マルチドメイン環境でのFMC外部認証の設定

内容

はじめに

このドキュメントでは、中央集中型RADIUS認証にCisco ISEを活用しながら、Cisco FMC内でマルチテナント（マルチドメイン）を実装する方法について説明します。

前提条件

要 件

次の項目に関する知識があることが推奨されます。

- GUIまたはシェルを使用したCisco Secure Firewall Management Centerの初期設定
- サブドメインと外部認証オブジェクトを作成するための、FMCのグローバルドメインでの完全な管理者権限。
- ISE 上での認証ポリシーおよび認可ポリシーの設定.
- RADIUS の基礎知識

使用するコンポーネント

- Cisco Secure FMC:vFMC 7.4.2（マルチドメインの安定性を確保するために以降で推奨）
- ドメイン構造： 3レベルの階層（「グローバル」 > 「第2レベルのサブドメイン」）。

- Cisco Identity Services Engine:ISE 3.3

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

バックグラウンド情報

大規模なエンタープライズ環境やマネージドセキュリティサービスプロバイダー(MSSP)のシナリオでは、ネットワーク管理を個別の管理境界にセグメント化する必要があることがよくあります。このドキュメントでは、複数のドメインをサポートするようにFMCを設定する方法について説明します。特に、MSSPがRetail-AとFinance-Bの2つのクライアントを管理する実際の例を対象とします。Cisco ISEを介した外部RADIUS認証を使用することにより、管理者は、ユーザに対して、各自のユーザドメインへのアクセス権のみを、各自の一元化されたクレデンシャルに基づいて自動的に付与することができます。

Cisco Secure Firewallシステムは、ドメインを使用してマルチテナントを実装します。

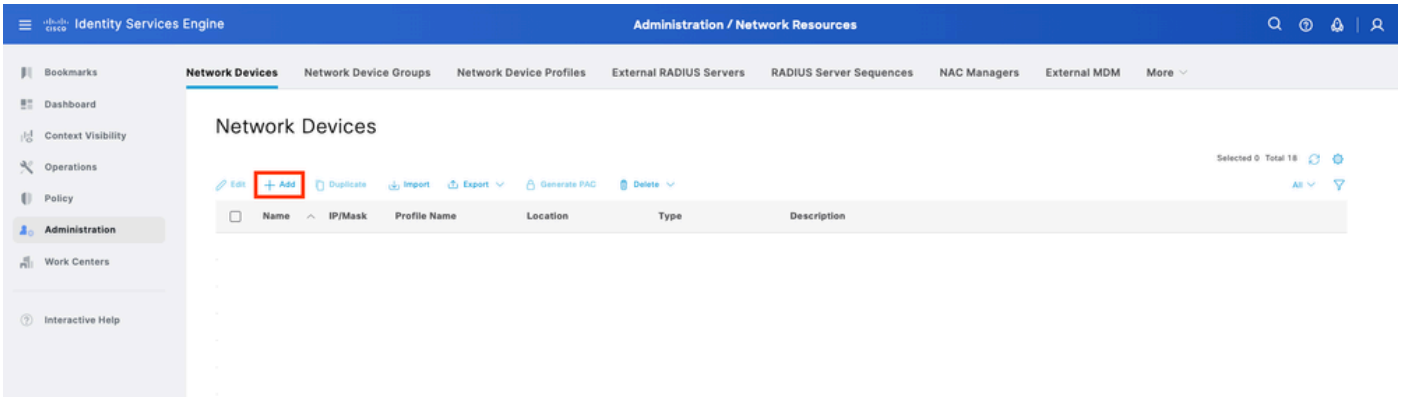
- ドメイン階層：階層はグローバルドメインから始まります。2レベルまたは3レベルの構造に最大100のサブドメインを作成できます。
- リーフドメイン：階層の一番下にあり、サブドメインを持たないドメインです。重要な点は、各管理対象FTDデバイスは、1つのリーフドメインに関連付けられている必要があるということです。
- RADIUSクラス属性（属性25）：マルチドメイン設定では、FMCはISEから返されたRADIUSクラス属性を使用して、認証されたユーザを特定のドメインおよびユーザロールにマッピングします。これにより、単一のRADIUSサーバがログイン時に異なるユーザセグメント（Retail-AとFinance-Bなど）にユーザを動的に割り当てることができます。

コンフィギュレーション

ISE 設定

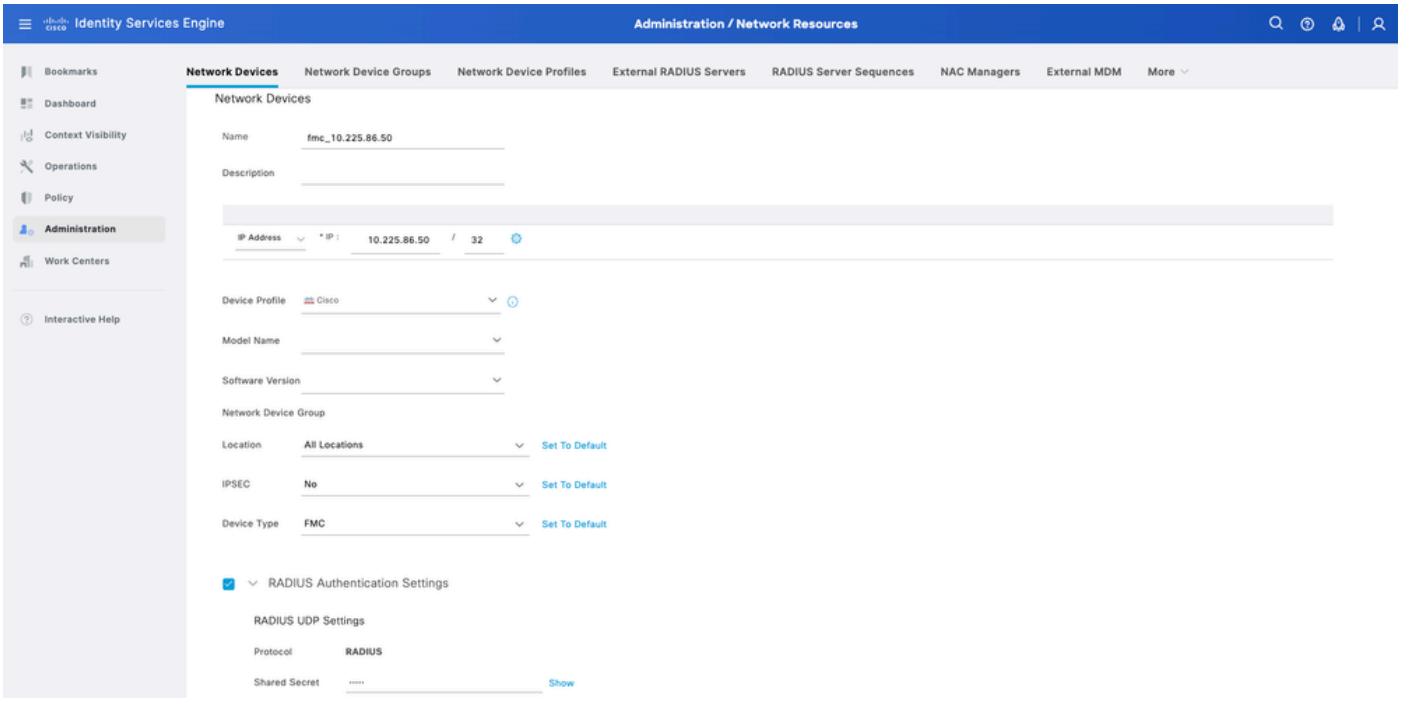
ネットワークデバイスの追加

ステップ 1：Administration > Network Resources > Network Devices > Addの順に移動します。



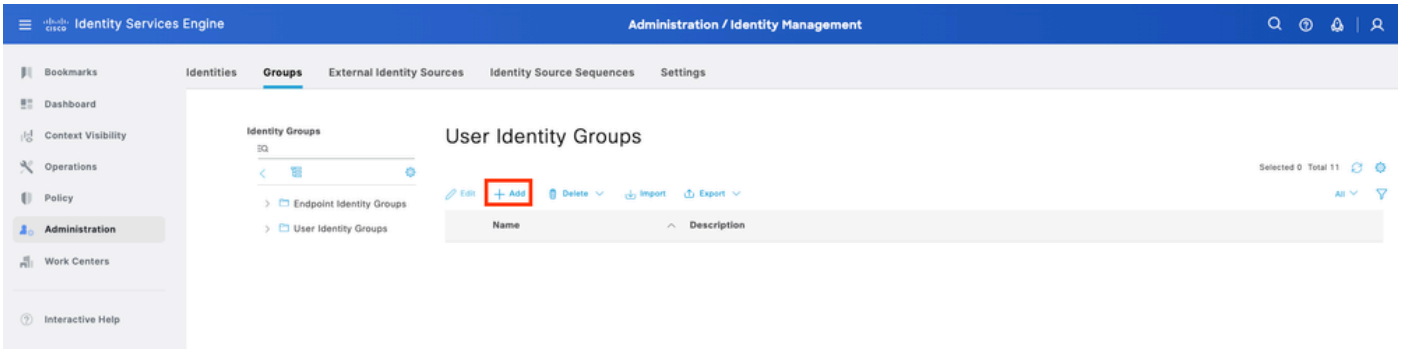
ステップ 2ネットワークデバイスオブジェクトに名前を割り当て、FMC IPアドレスを挿入します。

RADIUSチェックボックスをオンにして、共有秘密を定義します。後で同じキーを使用してFMCを設定する必要があります。完了したら、Saveをクリックします。

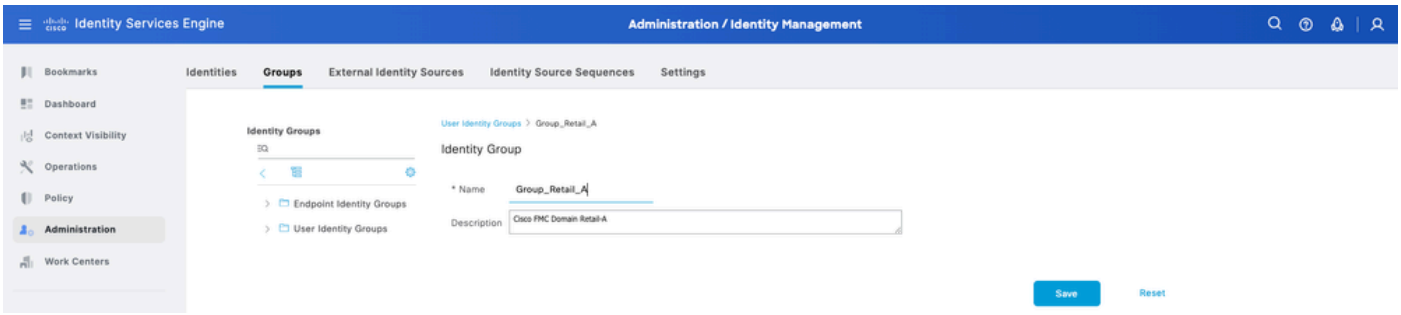


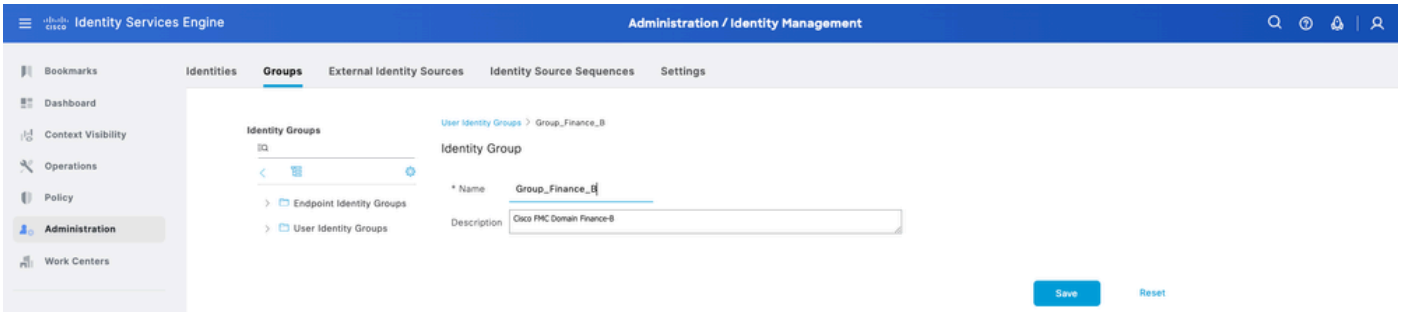
ローカルユーザIDグループとユーザの作成

ステップ 3必要なユーザIDグループを作成します。Administration > Identity Management > Groups > User Identity Groups > Addの順に移動します。

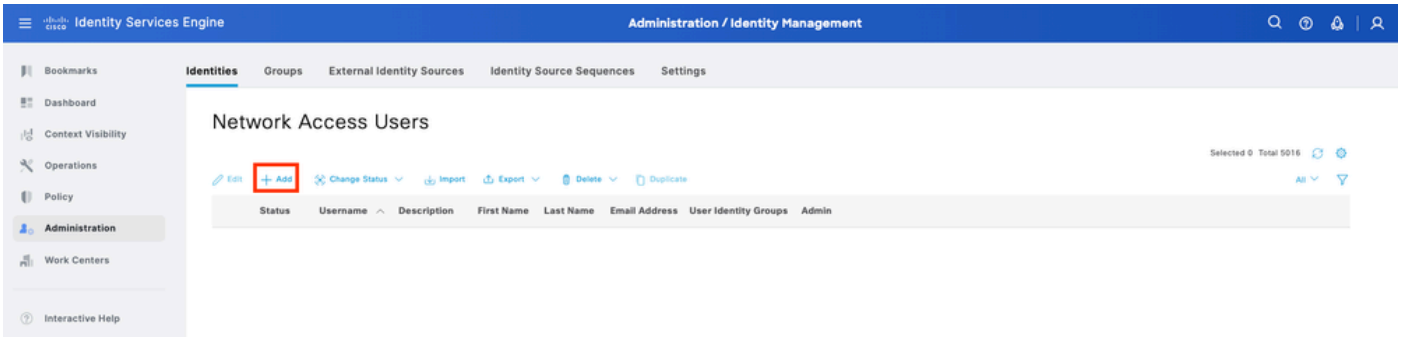


ステップ 4各グループに名前を付け、保存を個別に行います。この例では、管理者ユーザのグループを作成します。Group_Retail_AとGroup_Finance_Bの2つのグループを作成します。

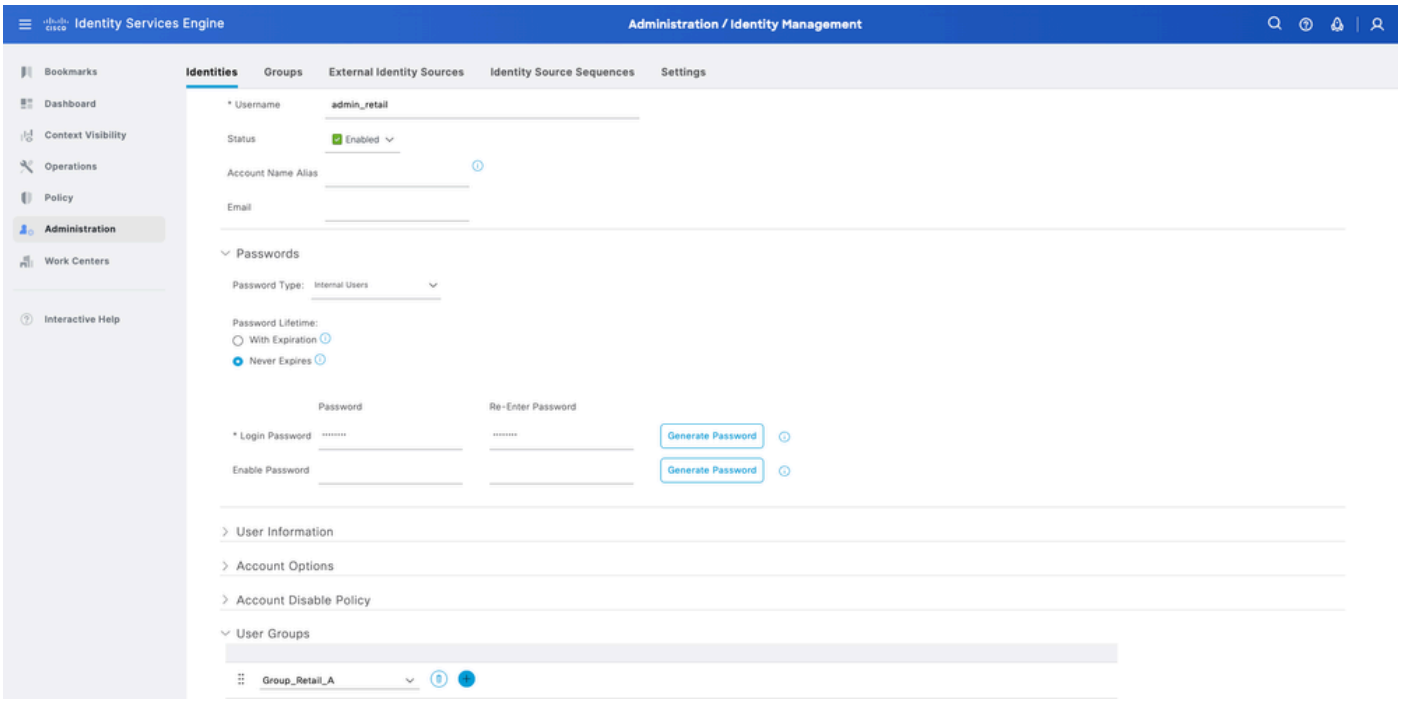




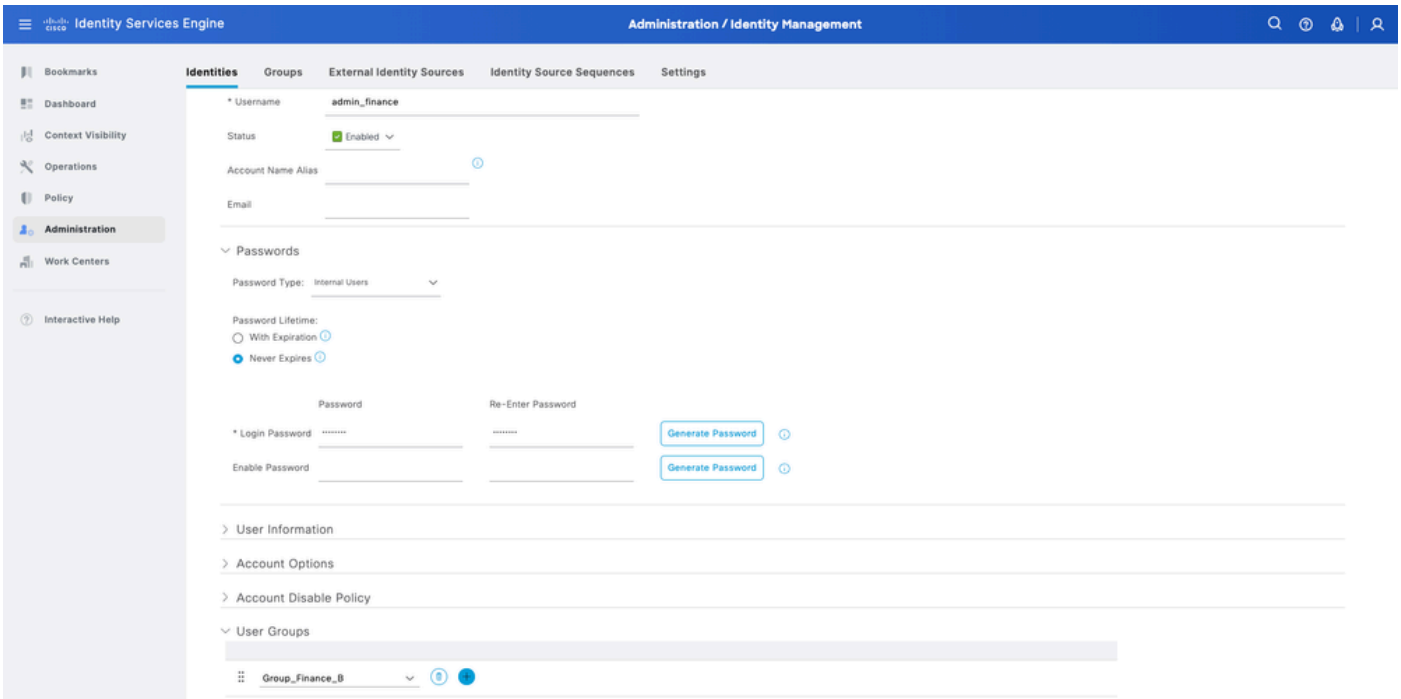
ステップ 5ローカルユーザを作成し、対応するグループに追加します。Administration > Identity Management > Identities > Addの順に移動します。



ステップ 5.1：まず、管理者権限を持つユーザを作成します。それには、admin_retail、password、およびグループGroup_Retail_Aという名前を割り当てます。

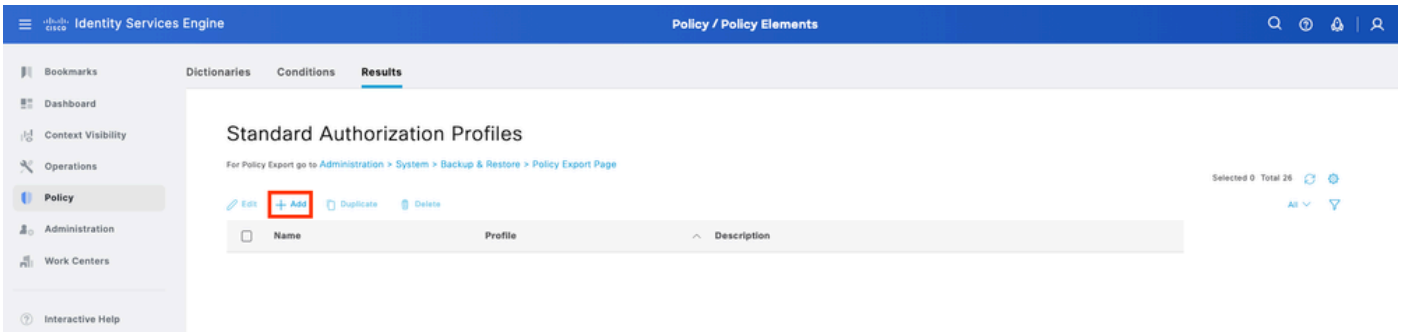


ステップ 5.2：まず、管理者権限を持つユーザを作成します。これに、admin_finance、password、およびグループGroup_Finance_Bという名前を割り当てます。



認可プロファイルの作成

ステップ 6FMC Web Interface Adminユーザの認可プロファイルを作成します。Policy > Policy Elements > Results > Authorization > Authorization Profiles > Addの順に移動します。

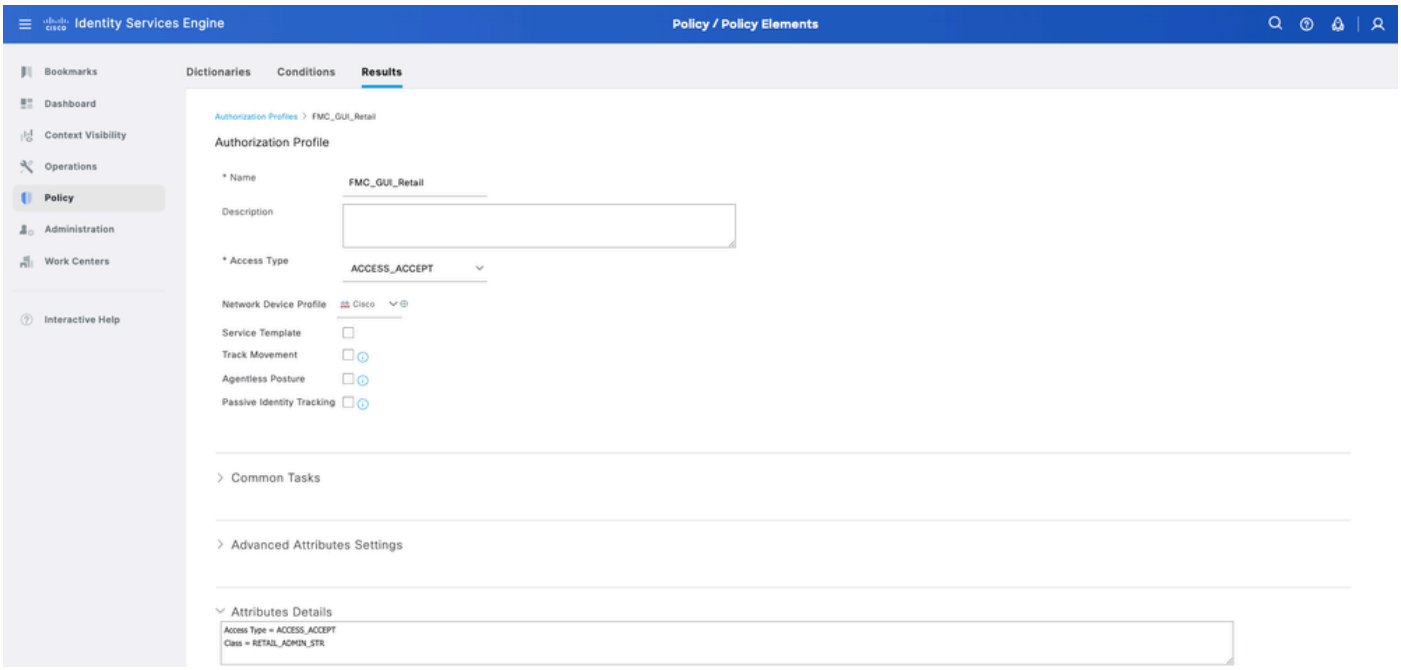


認可プロファイルの名前を定義し、アクセスタイプはACCESS_ACCEPTのままにします。

Advanced Attributes Settingsで、値を指定してRadius > Class—[25]を追加し、Submitをクリックします。

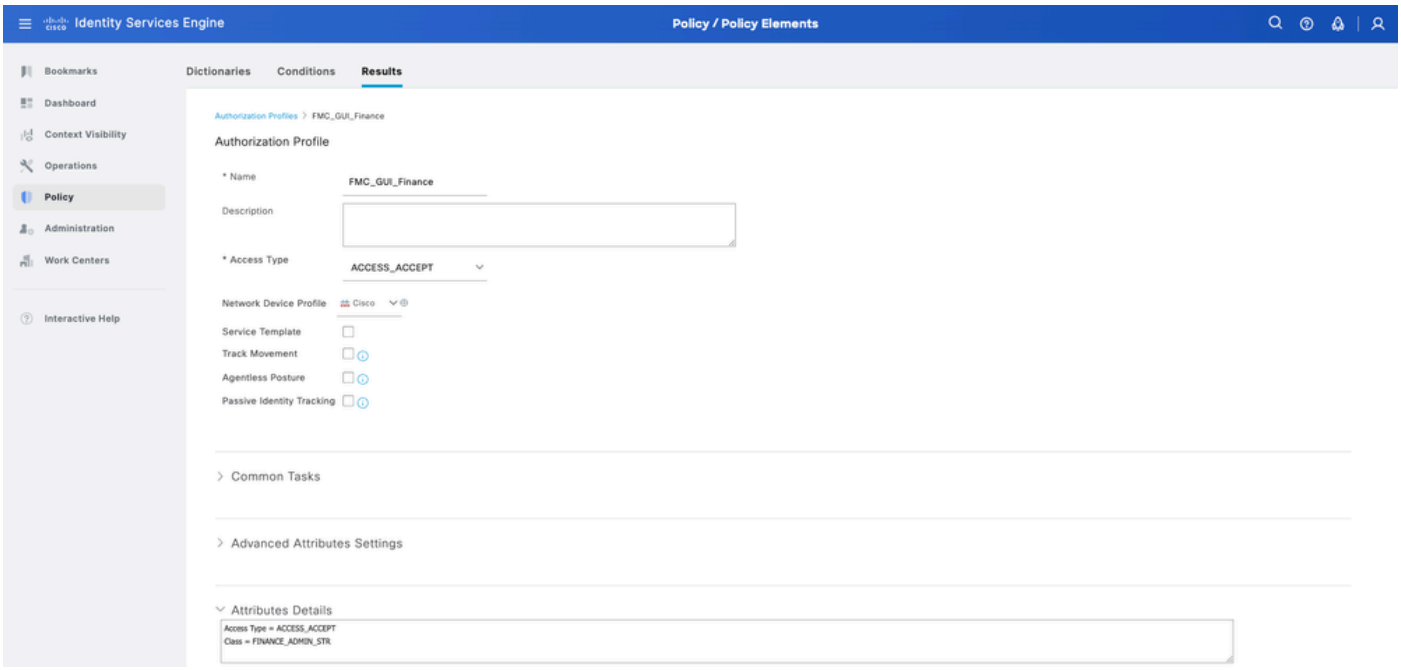
ステップ 6.1：Retailプロファイル： Advanced Attributes Settingsで、値RETAIL_ADMIN_STRのRadius:Classを追加します。

ヒント：ここでは、RETAIL_ADMIN_STRは任意にすることができます。同じ値のニーズがFMC側にも配置されていることを確認します。



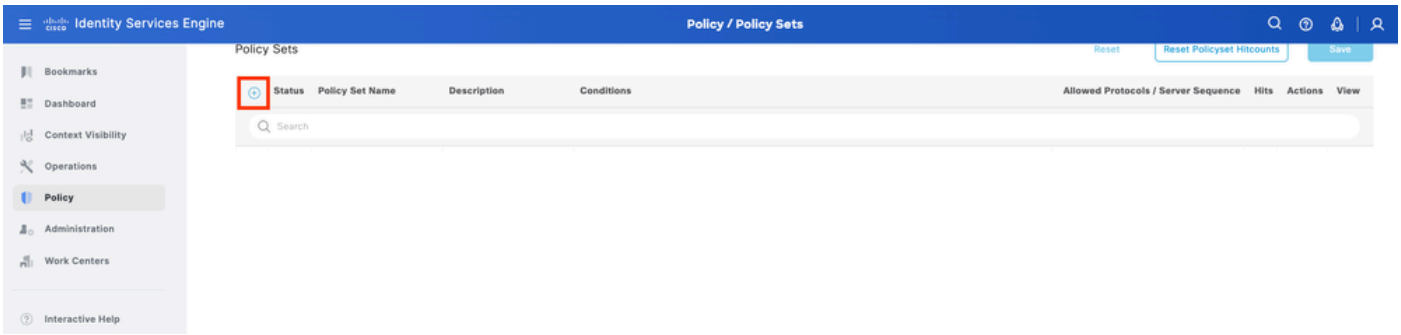
ステップ 6.2：プロファイルFinance:Advanced Attributes Settingsで、値がFINANCE_ADMIN_STRのRadius:Classを追加します。

ヒント：ここでは、FINANCE_ADMIN_STRは任意の値にすることができます。同じ値がFMC側にも配置されていることを確認してください。



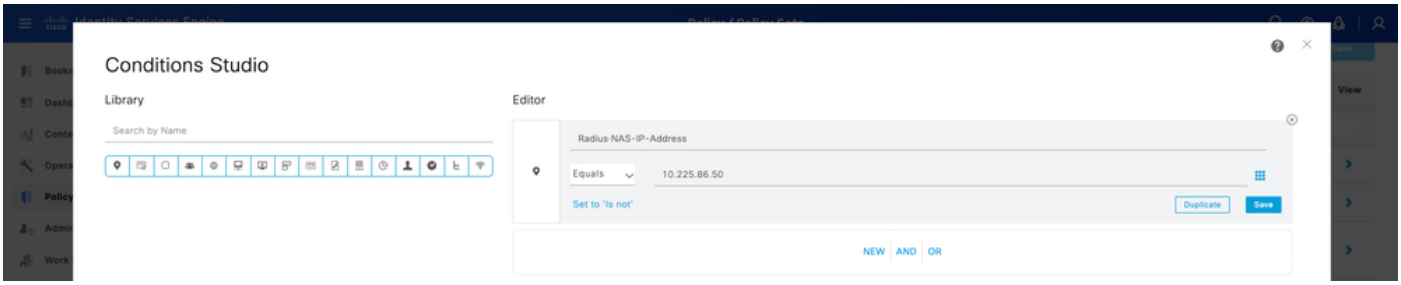
新しいポリシーセットの追加

ステップ 7FMCのIPアドレスに一致するポリシーセットを作成します。これは、他のデバイスがユーザにアクセス権を付与するのを防ぐためです。左上隅にあるPolicy > Policy Sets > Plus sign iconの順に移動します。



ステップ 8.1：新しい品目がポリシーセットの一番上に配置されます。

新しいポリシーに名前を付け、FMCのIPアドレスに一致するRADIUS NAS-IP-Address属性の上位条件を追加します。Useをクリックして変更を保存し、エディタを終了します。



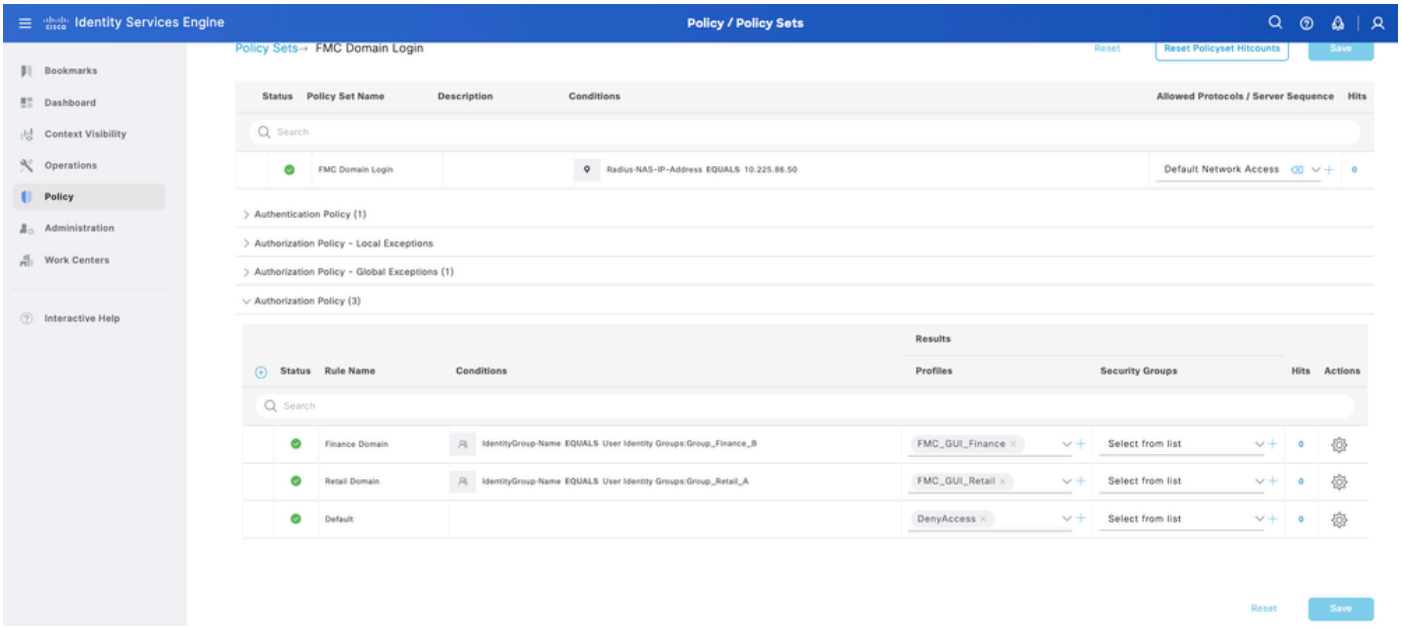
ステップ 8.2：完了したら、Saveを押します。

ステップ 9行の最後にあるsetアイコンをクリックして、新しいポリシーセットを表示します。

Authorization Policyメニューを展開し、プラス記号アイコンを押して新しいルールを追加し、管理者権限を持つユーザにアクセスできるようにします。名前を指定します。

条件を設定して、Dictionary Identity Group with Attribute Name Equalsに一致させ、User Identity Groupsを選択します。許可ポリシーで、ルールを作成します。

- ルール1：ユーザーIDグループがGroup_Retail_Aの場合、プロファイルRetailを割り当てます。
- ルール2：ユーザIDグループがGroup_Finance_Bの場合、プロファイルFinanceを割り当てます。



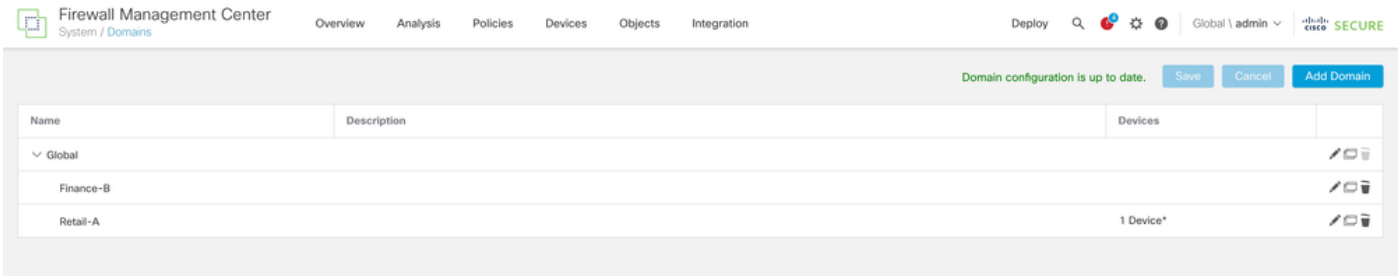
ステップ 10各ルールの認可プロファイルをそれぞれ設定し、Saveをクリックします。

FMCの設定

FMC認証用のISE RADIUSサーバの追加

ステップ1：ドメイン構造を確立します。

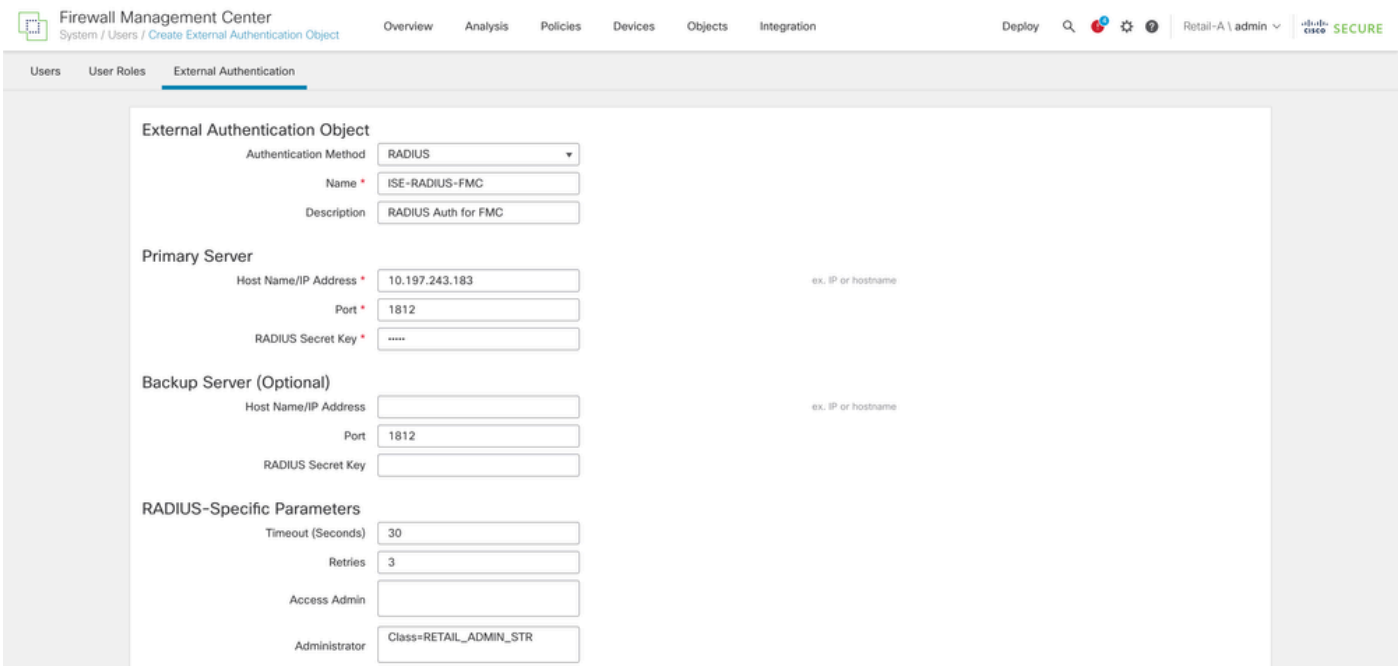
- FMCグローバルドメインにログインします。
- Administration > Domainsの順に移動します。
- Add Domainをクリックして、Retail-AとFinance-BをGlobalのサブドメインとして作成します。



手順2.1：ドメインの下の外部認証オブジェクトをRetail-Aに設定します

- ドメインをRetail-Aに切り替えます。
- System > Users > External Authenticationの順に移動します。
- Add External Authentication Objectを選択し、RADIUSを選択します。
- ISE IPアドレスと、先に設定した共有秘密を入力します。
- RADIUS-Specific Parameters > Administrator > class=RETAIL_ADMIN_STRを入力します。

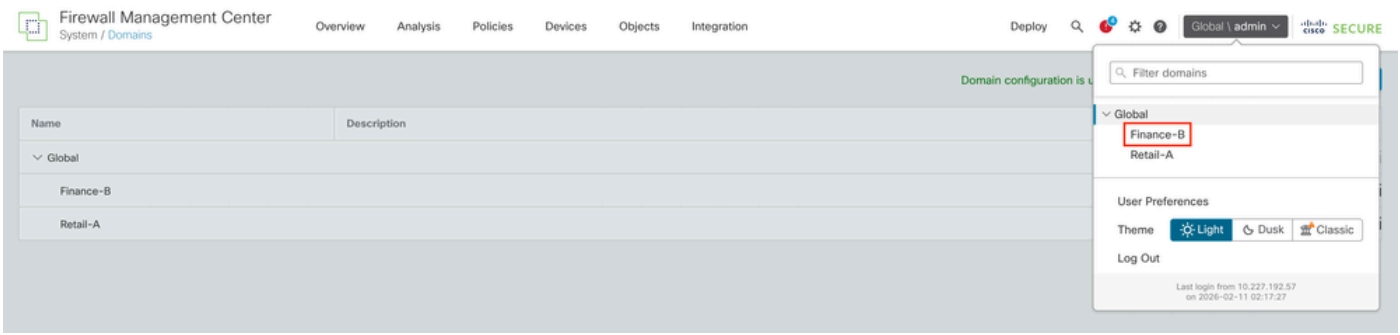
ヒント:ISEの認可プロファイルで設定したクラスと同じ値を使用してください。

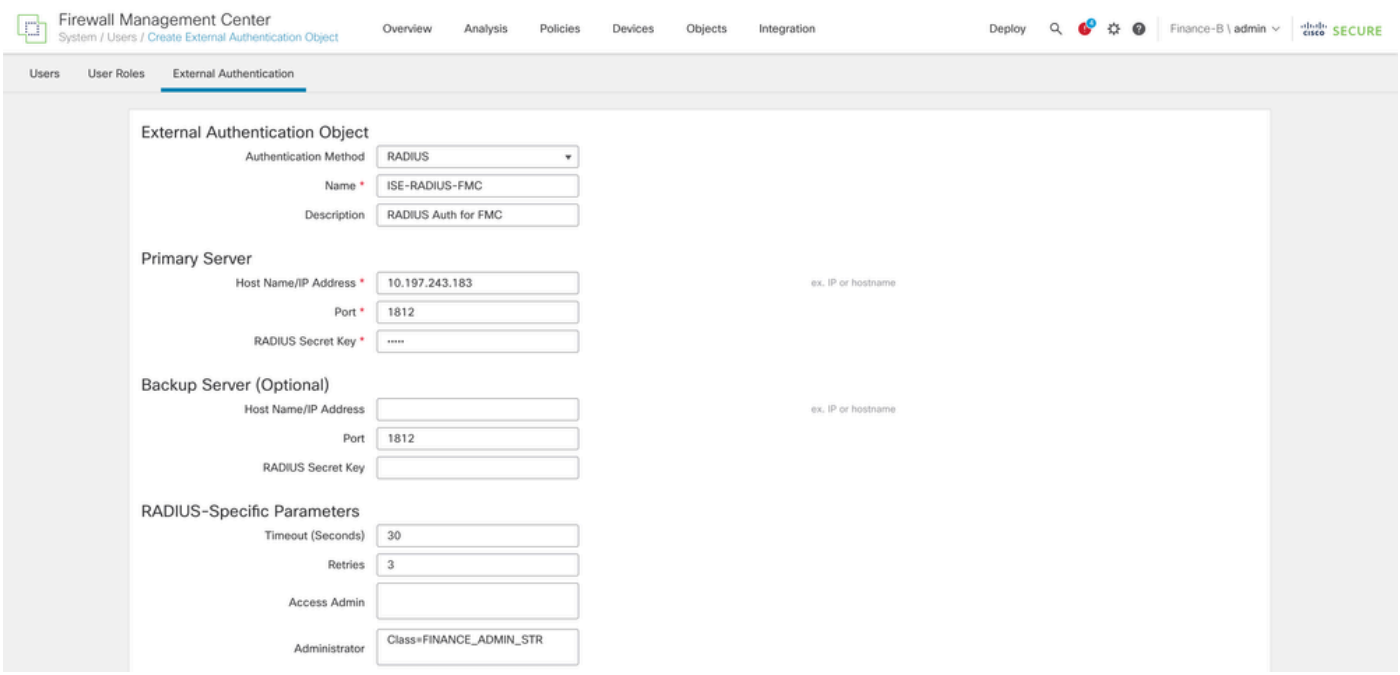


ステップ2.2:Finance-Bへのドメインで外部認証オブジェクトを設定する

- ドメインをFinance-Bに切り替えます。
- System > Users > External Authenticationの順に移動します。
- Add External Authentication Objectを選択し、RADIUSを選択します。
- ISE IPアドレスと、以前に設定した共有秘密を入力します。
- RADIUS-Specific Parameters > Administrator > class=FINANCE_ADMIN_STRを入力します。

ヒント:ISEの認可プロファイルで設定したクラスと同じ値を使用してください。





ステップ3：認証の有効化：オブジェクトを有効にし、シェル認証方式として設定します。SaveおよびApplyをクリックします。

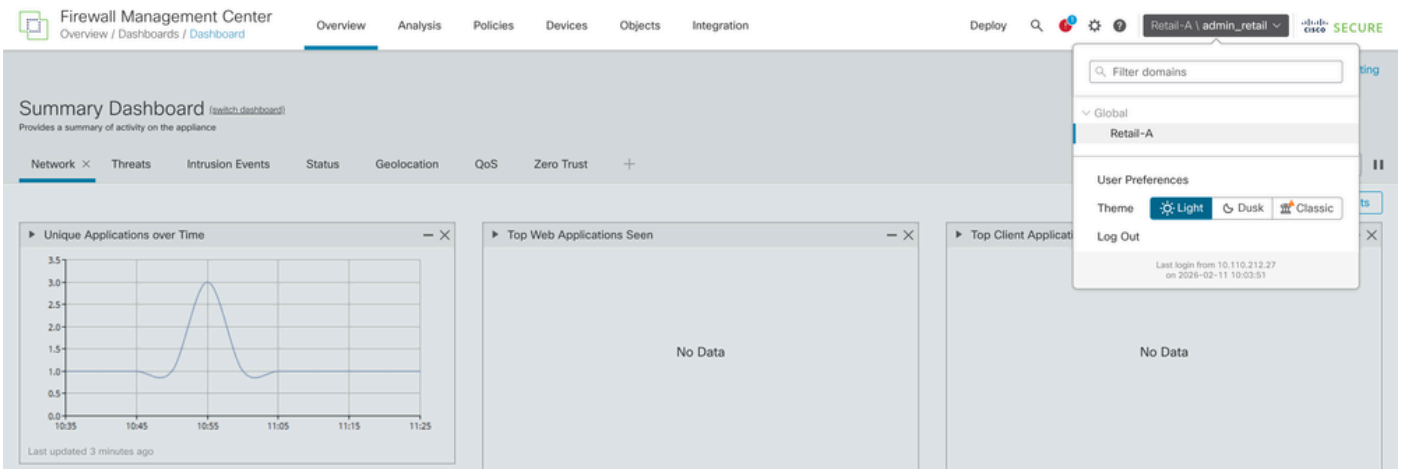
検証

クロスドメインログインテスト

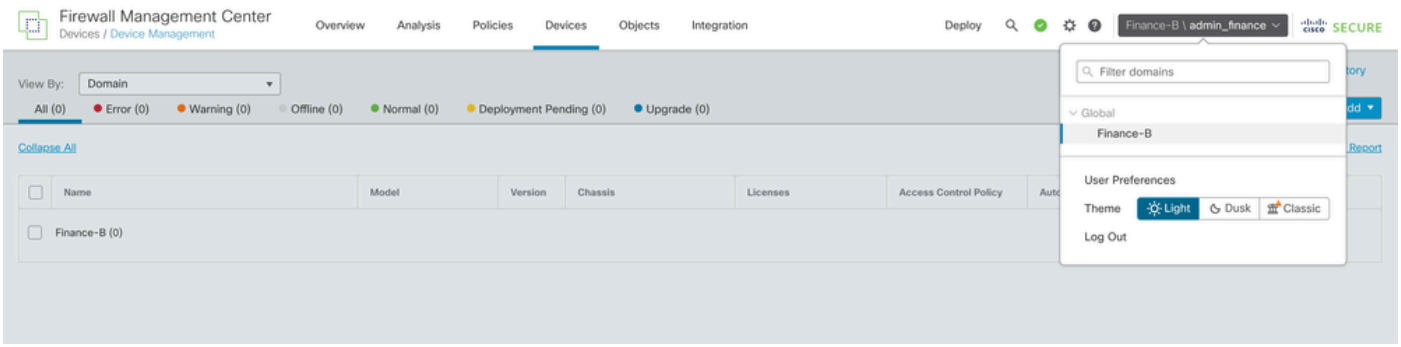
- admin_retailを使用して、FMC Webインターフェイスへのログインを試みます。UIの右上に表示されるCurrent DomainがRetail-Aであることを確認します。

ヒント：特定のドメインにログインするときは、ユーザ名の形式domain_name\radius_user_mapped_with_that_domainを使用します。

たとえば、小売管理者ユーザーがログインする必要がある場合、ユーザー名はRetail-A\admin_retailで、対応するパスワードを入力する必要があります。



- admin_financeとしてログアウトし、ログインします。ユーザがFinance-Bドメインに制限され、Retail-Aデバイスを表示できないことを確認します。

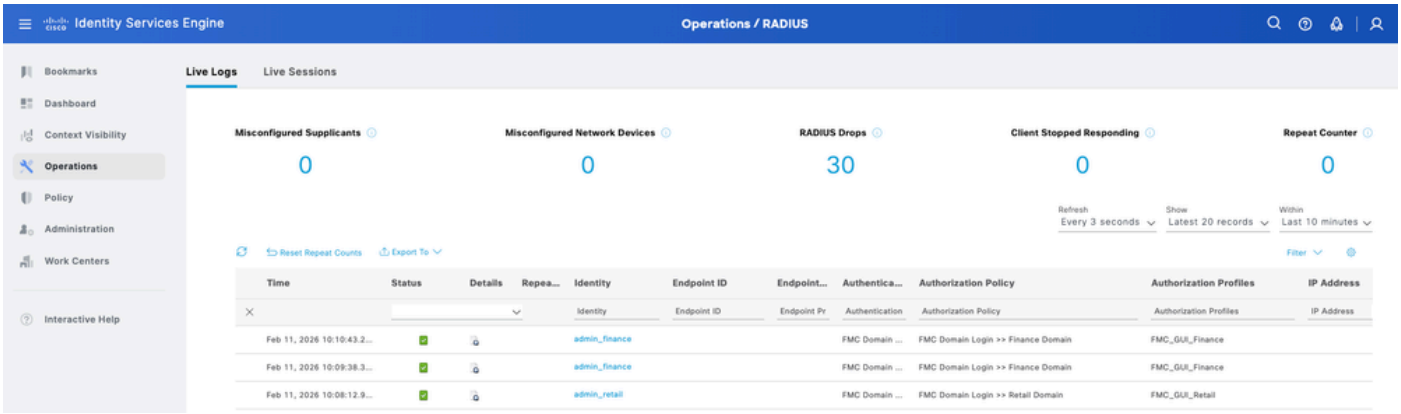


FMC内部テスト

FMCで、RADIUSサーバ設定に移動します。「その他のテストパラメータ」セクションを使用して、テスト用のユーザ名とパスワードを入力します。テストに成功すると、緑色の成功メッセージが表示されます。

ISE ライブログ

- Cisco ISEで、Operations > RADIUS > Live Logsの順に移動します。



- 認証要求がPassステータスを示していること、および正しい許可プロファイル（および関連付けられたクラス文字列）がRADIUS Access-Acceptパケットで送信されたことを確認します。

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

関連情報

RADIUSサーバとしてISEを使用したFMCおよびFTD外部認証の設定

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。