在多域环境中配置FMC外部身份验证

目录

简介

本文档介绍在思科FMC中实施多租户（多域），同时利用思科ISE进行集中式RADIUS身份验证。

先决条件

要求

建议了解以下主题：

- 通过GUI和/或外壳对Cisco安全防火墙管理中心进行初始配置。
- 在FMC的全局域中拥有创建子域和外部身份验证对象的完全管理员权限。
- 在ISE上配置身份验证和授权策略。
- 基本RADIUS知识

使用的组件

- 思科安全FMC:vFMC 7.4.2（为实现多域稳定性而推荐或更高版本）
- 域结构：三级层次结构（全局>二级子域）。
- 思科身份服务引擎：ISE 3.3

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

在大规模企业环境或托管安全服务提供商(MSSP)方案中，通常必须将网络管理划分到不同的管理边界中。本文档介绍如何将FMC配置为支持多个域，尤其是对于MSSP管理两个客户端的真实示例：零售A和财务B。通过使用外部RADIUS身份验证通过Cisco ISE，管理员可以确保根据用户的集中凭证，自动授予用户仅对其各自用户域的访问权限。

思科安全防火墙系统使用域实施多租户。

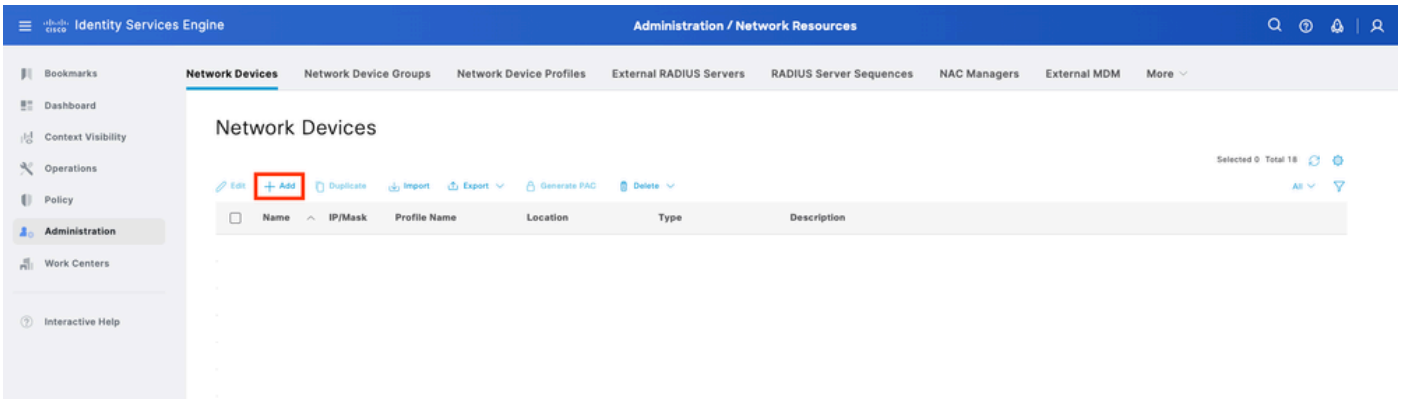
- 域层次结构：层次结构从全局域开始。您可以在两层或三层结构中创建多达100个子域。
- 枝叶域：这些是位于层次结构底部的域，没有其他子域。关键是，每个托管FTD设备必须仅与一个枝叶域关联。
- RADIUS类属性（属性25）：在多域设置中，FMC使用ISE返回的RADIUS类属性将经过身份验证的用户映射到特定域和用户角色。这允许单个RADIUS服务器在登录时将用户动态分配到不同的用户段（例如，Retail-A与Finance-B）。

配置

ISE 配置

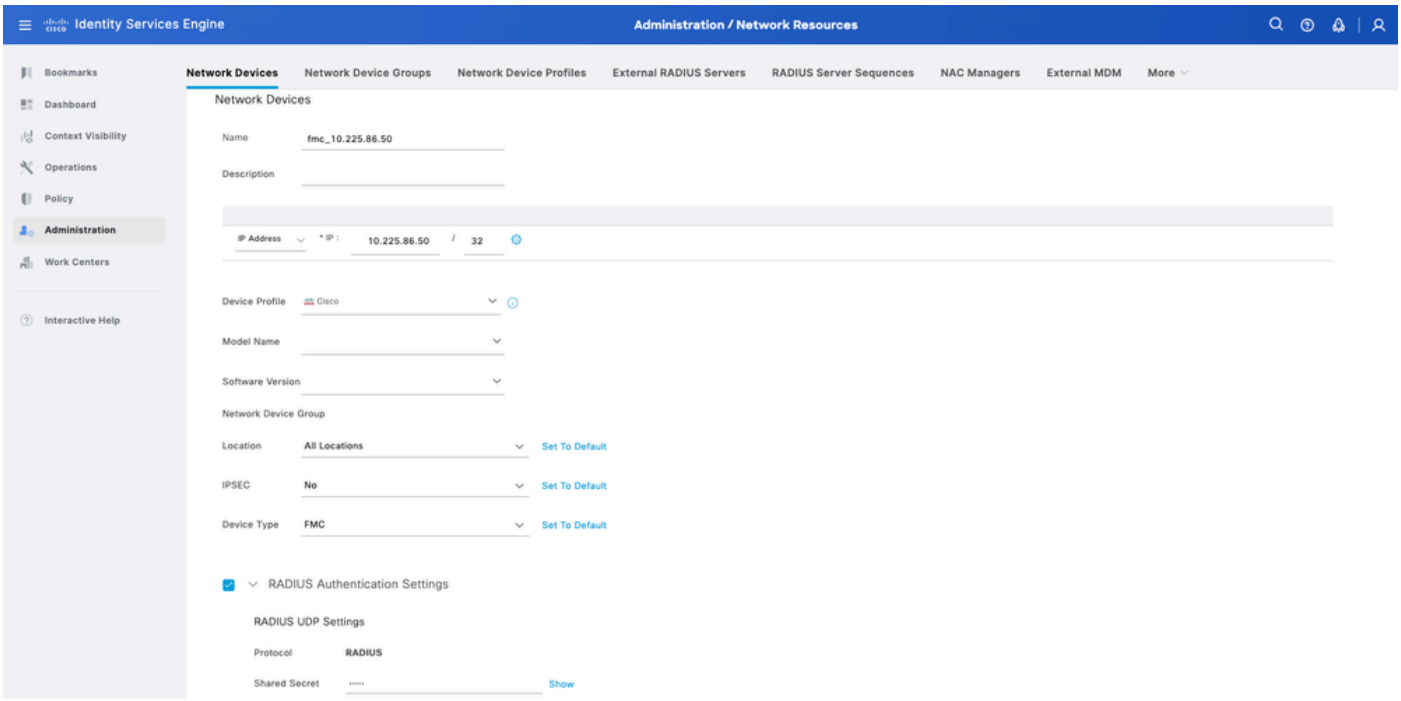
添加网络设备

步骤1.导航到管理> Network Resources > Network Devices > Add。



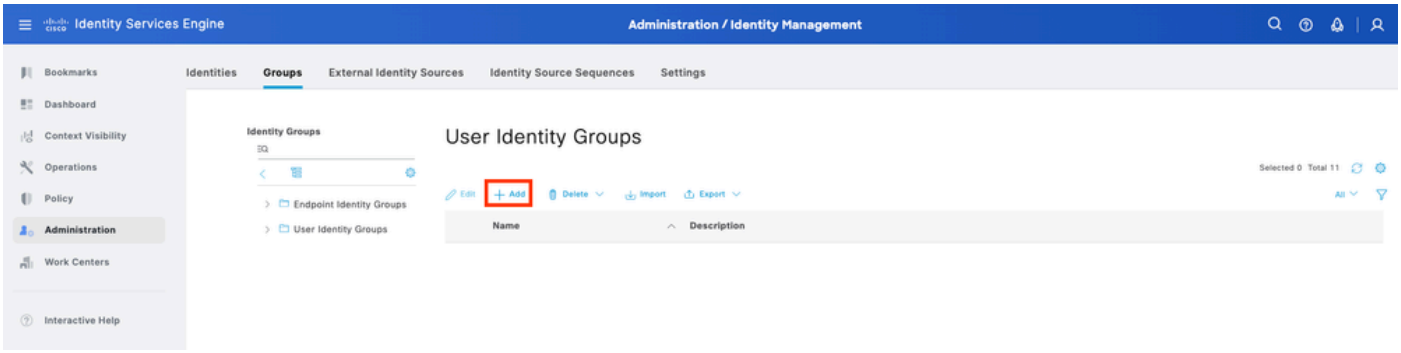
步骤2.为网络设备对象分配Name并插入FMC IP地址。

选中RADIUS复选框并定义共享密钥。稍后必须使用该密钥来配置FMC。完成后，单击Save。

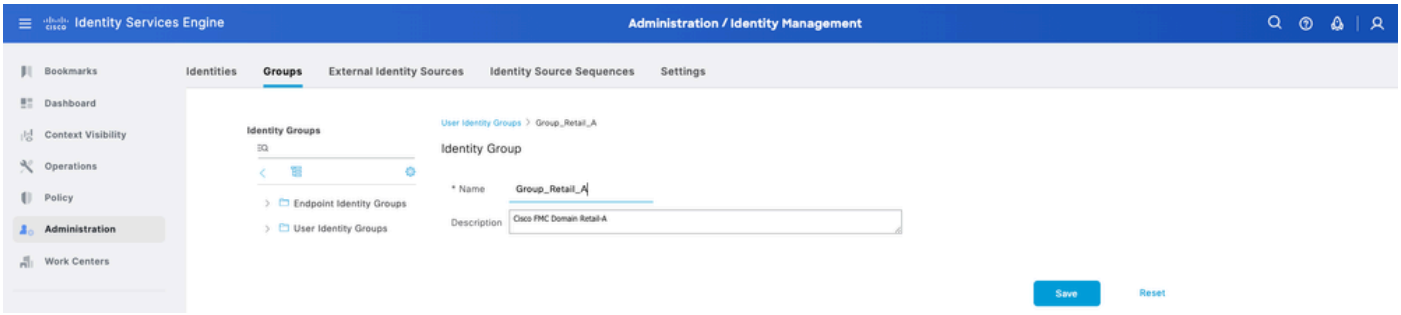


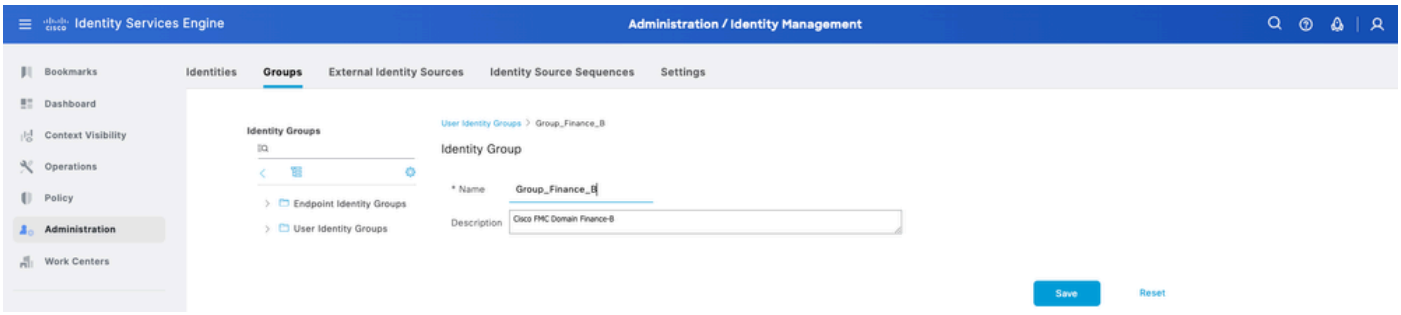
创建本地用户身份组和用户

步骤3.创建所需的用户身份组。导航到Administration > Identity Management > Groups > User Identity Groups > Add。

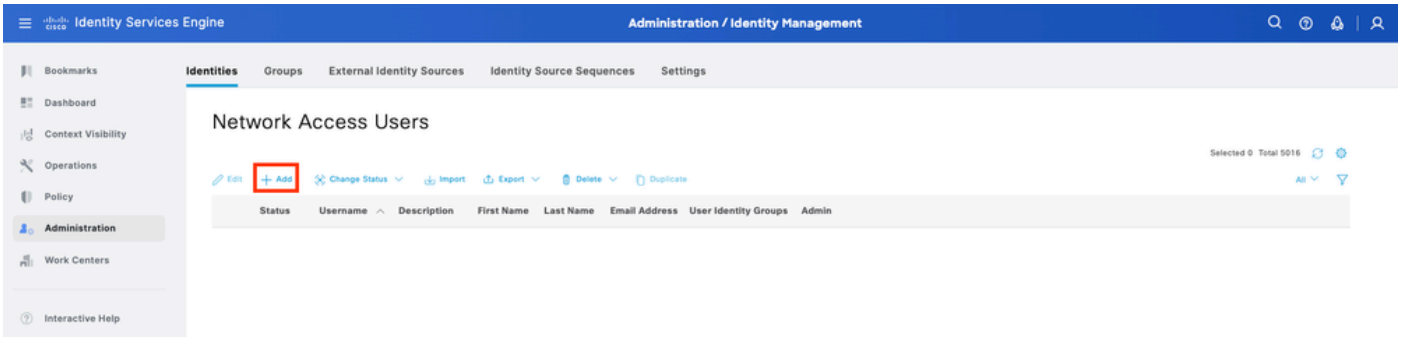


步骤4.为每个组指定一个名称并单独保存。在本例中，您正在为管理员用户创建组。创建两个组：Group_Retail_A和Group_Finance_B。

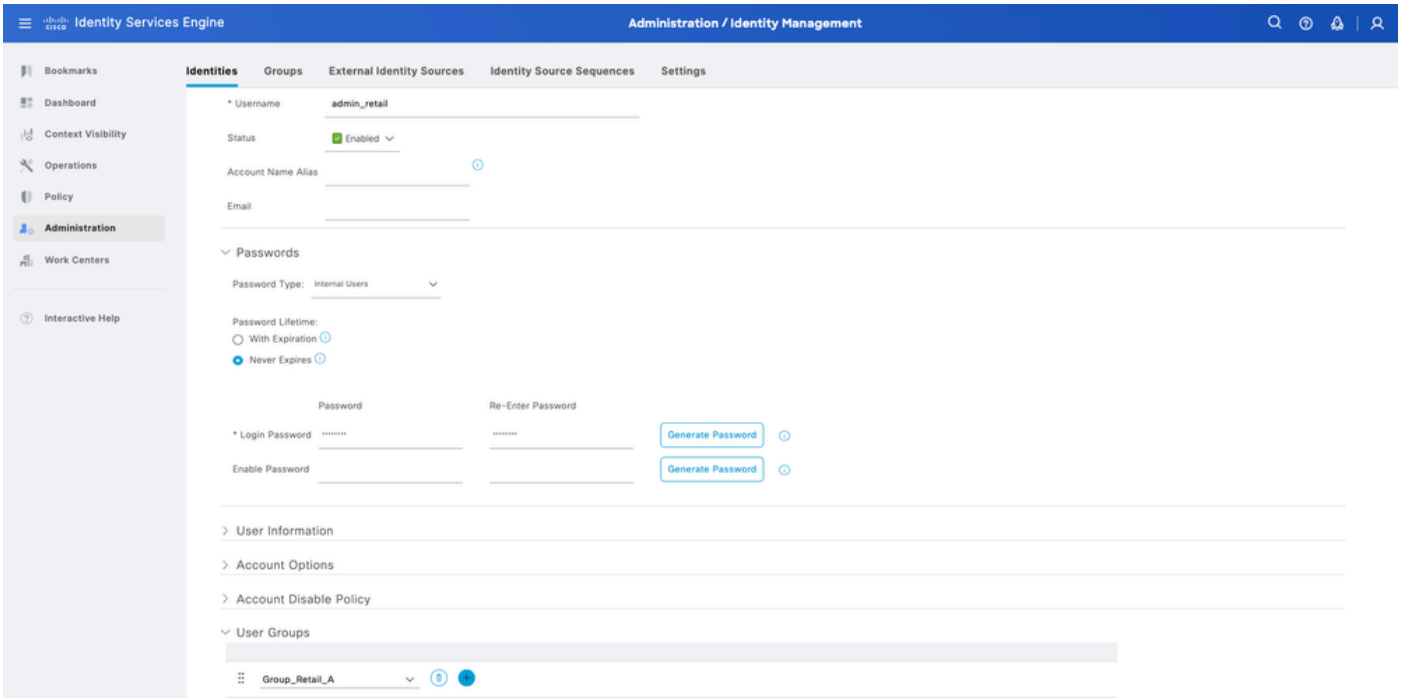




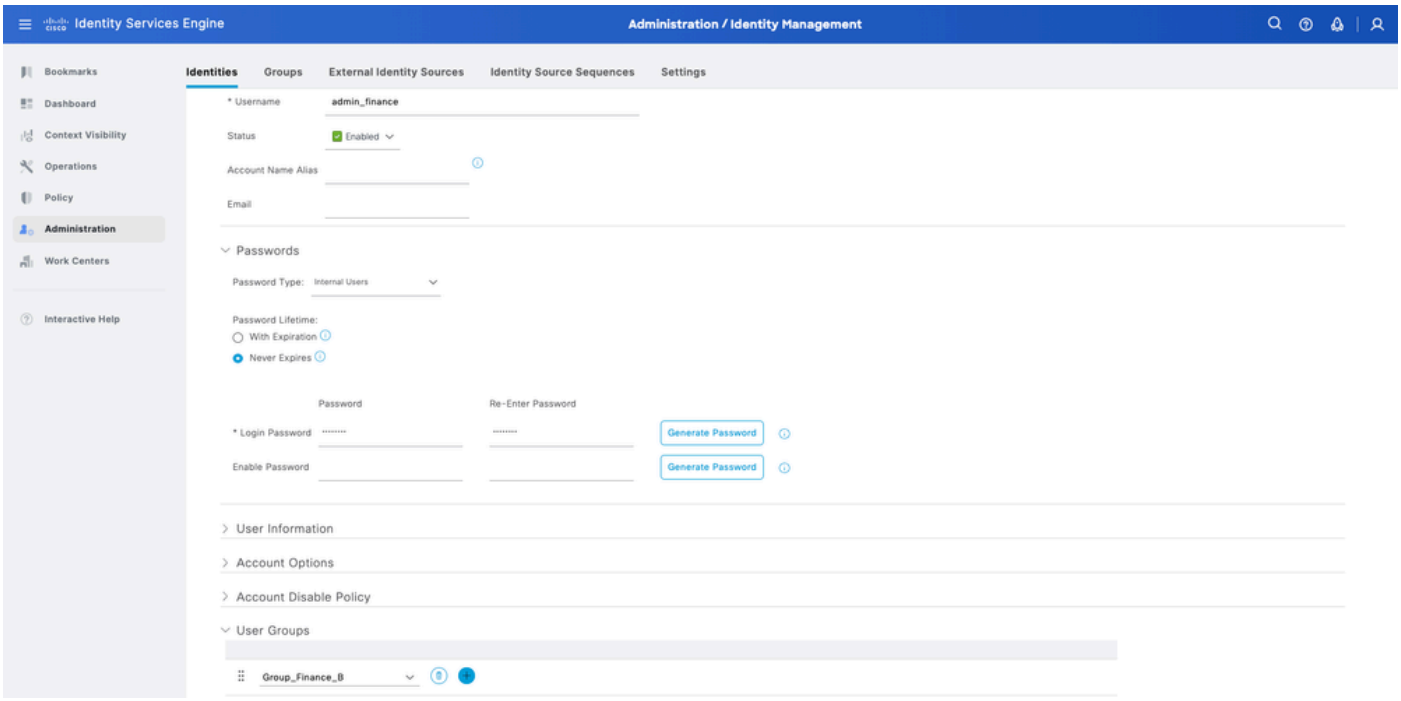
步骤5.创建本地用户并将其添加到其往来行组。导航到Administration> Identity Management > Identities > Add。



步骤5.1.首先创建具有管理员权限的用户。为其分配名称admin_retail、密码和组Group_Retail_A。

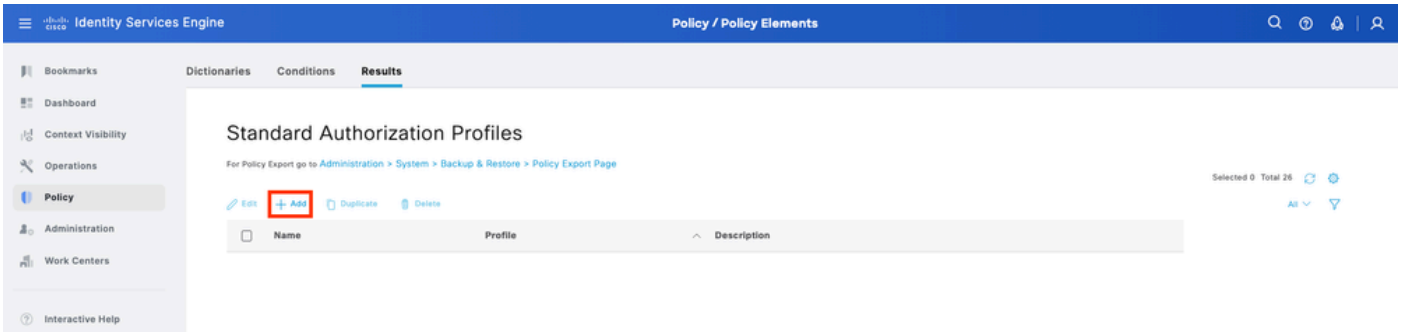


步骤5.2.首先创建具有管理员权限的用户。为其分配名称admin_finance、password和组Group_Finance_B。



创建授权配置文件

步骤6.为FMC Web界面管理员用户创建授权配置文件。导航到Policy> Policy Elements > Results > Authorization > Authorization Profiles > Add。

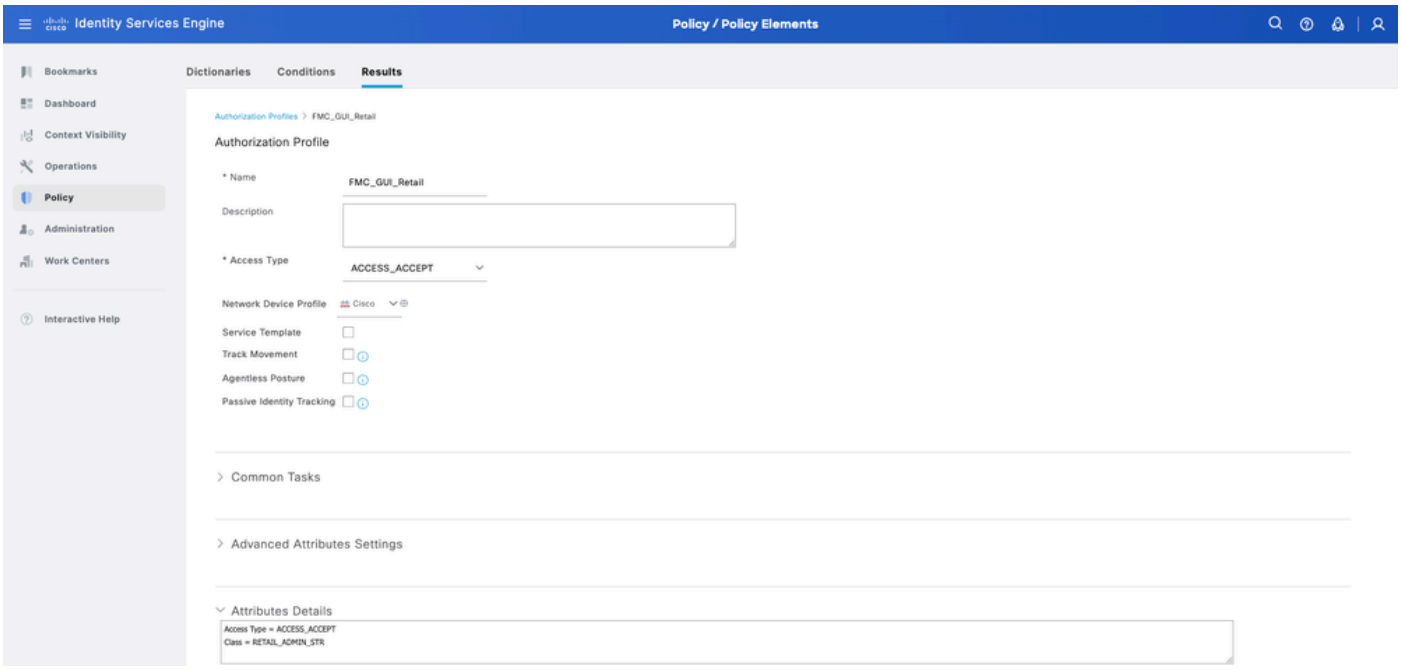


定义授权配置文件的名称，将访问类型保留为ACCESS_ACCEPT。

在Advanced Attributes Settings下，添加带有值的Radius > Class— [25]，然后点击Submit。

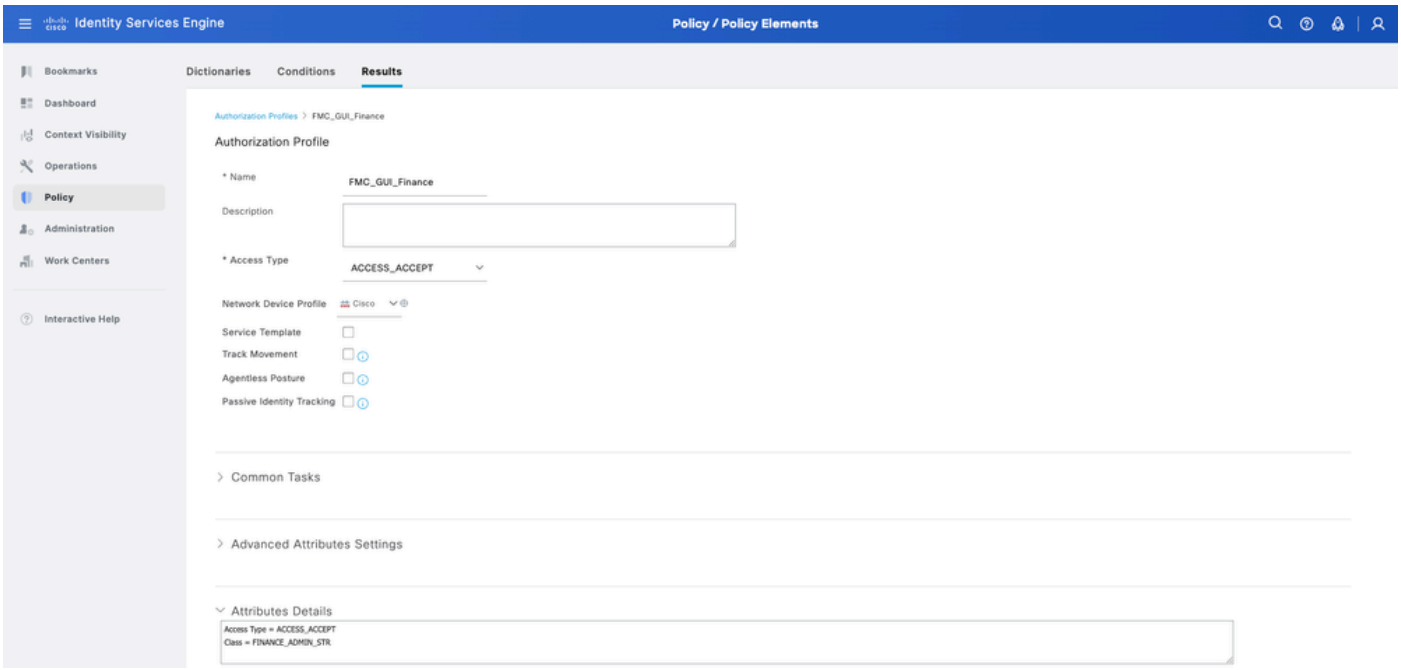
第6.1步：配置文件零售：在Advanced Attributes Settings下，添加值为RETAIL_ADMIN_STR的Radius:Class。

提示：此处RETAIL_ADMIN_STR可以是任何内容；确保在FMC一侧也具有相同的价值需求。



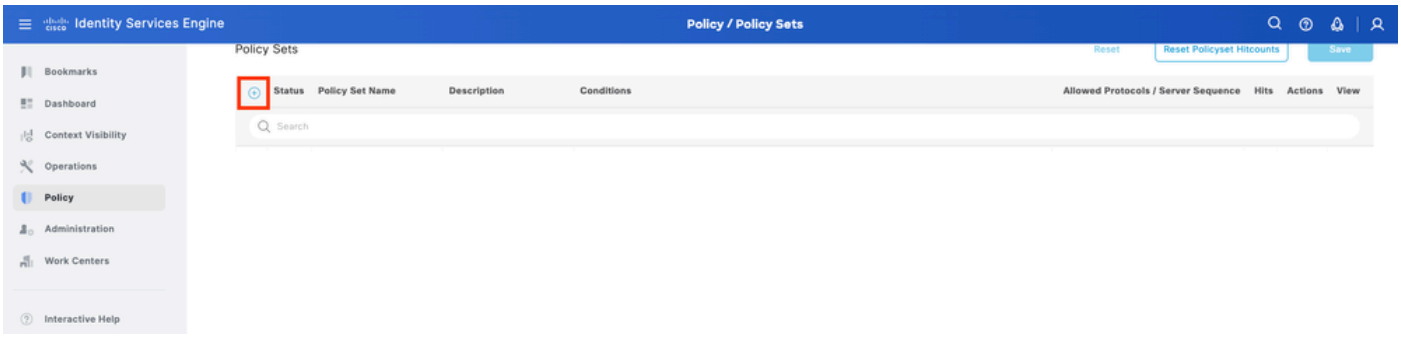
第6.2步：配置文件财务：在Advanced Attributes Settings下，添加值为FINANCE_ADMIN_STR的Radius:Class。

提示：这里FINANCE_ADMIN_STR可以是任何字符；确保在FMC一侧也放置相同的值。



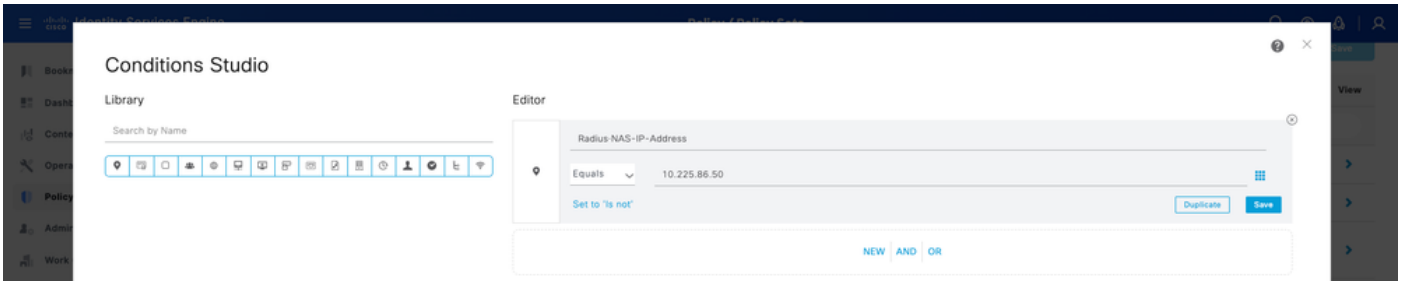
添加新策略集

步骤7.创建与FMC IP地址匹配的策略集。这是为了防止其他设备向用户授予访问权限。导航到位于左上角的Policy > Policy Sets > Plus sign图标。



步骤8.1.新行位于策略集的顶部。

命名新策略，并为与FMC IP地址匹配的RADIUS NAS-IP-Address属性添加顶部条件。单击Use以保留更改并退出编辑器。



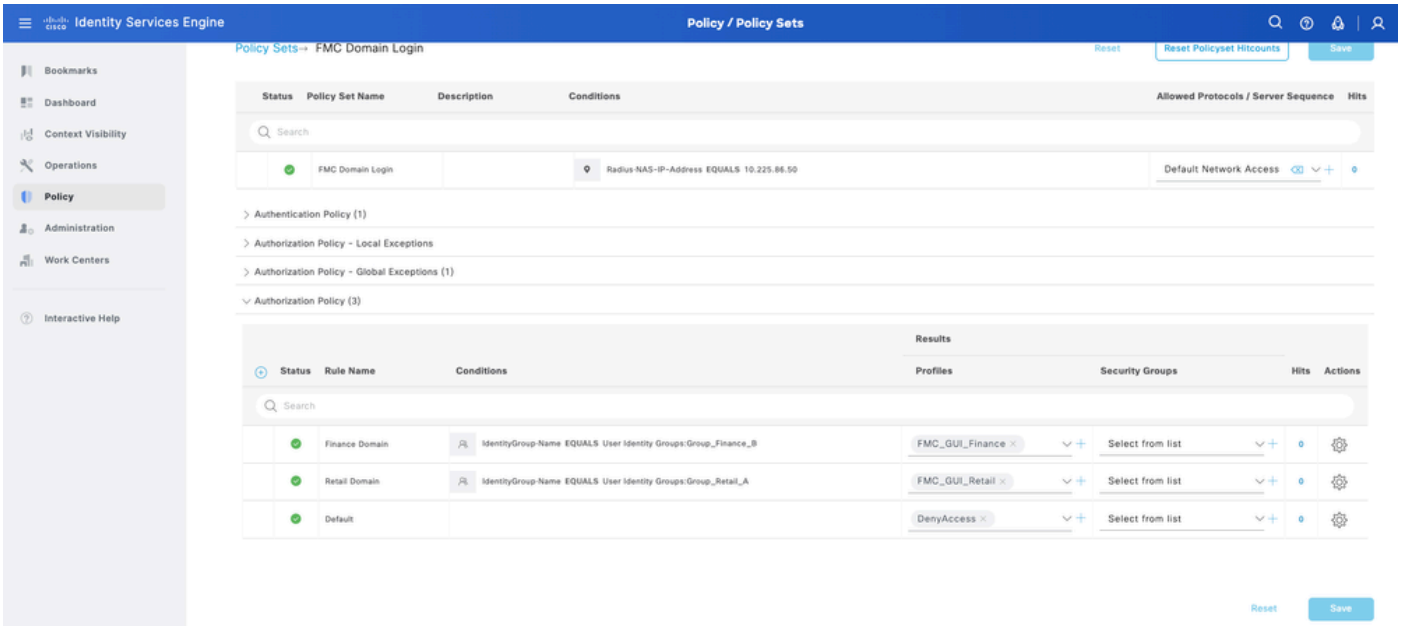
步骤8.2.完成后，单击Save。

步骤9.点击行尾的set图标查看新的策略集。

展开Authorization Policy菜单并推送Plus符号图标以添加新的规则，以允许访问具有管理员权限的用户。给它一个名字。

设置条件以匹配Dictionary Identity Group with Attribute Name Equals并选择User Identity Groups。在Authorization Policy下，创建规则：

- 规则 1：如果用户身份组等于Group_Retail_A，请分配配置文件零售。
- 规则 2：如果用户身份组等于Group_Finance_B，请分配配置文件财务。



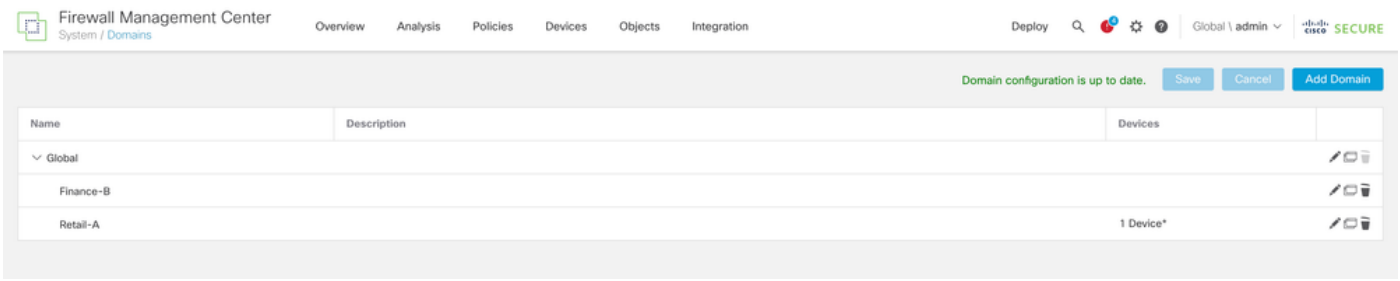
步骤10.分别为每个规则设置Authorization Profiles，然后点击Save。

FMC配置

添加用于FMC身份验证的ISE RADIUS服务器

步骤1：建立域结构：

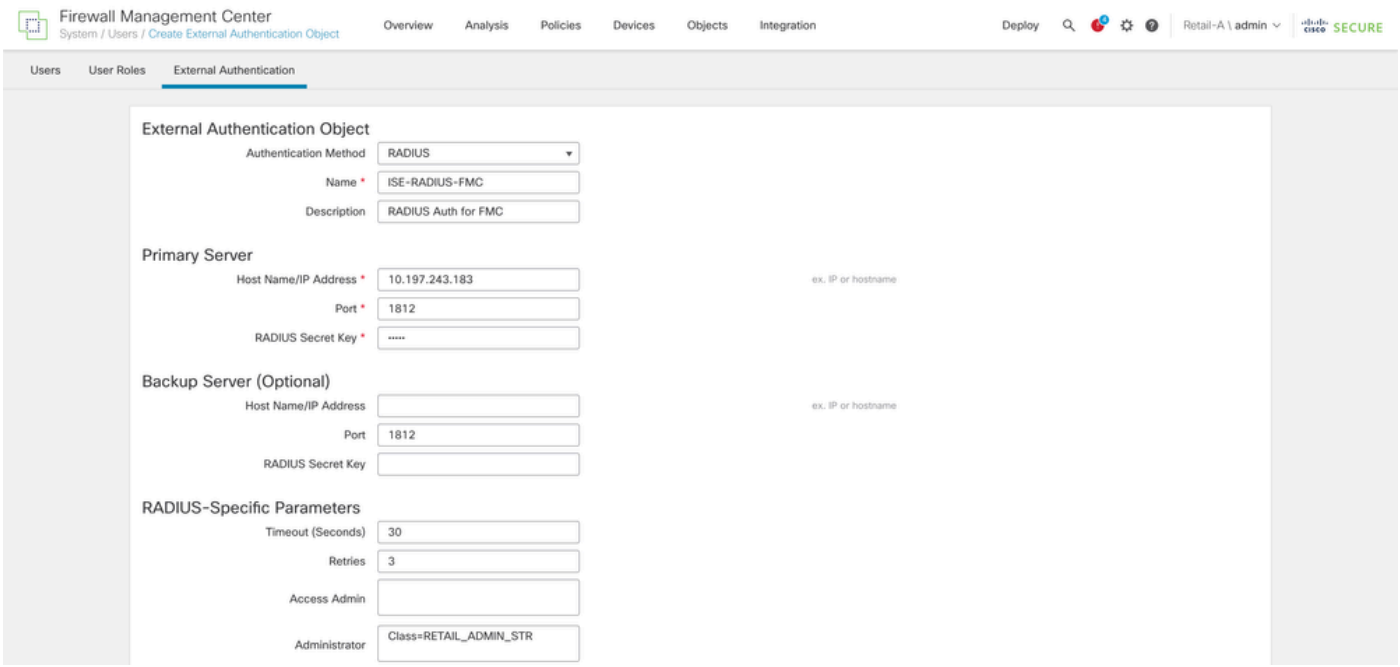
- 登录FMC全局域。
- 导航到管理> 域。
- 单击Add Domain将Retail-A和Finance-B创建为Global的子域。



第 2.1 步： 将域下的外部身份验证对象配置为Retail-A

- 将域切换到Retail-A。
- 导航到System > Users > External Authentication。
- 选择Add External Authentication Object，然后选择RADIUS。
- 输入先前配置的ISE IP地址和共享密钥。
- 输入RADIUS特定参数>管理员> class=RETAIL_ADMIN_STR

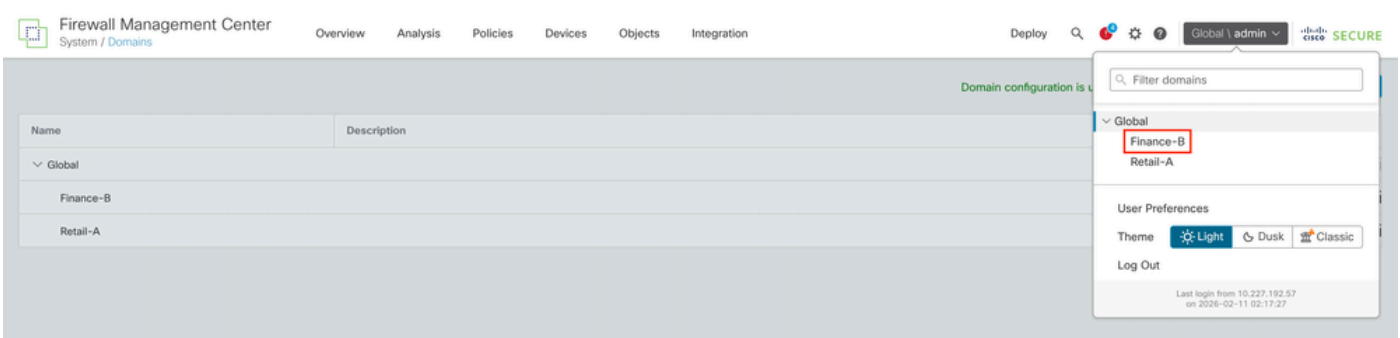
提示：对class使用与ISE的授权配置文件下配置的相同值。

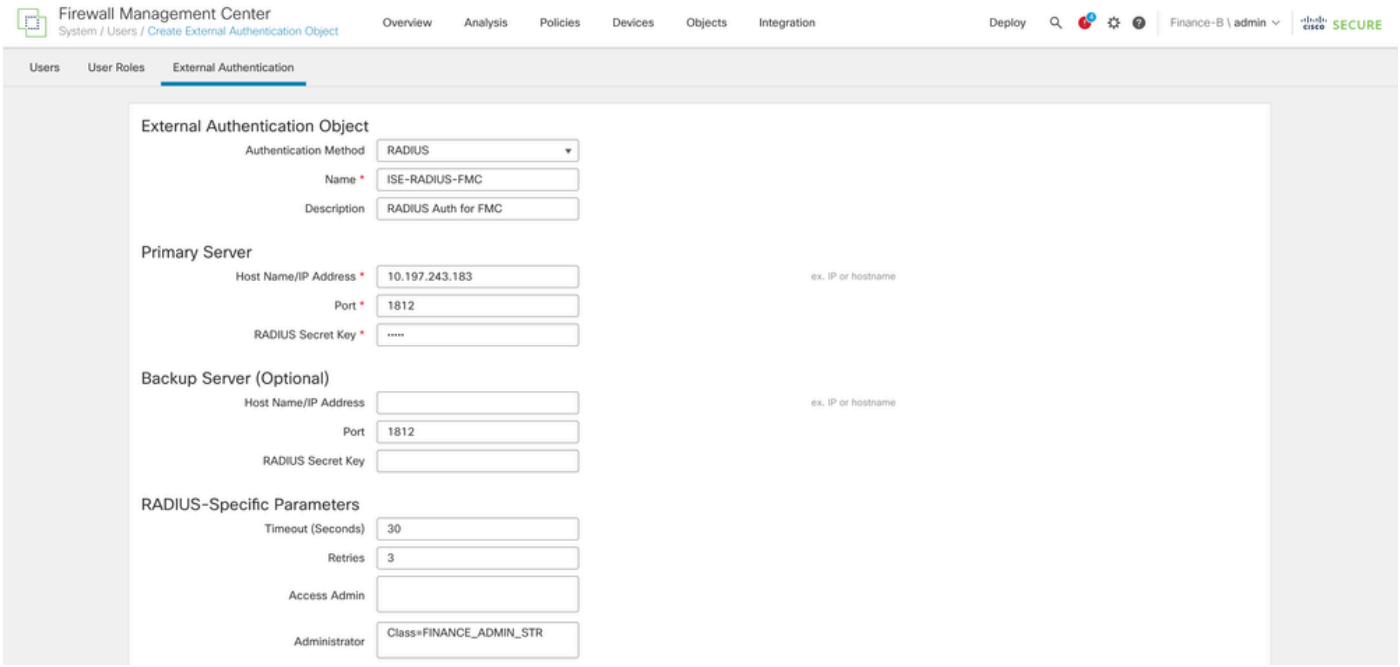


第 2.2 步： 将域下的外部身份验证对象配置为Finance-B

- 将域切换到Finance-B。
- 导航到System > Users > External Authentication。
- 选择Add External Authentication Object，然后选择RADIUS。
- 输入先前配置的ISE IP地址和共享密码。
- 输入RADIUS-Specific Parameters > Administrator > class=FINANCE_ADMIN_STR

提示：对class使用与ISE的授权配置文件下配置的相同值。





第 3 步： 激活身份验证：启用该对象，并将其设置为Shell Authentication方法。单击Save和Apply。

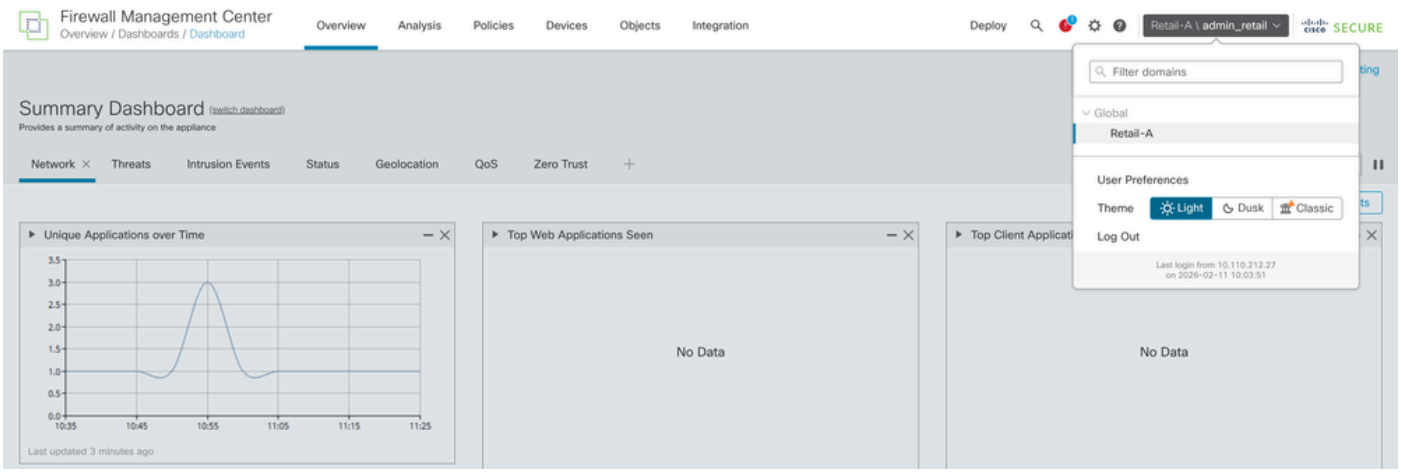
确认

跨域登录测试

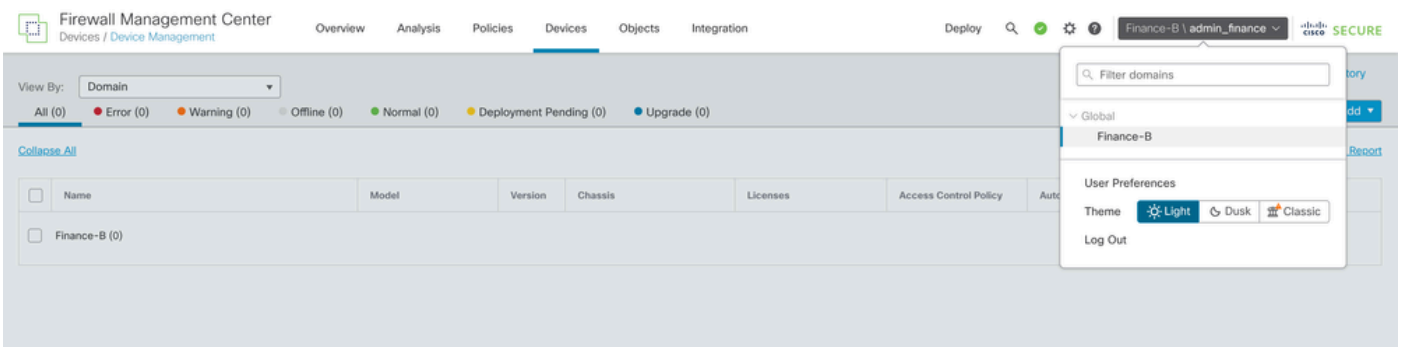
- 尝试使用admin_retail登录到FMC Web界面。验证UI右上角显示的当前域是Retail-A。

提示：登录到特定域时，请使用用户名格式domain_name\radius_user_mapped_with_that_domain。

例如，如果Retail admin用户需要登录，则用户名必须为Retail-A\admin_retail和相应的密码。



- 注销并以admin_finance身份登录。验证用户是否被限制到Finance-B域且无法看到Retail-A设备。

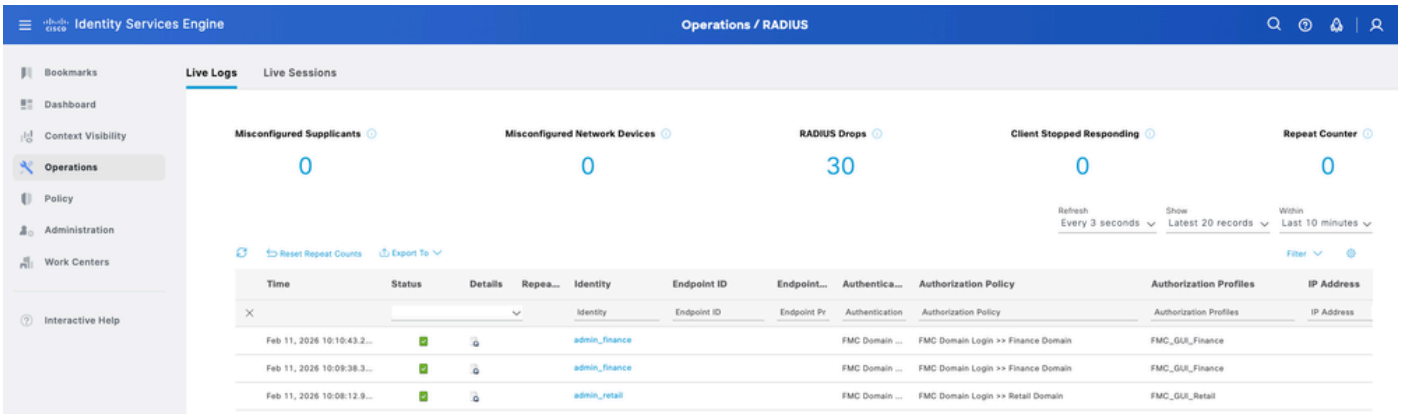


FMC内部测试

导航到FMC中的RADIUS服务器设置。使用其他测试参数部分输入测试用户名和密码。成功的测试必须显示绿色的“成功”消息。

ISE 实时日志

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



- 确认身份验证请求显示Pass状态，并且在RADIUS Access-Accept数据包中发送了正确的授权配置文件（和关联的类字符串）。

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

相关信息

配置 FMC 和 FTD 使用 ISE 作为 RADIUS 服务器进行外部身份验证

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。