Configurazione dell'autenticazione esterna di FMC in ambienti multidominio

Sommario

Introduzione

In questo documento viene descritta l'implementazione della multitenancy (multidominio) nell'FMC Cisco e viene usata la tecnologia Cisco ISE per l'autenticazione RADIUS centralizzata.

Prerequisiti

Requisiti

È consigliabile conoscere i seguenti argomenti:

- Configurazione iniziale di Cisco Secure Firewall Management Center tramite GUI e/o shell.
- Privilegi di amministratore completi nel dominio globale della console centrale di gestione del sistema per creare sottodomini e oggetti di autenticazione esterna.
- Configurazione dei criteri di autenticazione e autorizzazione su ISE.
- Conoscenze base di RADIUS

Componenti usati

- Cisco Secure FMC: vFMC 7.4.2 (o versione successiva consigliata per la stabilità multidominio)
- Struttura dominio: Una gerarchia a tre livelli (Globale > Sottodomini di secondo livello).
- Cisco Identity Services Engine: ISE 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.

Premesse

Negli ambienti aziendali su larga scala o negli scenari MSSP (Managed Security Service Provider), è spesso necessario segmentare la gestione della rete in confini amministrativi distinti. In questo documento viene descritto come configurare FMC per il supporto di più domini, in particolare per un esempio reale in cui un provider di servizi condivisi gestisce due client: Retail-A e Finance-B. Utilizzando l'autenticazione RADIUS esterna tramite Cisco ISE, gli amministratori possono garantire che gli utenti ricevano automaticamente la concessione dell'accesso solo ai rispettivi domini in base alle credenziali centralizzate.

Il sistema Cisco Secure Firewall utilizza i domini per implementare la multitenancy.

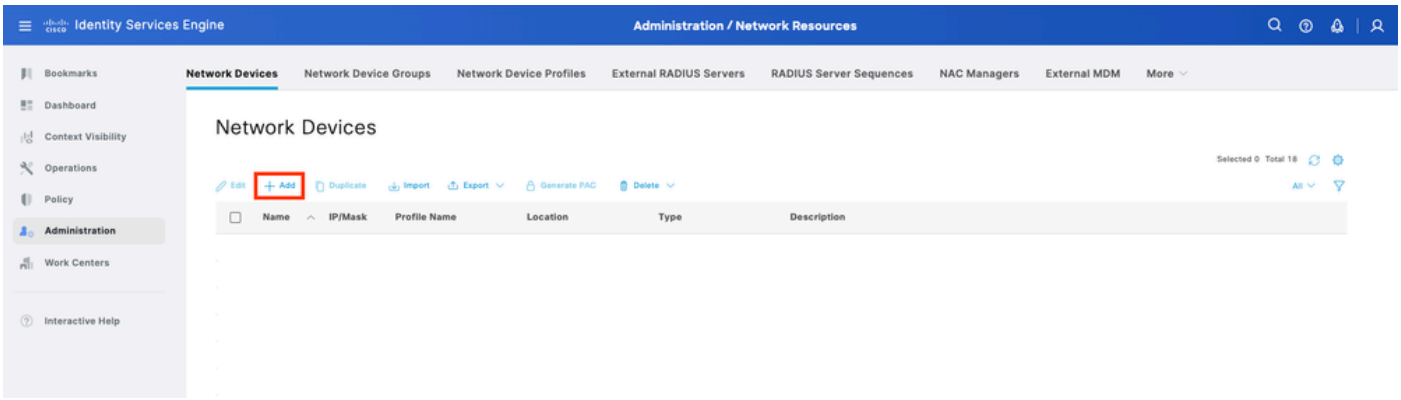
- Gerarchia dominio: La gerarchia inizia dal dominio globale. È possibile creare fino a 100 sottodomini in una struttura a due o tre livelli.
- Domini foglia: Si tratta di domini nella parte inferiore della gerarchia senza ulteriori sottodomini. È fondamentale che ciascun dispositivo FTD gestito sia associato esattamente a un dominio foglia.
- Attributo classe RADIUS (attributo 25): In un'installazione multidominio, il FMC utilizza l'attributo RADIUS Class restituito da ISE per mappare un utente autenticato a un dominio e a un ruolo utente specifici. Questo consente a un singolo server RADIUS di assegnare dinamicamente gli utenti a diversi segmenti di utenti (ad esempio, Retail-A e Finance-B) al momento dell'accesso.

Configurazione

Configurazione di ISE

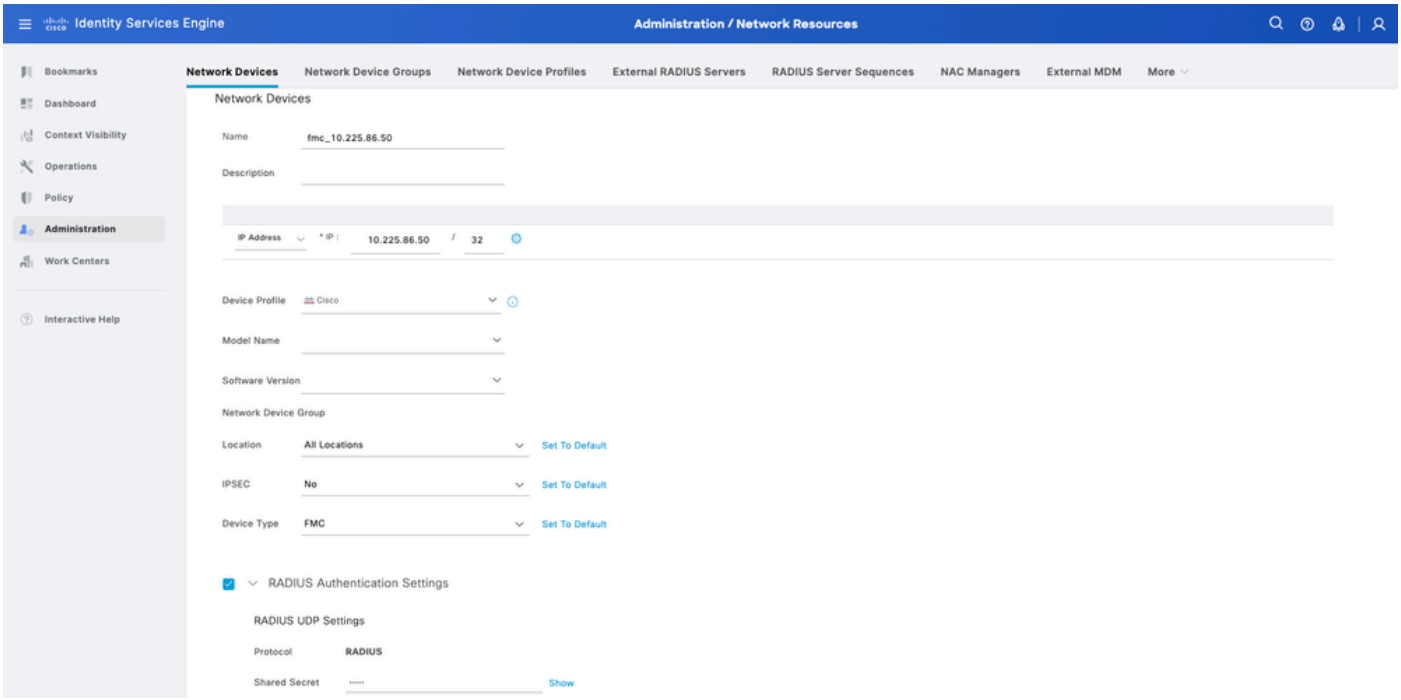
Aggiungi dispositivi di rete

Passaggio 1. Passare a Amministrazione > Risorse di rete > Dispositivi di rete > Aggiungi.



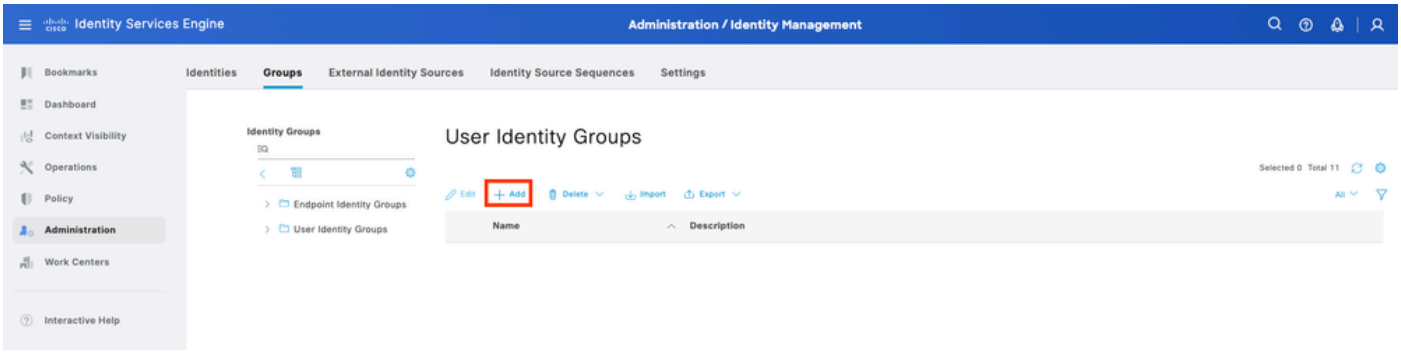
Passaggio 2. Assegnare un nome all'oggetto dispositivo di rete e inserire l'indirizzo IP del CCP.

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.

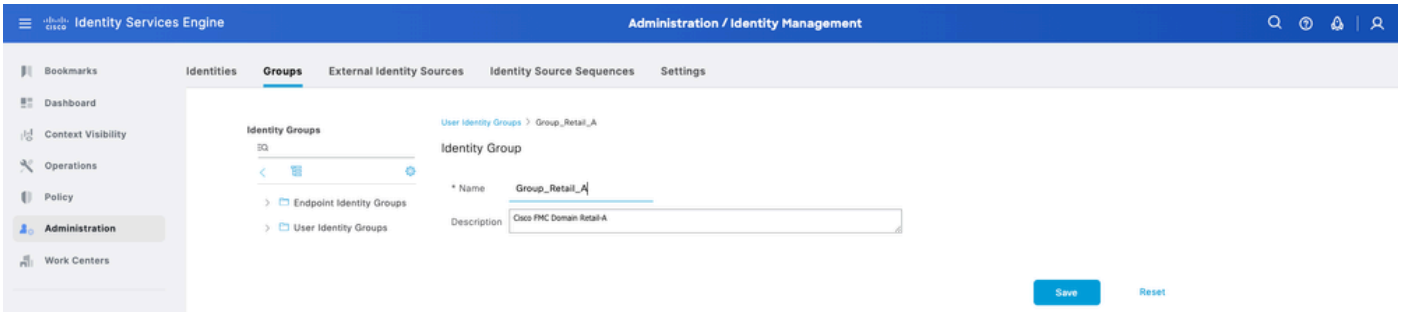


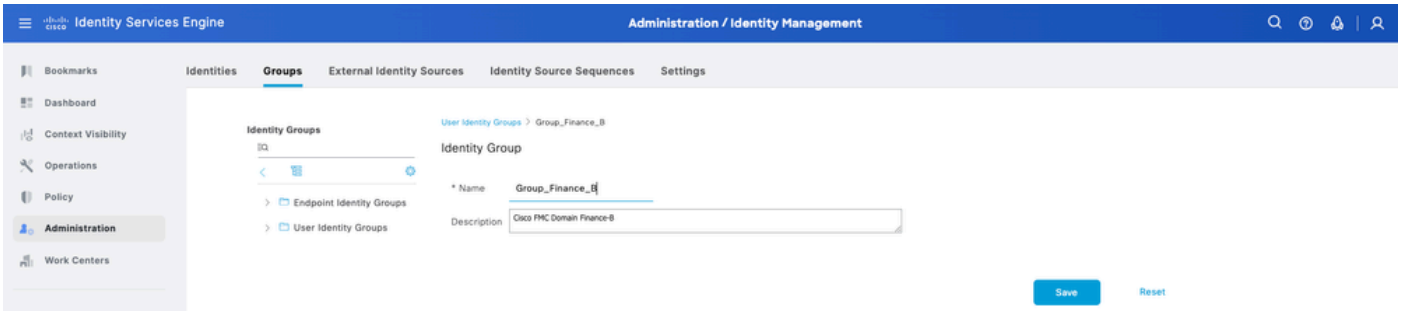
Creare i gruppi di identità e gli utenti locali

Passaggio 3. Creare i gruppi di identità utente richiesti. Passare a Amministrazione > Gestione delle identità > Gruppi > Gruppi identità utente > Aggiungi.

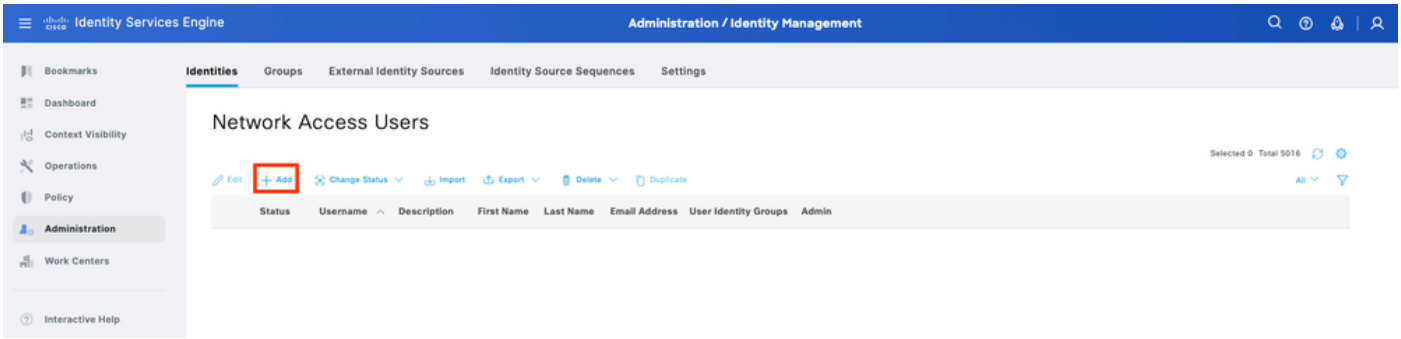


Passaggio 4. Assegnare un nome a ogni gruppo e salvare singolarmente. In questo esempio viene creato un gruppo per gli utenti Administrator. Creare due gruppi: Group_Retail_A e Group_Finance_B.

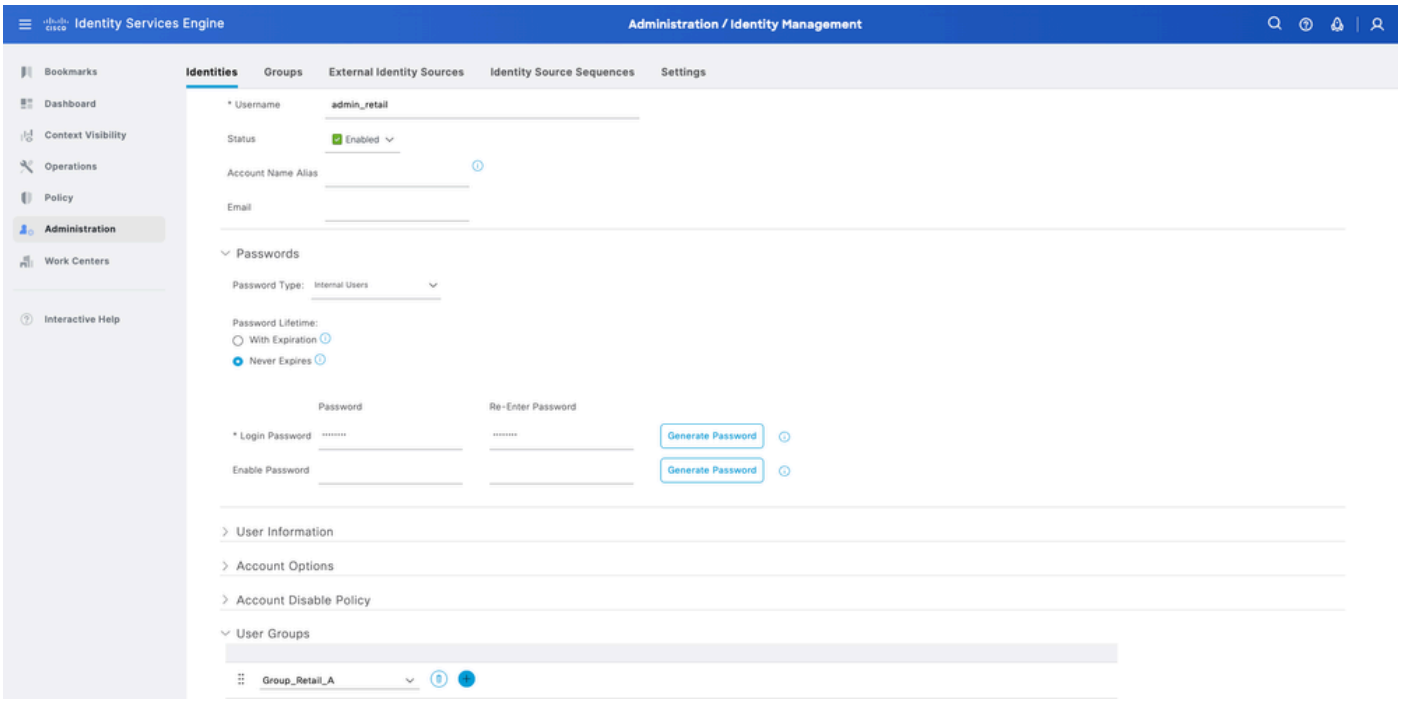




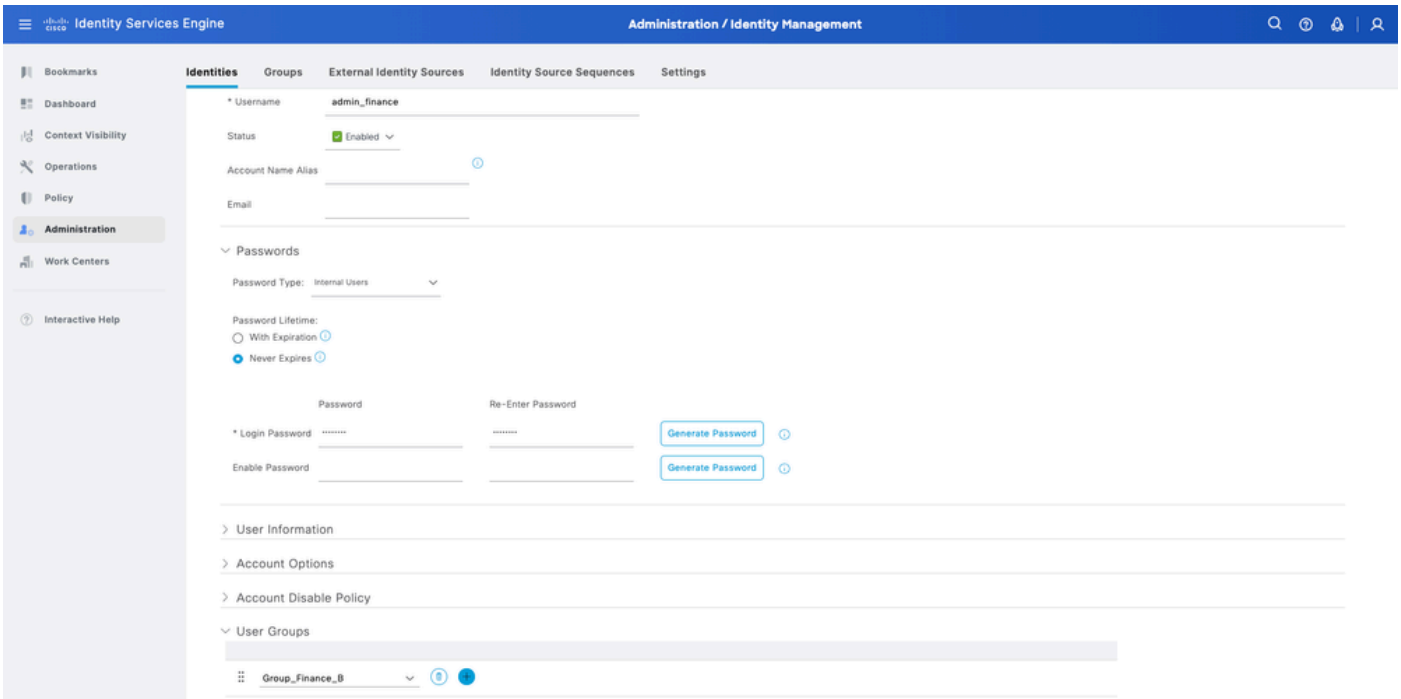
Passaggio 5. Creare gli utenti locali e aggiungerli al gruppo corrispondente. Passare a Amministrazione > Gestione delle identità > Identità > Aggiungi.



Passaggio 5.1. Creare innanzitutto l'utente con diritti di amministratore. Assegnare un nome al gruppo admin_retail, la password e il gruppo Group_Retail_A.

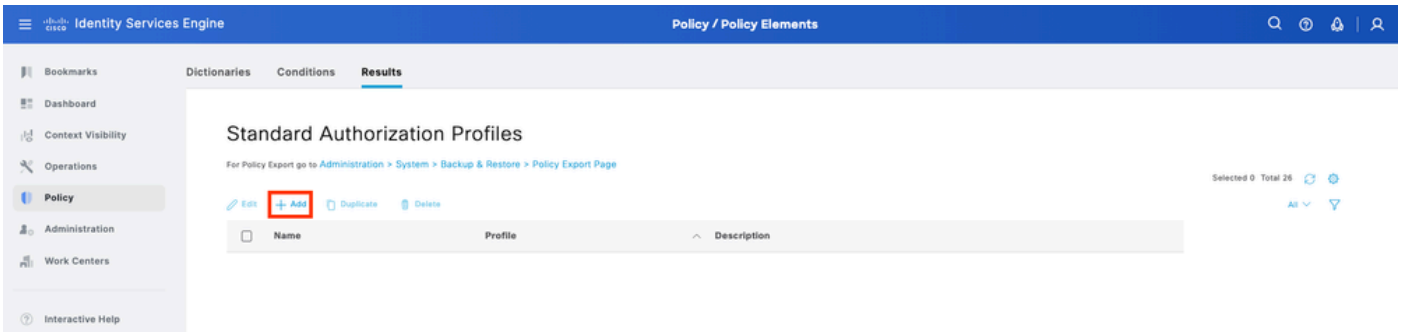


Passaggio 5.2. Creare innanzitutto l'utente con diritti di amministratore. Assegnare un nome a admin_finance, la password e il gruppo Group_Finance_B.



Creare i profili di autorizzazione

Passaggio 6. Creare il profilo di autorizzazione per l'utente Amministratore interfaccia Web di FMC. Passare a Criterio > Elementi criteri > Risultati > Autorizzazione > Profili autorizzazione > Aggiungi.

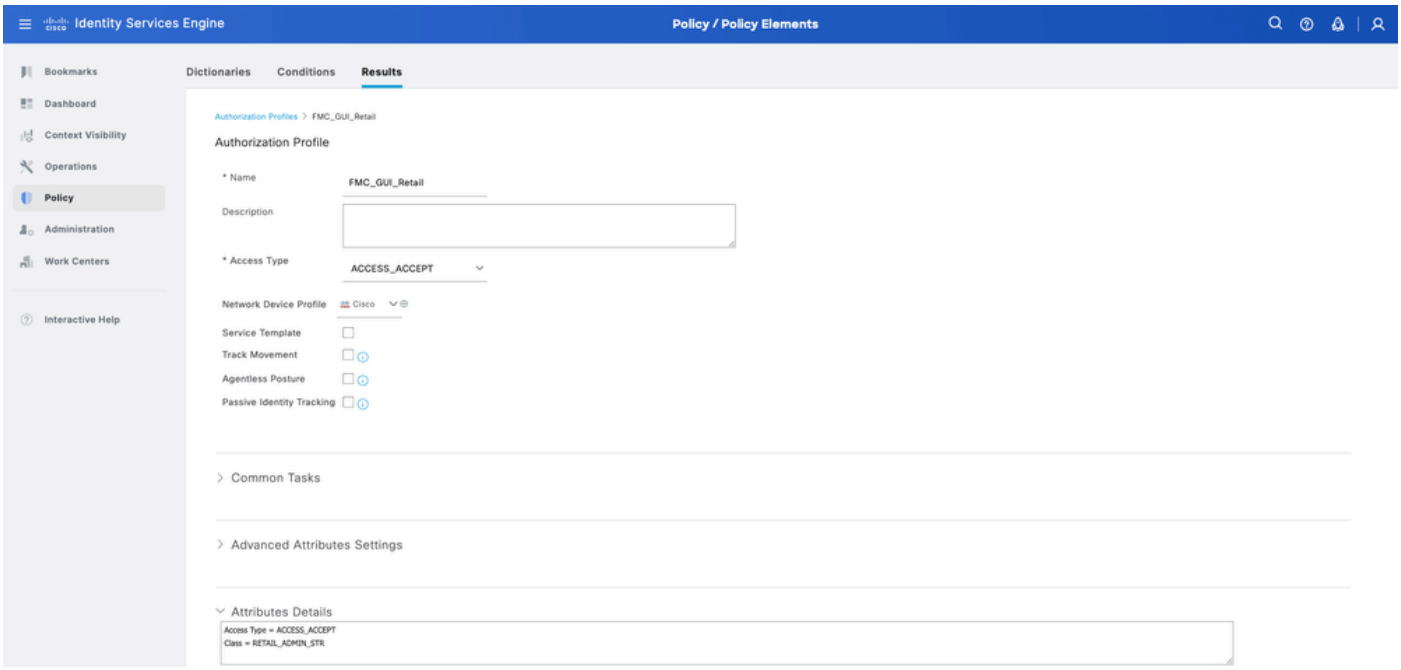


Assegnare un nome al profilo di autorizzazione e lasciare il campo Tipo di accesso impostato su ACCESS_ACCEPT.

In Impostazioni avanzate attributi (Advanced Attributes Settings), aggiungete Radius > Class—[25] con il valore e fate clic su Invia (Submit).

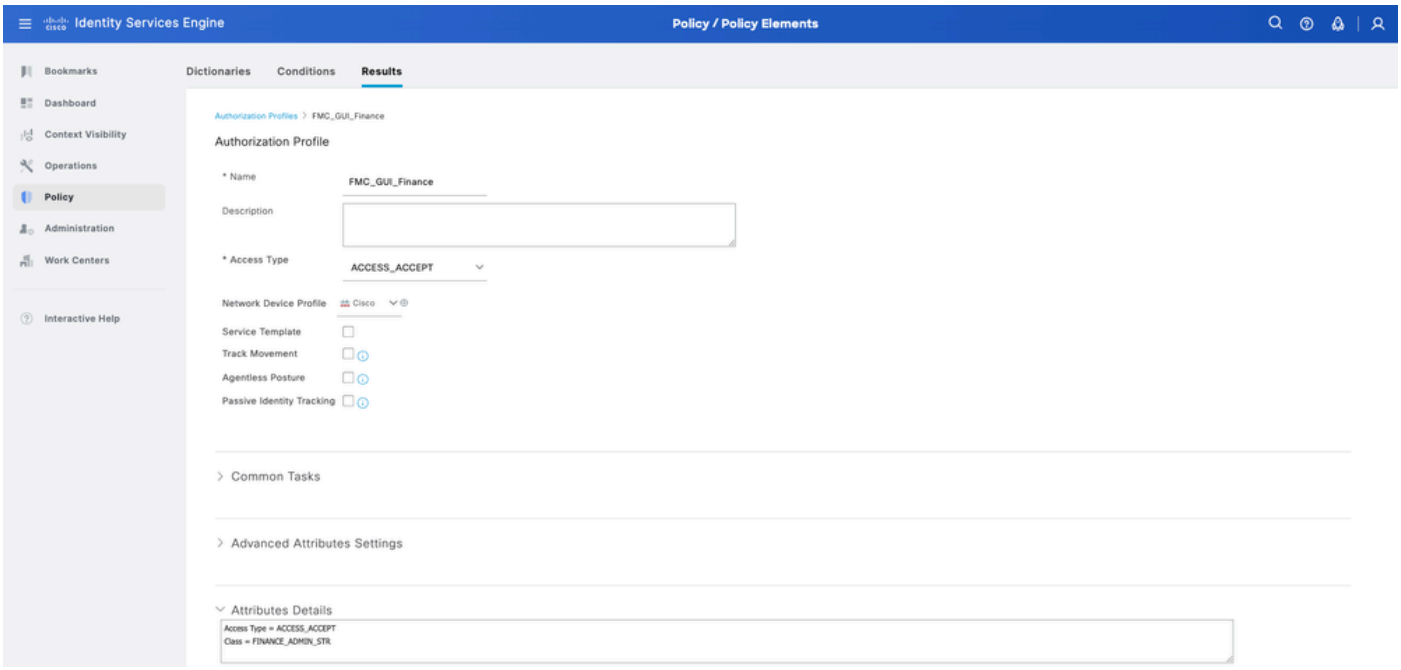
Passaggio 6.1. Profilo di vendita al dettaglio: In Impostazioni avanzate attributi aggiungere Radius:Class con il valore RETAIL_ADMIN_STR.

Suggerimento: Qui RETAIL_ADMIN_STR può essere qualsiasi cosa; accertarsi che anche il CCP abbia le stesse esigenze in termini di valore.



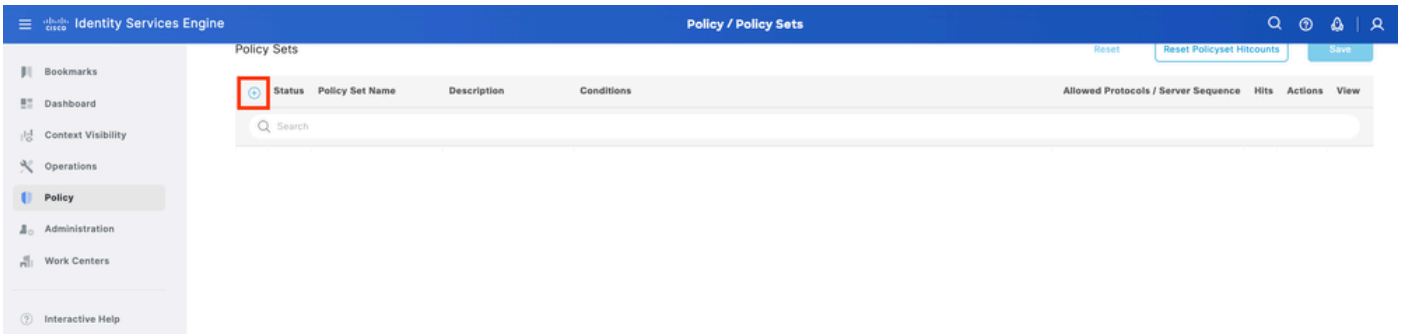
Passaggio 6.2 Finanza profilo: In Impostazioni avanzate attributi aggiungere Radius:Class con il valore FINANCE_ADMIN_STR.

Suggerimento: Qui FINANCE_ADMIN_STR può essere qualsiasi cosa; assicurarsi che lo stesso valore sia inserito anche sul lato FMC.



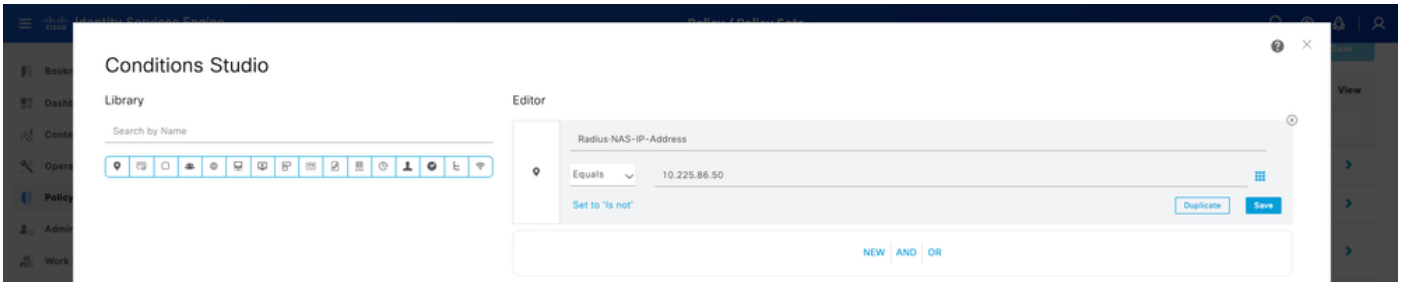
Aggiungi nuovo set di criteri

Passaggio 7. 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 Criterio > Set di criteri > Icona del segno più 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. Fate clic su Usa (Use) per mantenere le modifiche e uscire dall'editor.



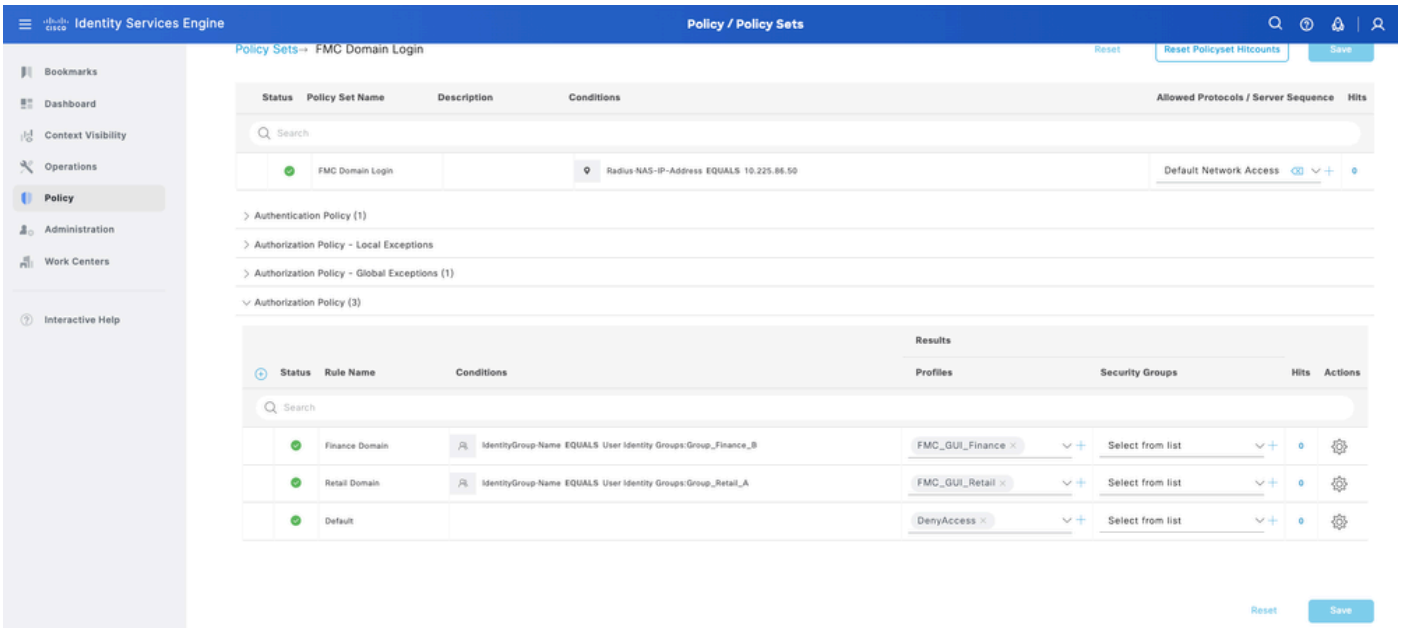
Passaggio 8.2. Al termine, fare clic su Save (Salva).

Passaggio 9. Visualizzare il nuovo set di criteri facendo clic sull'icona set situata alla fine della riga.

Espandere il menu Criteri di autorizzazione e fare clic sull'icona con il segno più per aggiungere una nuova regola che consenta 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 e scegliere Gruppi di identità utente. In Criteri di autorizzazione creare le regole seguenti:

- Regola 1: Se Gruppo di identità utente è uguale a Gruppo_Retail_A, assegnare il profilo Retail.
- Regola 2: Se Gruppo di identità utente è uguale a Group_Finance_B, assegnare la funzione Contabilità profilo.



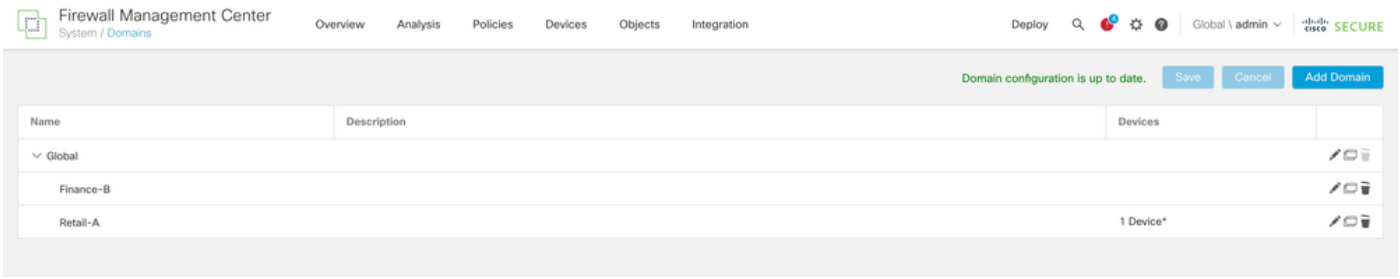
Passaggio 10. Impostare i profili di autorizzazione rispettivamente per ogni regola e fare clic su Salva.

Configurazione FMC

Aggiunta del server ISE RADIUS per l'autenticazione FMC

Passaggio 1. Definizione della struttura di dominio:

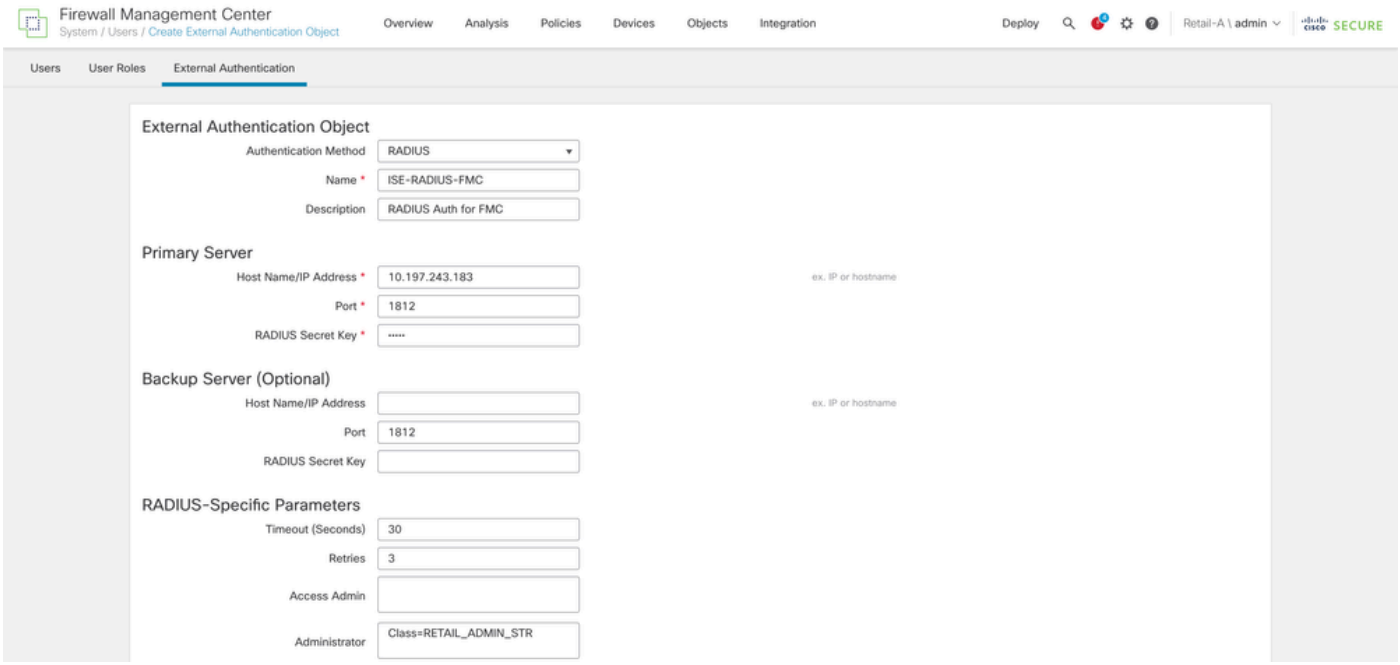
- Accedere al dominio globale FMC.
- Passare a Amministrazione > Domini.
- Fare clic su Aggiungi dominio per creare Retail-A e Finance-B come sottodomini di Global.



Passaggio 2.1. Configurare l'oggetto autenticazione esterna nel dominio su Retail-A

- Passare il dominio a Retail-A.
- Selezionare Sistema > Utenti > Autenticazione esterna.
- Selezionare Add External Authentication Object (Aggiungi oggetto autenticazione esterno) e scegliere RADIUS.
- Immettere l'indirizzo IP di ISE e il segreto condiviso configurato in precedenza.
- Immettere i parametri specifici di RADIUS > Amministratore > classe=RETAIL_ADMIN_STR

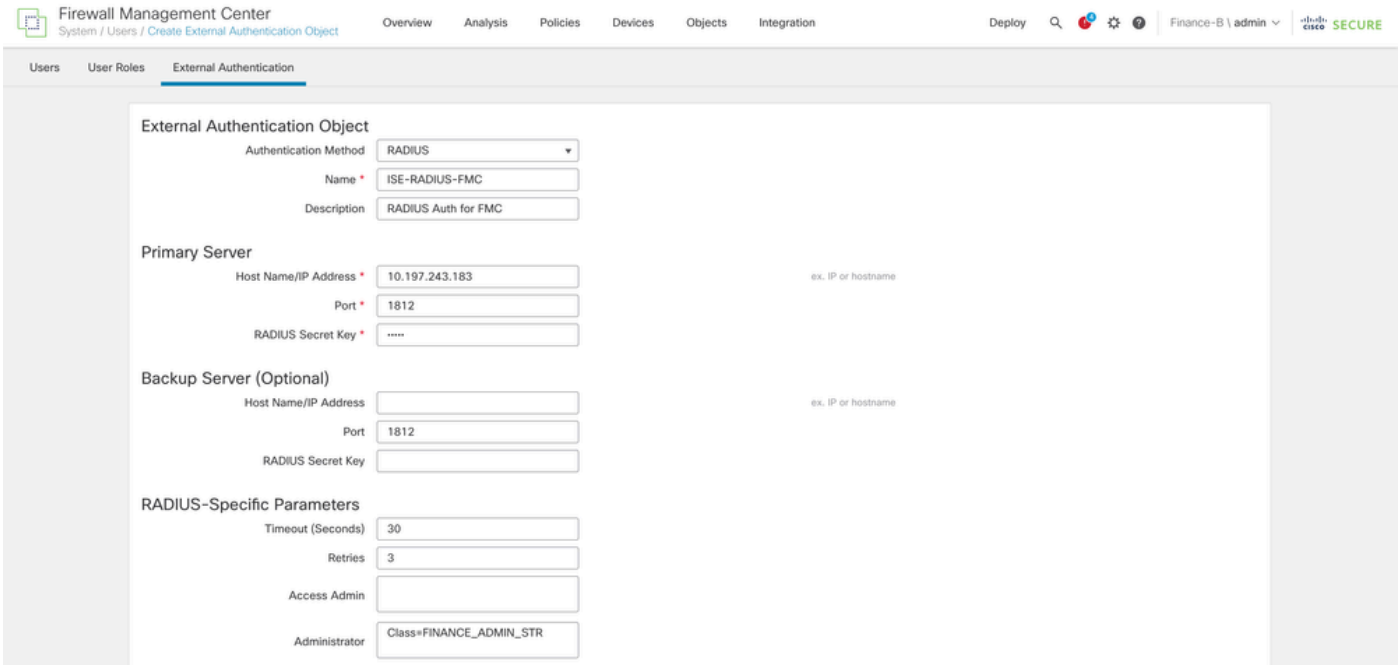
Suggerimento: Utilizzare lo stesso valore per class configurato in Authorization Profiles of ISE (Profili di autorizzazione di ISE).



Passaggio 2.2. Configurare l'oggetto autenticazione esterna nel dominio su Finance-B

- Passare Domain a Finance-B.
- Selezionare Sistema > Utenti > Autenticazione esterna.
- Selezionare Add External Authentication Object (Aggiungi oggetto autenticazione esterno) e scegliere RADIUS.
- Immettere l'indirizzo IP di ISE e il segreto condiviso configurati in precedenza.
- Immettere i parametri specifici di RADIUS > Amministratore > class=FINANCE_ADMIN_STR

Suggerimento: Utilizzare lo stesso valore per class configurato in Authorization Profiles of ISE (Profili di autorizzazione di ISE).



Passaggio 3. Attiva autenticazione: Abilitare l'oggetto e impostarlo come metodo di autenticazione shell. Fare clic su Save and Apply (Salva e applica).

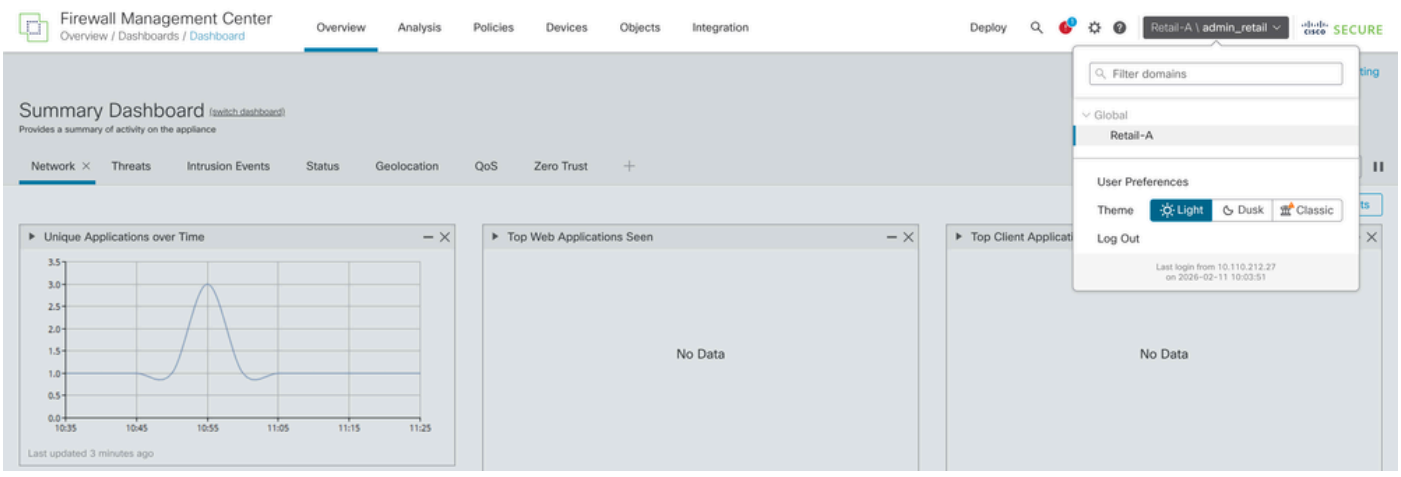
Verifica

Test di accesso tra domini

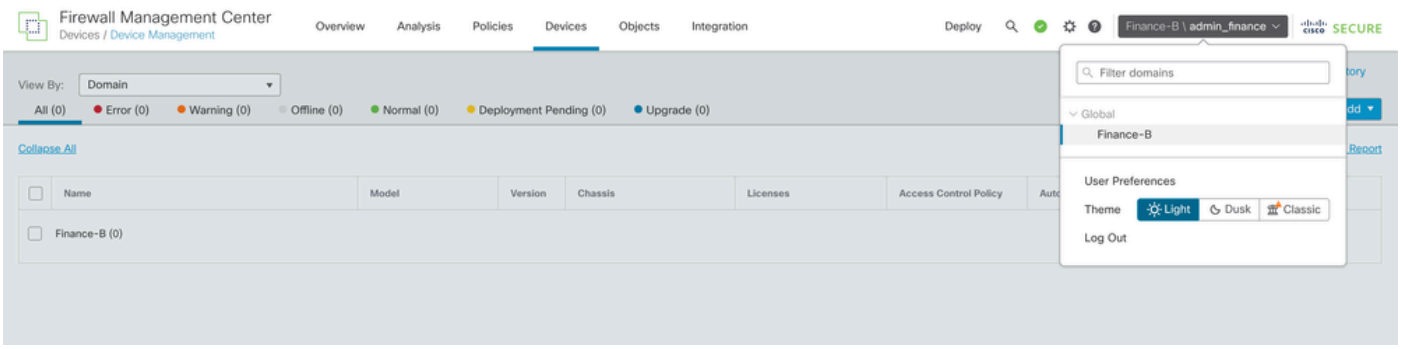
- Tentare di accedere all'interfaccia Web di FMC utilizzando admin_retail. Verificare che il Dominio corrente visualizzato nella parte superiore destra dell'interfaccia utente sia Retail-A.

Suggerimento: Quando si accede a un dominio specifico, utilizzare il formato nome_utente nome_dominio\radius_user_mapped_with_that_domain.

Ad esempio, se l'utente amministratore di Retail deve eseguire l'accesso, il nome utente deve essere Retail-A\admin_retail e la password corrispondente.



- Uscire e accedere come admin_finance. Verificare che l'utente sia limitato al dominio Finance-B e che non sia in grado di visualizzare i dispositivi Retail-A.

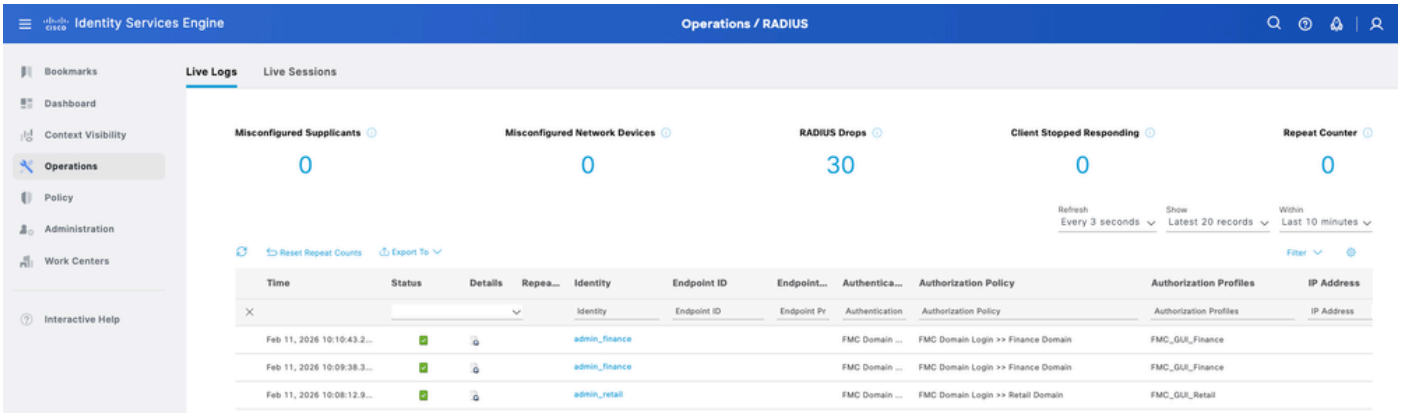


Test interni FMC

Passare alle impostazioni del server RADIUS nel FMC. Utilizzare la sezione Parametri di test aggiuntivi per immettere un nome utente e una password di test. Se il test ha esito positivo, deve essere visualizzato un messaggio verde di operazione riuscita.

log ISE in tempo reale

- In Cisco ISE, selezionare Operations > RADIUS > Live Log.



- Confermare che le richieste di autenticazione mostrino uno stato di superamento e che il profilo di autorizzazione corretto (e la stringa della classe associata) sia stato inviato nel pacchetto RADIUS Access-Accept.

Overview

Event	5200 Authentication succeeded
Username	admin_finance
Endpoint Id	
Endpoint Profile	
Authentication Policy	FMC Domain Login >> Default
Authorization Policy	FMC Domain Login >> Finance Domain
Authorization Result	FMC_GUI_Finance

Authentication Details

Source Timestamp	2026-02-11 16:40:43.275
Received Timestamp	2026-02-11 22:10:43.275
Policy Server	eagle
Event	5200 Authentication succeeded
Username	admin_finance
User Type	User
Authentication Identity Store	Internal Users
Identity Group	User Identity Groups:Group_Finance_B

Result

Class	FINANCE_ADMIN_STR
Class	CACS:0ac5f3b7m0vFomvHHyC_igO13NsO1DZN6QciDbrc0cwlaYWHMto:eagle/556377151/553

Informazioni correlate

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