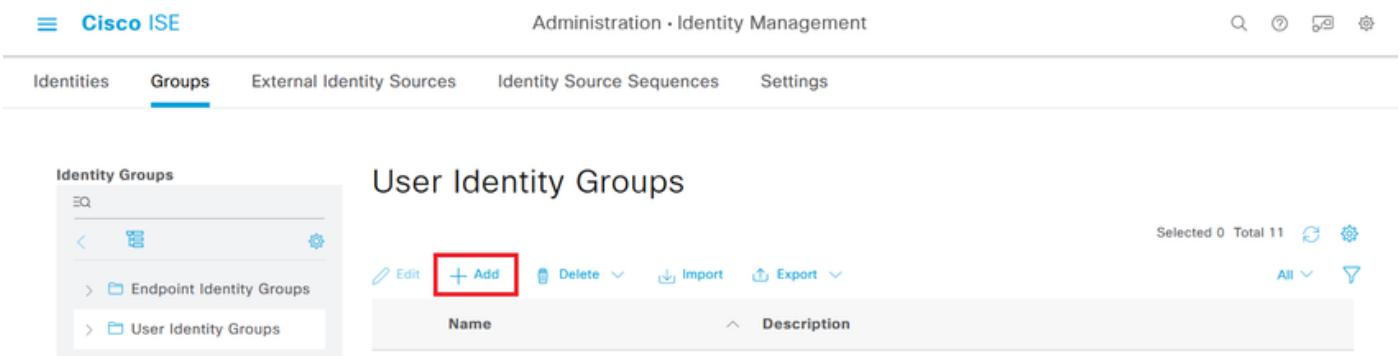
Al termine, fare clic su Salva.



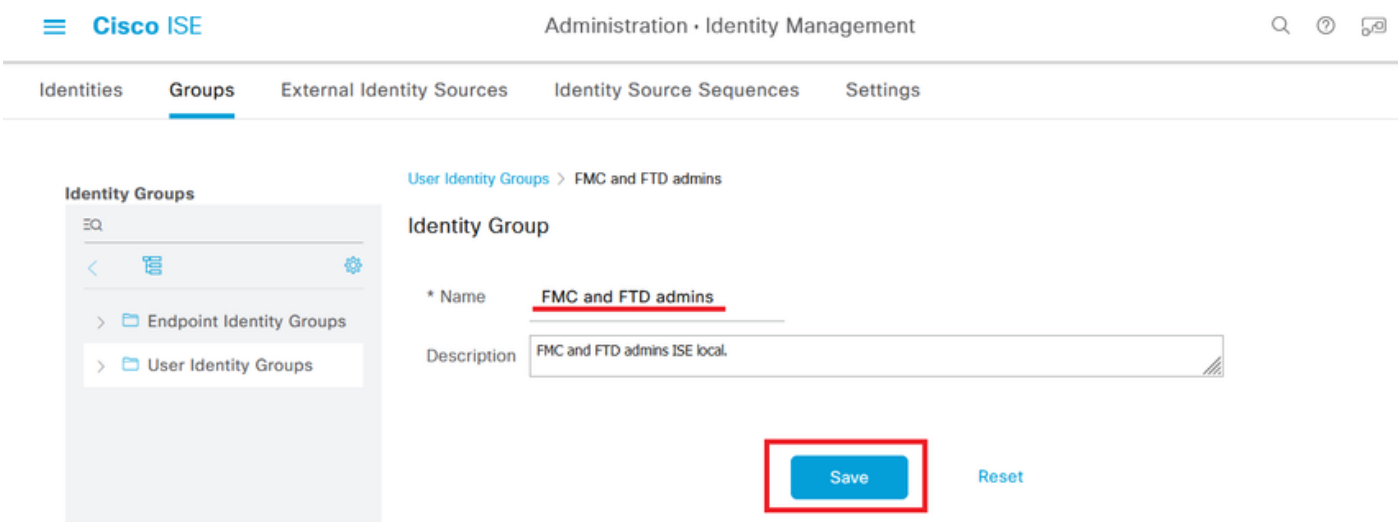
Passaggio 2.3. Verificare che entrambe le periferiche siano visualizzate in Periferiche di rete.



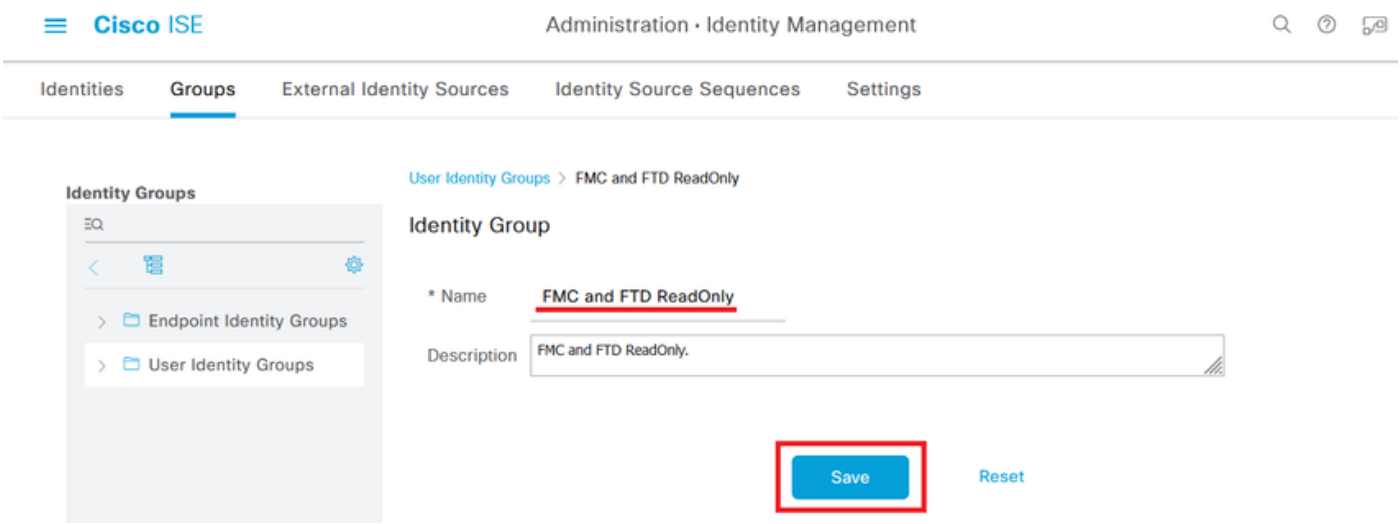
Passaggio 3. Creare i gruppi di identità utente richiesti. Passare all'icona del hamburger situata nell'angolo superiore sinistro > Amministrazione > Gestione delle identità > Gruppi > Gruppi identità utente > + Aggiungi



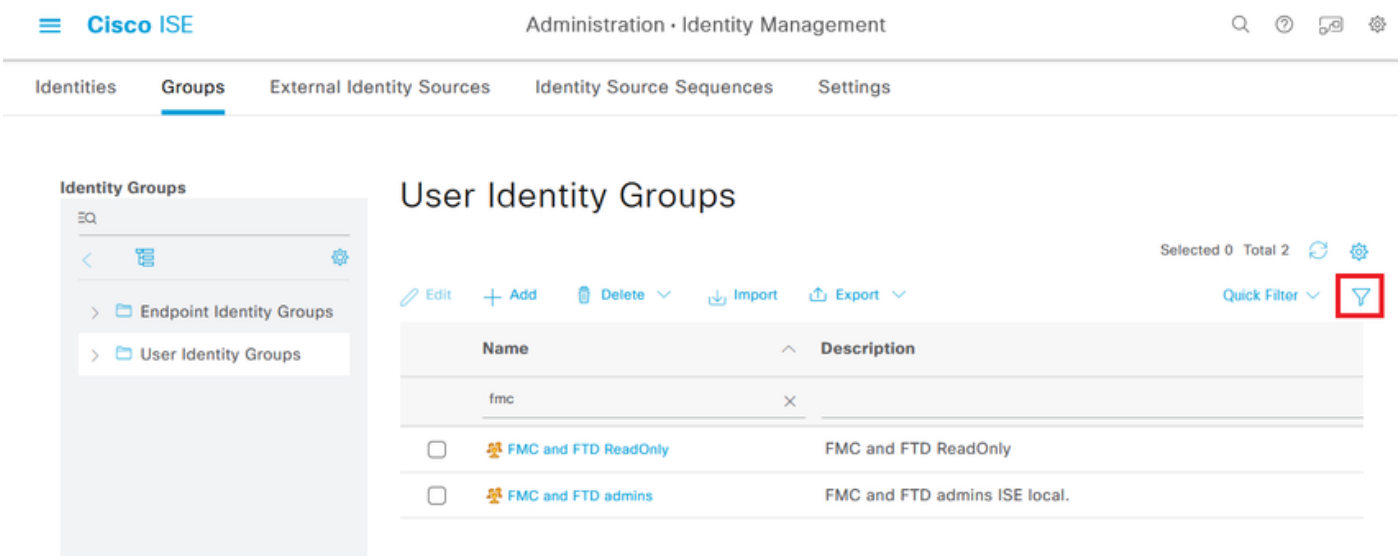
Passaggio 4. Assegnare un nome a ogni gruppo e scegliere Salva singolarmente. In questo esempio viene creato un gruppo per gli utenti con privilegi di amministratore e un altro per gli utenti di sola lettura. Creare innanzitutto il gruppo per l'utente con diritti di amministratore.



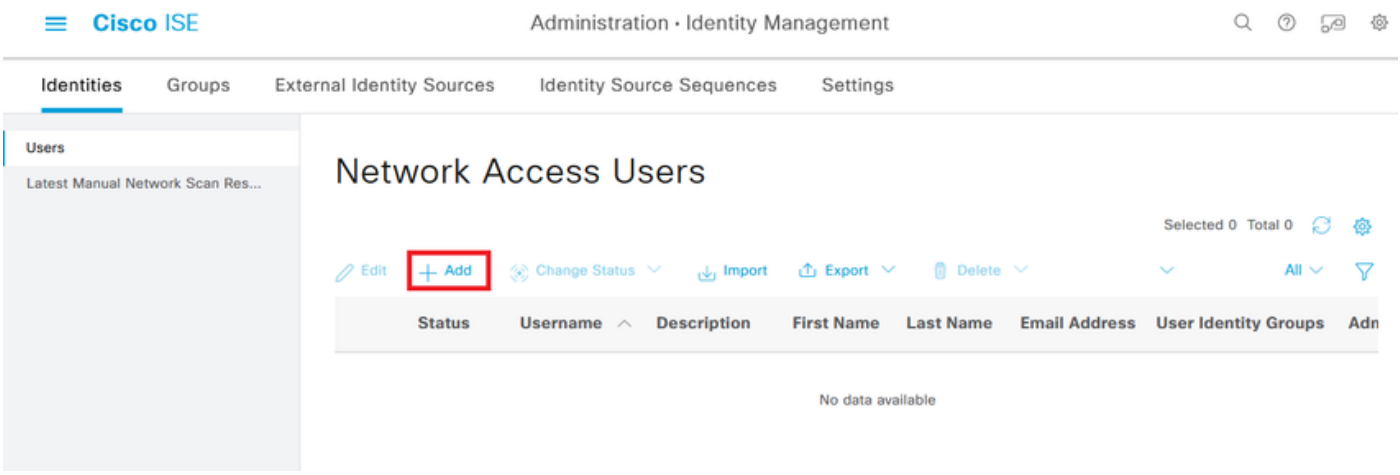
Passaggio 4.1. Creare il secondo gruppo per l'utente ReadOnly.



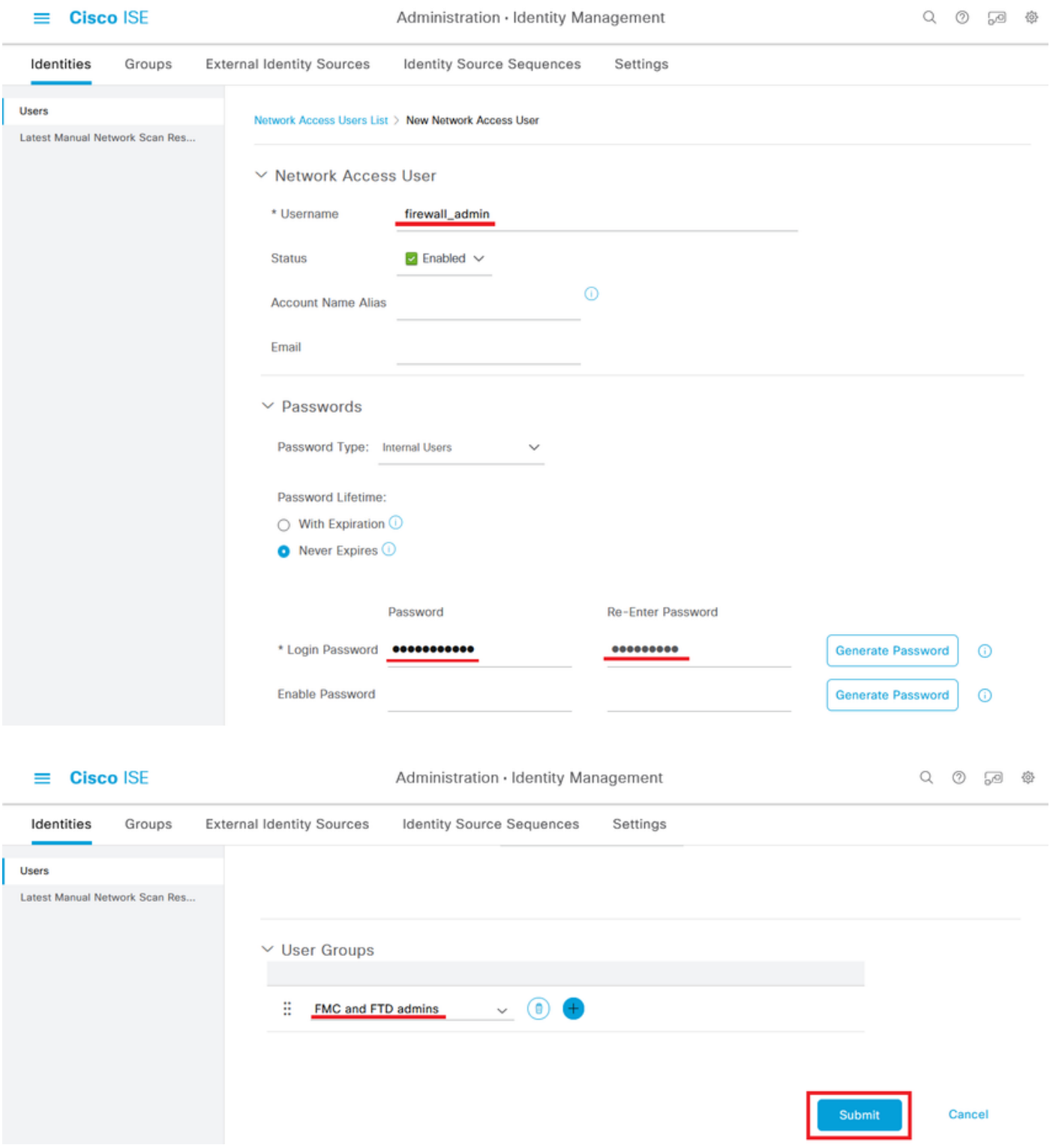
Passaggio 4.2. Verificare che entrambi i gruppi siano visualizzati nell'elenco Gruppi identità utente. Utilizzare il filtro per trovarli facilmente.



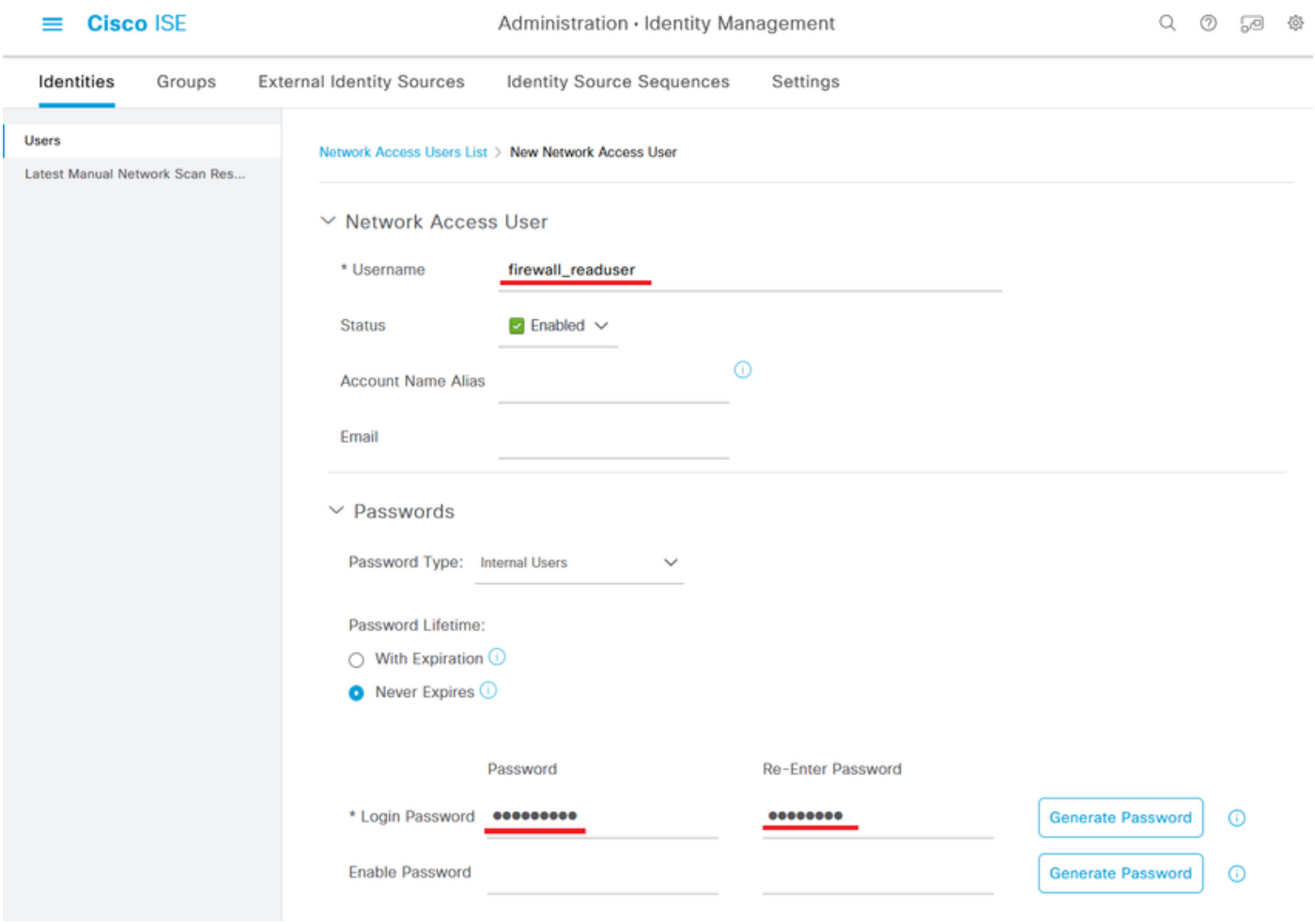
Passaggio 5. Creare gli utenti locali e aggiungerli al gruppo corrispondente. Passare a > Amministrazione > Gestione delle identità > Identità > + Aggiungi.

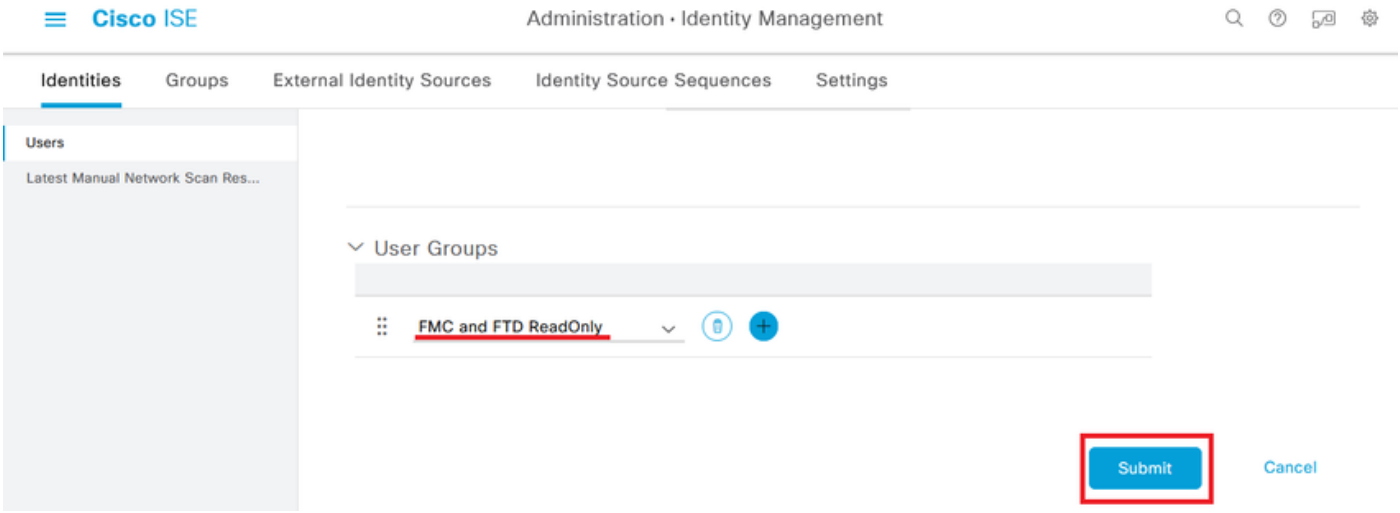


Passaggio 5.1. Creare innanzitutto l'utente con diritti di amministratore. Assegnare un nome, una password e il gruppo FMC e FTD admins.



Passaggio 5.2. Aggiungere l'utente con diritti di sola lettura. Assegnare un nome, una password e il gruppo FMC e FTD ReadOnly.



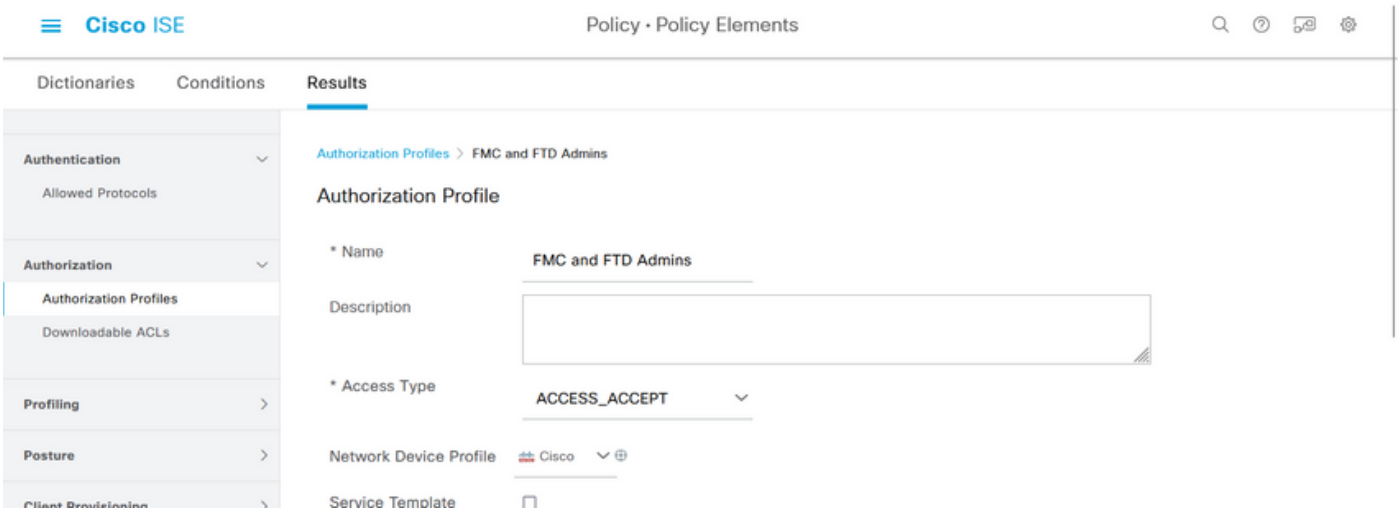


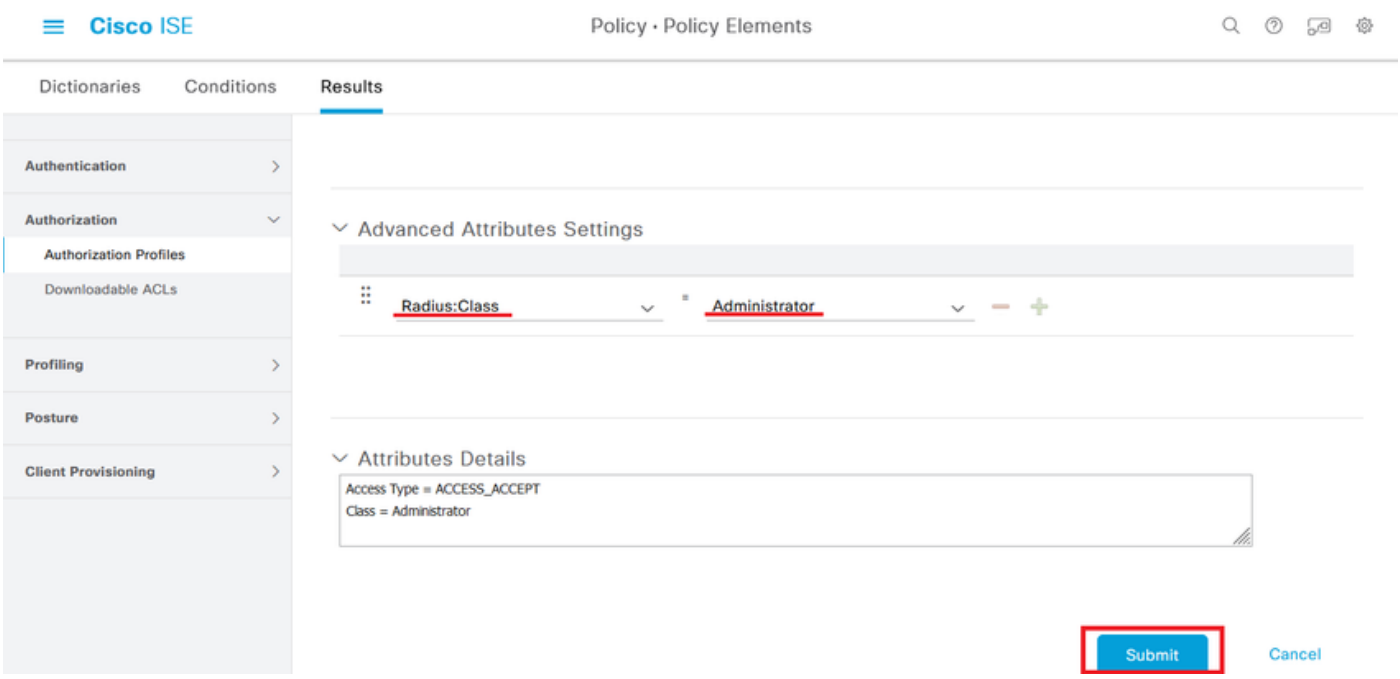
Passaggio 6. Creare il profilo di autorizzazione per l'utente Admin.

Passare a

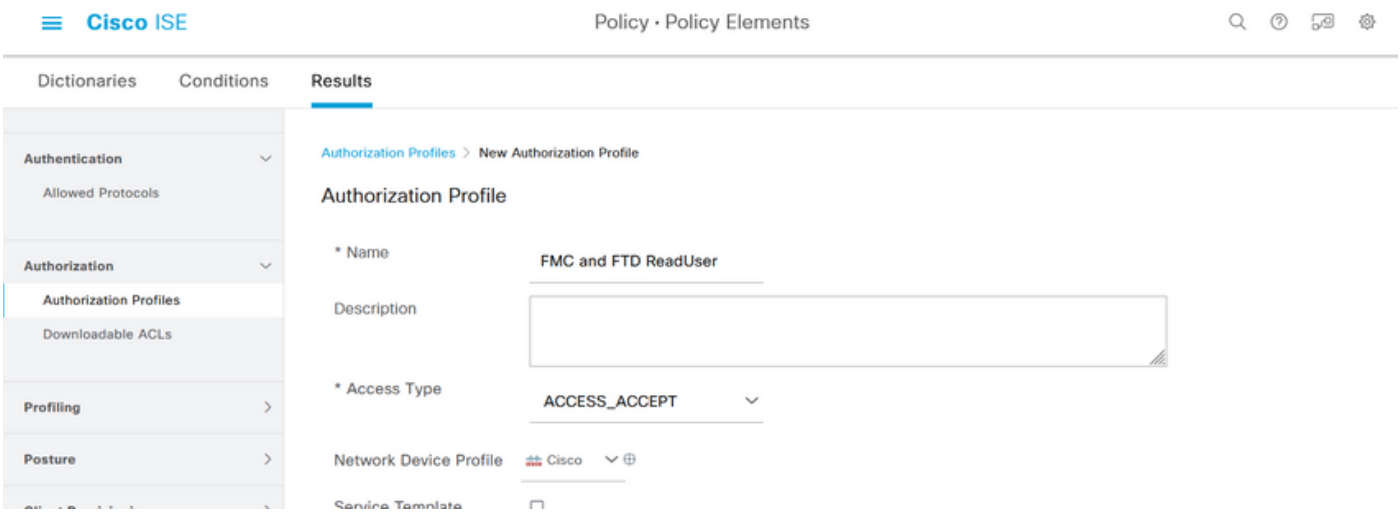
> Criterio > Elementi criteri > Risultati > Autorizzazione > Profili di autorizzazione > +Aggiungi.

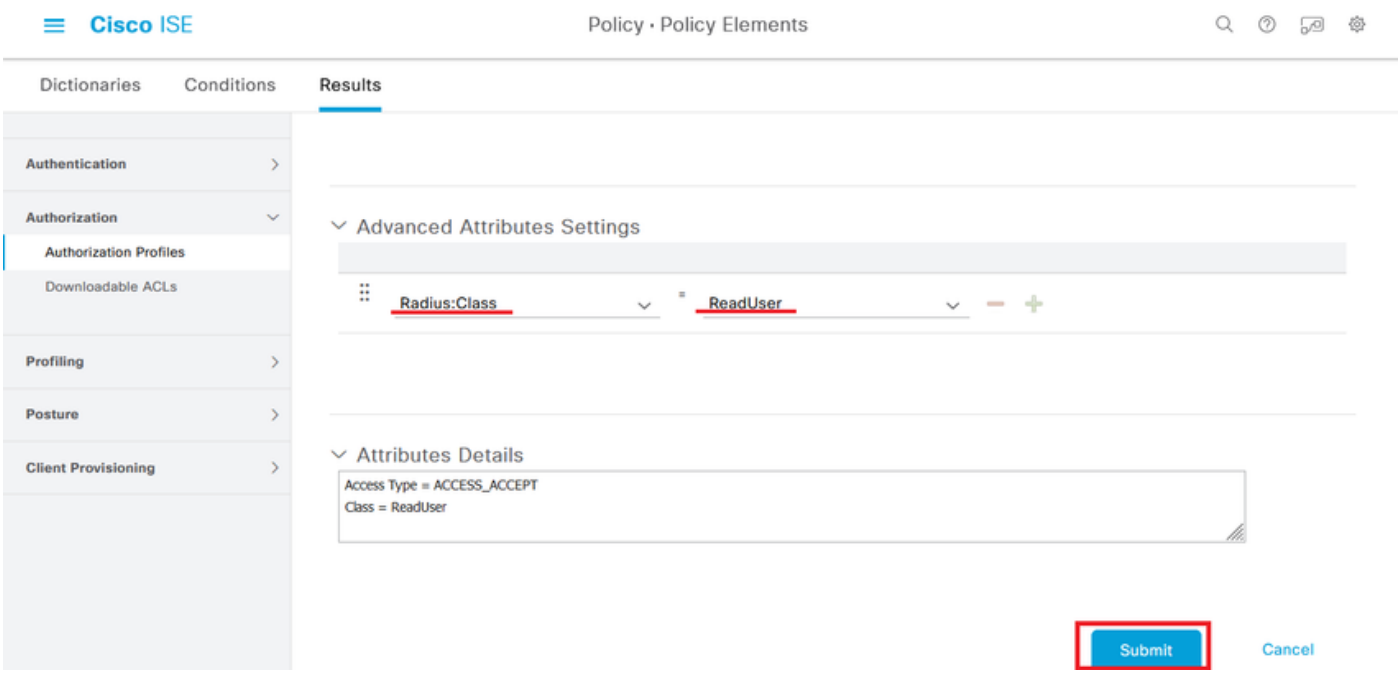
Definire un nome per il profilo di autorizzazione, lasciare il tipo di accesso impostato su ACCESS_ACCEPT e in Impostazioni avanzate attributi aggiungere un raggio > Classe—[25] con il valore Administrator e fare clic su Submit (Invia).





Passaggio 7. Ripetere il passaggio precedente per creare il profilo di autorizzazione per l'utente di sola lettura. Creare la classe Radius con il valore ReadUser invece di Administrator.

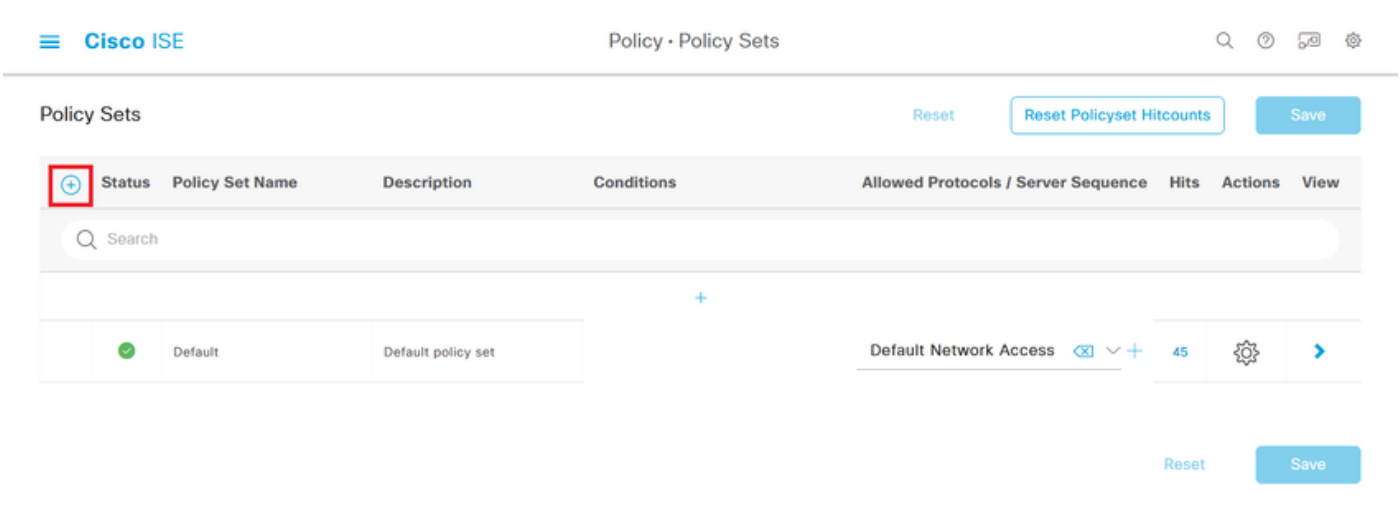




Passaggio 8. Creare un set di criteri corrispondente all'indirizzo IP del CCP. In questo modo si impedisce ad altre periferiche di concedere l'accesso agli utenti.

Selezionare
> Criterio > Set di criteri > icona

posizionata nell'angolo superiore sinistro.

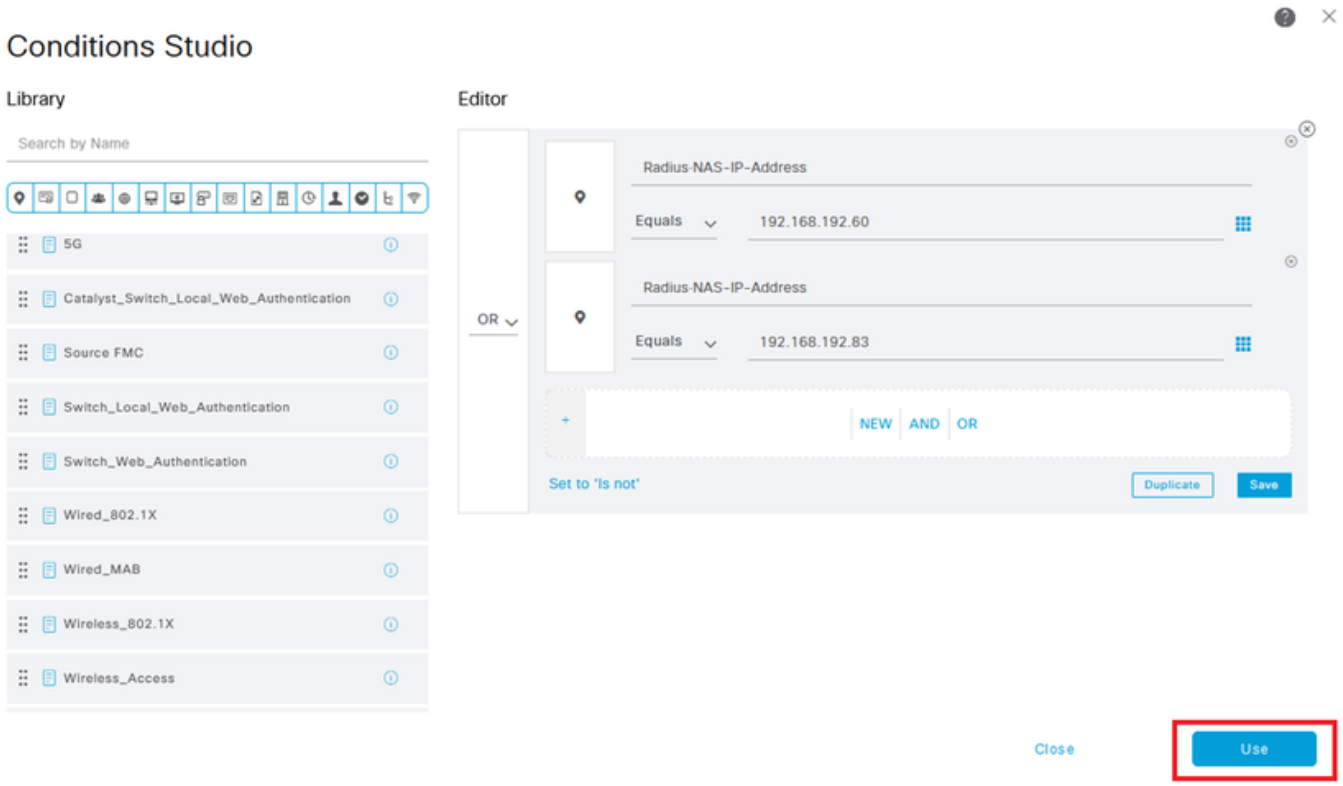


Passaggio 8.1. Una nuova riga viene posizionata all'inizio dei set di criteri.

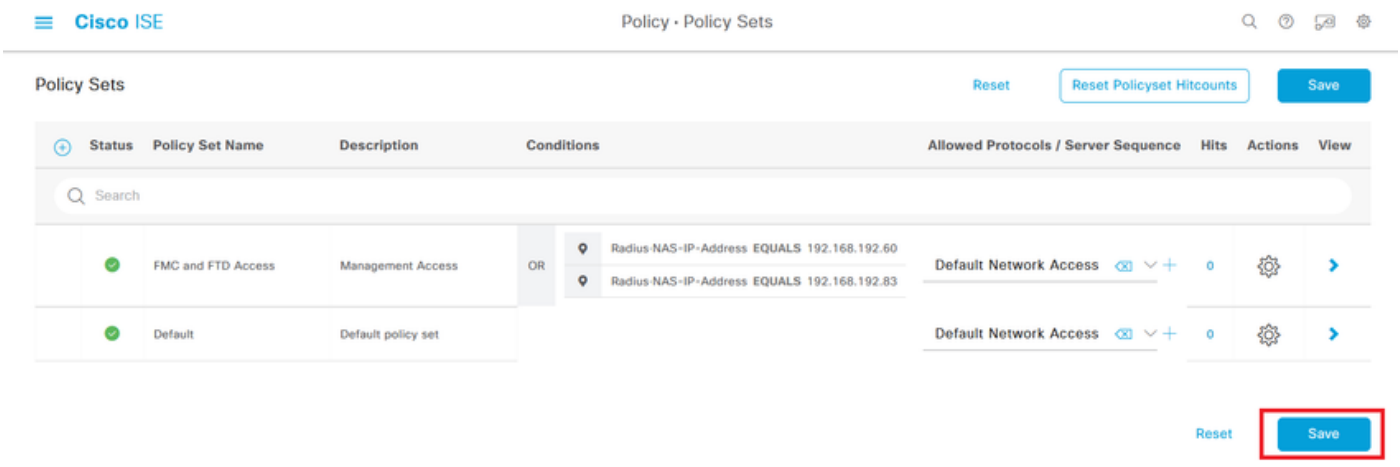
Assegnare un nome al nuovo criterio e aggiungere una condizione superiore per l'attributo RADIUS NAS-IP-Address corrispondente all'indirizzo IP della console centrale di gestione.

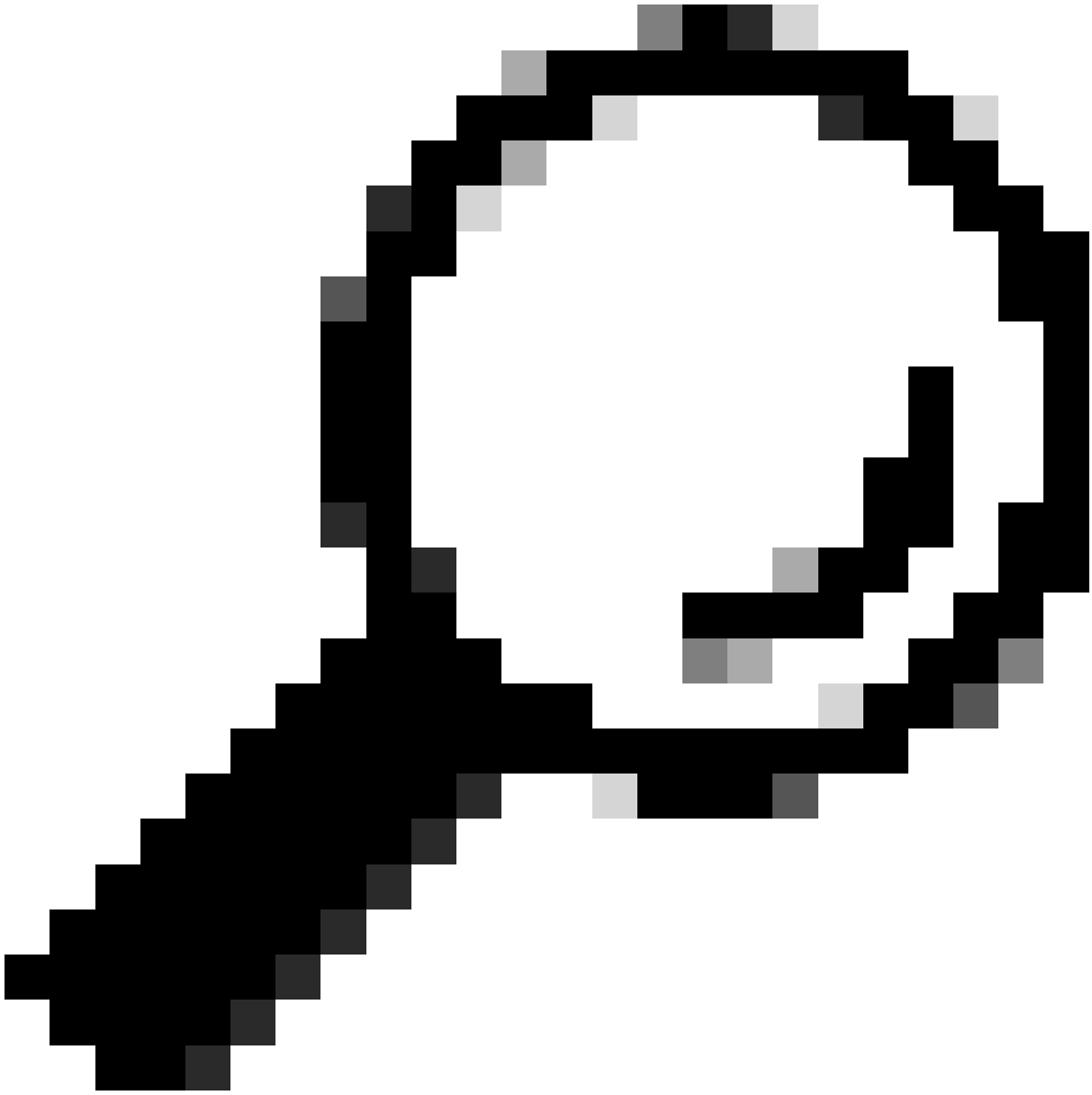
Aggiungere una seconda condizione con la congiunzione OR per includere l'indirizzo IP dell'FTD.

Fate clic su Usa (Use) per mantenere le modifiche e uscire dall'editor.



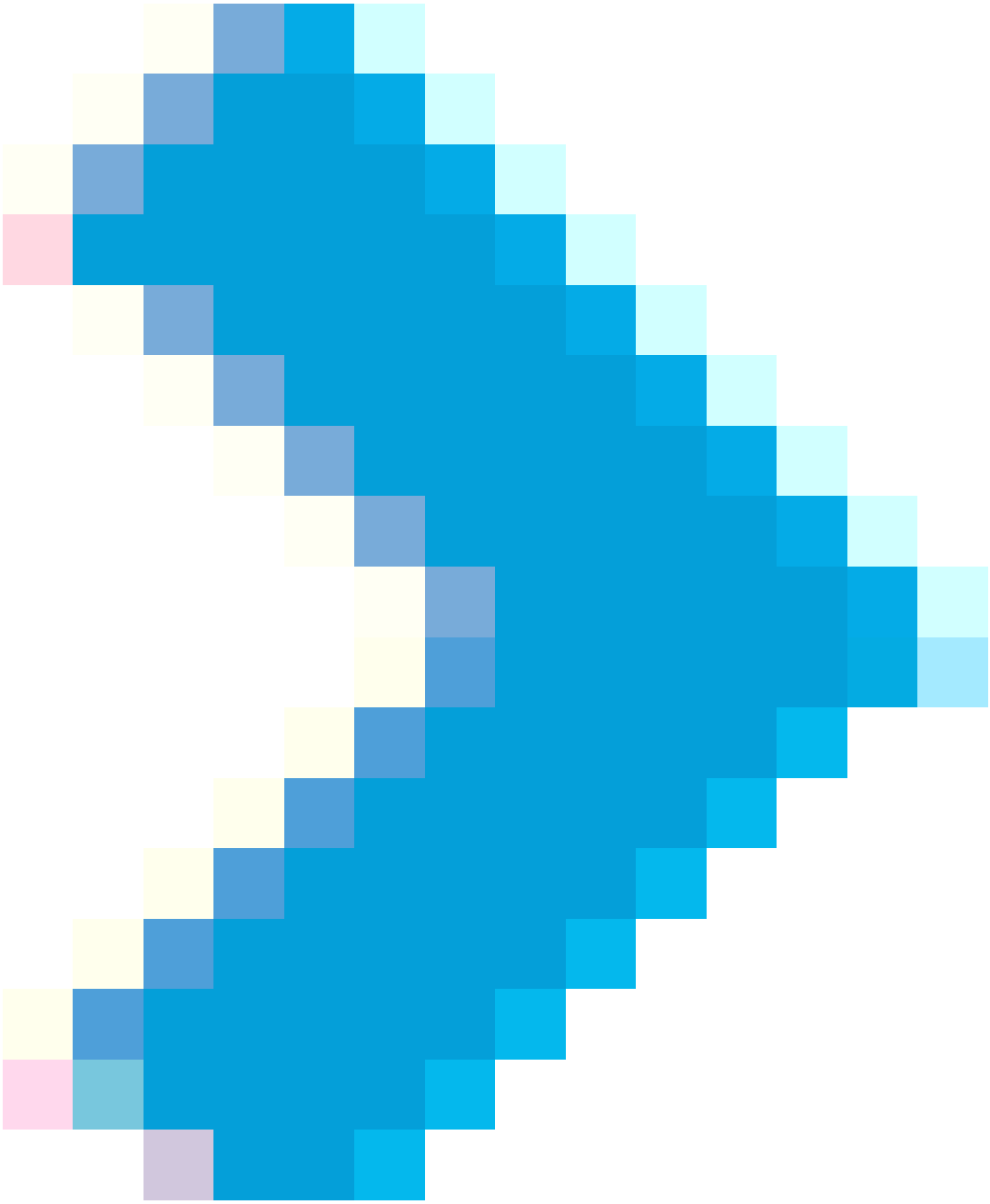
Passaggio 8.2. Al termine, fare clic su Salva.





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 9. Visualizzare il nuovo set di criteri facendo clic sull



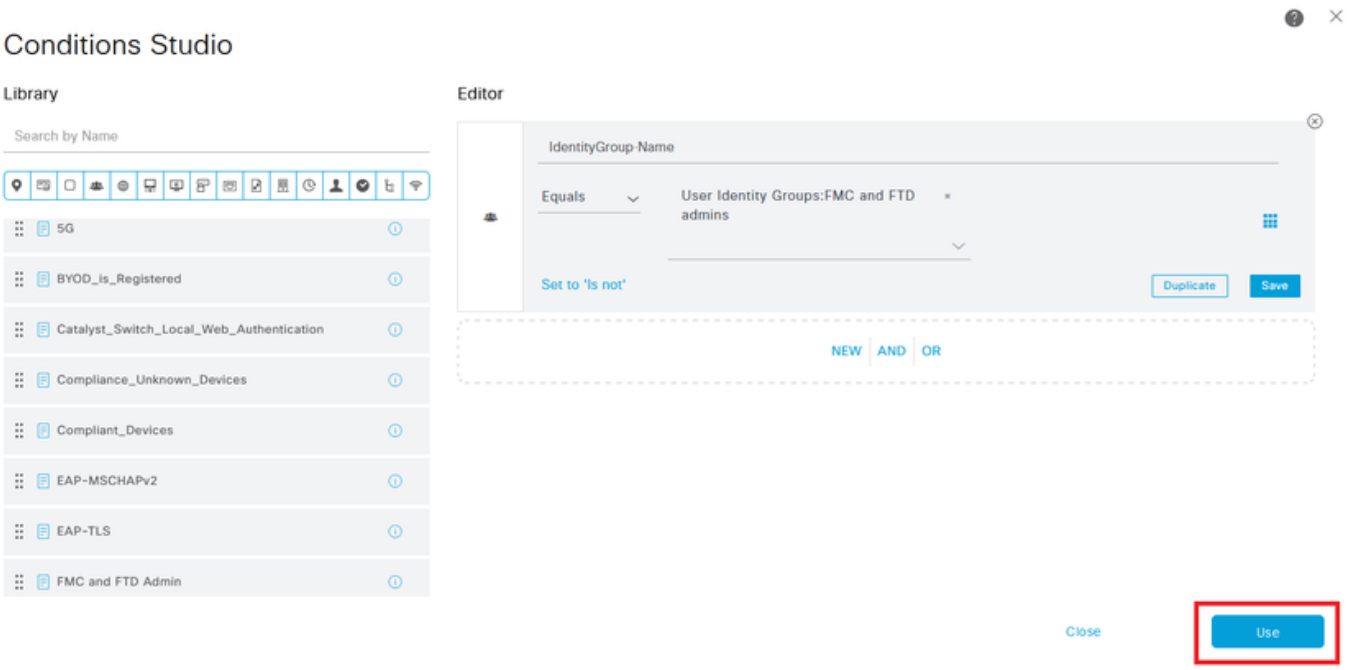
'icona posizionata alla fine della riga.

Espandere il menu Criteri di autorizzazione e fare clic sull

'icona per aggiungere una nuova regola per consentire l'accesso all'utente con diritti di amministratore.

Dagli un nome.

Impostare le condizioni in modo che corrispondano al gruppo di identità del dizionario con Nome attributo Uguale a Gruppi di identità utente: Amministratori FMC e FTD (il nome del gruppo creato nel passaggio 4) e fare clic su Usa.

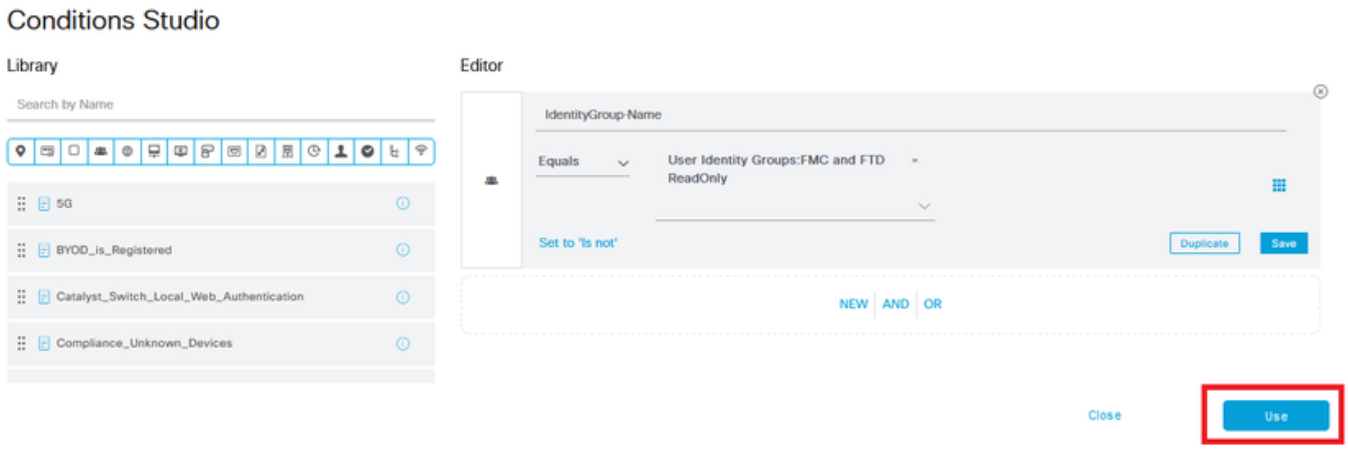


Passaggio 10. Fare clic sull'icona per aggiungere una seconda regola per consentire l'accesso all'utente con diritti di sola lettura.

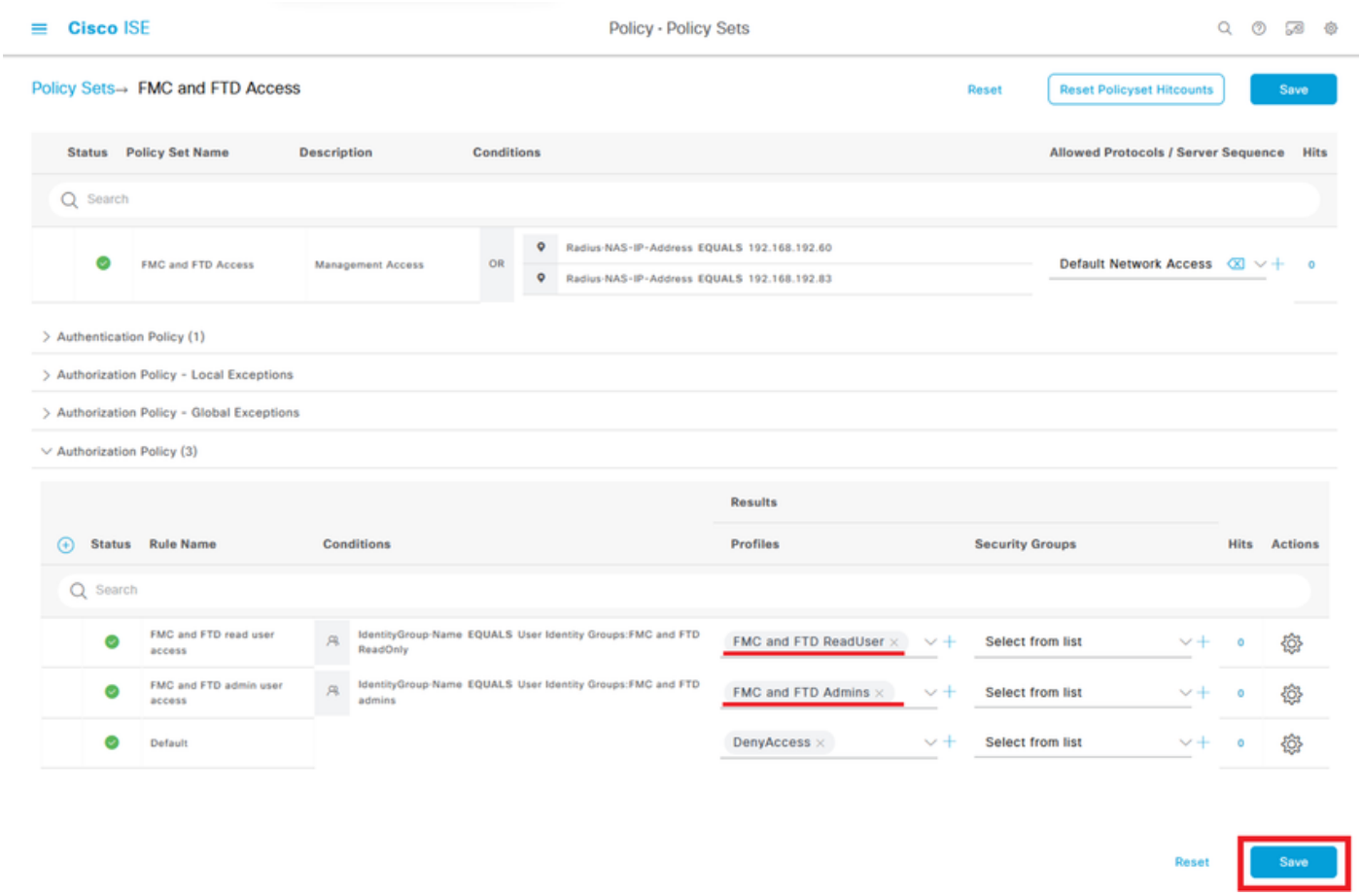
Dagli un nome.

Impostare le condizioni in modo che corrispondano al gruppo di identità del dizionario con Nome

attributo Uguale a Gruppi di identità utente: FMC e FTD Sola lettura (il nome del gruppo creato al passaggio 4) e fare clic su Usa.

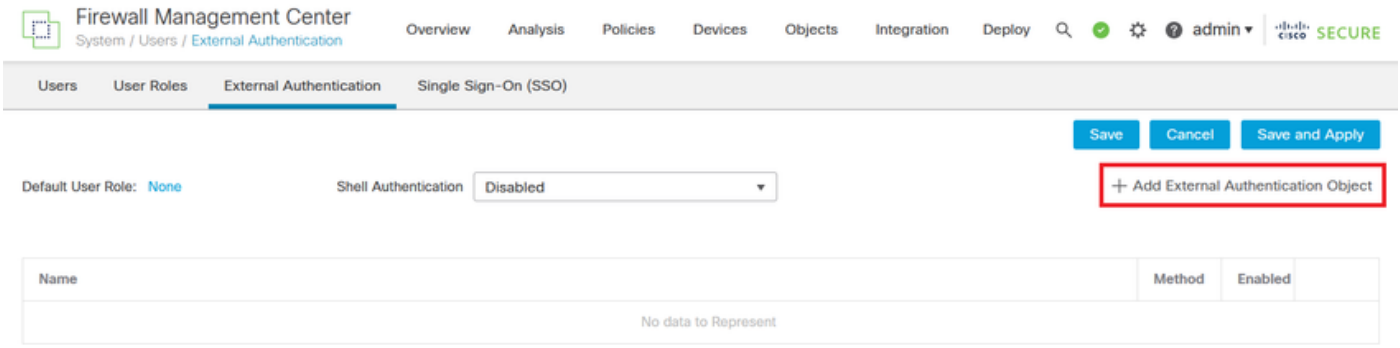


Passaggio 11. Impostare i profili di autorizzazione per ogni regola e fare clic su Salva.



Configurazione FMC

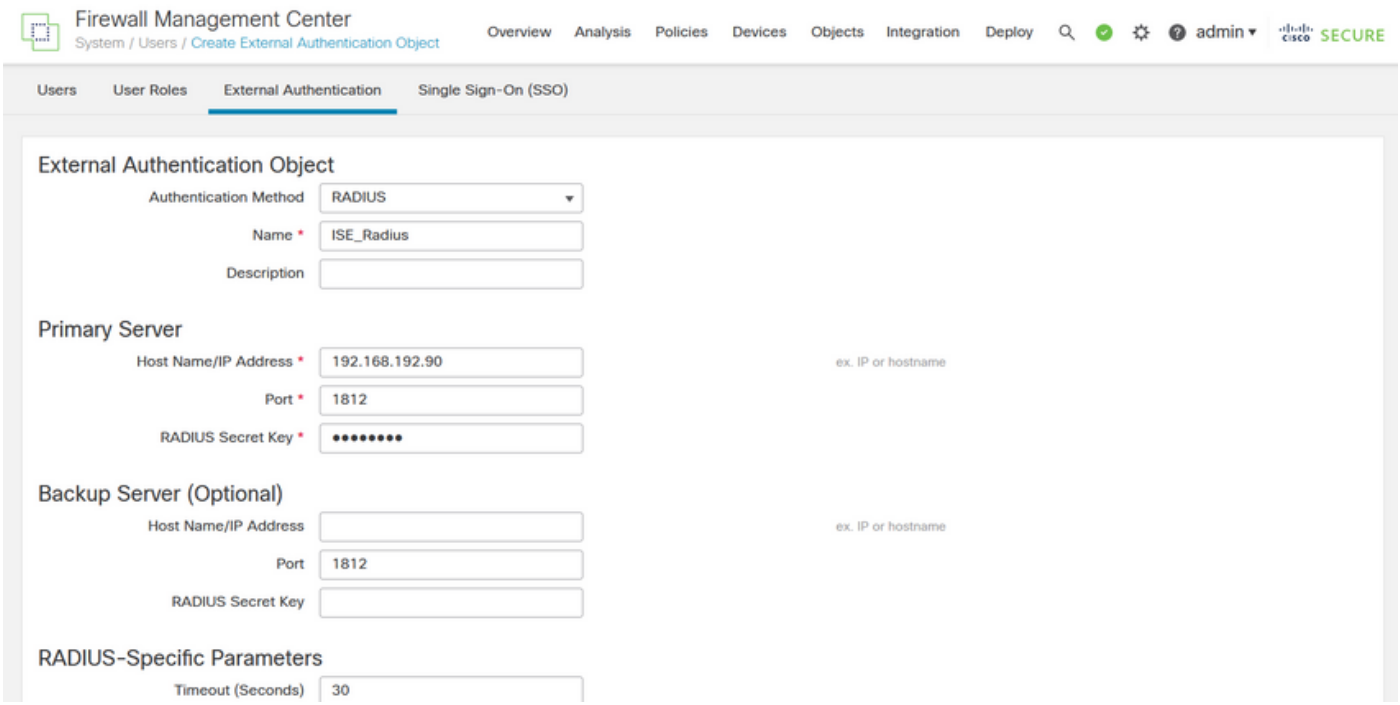
Passaggio 1. Creare l'oggetto di autenticazione esterna in Sistema > Utenti > Autenticazione esterna > + Aggiungi oggetto di autenticazione esterna.



Passaggio 2. Selezionare RADIUS come metodo di autenticazione.

In Oggetto autenticazione esterna assegnare un nome al nuovo oggetto.

Quindi, nell'impostazione Server primario, inserire l'indirizzo IP ISE e la stessa chiave privata RADIUS usata nel passo 2 della configurazione ISE.

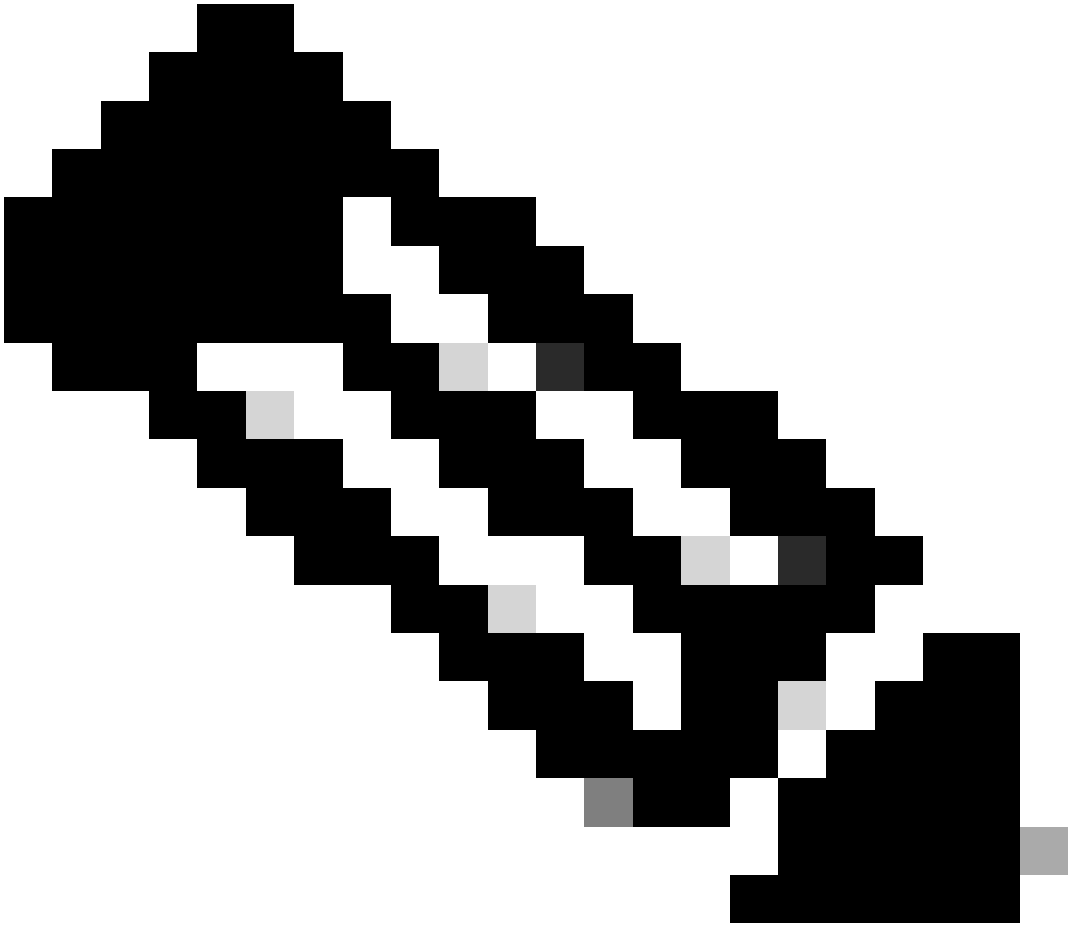


Passaggio 3. Inserire i valori degli attributi della classe RADIUS configurati nei passaggi 6 e 7 della configurazione ISE: Administrator e ReadUser rispettivamente per firewall_admin e firewall_readuser.

RADIUS-Specific Parameters

Timeout (Seconds)	30
Retries	3
Access Admin	
Administrator	Class=Administrator
Discovery Admin	
External Database User	
Intrusion Admin	
Maintenance User	
Network Admin	
Security Analyst	
Security Analyst (Read Only)	Class=ReadUser
Security Approver	
Threat Intelligence Director (TID) User	
Default User Role	Access Admin Administrator Discovery Admin External Database User

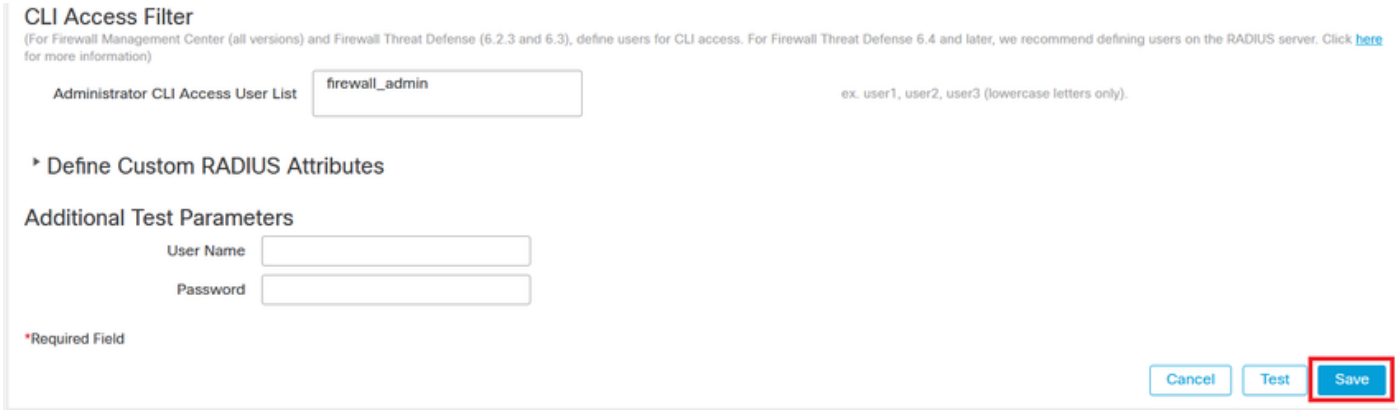
To specify the default user role if user is not found in any group



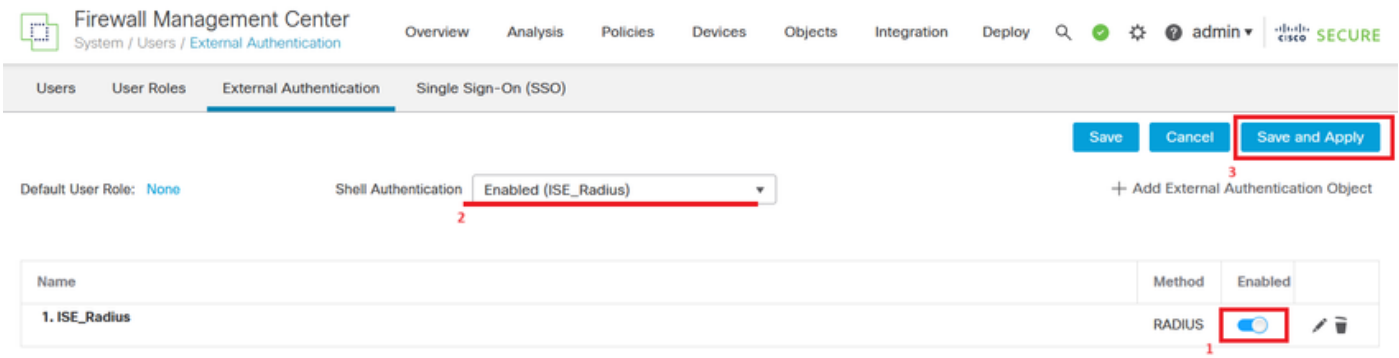
Nota: l'intervallo di timeout è diverso per l'FTD e il FMC, quindi se si condivide un oggetto e si modifica il valore predefinito di 30 secondi, assicurarsi di non superare l'intervallo di timeout più piccolo (1-300 secondi) per i dispositivi FTD. Se si imposta il timeout su un valore superiore, la configurazione RADIUS di difesa dalle minacce non funziona.

Passaggio 4. Compilare l'elenco degli utenti di accesso alla CLI dell'amministratore in CLI Access Filter con i nomi utente autorizzati ad accedere alla CLI.

Fare clic su Save (Salva) una volta terminato.

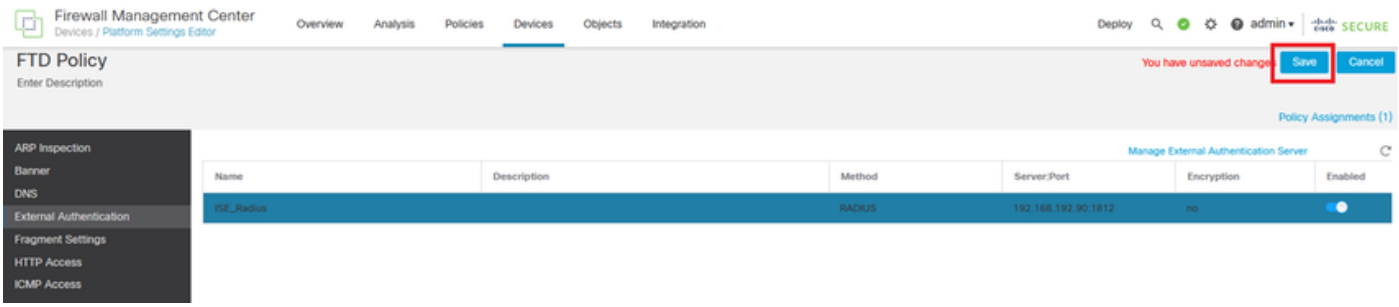


Passaggio 5. Attivare il nuovo oggetto. Impostarlo come metodo di autenticazione della shell per FMC e fare clic su Salva e applica.

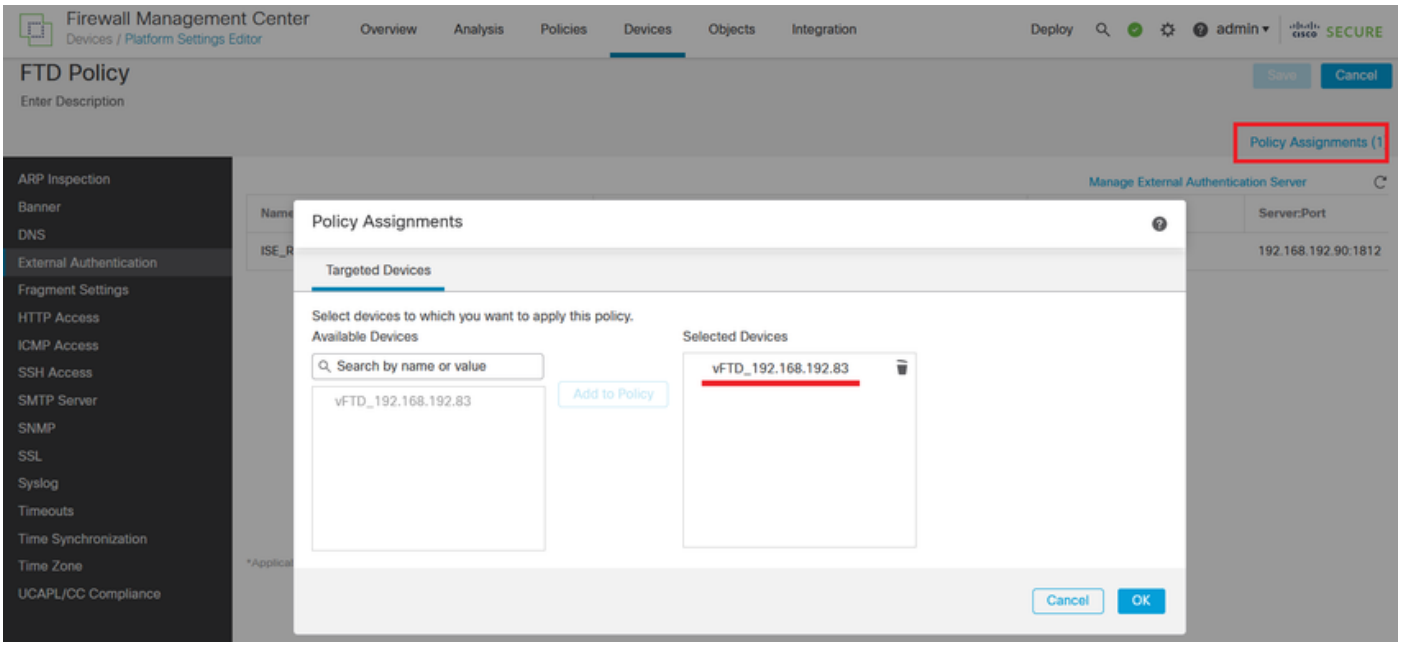


Configurazione FTD

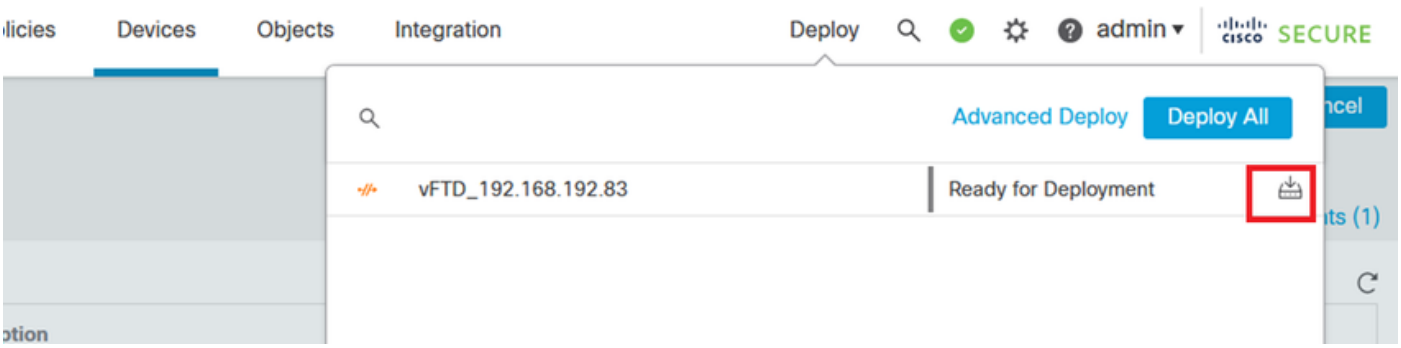
Passaggio 1. Nell'interfaccia utente di FMC, selezionare Devices > Platform Settings (Dispositivi > Impostazioni piattaforma). Modificare il criterio corrente o crearne uno nuovo se non si dispone di alcuna assegnazione all'FTD a cui è necessario accedere. Abilitare il server RADIUS in Autenticazione esterna e fare clic su Salva.



Passaggio 2. Accertarsi che l'FTD a cui è necessario accedere sia elencato in Assegnazioni criteri come dispositivo selezionato.

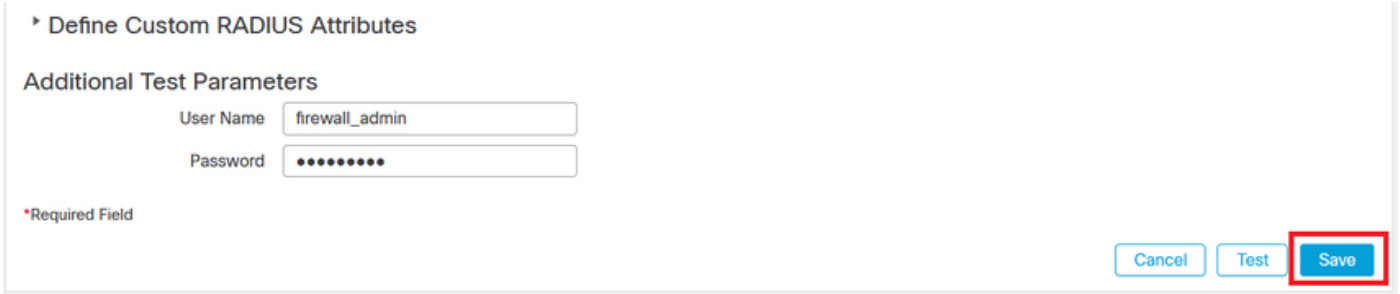


Passaggio 3. Distribuire le modifiche.

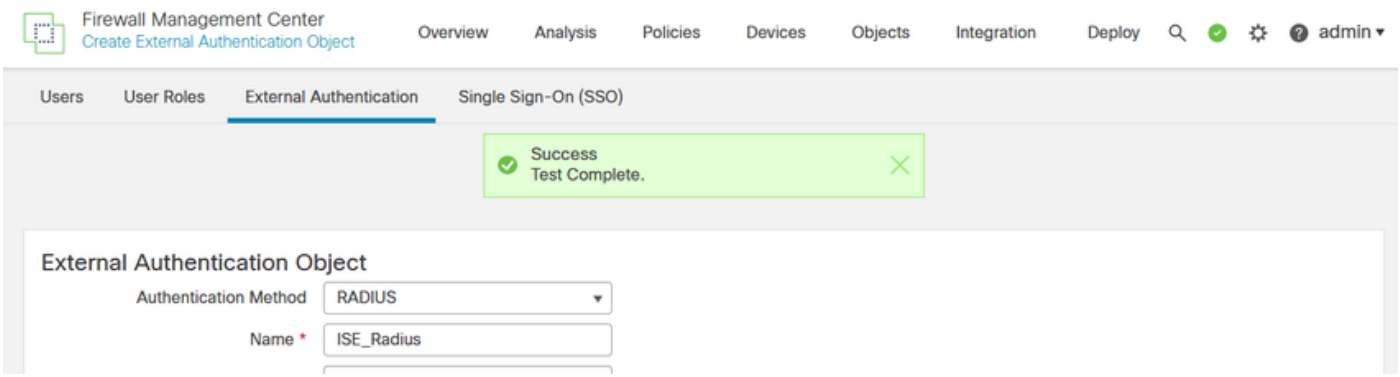


Verifica

- Verificare che la nuova distribuzione funzioni correttamente.
- Nell'interfaccia utente di FMC passare alle impostazioni del server RADIUS e scorrere verso il basso fino alla sezione Parametri di test aggiuntivi.
- Immettere un nome utente e una password per l'utente ISE e fare clic su Test.



- Se il test ha esito positivo, nella parte superiore della finestra del browser viene visualizzato il messaggio verde Test completato.



- Per ulteriori informazioni, espandere Dettagli in Output test.

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).