在多域環境中配置FMC外部身份驗證

目錄

簡介

本檔案介紹在思科FMC中實施多租戶（多域），同時利用思科ISE進行集中式RADIUS身份驗證。

必要條件

需求

建議瞭解以下主題：

- Cisco Secure Firewall Management Center通過GUI和/或外殼進行初始配置。
- 在FMC的全域性域中擁有建立子域和外部身份驗證對象的完全管理員許可權。
- 在ISE上配置身份驗證和授權策略。
- 基本RADIUS知識

採用元件

- Cisco Secure FMC:vFMC 7.4.2（或推薦用於多域穩定性的更高版本）
- 域結構：三級層次結構（全域性>二級子域）。
- 思科身份識別服務引擎：ISE 3.3

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

在大規模企業環境或託管安全服務提供商(MSSP)方案中，通常必須將網路管理劃分為不同的管理邊界。本文檔介紹如何將FMC配置為支援多個域 — 具體針對MSSP管理兩個客戶端的真實示例：零售A和財務B。通過使用通過思科ISE的外部RADIUS身份驗證，管理員可以確保根據使用者的集中憑據自動授予使用者僅對其各自使用者域的訪問許可權。

思科安全防火牆系統使用域實施多租戶。

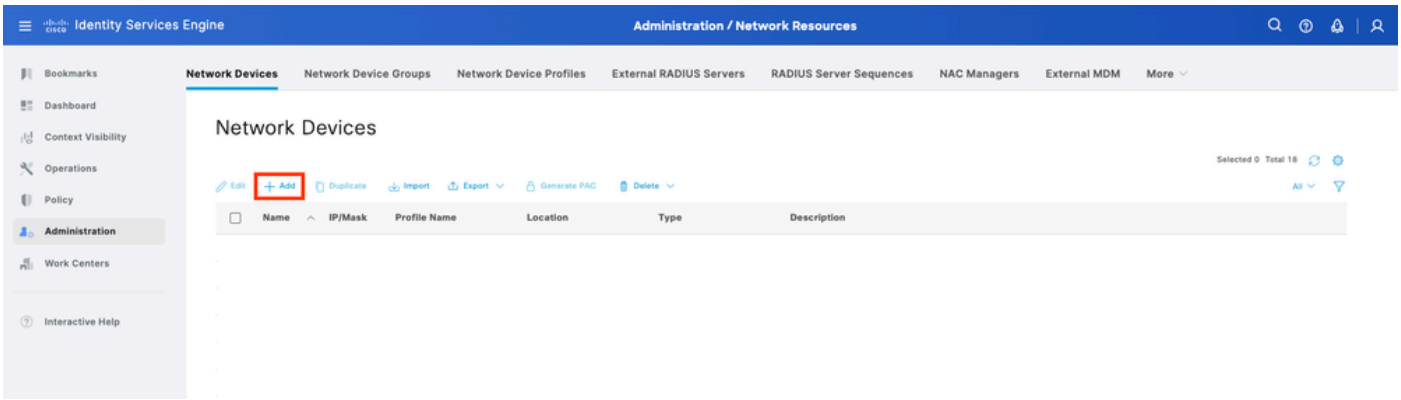
- 域層次結構：層次結構從全域性域開始。您最多可以在兩層或三層結構中建立100個子域。
- 枝葉域：這些是位於層次結構底部的域，沒有其他子域。關鍵是，每個受管FTD裝置必須僅與一個枝葉域關聯。
- RADIUS類別屬性（屬性25）：在多域設定中，FMC使用ISE返回的RADIUS類屬性將已驗證使用者對映到特定域和使用者角色。這允許單個RADIUS伺服器在登入時將使用者動態分配到不同的使用者段（例如，Retail-A與Finance-B）。

組態

ISE 組態

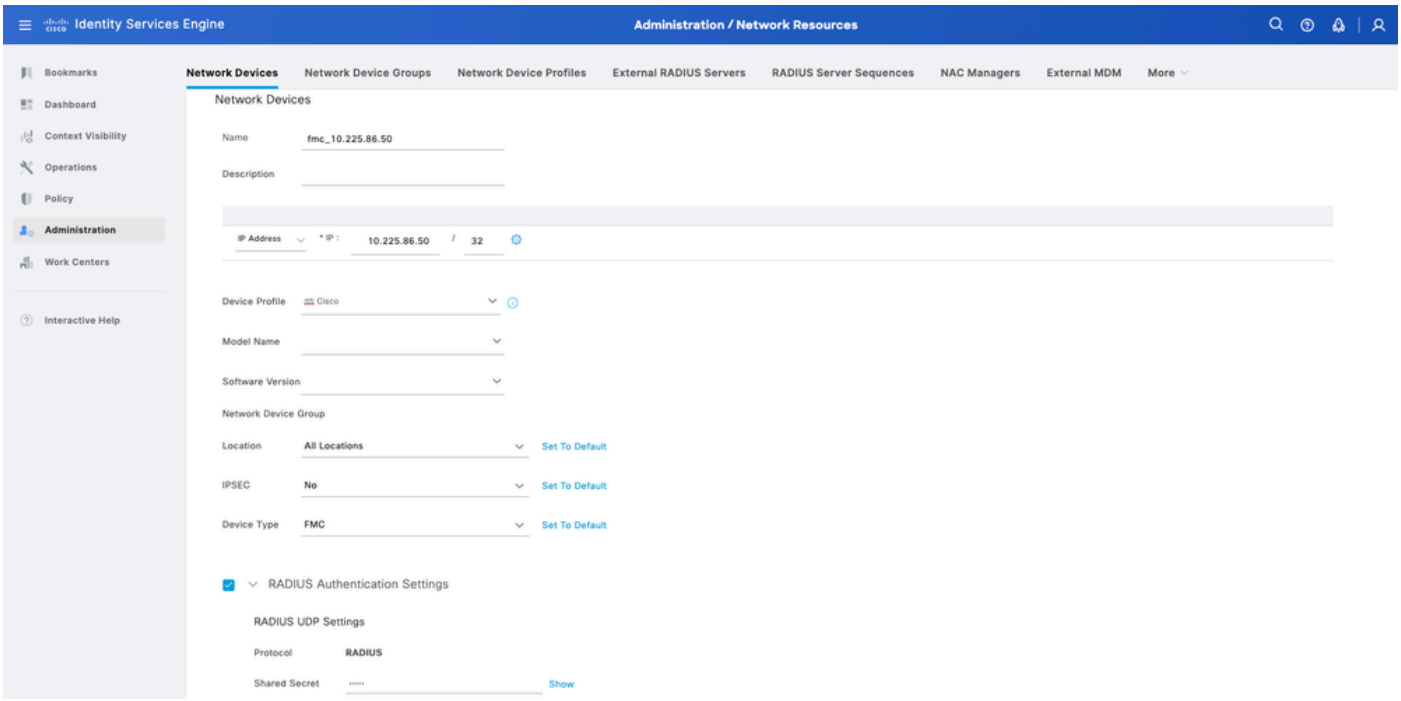
新增網路裝置

步驟1.導覽至Administration > Network Resources > Network Devices > Add。



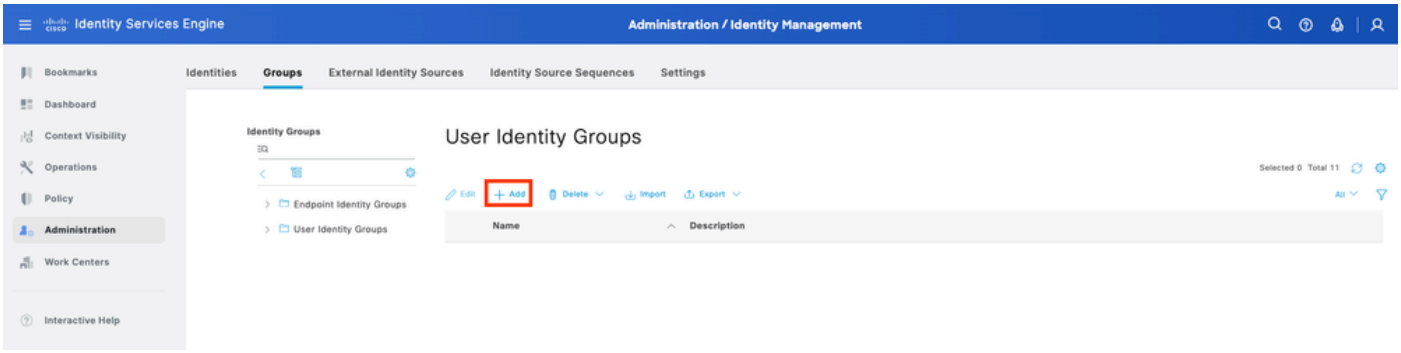
步驟2.為網路裝置對象分配Name並插入FMC IP地址。

勾選「RADIUS」覈取方塊並定義共用密碼。稍後必須用相同的金鑰來配置FMC。完成後，按一下「Save」。

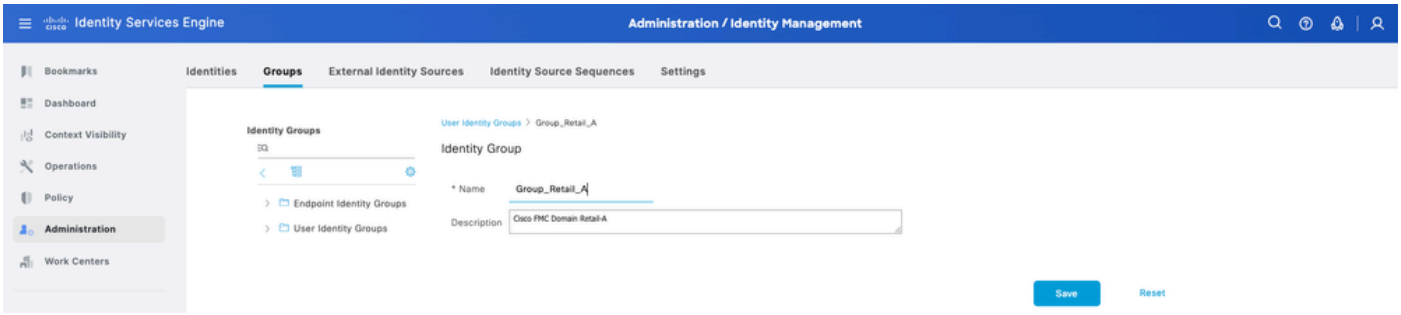


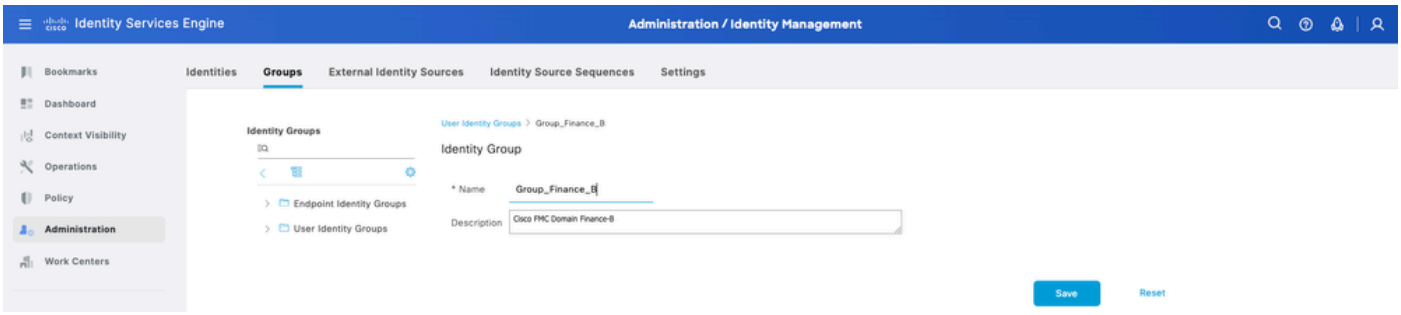
建立本地使用者身份組和使用者

步驟3.建立所需的使用者身份組。導航到Administration > Identity Management > Groups > User Identity Groups > Add。

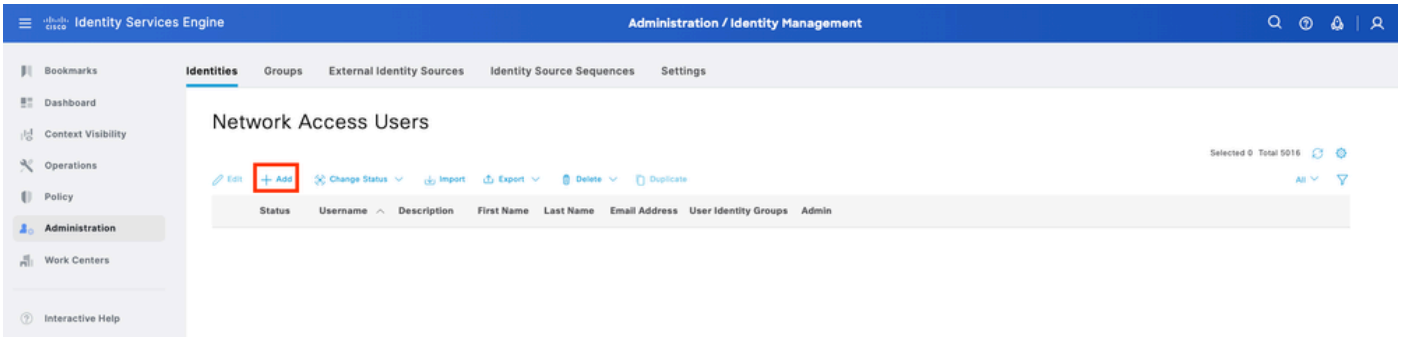


步驟4.為每個組指定一個名稱並單獨儲存。在本示例中，您正在為管理員使用者建立組。建立兩個組：Group_Retail_A和Group_Finance_B。

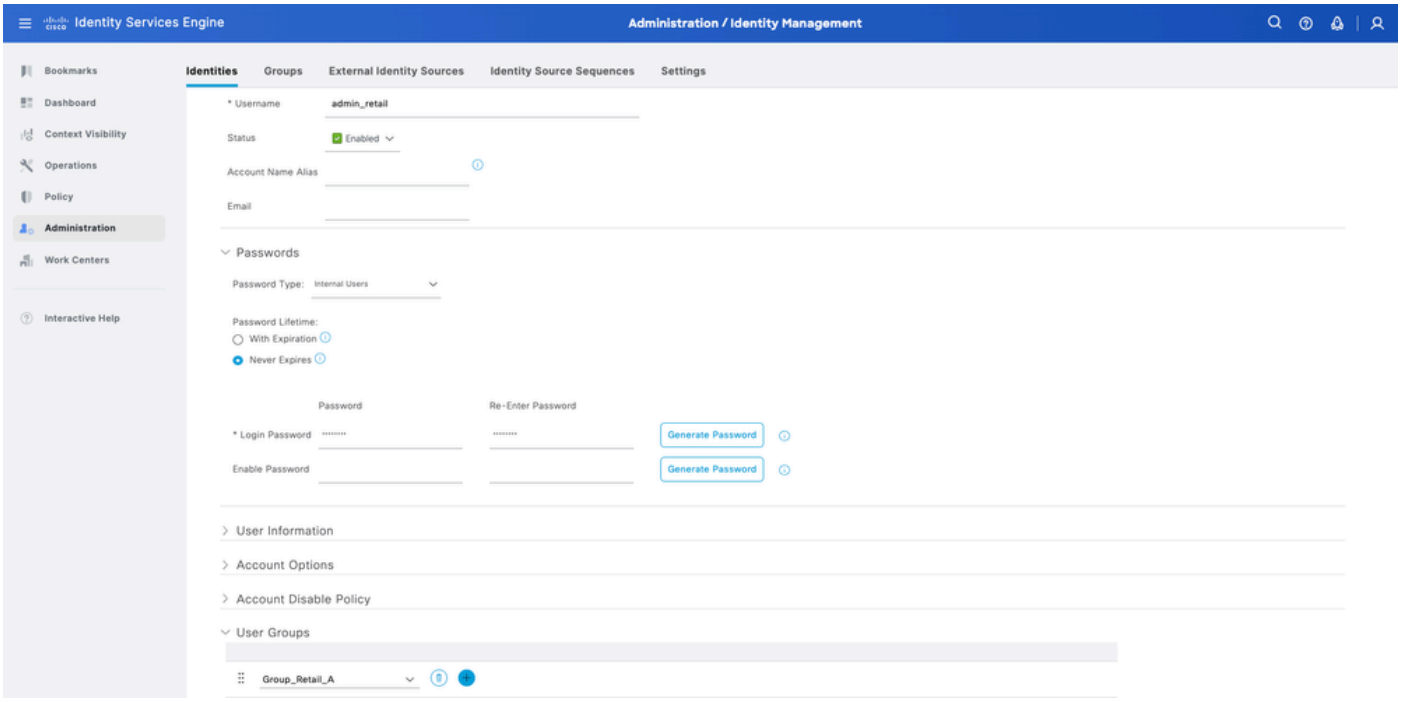




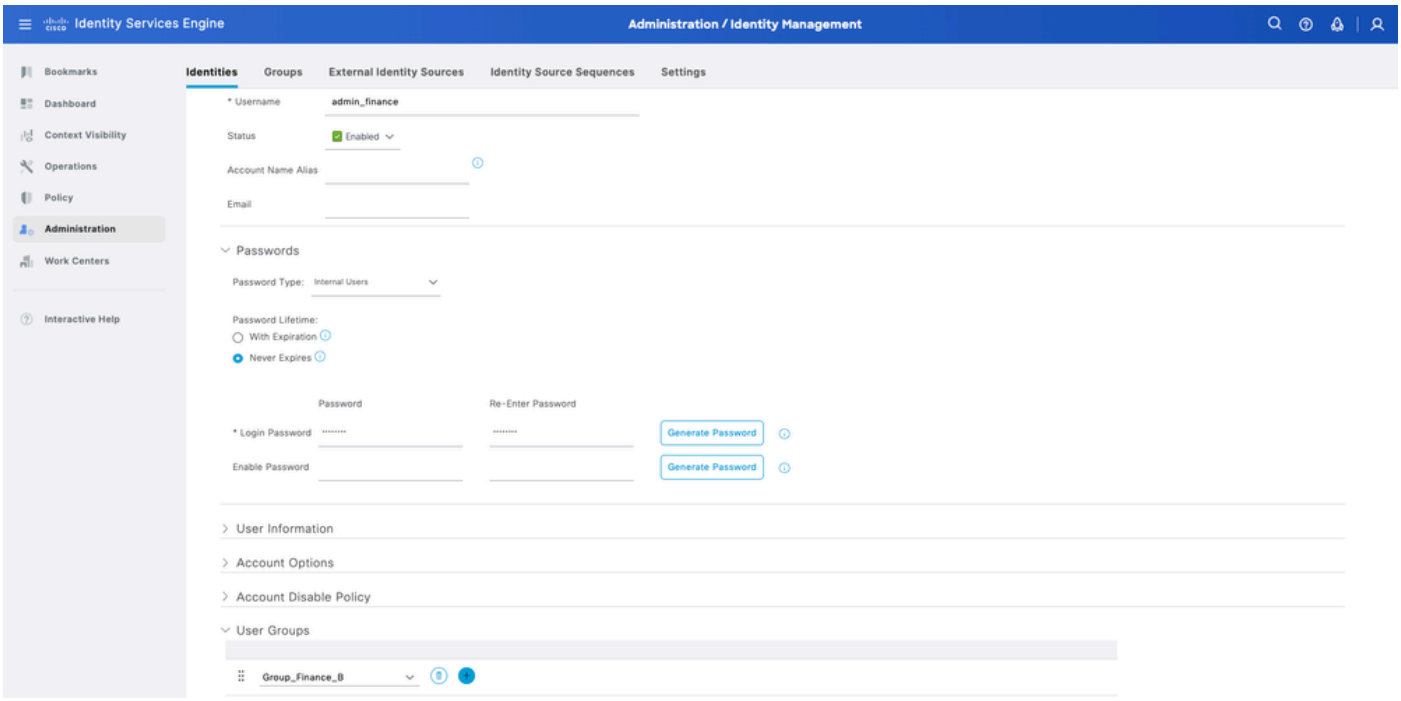
步驟5.建立本地使用者並將其新增到其往來行組。導航到Administration > Identity Management > Identities > Add。



步驟5.1.首先建立具有管理員許可權的使用者。為其分配名稱admin_retail、password和組Group_Retail_A。

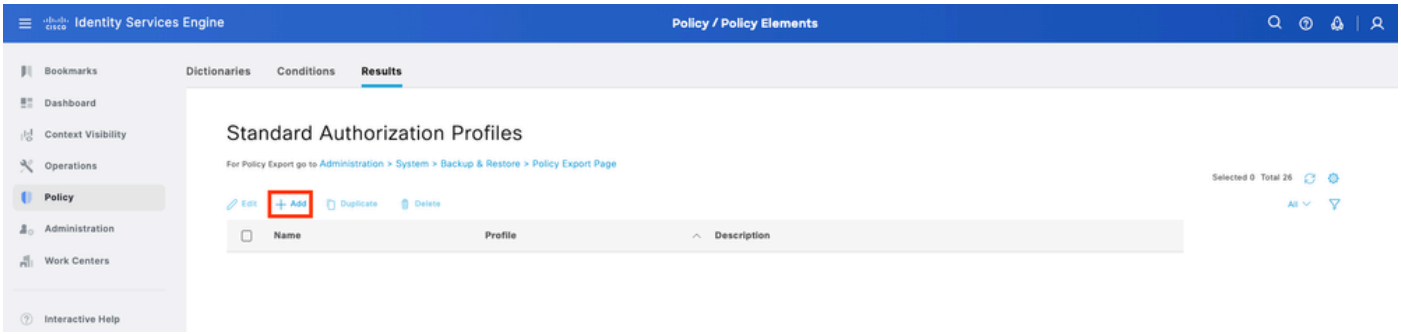


步驟5.2.首先建立具有管理員許可權的使用者。為其分配名稱admin_finance、password和組Group_Finance_B。



建立授權配置檔案

步驟6.為FMC Web Interface Admin使用者建立授權配置檔案。導航至Policy>Policy元素>結果>授權>授權配置檔案> Add。

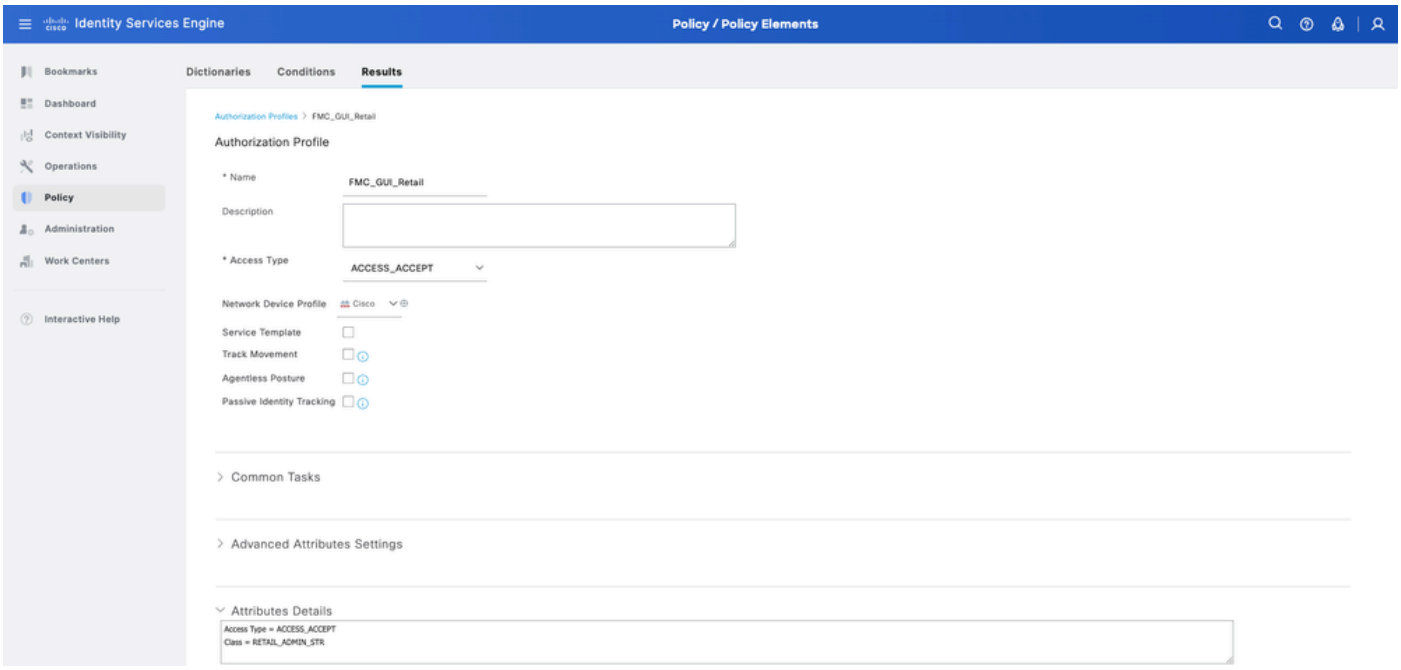


定義授權配置檔案的名稱，將訪問型別保留為ACCESS_ACCEPT。

在「高級屬性設定」下，新增包含值的Radius > Class—[25]，然後點選「提交」。

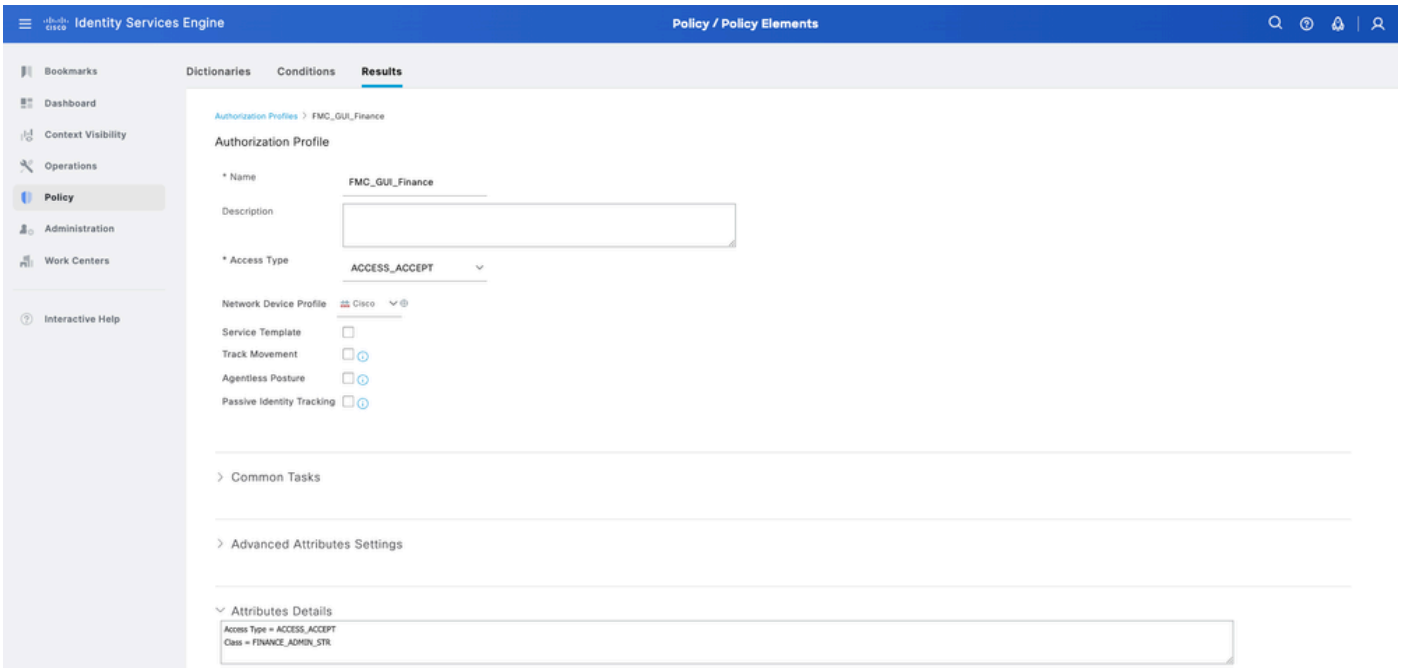
步驟6.1.配置檔案零售：在Advanced Attributes Settings下，新增值為RETAIL_ADMIN_STR的Radius:Class。

提示：其中RETAIL_ADMIN_STR可以是任何內容；確保在FMC一側也放置相同的值需求。



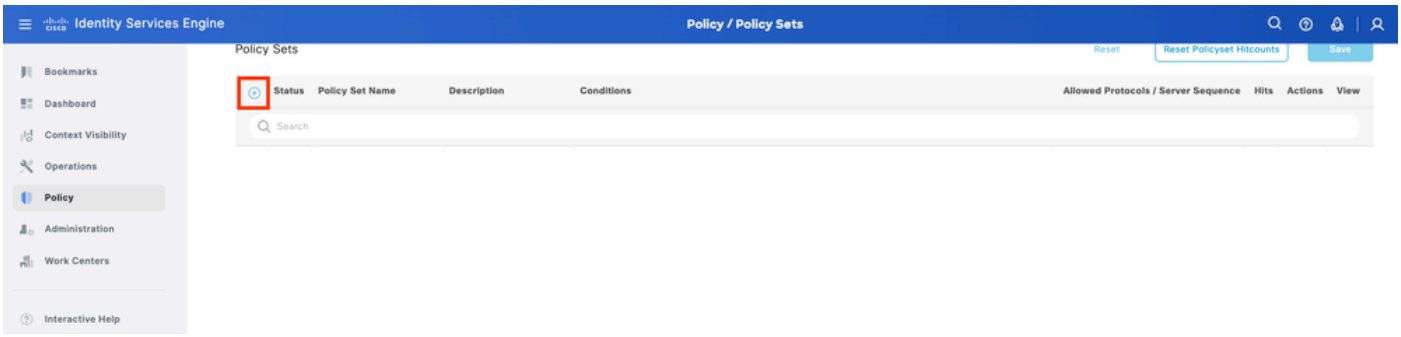
步驟6.2.配置檔案財務：在Advanced Attributes Settings下，新增值為FINANCE_ADMIN_STR的Radius:Class。

提示：其中FINANCE_ADMIN_STR可以是任何內容；確保在FMC一側也輸入相同的值。



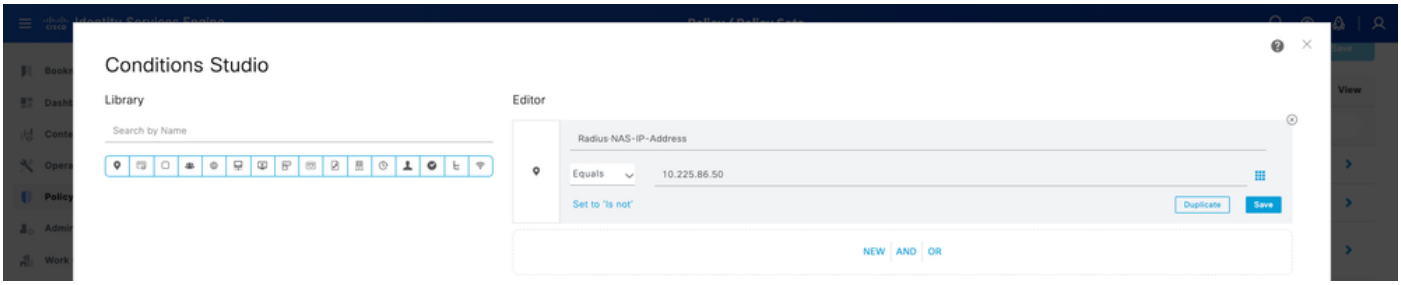
新增新策略集

步驟7.建立與FMC IP地址匹配的策略集。這是為了防止其他裝置向使用者授予訪問許可權。導航到Policy > Policy Sets > Plus sign圖示，該圖示位於左上角。



步驟8.1.新行位於策略集的頂部。

命名新策略，並新增與FMC IP地址匹配的RADIUS NAS-IP-Address屬性的頂級條件。按一下Use以保留更改並退出編輯器。



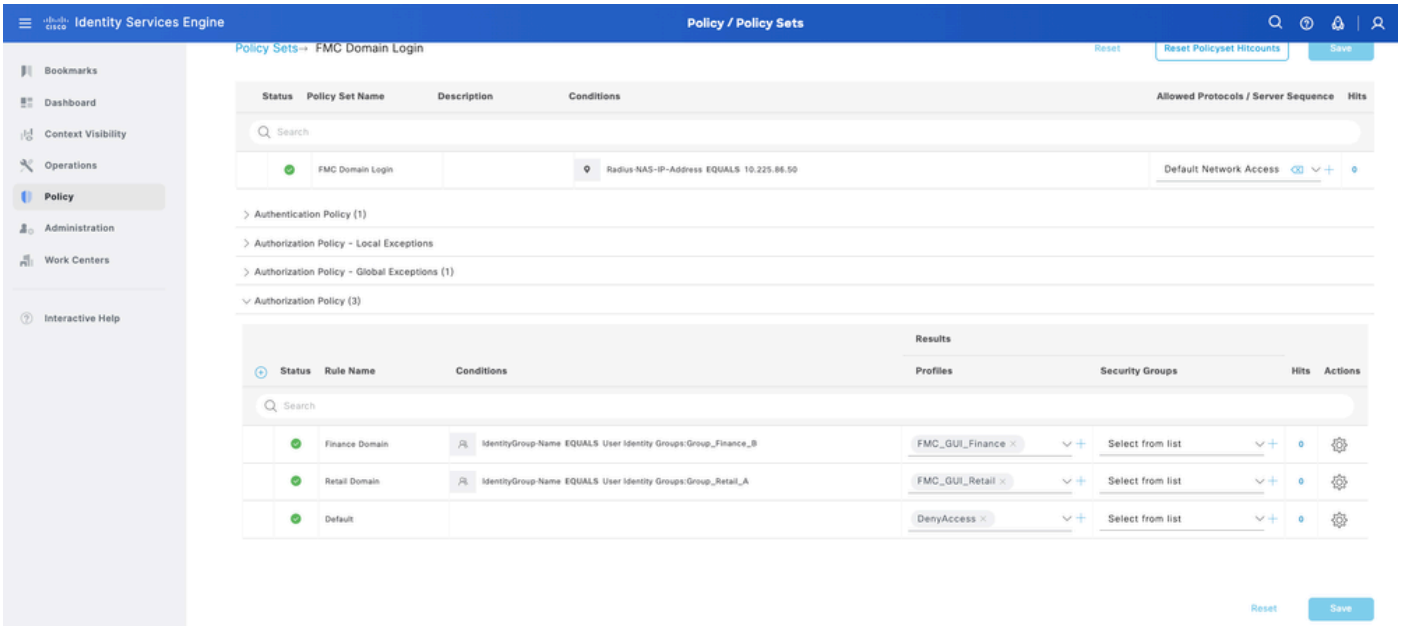
步驟8.2.完成後，按一下Save。

步驟9.按一下位於行尾的set圖示檢視新的策略集。

展開Authorization Policy選單，並推送Plus符號圖示以新增新規則，以允許訪問具有管理員許可權的使用者。給它一個名字。

設定條件以匹配屬性名稱等於(Attribute Name Equals)的字典身份組，然後選擇使用者身份組。在Authorization Policy下，建立規則：

- Rule 1:如果使用者身份組等於Group_Retail_A，請分配配置檔案零售。
- 規則2:如果使用者身份組等於Group_Finance_B，請分配配置檔案財務。



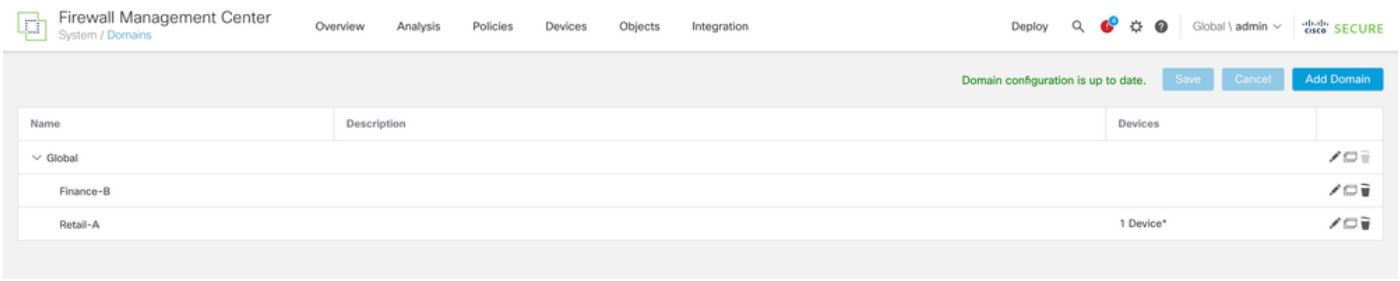
步驟10.分別為每個規則設定Authorization Profiles，然後點選Save。

FMC配置

新增用於FMC身份驗證的ISE RADIUS伺服器

步驟 1. 建立域結構：

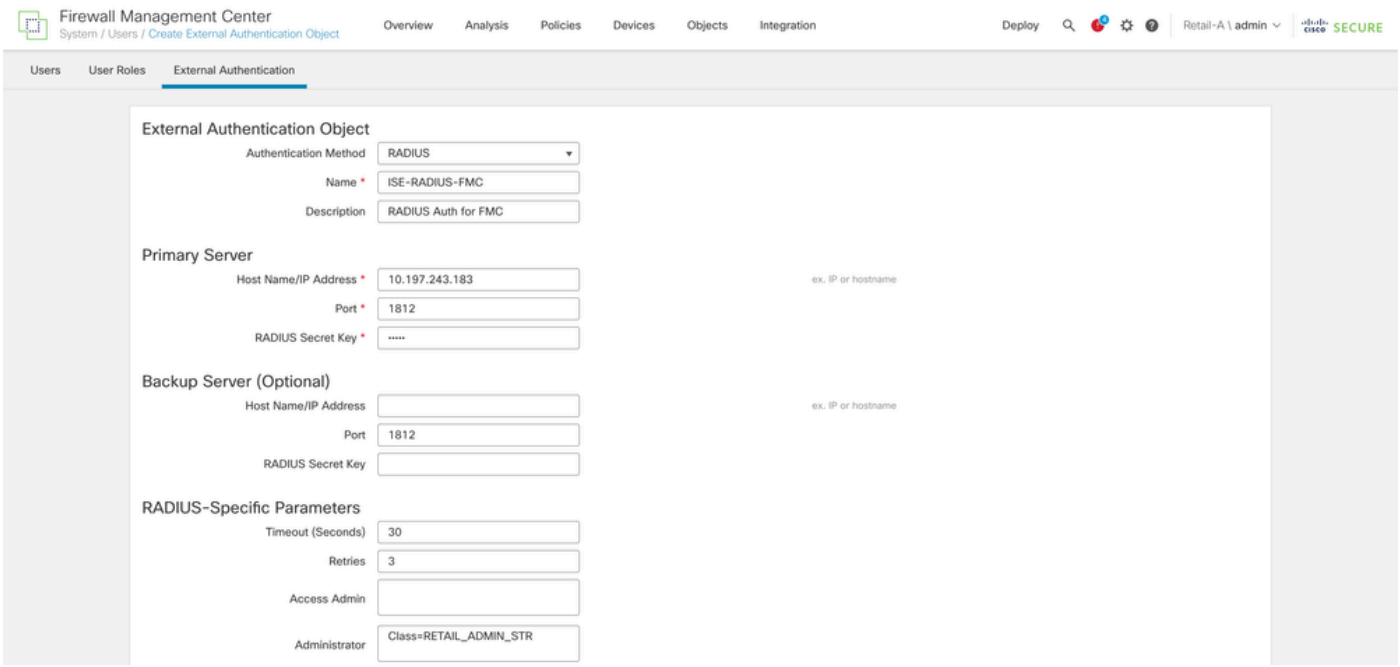
- 登入到FMC全域性域。
- 導覽至Administration > Domains。
- 按一下Add Domain以將Retail-A和Finance-B建立為Global的子域。



步驟 2.1. 將域下的外部身份驗證對象配置為Retail-A

- 將域切換到Retail-A。
- 導覽至System > Users > External Authentication。
- 選擇Add External Authentication Object，然後選擇RADIUS。
- 輸入先前配置的ISE IP地址和共用金鑰。
- 輸入RADIUS特定引數>管理員> class=RETAIL_ADMIN_STR

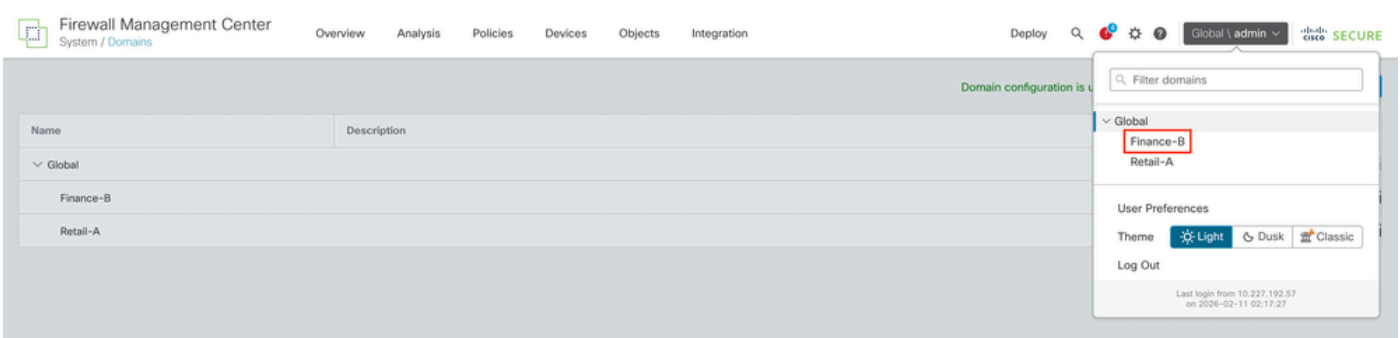
提示：對ISE的授權配置檔案下配置的類使用相同的值。

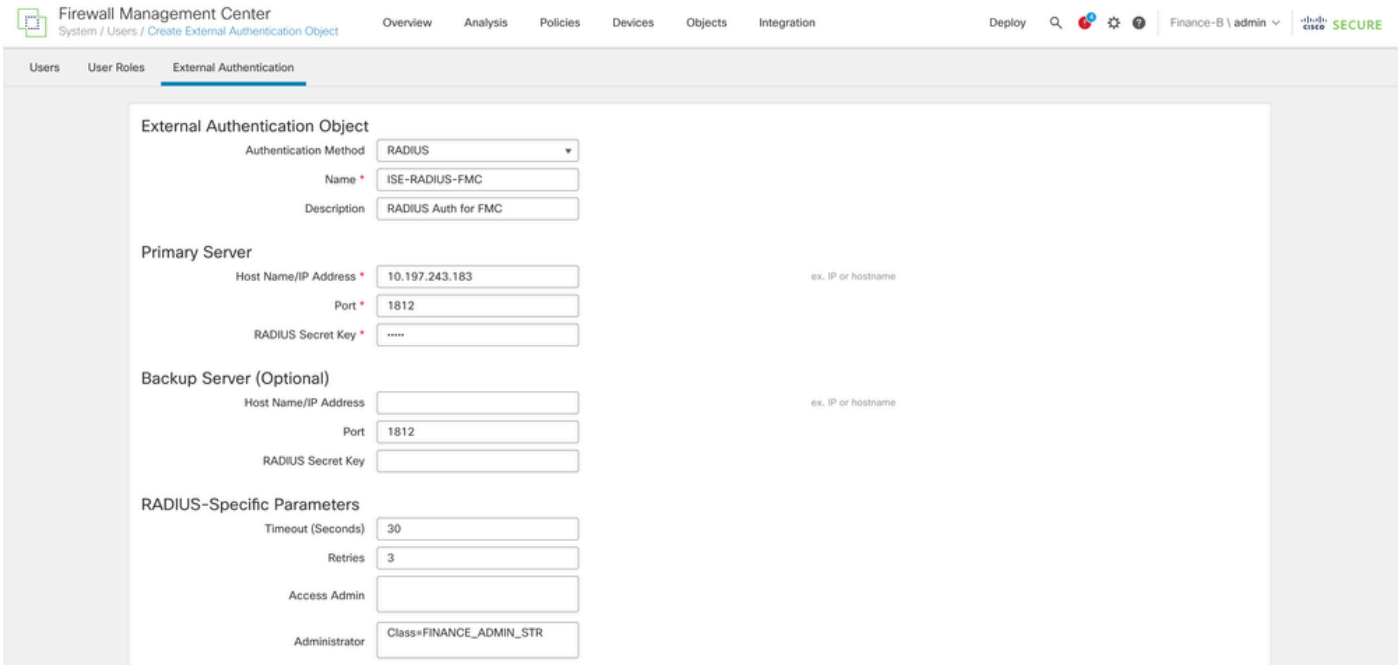


步驟 2.2. 將域下的外部身份驗證對象配置為Finance-B

- 將Domain切換到Finance-B。
- 導覽至System > Users > External Authentication。
- 選擇Add External Authentication Object，然後選擇RADIUS。
- 輸入ISE IP地址和Shared Secret之前配置。
- 輸入RADIUS特定引數>管理員> class=FINANCE_ADMIN_STR

提示：對ISE的授權配置檔案下配置的類使用相同的值。





步驟 3. 啟用身份驗證：啟用對象並將其設定為Shell Authentication方法。按一下「Save」和「Apply」。

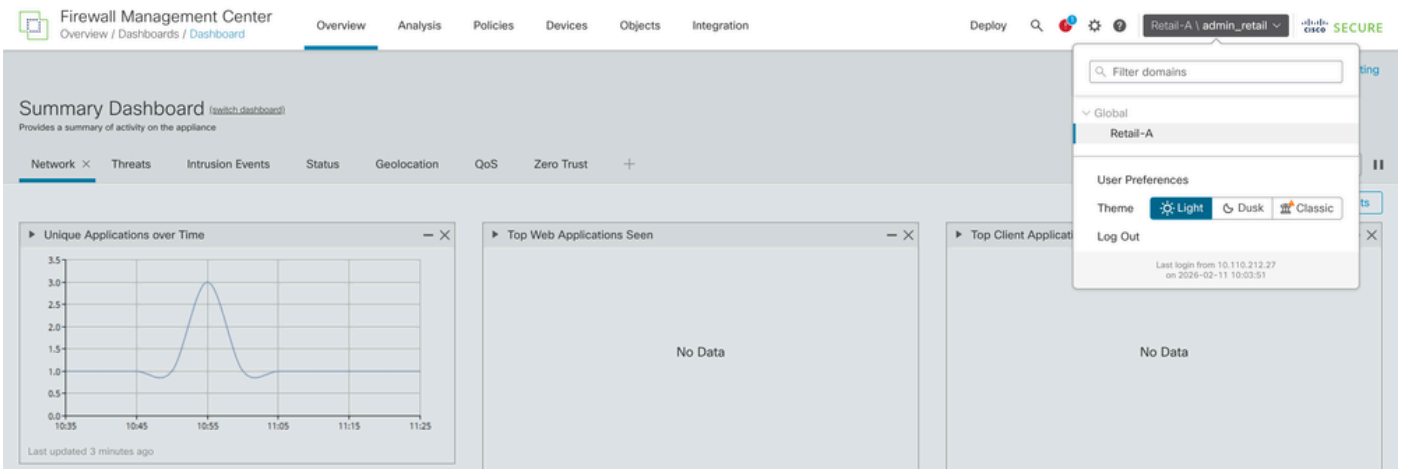
驗證

跨域登入測試

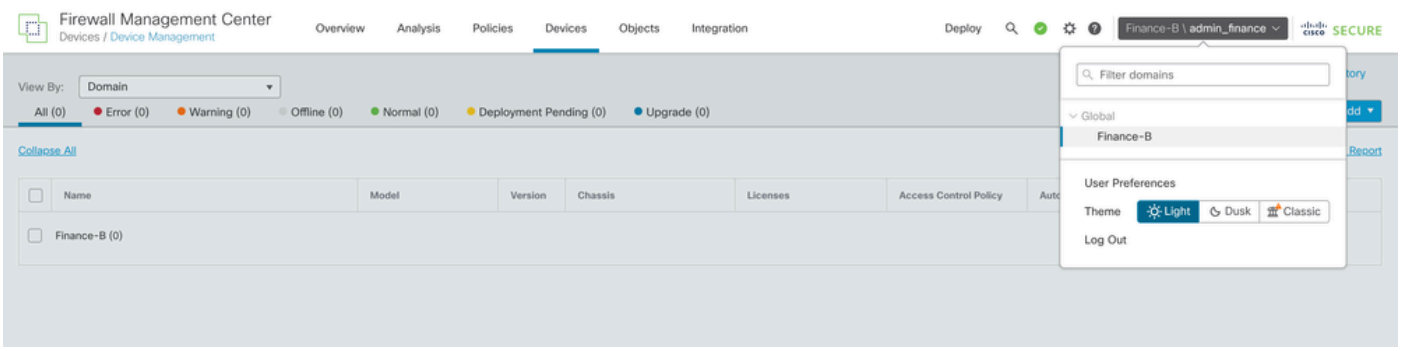
- 嘗試使用admin_retail登入到FMC Web介面。驗證UI右上角顯示的當前域是否為Retail-A。

提示：登入到特定域時，請使用使用者名稱格式domain_name\radius_user_mapped_with_that_domain。

例如，如果Retail admin使用者需要登入，則使用者名稱必須為Retail-A\admin_retail和相應的密碼。



- 註銷並以admin_finance身份登入。驗證使用者是否僅限於Finance-B域且無法看到Retail-A裝置。

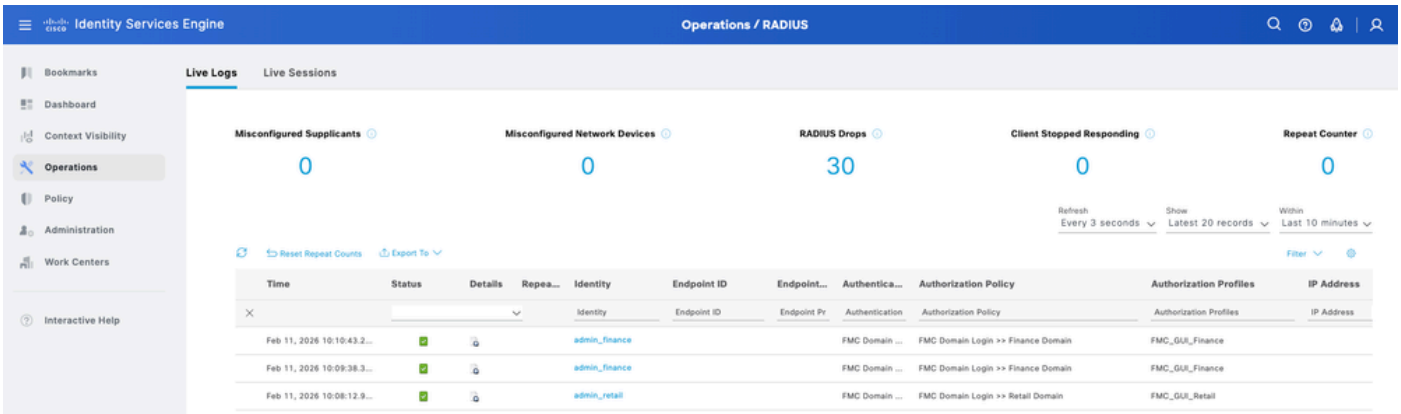


FMC內部測試

導覽至FMC中的RADIUS伺服器設定。使用其他測試引數部分輸入測試使用者名稱和密碼。成功的測試必須顯示綠色的「成功」消息。

ISE 即時記錄

- 在Cisco ISE中，導航到Operations > RADIUS > Live Logs。



- 確認身份驗證請求顯示Pass狀態，並確認已在RADIUS Access-Accept資料包中傳送正確的授權配置檔案（和相關類別字串）。

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

相關資訊

[將ISE作為RADIUS伺服器配置FMC和FTD外部身份驗證]

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。