Externe FMC-Authentifizierung in einer Umgebung mit mehreren Domänen konfigurieren

Inhalt

Einleitung

In diesem Dokument wird die Implementierung einer Multi-Tenant-Funktion (mehrere Domänen) innerhalb des Cisco FMC bei gleichzeitiger Nutzung der Cisco ISE für eine zentralisierte RADIUS-Authentifizierung beschrieben.

Voraussetzungen

Anforderungen

Es wird empfohlen, über Kenntnisse in den folgenden Themen zu verfügen:

- Erstkonfiguration von Cisco Secure Firewall Management Center über GUI und/oder Shell.
- Vollständige Admin-Berechtigungen in der globalen Domäne des FMC zum Erstellen von Subdomänen und externen Authentifizierungsobjekten.
- Konfigurieren von Authentifizierungs- und Autorisierungsrichtlinien auf der ISE
- Grundlegendes RADIUS-Wissen

Verwendete Komponenten

- Cisco Secure FMC: vFMC 7.4.2 (oder höher für Multi-Domain-Stabilität empfohlen)
- Domänenstruktur: Eine dreistufige Hierarchie (Global > Subdomänen der zweiten Ebene).
- Cisco Identity Services Engine: ISE 3.3

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

In groß angelegten Unternehmensumgebungen oder Managed Security Service Provider (MSSP)-Szenarien ist es häufig erforderlich, das Netzwerkmanagement in unterschiedliche administrative Grenzen aufzuteilen. In diesem Dokument wird beschrieben, wie das FMC zur Unterstützung mehrerer Domänen konfiguriert werden kann. Dies gilt insbesondere für ein Beispiel aus der Praxis, bei dem ein MSSP zwei Clients verwaltet: Retail-A und Finance-B. Durch die Verwendung externer RADIUS-Authentifizierung über die Cisco ISE können Administratoren sicherstellen, dass Benutzer automatisch nur auf ihre jeweiligen Benutzerdomänen zugreifen können, basierend auf ihren zentralen Anmeldeinformationen.

Das Cisco Secure Firewall-System verwendet Domänen zur Implementierung von Multi-Tenant-Funktionen.

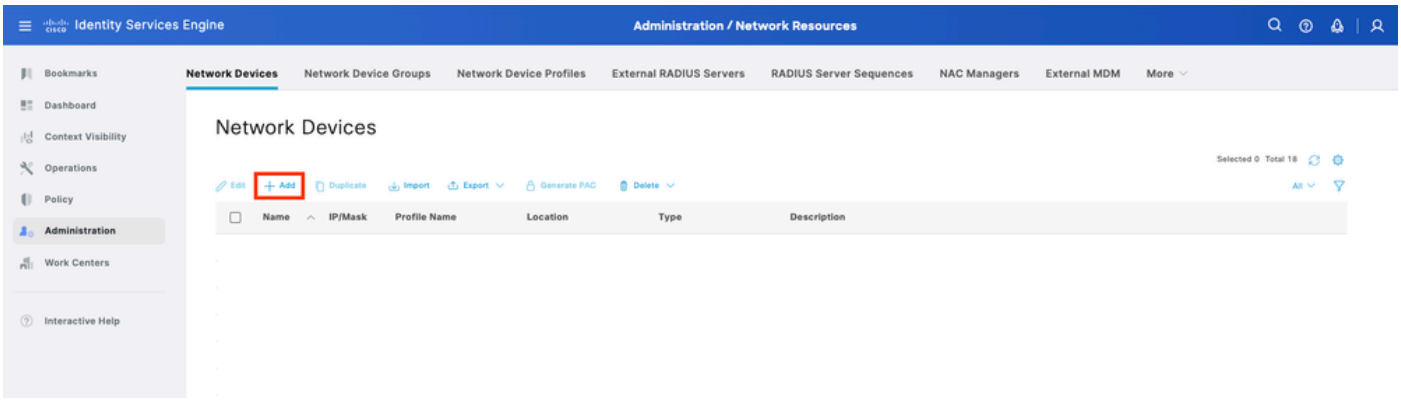
- Domänenhierarchie: Die Hierarchie beginnt bei der globalen Domäne. Sie können bis zu 100 Unterdomänen in einer Struktur mit zwei oder drei Ebenen erstellen.
- Leaf-Domänen: Dabei handelt es sich um Domänen am unteren Ende der Hierarchie ohne weitere Unterdomänen. Entscheidend ist, dass jedes verwaltete FTD-Gerät genau einer Leaf-Domäne zugeordnet werden muss.
- RADIUS-Klassenattribut (Attribut 25): Bei einer Konfiguration mit mehreren Domänen verwendet das FMC das von der ISE zurückgegebene RADIUS Class-Attribut, um einen authentifizierten Benutzer einer bestimmten Domäne und Benutzerrolle zuzuordnen. Auf diese Weise kann ein einzelner RADIUS-Server bei der Anmeldung Benutzer dynamisch verschiedenen Benutzersegmenten zuweisen (z. B. Retail-A und Finance-B).

Konfiguration

ISE-Konfiguration

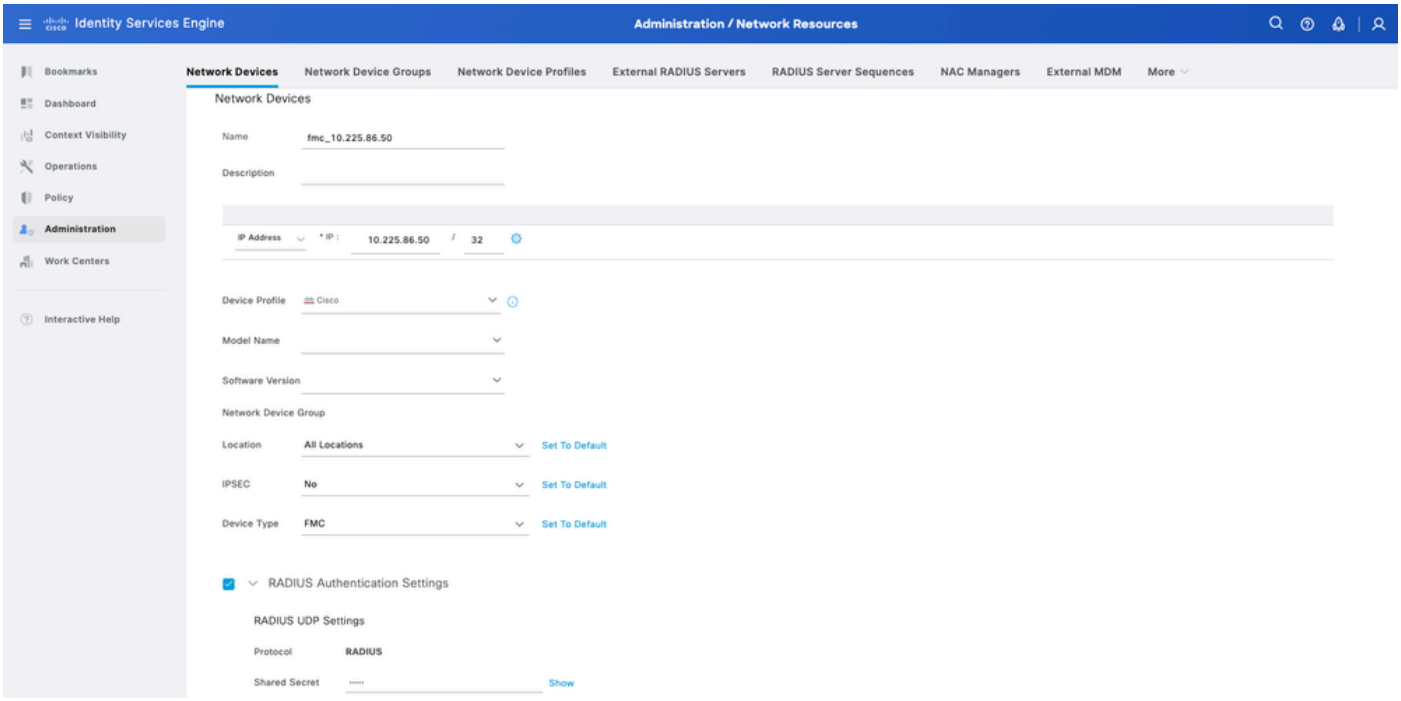
Netzwerkgeräte hinzufügen

Schritt 1: Navigieren Sie zu Administration > Network Resources > Network Devices > Add.



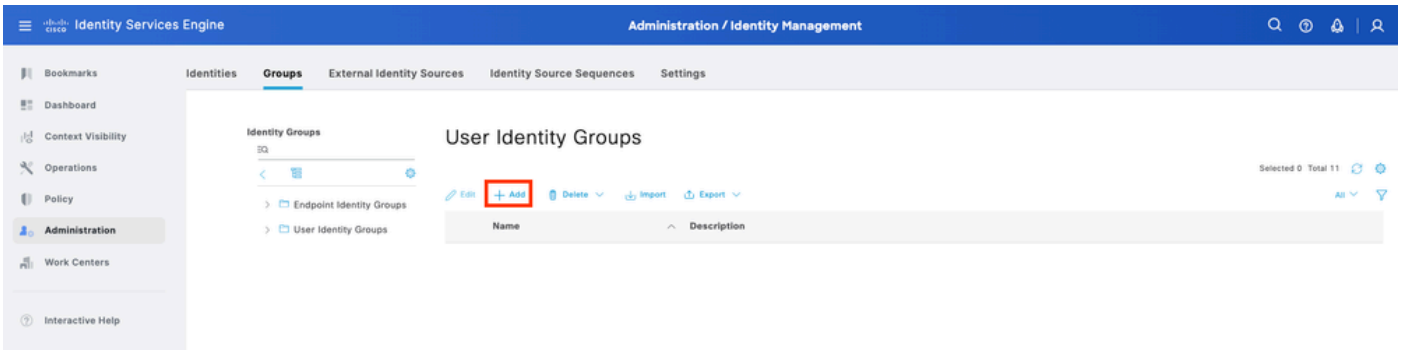
Schritt 2: Weisen Sie dem Netzwerkgeräteobjekt einen Namen zu, und fügen Sie die IP-Adresse des FMC ein.

Aktivieren Sie das Kontrollkästchen RADIUS, und definieren Sie einen gemeinsamen geheimen Schlüssel. Derselbe Schlüssel muss später zur Konfiguration des FMC verwendet werden. Klicken Sie abschließend auf Speichern.

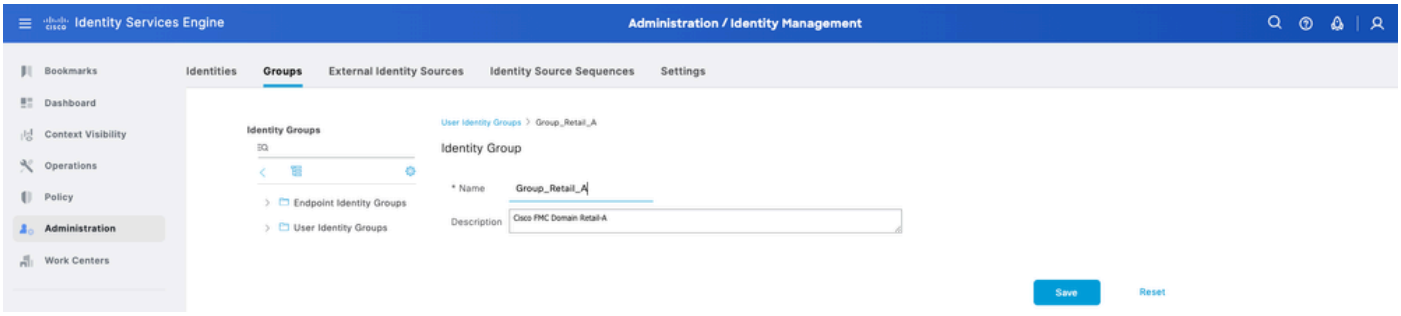


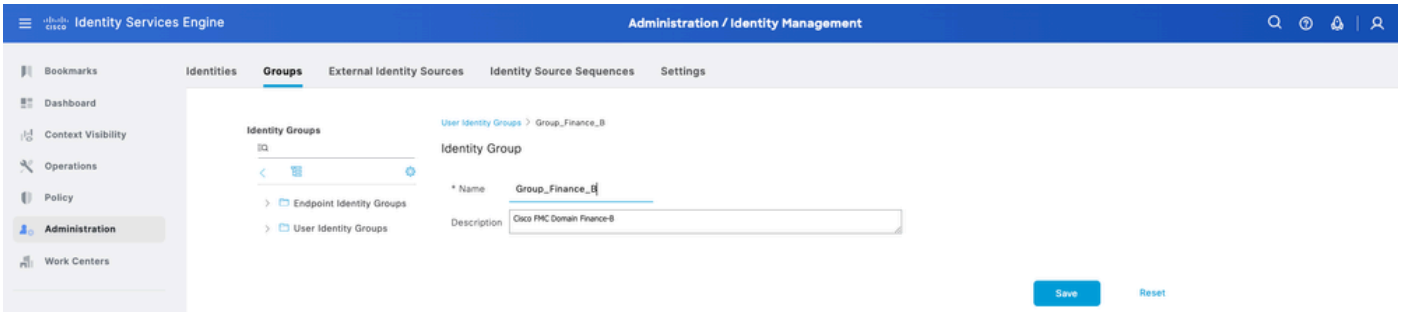
Lokale Benutzeridentitätsgruppen und Benutzer erstellen

Schritt 3: Erstellen der erforderlichen Benutzeridentitätsgruppen Navigieren Sie zu Administration > Identity Management > Groups > User Identity Groups > Add.

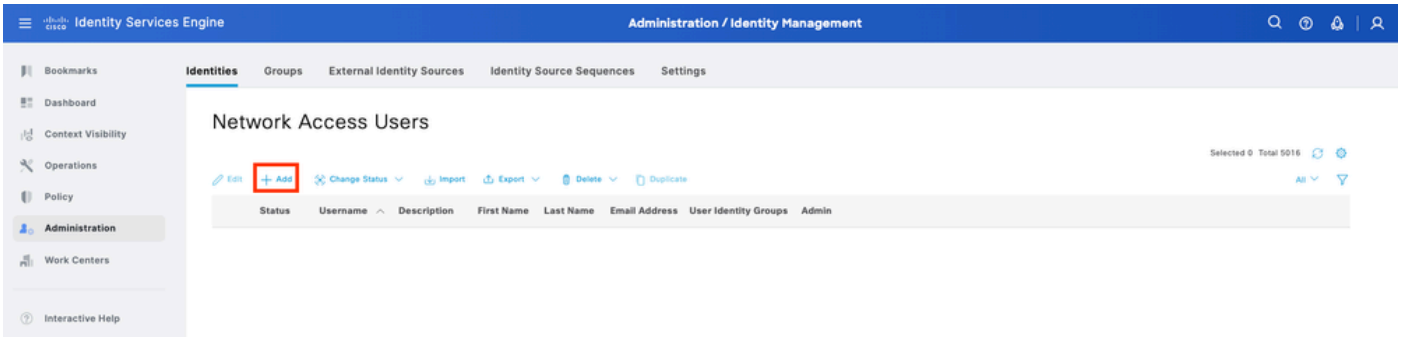


Schritt 4: Geben Sie jeder Gruppe einen Namen und speichern Sie einzeln. In diesem Beispiel erstellen Sie eine Gruppe für Administrator-Benutzer. Zwei Gruppen erstellen: Group_Retail_A und Group_Finance_B.

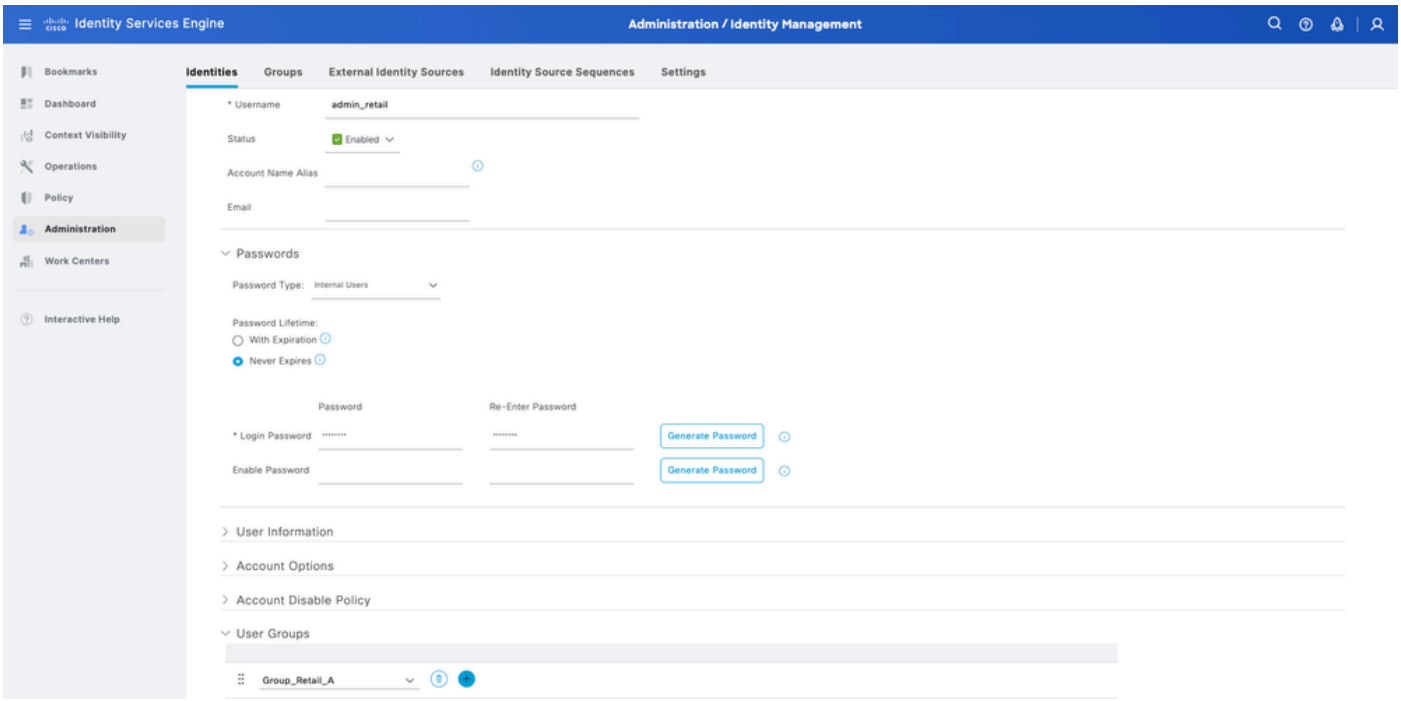




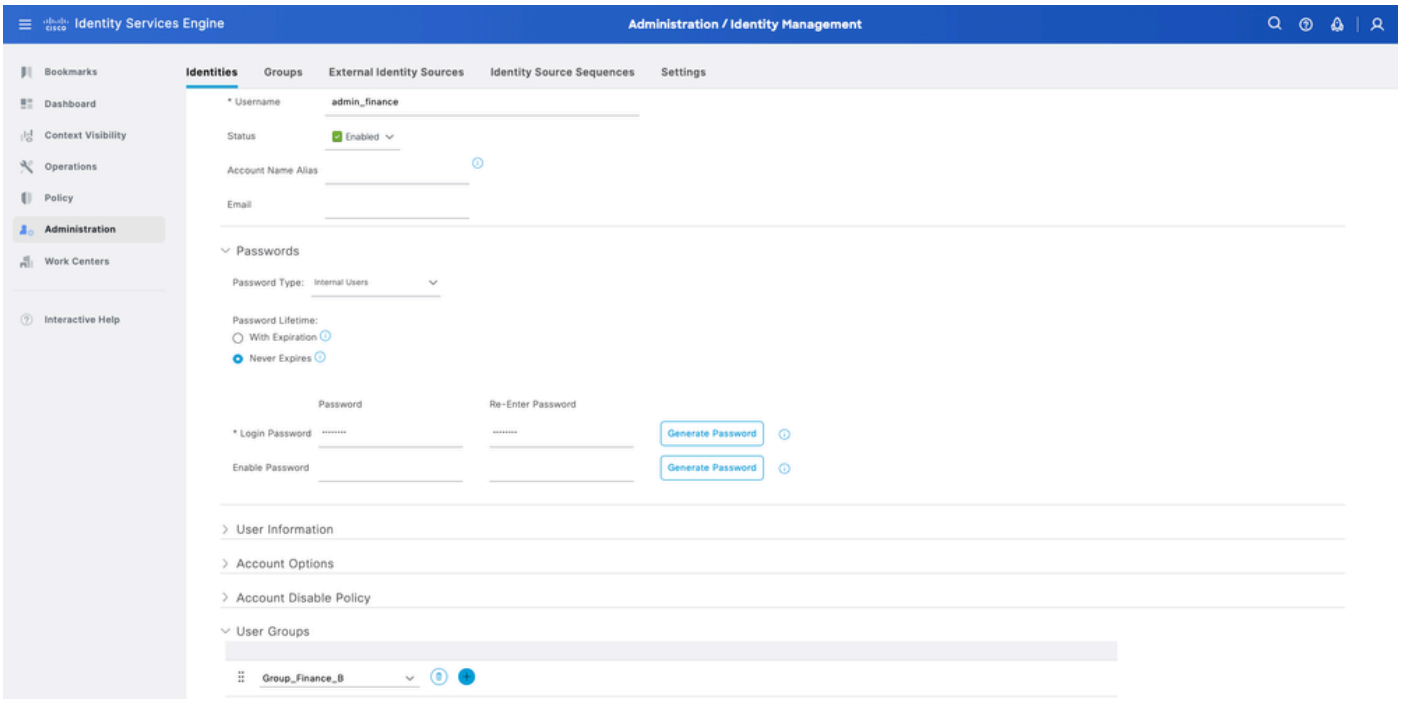
Schritt 5: Erstellen Sie die lokalen Benutzer, und fügen Sie sie der entsprechenden Gruppe hinzu. Navigieren Sie zu Administration > Identity Management > Identities > Add.



Schritt 5.1. Erstellen Sie zunächst den Benutzer mit Administratorrechten. Weisen Sie ihm einen Namen admin_retail, ein Kennwort und die Gruppe Group_Retail_A zu.

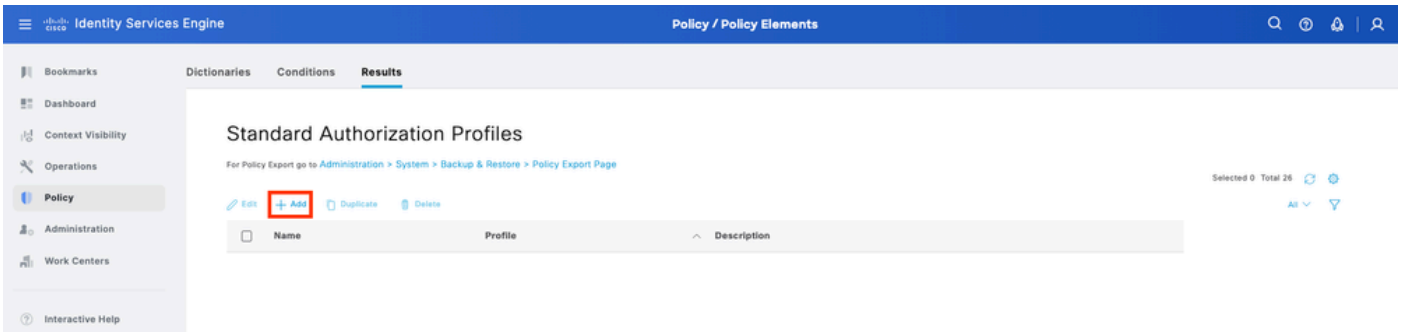


Schritt 5.2. Erstellen Sie zunächst den Benutzer mit Administratorrechten. Weisen Sie ihm einen Namen admin_finance, ein Kennwort und die Gruppe Group_Finance_B zu.



Erstellen der Autorisierungsprofile

Schritt 6: Erstellen Sie das Autorisierungsprofil für den FMC Web Interface Admin-Benutzer. Navigieren Sie zu Richtlinie > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile > Hinzufügen.

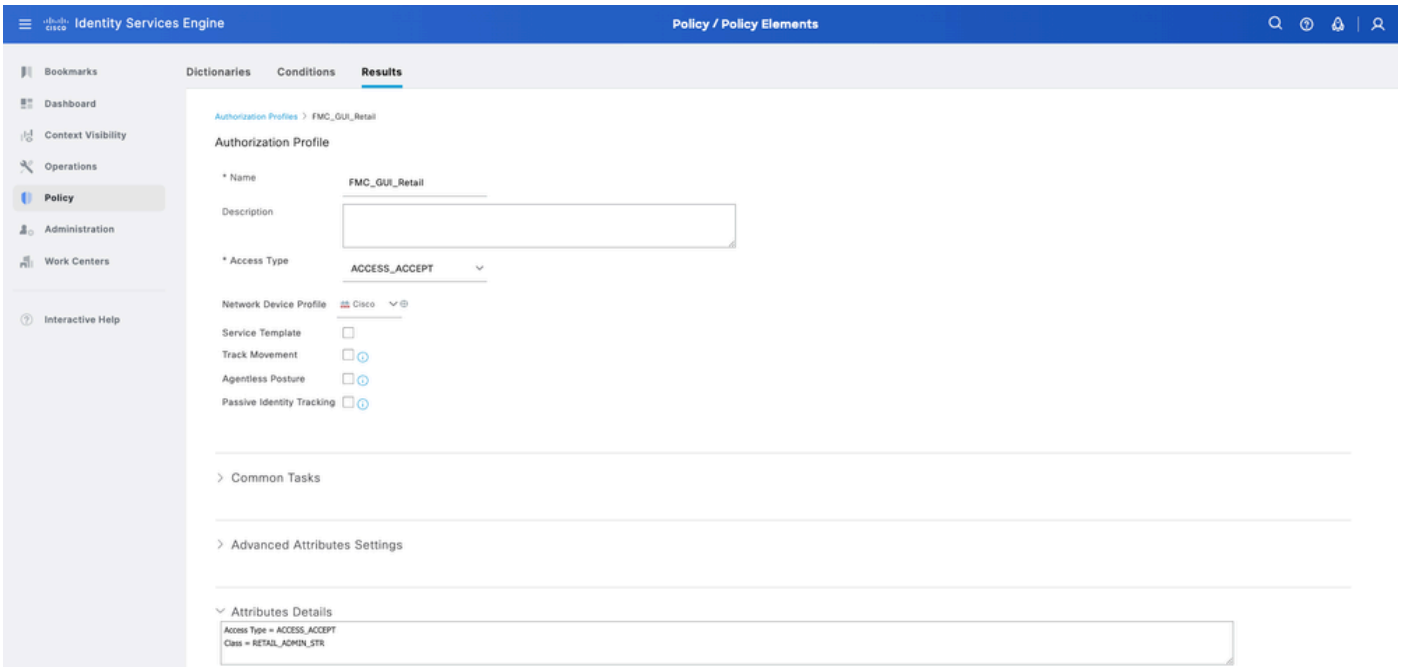


Definieren Sie einen Namen für das Autorisierungsprofil, und belassen Sie den Zugriffstyp bei ACCESS_ACCEPT.

Fügen Sie unter Erweiterte Attributeinstellungen einen Radius > Class—[25] mit dem Wert hinzu, und klicken Sie auf Senden.

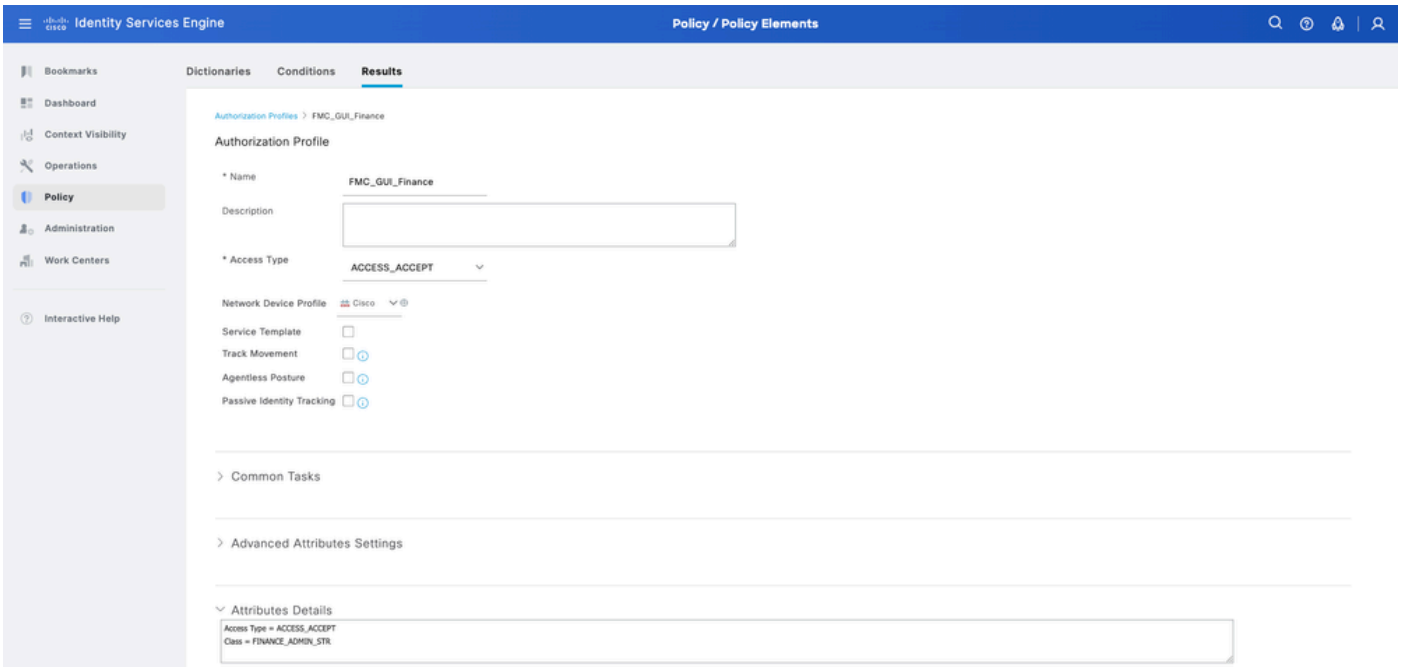
Schritt 6.1. Profil Einzelhandel: Fügen Sie unter Erweiterte Attributeinstellungen den Wert Radius:Class mit dem Wert RETAIL_ADMIN_STR hinzu.

Tipp: RETAIL_ADMIN_STR kann dabei beliebig sein. Stellen Sie sicher, dass die gleichen Wertanforderungen auch auf FMC-Seite gestellt werden.



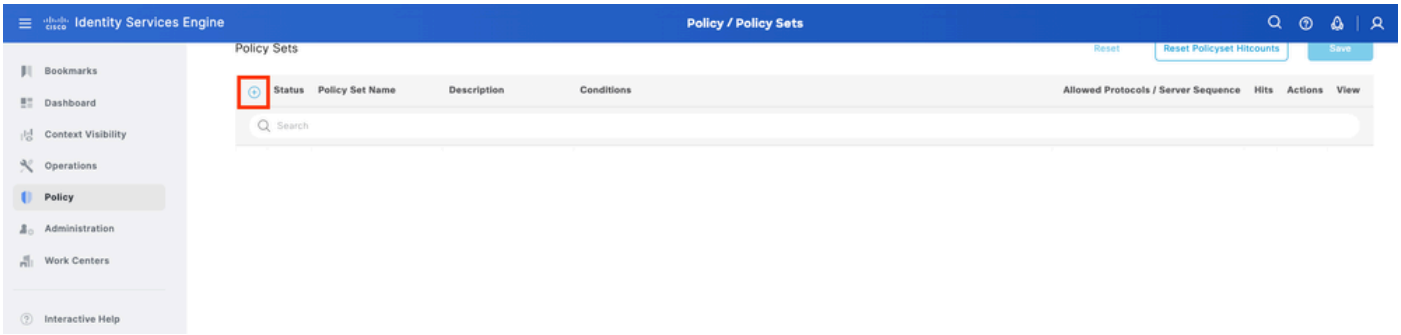
Schritt 6.2. Profil Finanzen: Fügen Sie unter Erweiterte Attributeinstellungen den Wert Radius:Class mit dem Wert FINANCE_ADMIN_STR hinzu.

Tipp: Hier kann FINANCE_ADMIN_STR beliebig sein. Stellen Sie sicher, dass der gleiche Wert auch auf FMC-Seite gesetzt wird.



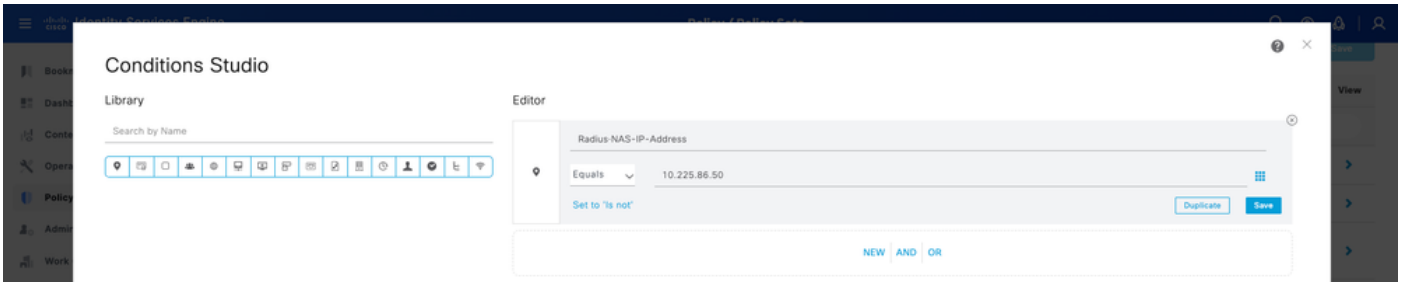
Hinzufügen eines neuen Richtliniensatzes

Schritt 7: Erstellen eines Policy Sets, das mit der IP-Adresse des FMC übereinstimmt Auf diese Weise wird verhindert, dass andere Geräte den Benutzern Zugriff gewähren. Navigieren Sie zu Policy > Policy Sets > Plus (Richtlinie > Richtliniensätze), das in der oberen linken Ecke platziert ist.



Schritt 8.1. Eine neue Zeile wird oben in Ihren Policy Sets platziert.

Nennen Sie die neue Richtlinie, und fügen Sie eine Bedingung für das RADIUS NAS-IP-Address-Attribut hinzu, das mit der FMC-IP-Adresse übereinstimmt. Klicken Sie auf Verwenden, um die Änderungen beizubehalten und den Editor zu verlassen.



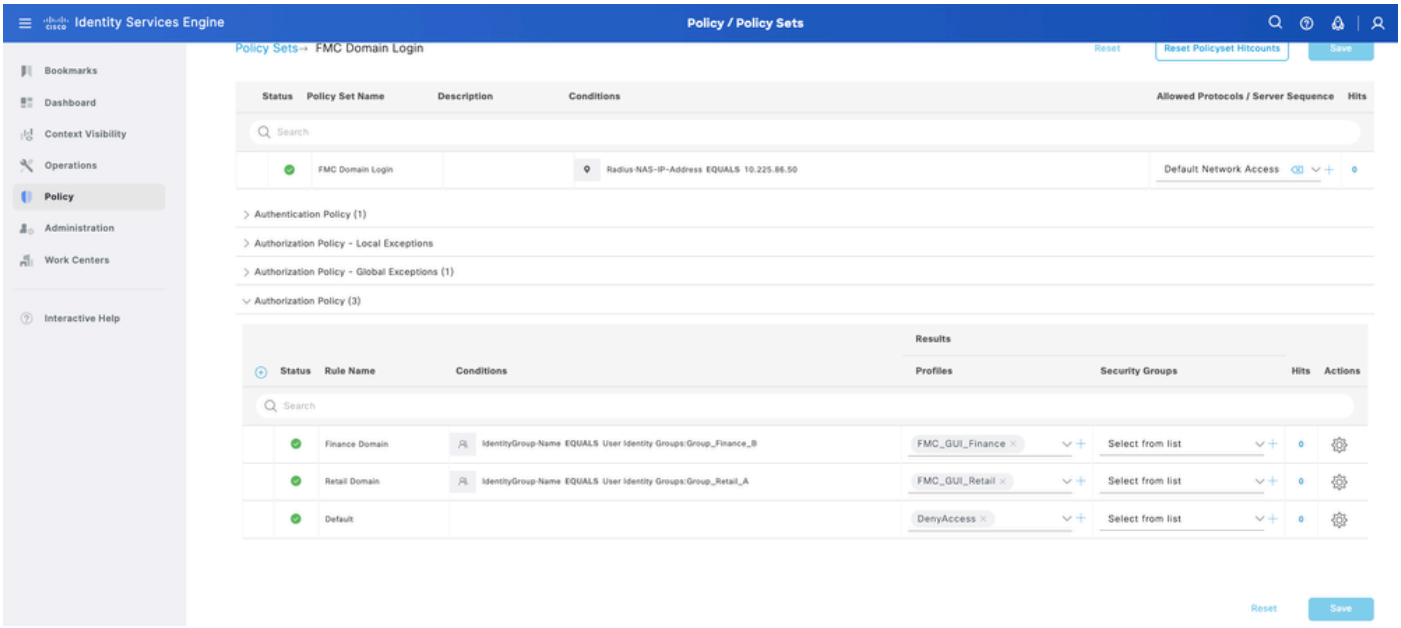
Schritt 8.2. Klicken Sie abschließend auf Speichern.

Schritt 9: Zeigen Sie das neue Policy Set an, indem Sie auf das Set-Symbol am Ende der Zeile klicken.

Erweitern Sie das Menü Autorisierungsrichtlinie, und drücken Sie das Pluszeichen, um eine neue Regel hinzuzufügen, um dem Benutzer mit Administratorrechten den Zugriff zu gewähren. Gib ihm einen Namen.

Legen Sie die Bedingungen für die Übereinstimmung der Dictionary-Identitätsgruppe mit Attributname gleich fest, und wählen Sie Benutzeridentitätsgruppen aus. Erstellen Sie unter der Autorisierungsrichtlinie folgende Regeln:

- Regel 1: Wenn die Benutzeridentitätsgruppe Group_Retail_A entspricht, weisen Sie das Profil Retail zu.
- Regel 2: Wenn die Benutzeridentitätsgruppe Group_Finance_B entspricht, weisen Sie das Profil Finance zu.



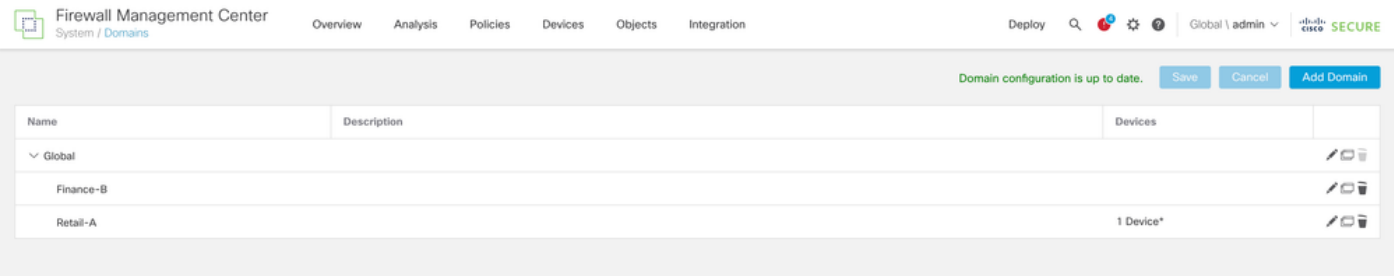
Schritt 10: Legen Sie die Autorisierungsprofile für jede Regel fest, und klicken Sie auf Speichern.

FMC-Konfiguration

ISE RADIUS-Server für FMC-Authentifizierung hinzufügen

Schritt 1: Einrichten der Domänenstruktur:

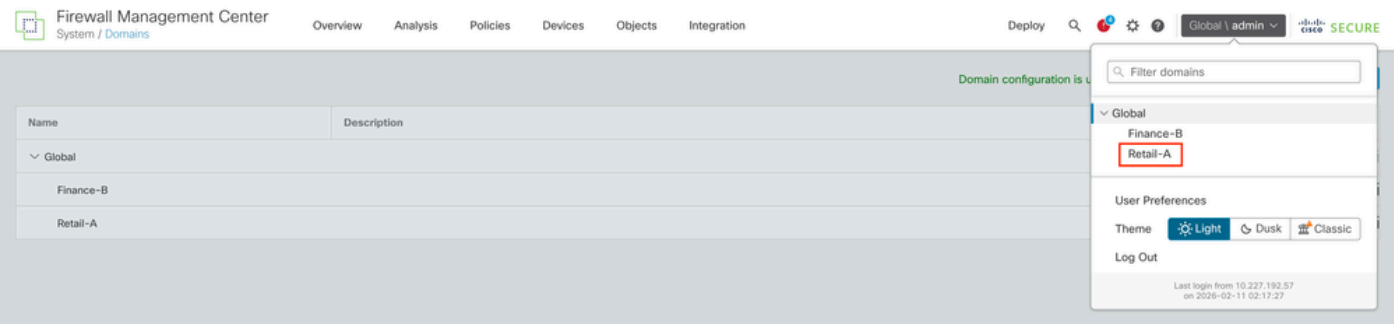
- Melden Sie sich bei der globalen FMC-Domäne an.
- Navigieren Sie zu Administration > Domains.
- Klicken Sie auf Add Domain (Domäne hinzufügen), um Retail-A und Finance-B als Subdomänen von Global zu erstellen.

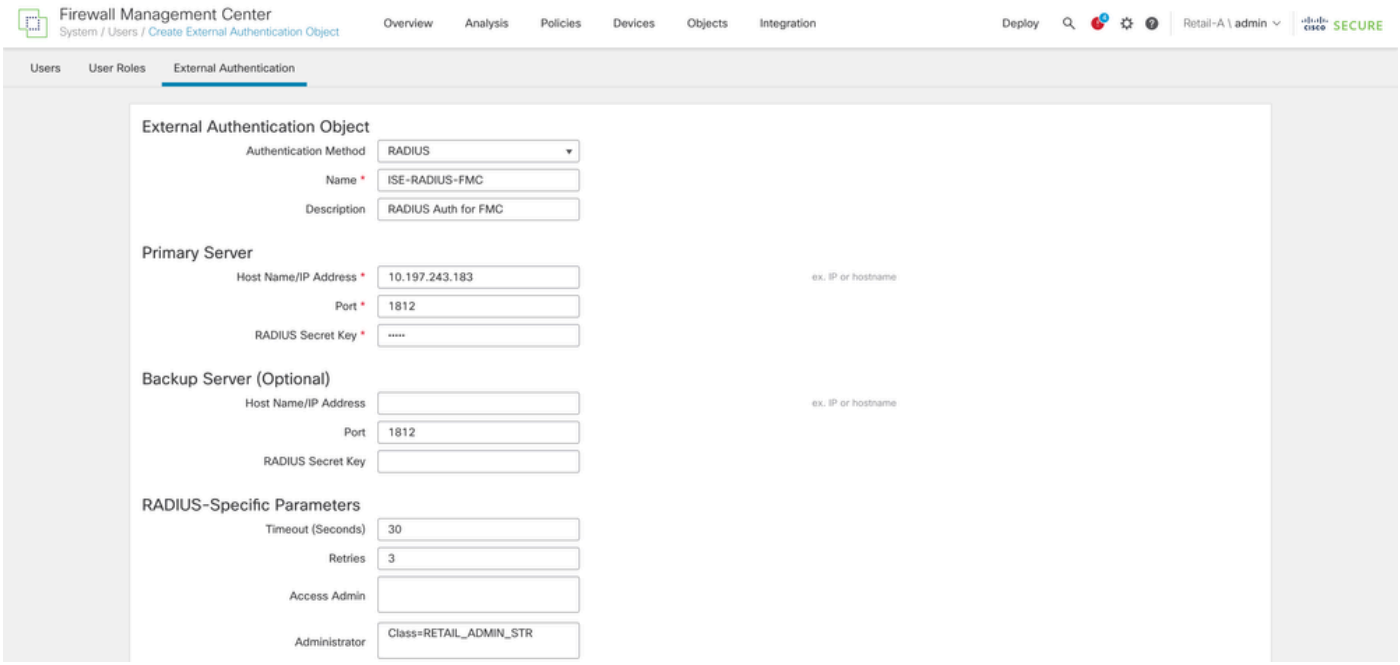


Schritt 2.1: Konfigurieren des externen Authentifizierungsobjekts unter Domäne für Retail-A

- Domain auf Retail-A umstellen.
- Navigieren Sie zu System > Users > External Authentication.
- Wählen Sie Externes Authentifizierungsobjekt hinzufügen aus, und wählen Sie RADIUS aus.
- Geben Sie die ISE-IP-Adresse und den zuvor konfigurierten gemeinsamen geheimen Schlüssel ein.
- Geben Sie die RADIUS-spezifischen Parameter > Administrator > class=RETAIL_ADMIN_STR ein.

Tipp: Verwenden Sie für die Klasse denselben Wert, der unter Autorisierungsprofile der ISE konfiguriert wurde.

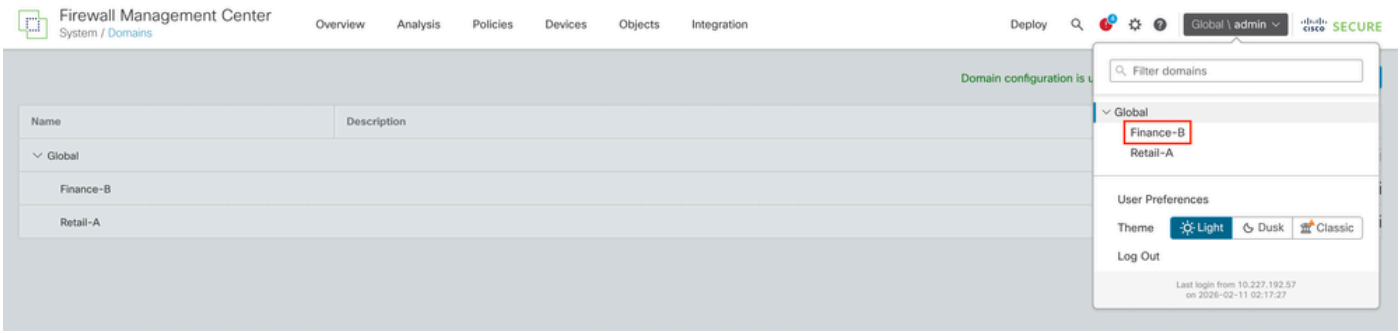


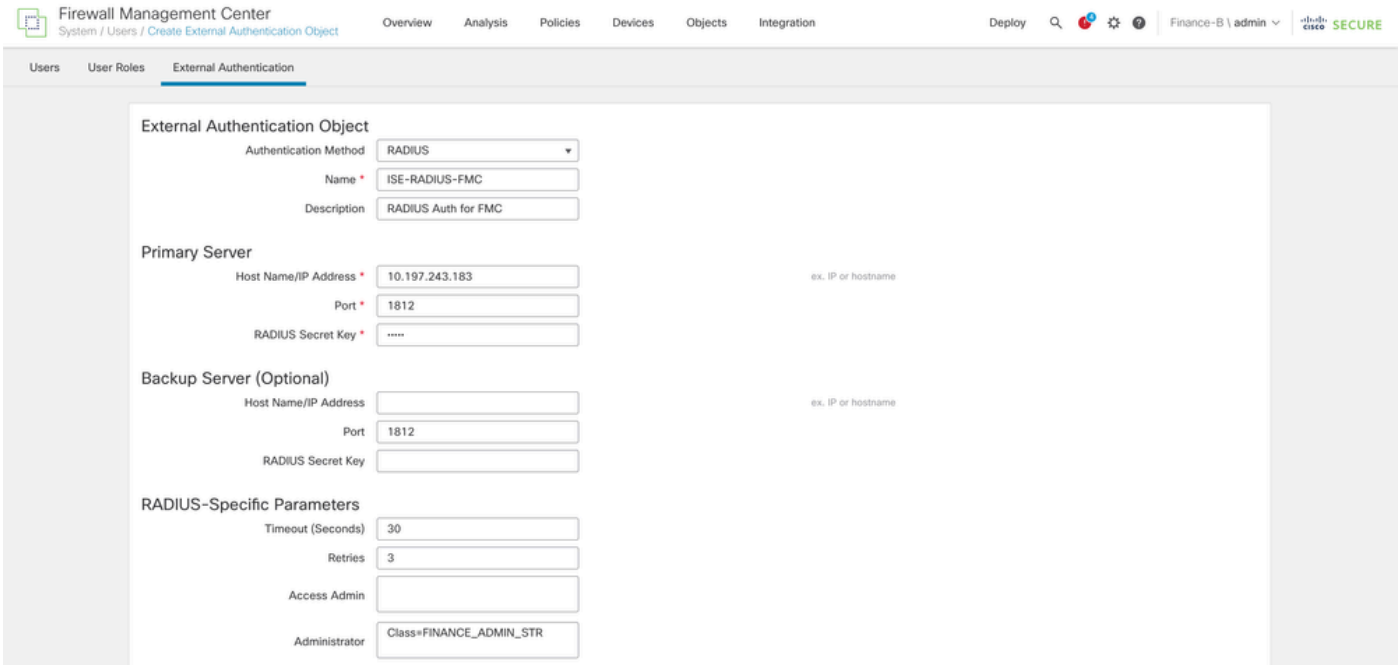


Schritt 2.2: Konfigurieren des externen Authentifizierungsobjekts unter Domäne für Finance-B

- Wechseln Sie zur Domäne Finance-B.
- Navigieren Sie zu System > Users > External Authentication.
- Wählen Sie Externes Authentifizierungsobjekt hinzufügen aus, und wählen Sie RADIUS aus.
- Geben Sie die ISE-IP-Adresse und den zuvor konfigurierten gemeinsamen geheimen Schlüssel ein.
- Geben Sie die RADIUS-spezifischen Parameter > Administrator > class=FINANCE_ADMIN_STR ein.

Tipp: Verwenden Sie für die Klasse denselben Wert, der unter Autorisierungsprofile der ISE konfiguriert wurde.





Schritt 3: Authentifizierung aktivieren: Aktivieren Sie das Objekt, und legen Sie es als Shell Authentication-Methode fest. Klicken Sie auf Speichern und Übernehmen.

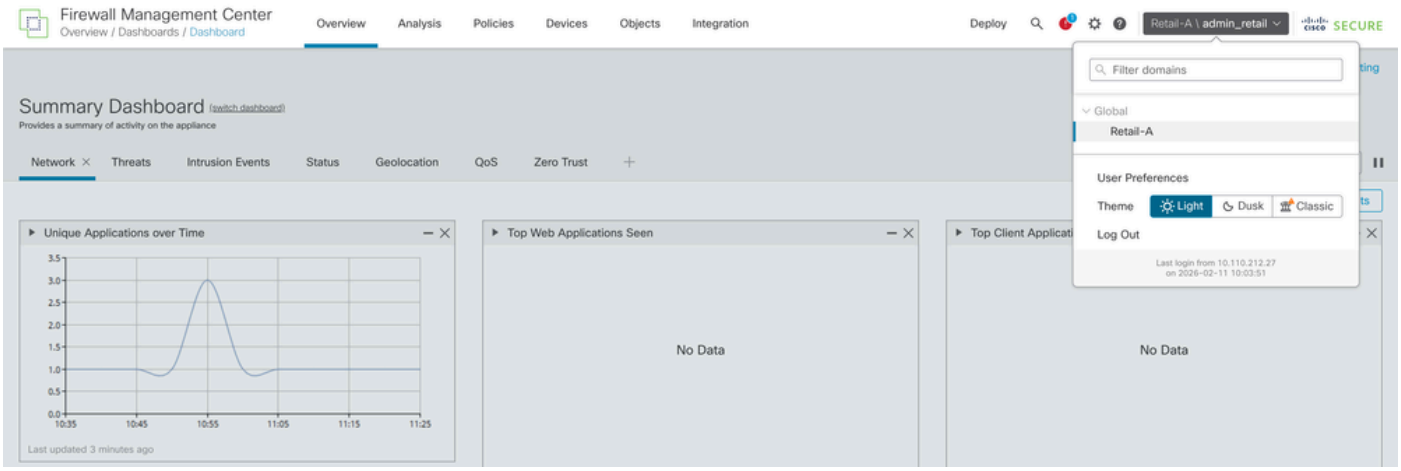
Verifizierung

Domänenübergreifender Anmeldetest

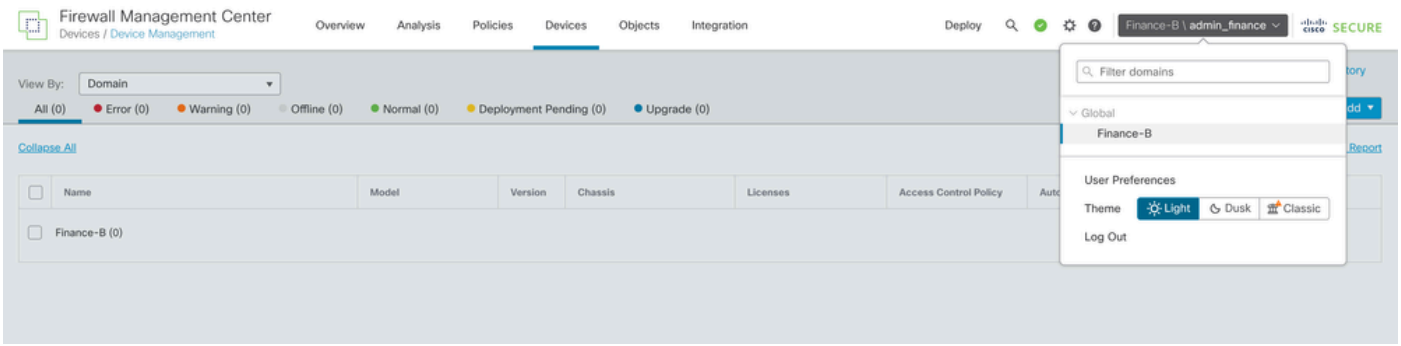
- Versuchen Sie, sich über admin_retail bei der FMC-Webschnittstelle anzumelden. Vergewissern Sie sich, dass die aktuelle Domäne oben rechts in der Benutzeroberfläche Retail-A ist.

Tipp: Wenn Sie sich bei einer bestimmten Domäne anmelden, verwenden Sie das folgende Format: Domain_name\radius_user_mapped_with_that_domain.

Wenn sich der Administrator-Benutzer für den Einzelhandel beispielsweise anmelden muss, muss der Benutzername "Retail-A\admin_retail" und das entsprechende Kennwort lauten.



- Melden Sie sich ab und als admin_finance an. Vergewissern Sie sich, dass der Benutzer auf die Finanz-B-Domäne beschränkt ist und die Geräte für Retail-A nicht sehen kann.

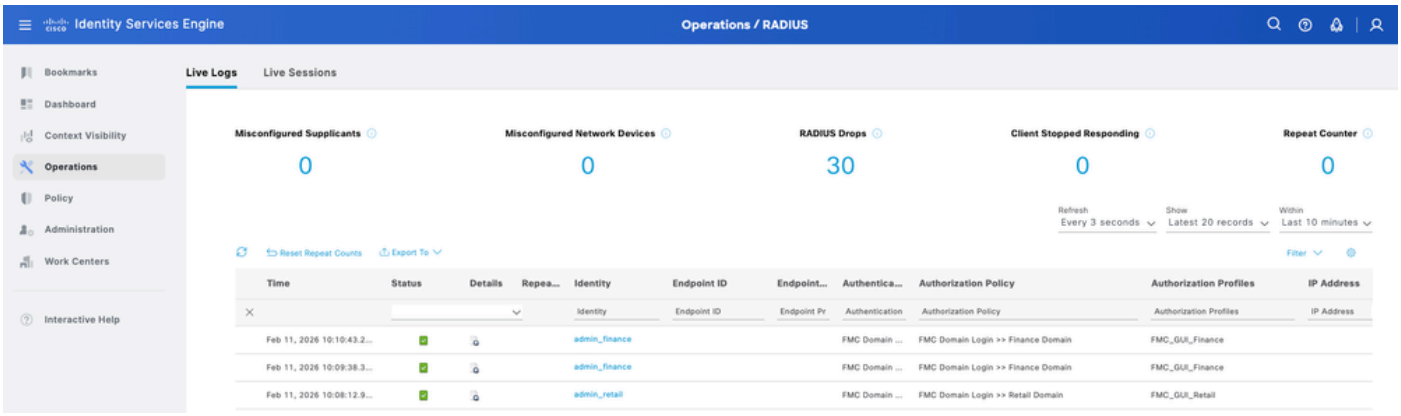


Interne FMC-Tests

Navigieren Sie zu den RADIUS-Servereinstellungen im FMC. Geben Sie im Abschnitt "Zusätzliche Testparameter" einen Testbenutzernamen und ein Testkennwort ein. Ein erfolgreicher Test muss eine grüne Erfolgsmeldung anzeigen.

ISE-Live-Protokolle

- Navigieren Sie in der Cisco ISE zu Operations > RADIUS > Live Logs (Betrieb > RADIUS > Live-Protokolle).



- Vergewissern Sie sich, dass die Authentifizierungsanforderungen den Status "Bestanden" aufweisen und dass das richtige Autorisierungsprofil (und die zugehörige Klassenzeichenfolge) im RADIUS-Access-Accept-Paket gesendet wurde.

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

Zugehörige Informationen

Externe FMC- und FTD-Authentifizierung mit ISE als RADIUS-Server konfigurieren

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.