ISEをRADIUSサーバとして使用するFMCおよびFTD外部認証の設定

内容

はじめに

このドキュメントでは、Secure Firewall Management Center(FMC)とファイアウォール脅威対策の外部認証設定の例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。

- Cisco Secure Firewall Management Centerの初期設定（GUIまたはシェル経由）
- 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

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- vFMC 7.2.5
- vFTD 7.2.5
- ISE 3.2.

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ました。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。

背景説明

セキュアファイアウォールシステムの管理ユーザおよび管理ユーザに対して外部認証を有効にすると、デバイスは外部認証オブジェクトで指定されているLightweight Directory Access Protocol(LDAP)またはRADIUSサーバを使用してユーザクレデンシャルを確認します。

外部認証オブジェクトは、FMCおよびFTDデバイスで使用できます。異なるアプライアンス/デバイスタイプ間で同じオブジェクトを共有したり、別々のオブジェクトを作成したりできます。

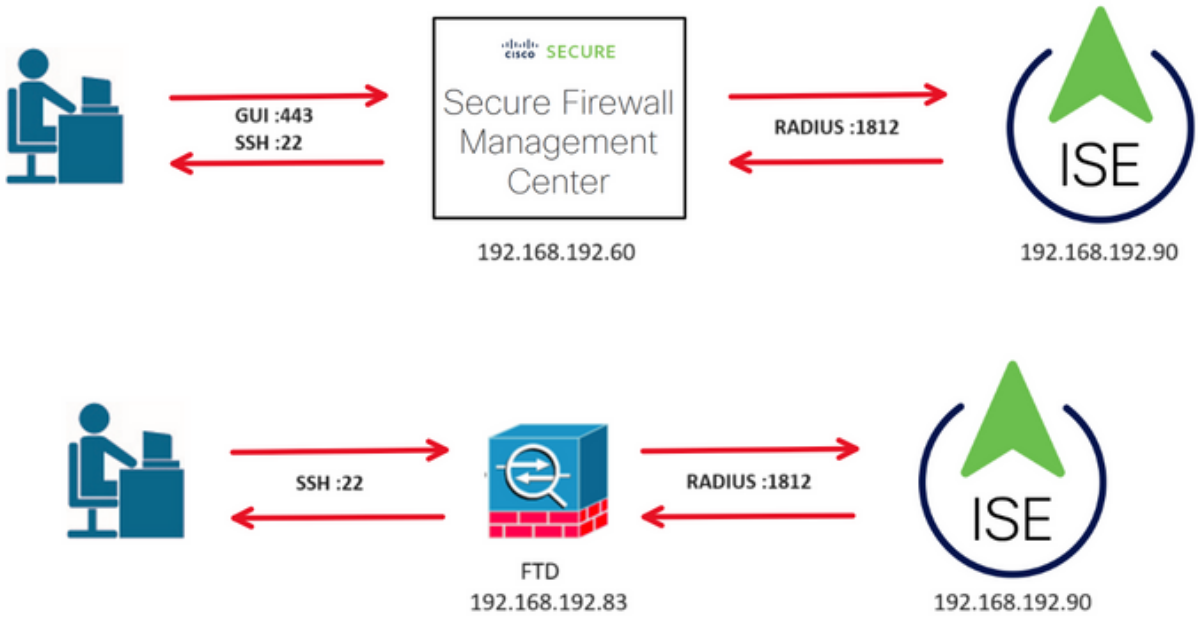
FMCの外部認証

Webインターフェイスアクセス用に複数の外部認証オブジェクトを設定できます。CLIまたはシェルアクセスに使用できる外部認証オブジェクトは1つだけです。

FTDの外部認証

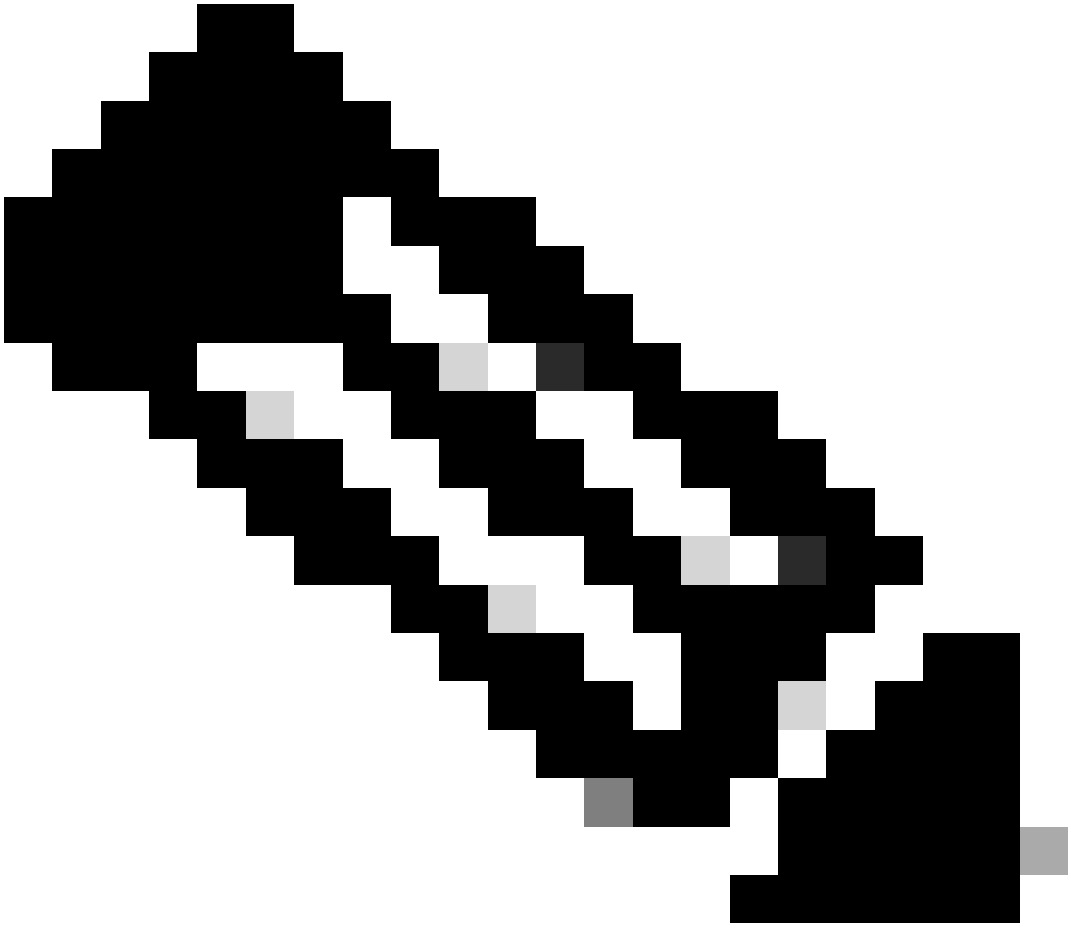
FTDでは、1つの外部認証オブジェクトしかアクティブにできません。

Network Topology



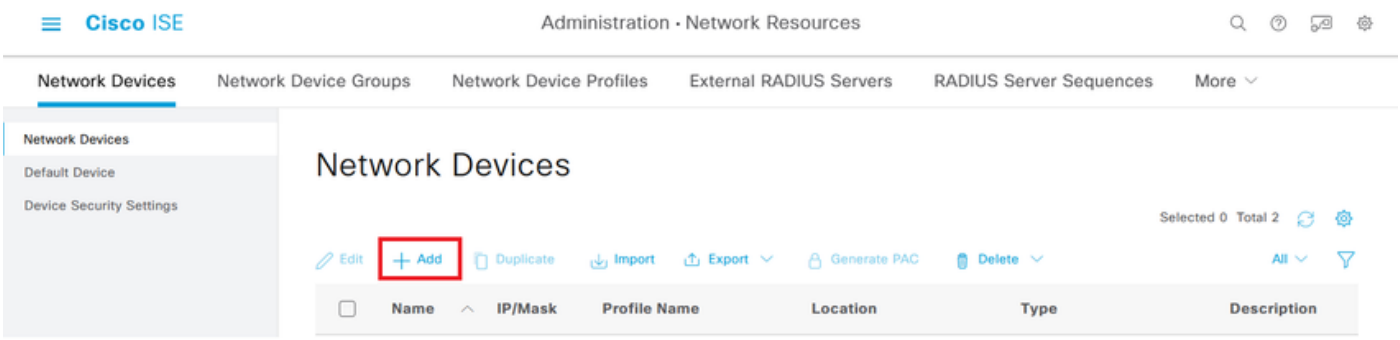
設定

ISE 設定



注:FMCなどのネットワークアクセスデバイス(NAD)用にISE認証および認可ポリシーを設定する方法は複数あります。このドキュメントで説明する例は、参照点として2つのプロファイル（1つは管理者権限を持ち、もう1つは読み取り専用）を作成し、ネットワークにアクセスするためのベースラインを満たすように調整できます。RADIUS属性値をFMCに返すISEで1つ以上の認可ポリシーを定義し、次にその属性値をFMCシステムポリシー設定で定義されたローカルユーザグループにマッピングできます。

ステップ 1：新しいネットワークデバイスを追加します。左上隅にあるバーガーアイコン >管理>ネットワークリソース>ネットワークデバイス> +追加に移動します。

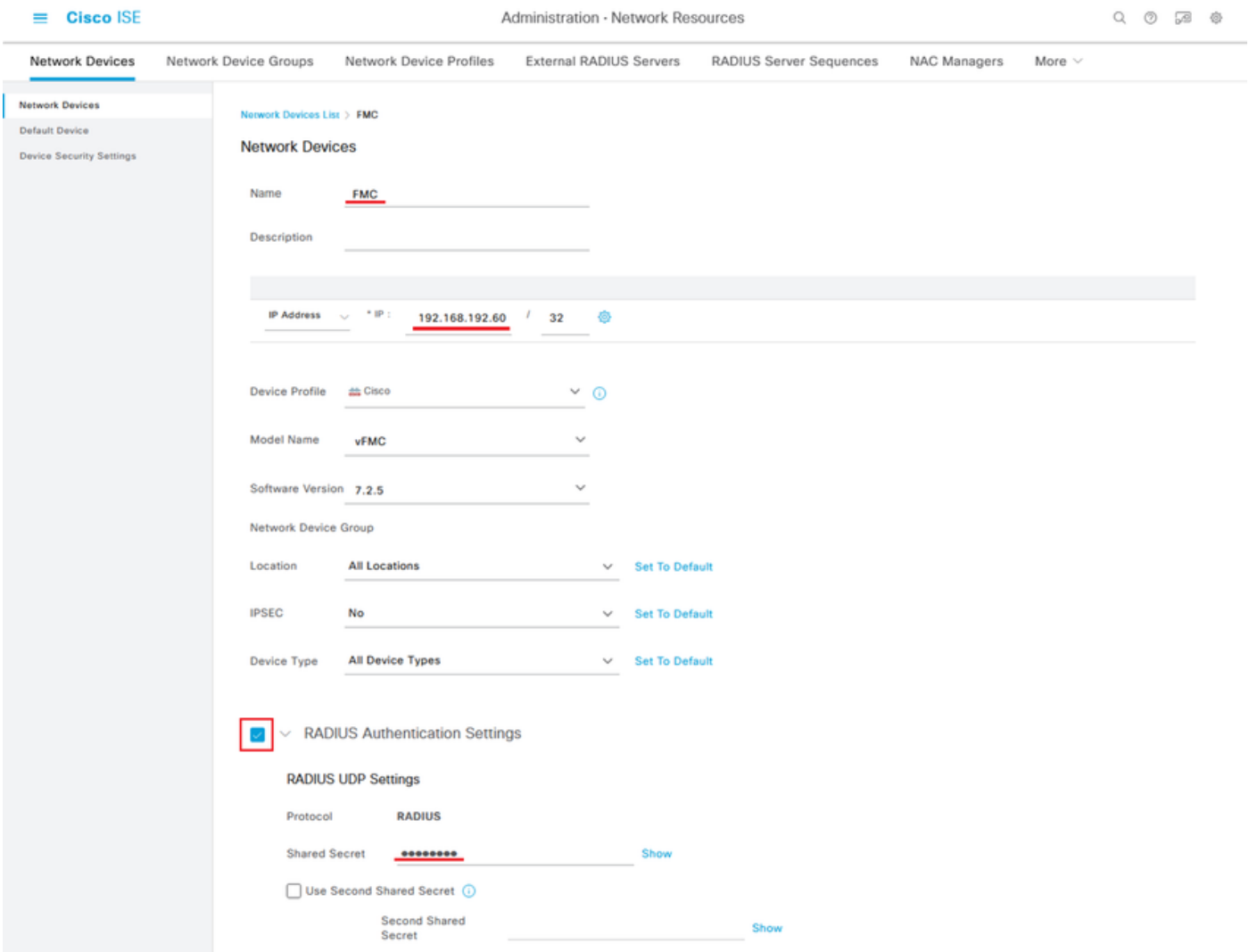


ステップ 2：ネットワークデバイスオブジェクトに名前を割り当て、FMCのIPアドレスを挿入します。

RADIUSの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。

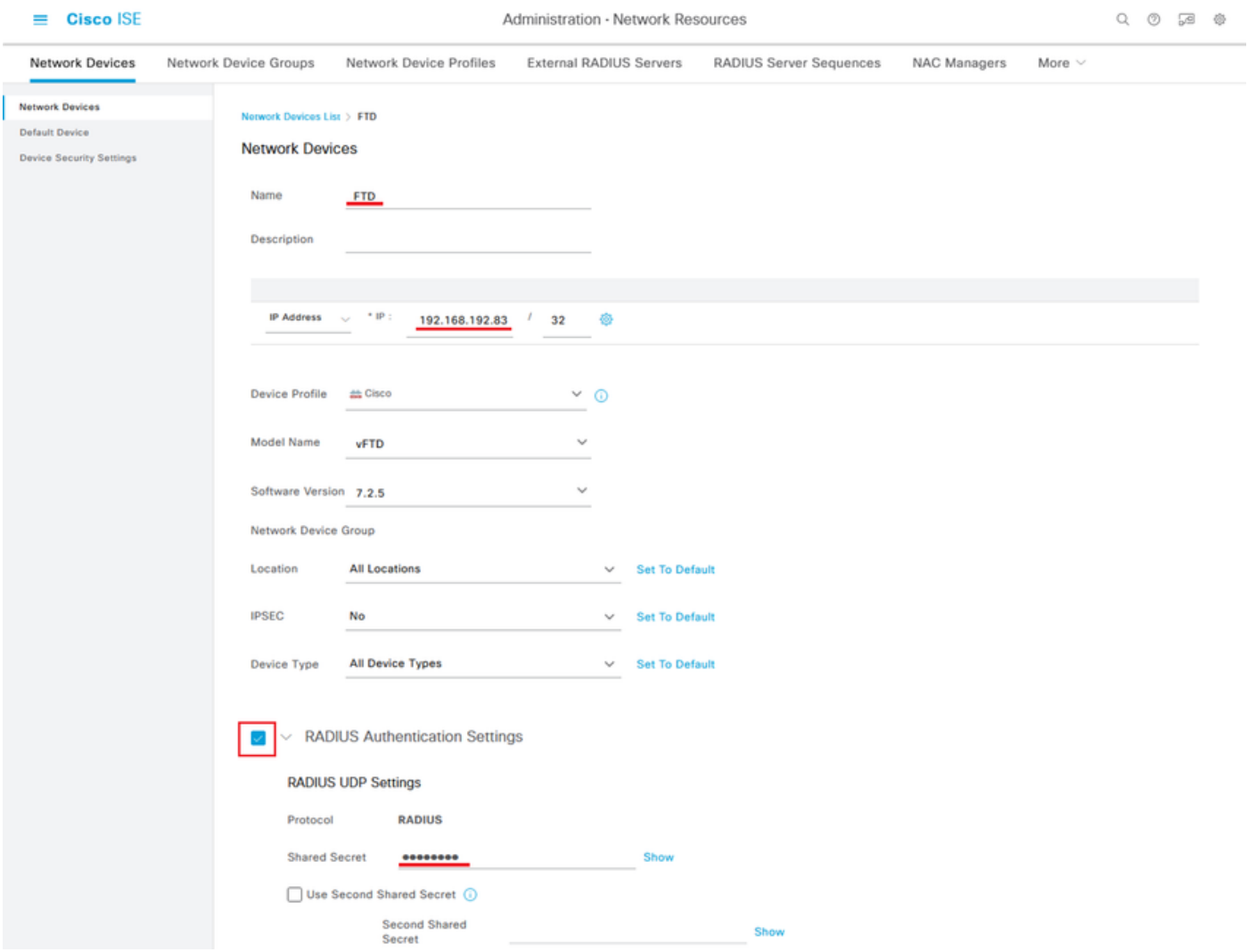


ステップ 2.1：同じ手順を繰り返してFTDを追加します。

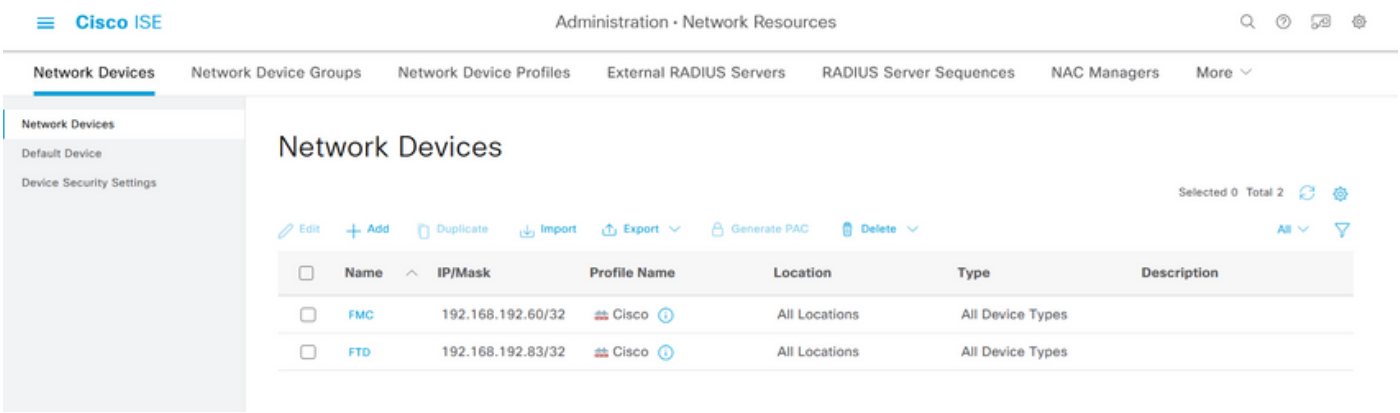
ネットワークデバイスオブジェクトに名前を割り当て、FTDのIPアドレスを挿入します。

RADIUSのチェックボックスをオンにして、共有秘密を定義します。

完了したら、Saveをクリックします。

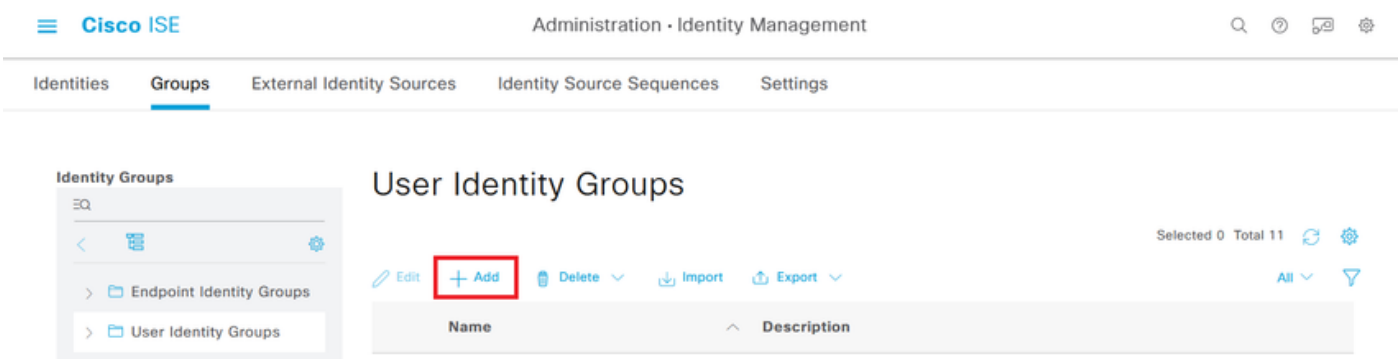


ステップ 2.3：両方のデバイスがネットワークデバイスの下に表示されていることを確認します。

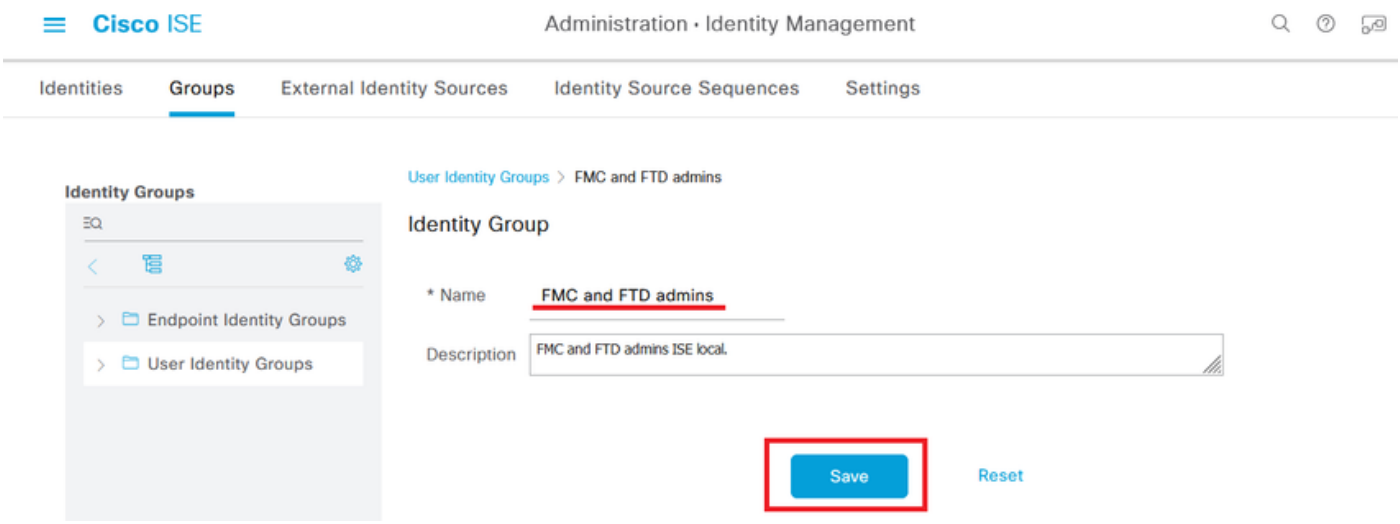


ステップ 3： 必要なユーザIDグループを作成します。左上隅にあるバーガーアイコン

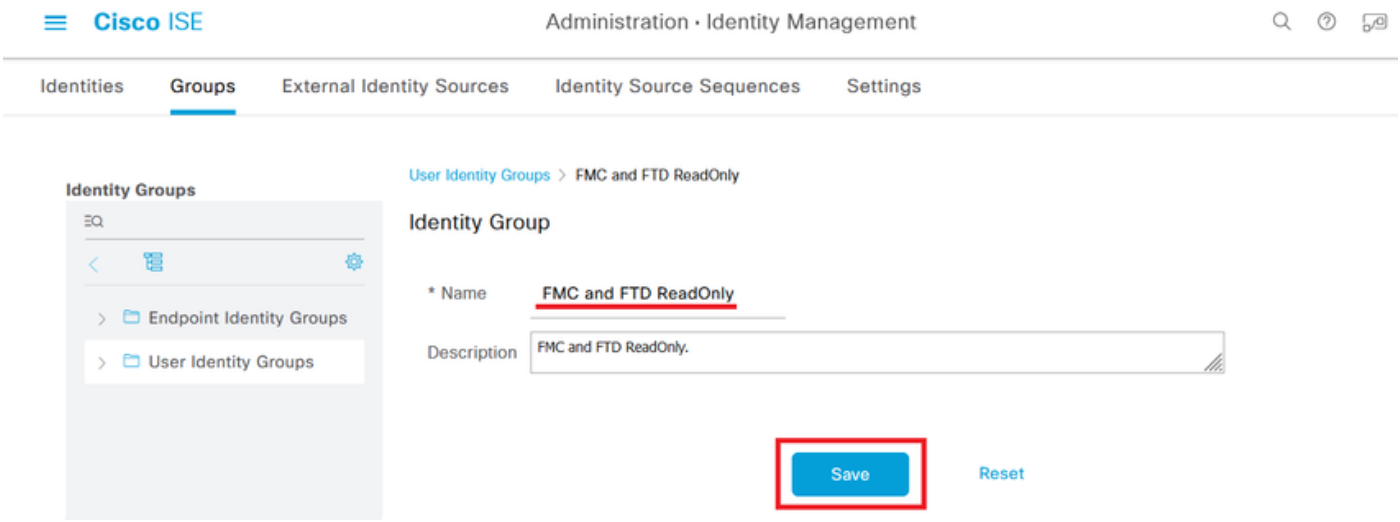
>管理>アイデンティティ管理>グループ>ユーザアイデンティティグループ> +追加に移動します



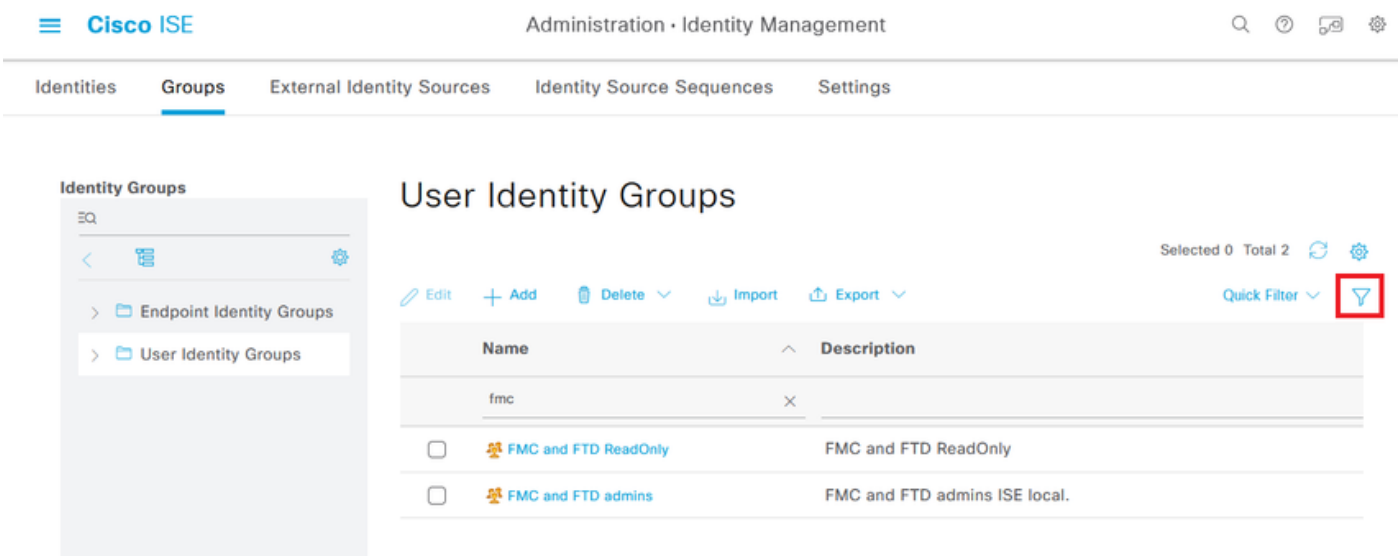
ステップ 4：各グループに名前を付けて、個別に保存します。この例では、管理者ユーザ用のグループと、読み取り専用ユーザ用のグループを作成します。まず、管理者権限を持つユーザのグループを作成します。



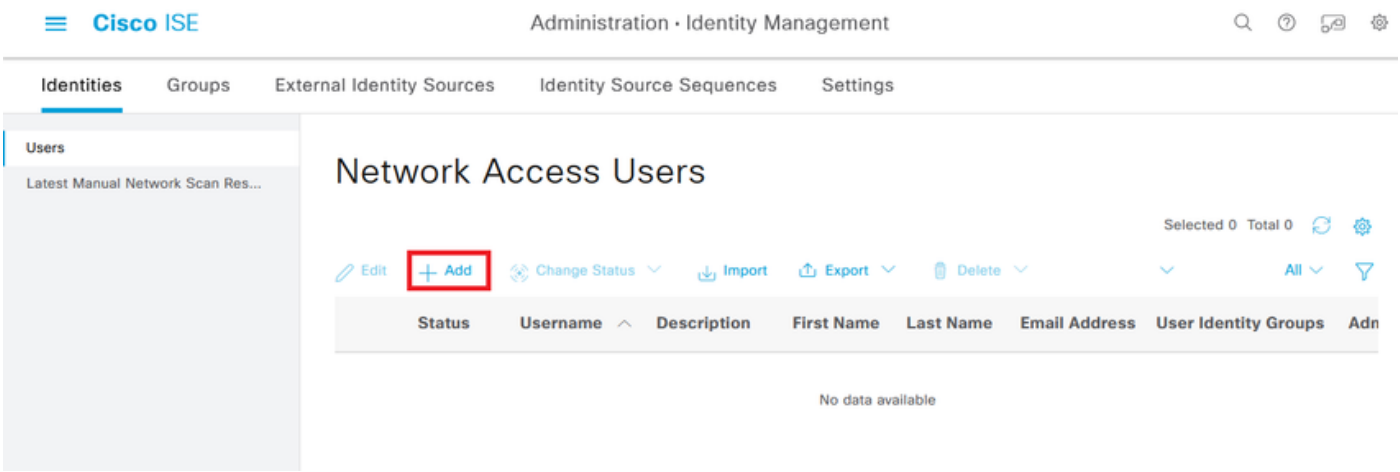
ステップ 4.1：ReadOnlyユーザの2番目のグループを作成します。



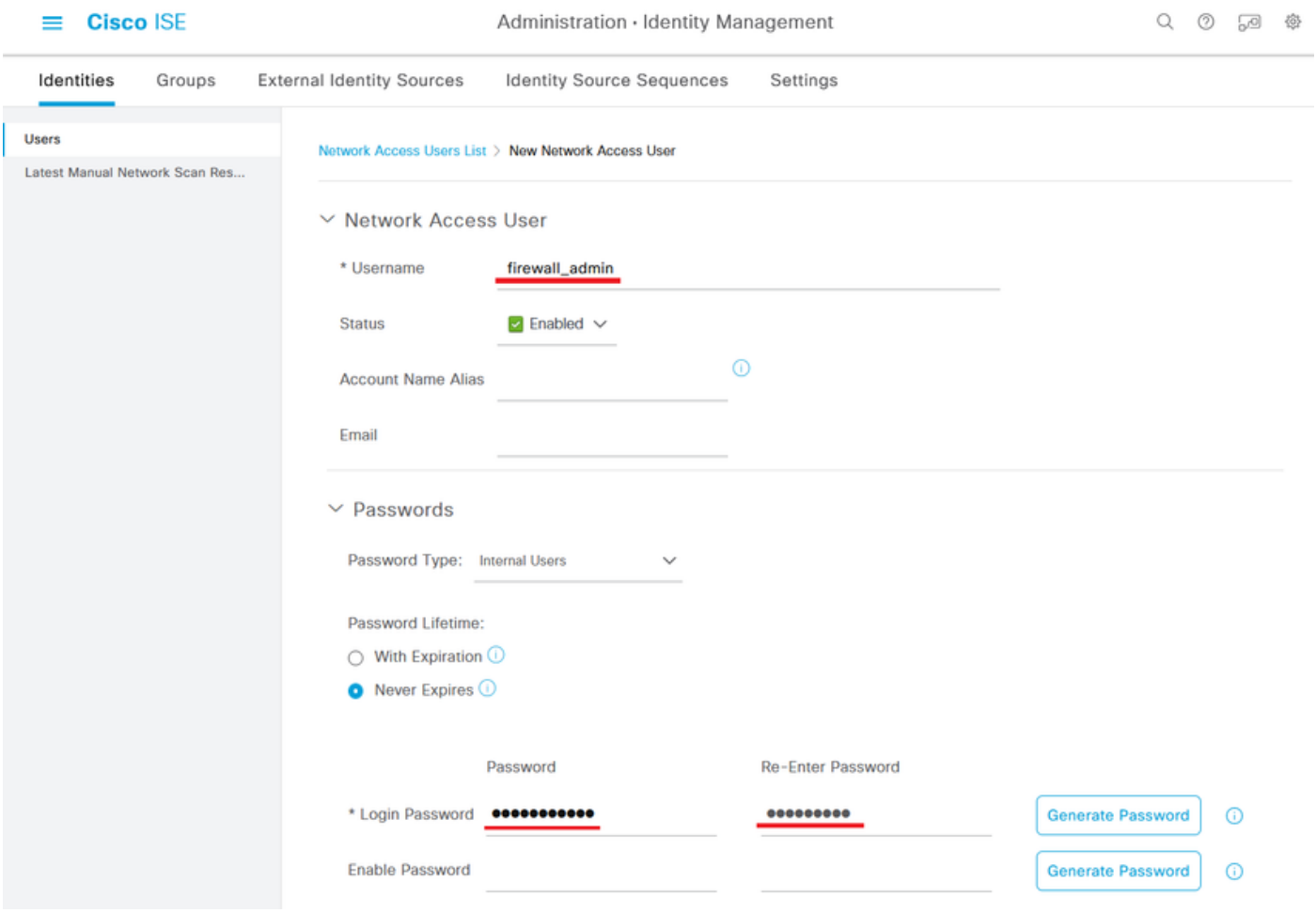
ステップ 4.2：両方のグループがUser Identity Groups Listの下に表示されていることを確認します。フィルタを使用すると、簡単に見つけることができます。

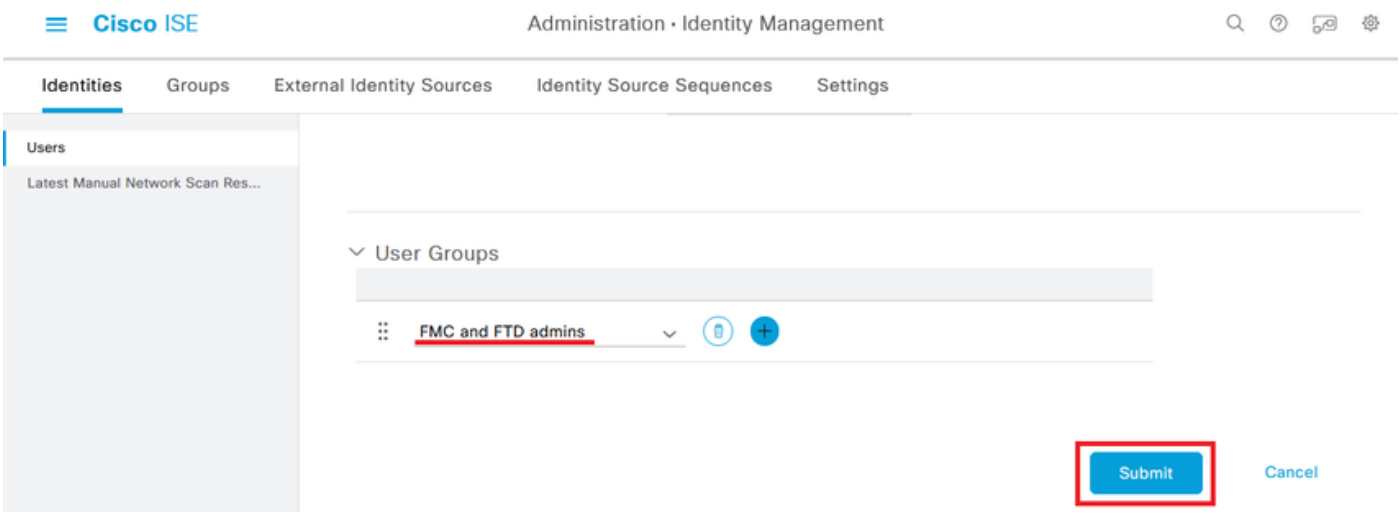


ステップ 5： ローカルユーザを作成し、対応するグループに追加します。
> Administration > Identity Management > Identities > + Addの順に移動します。

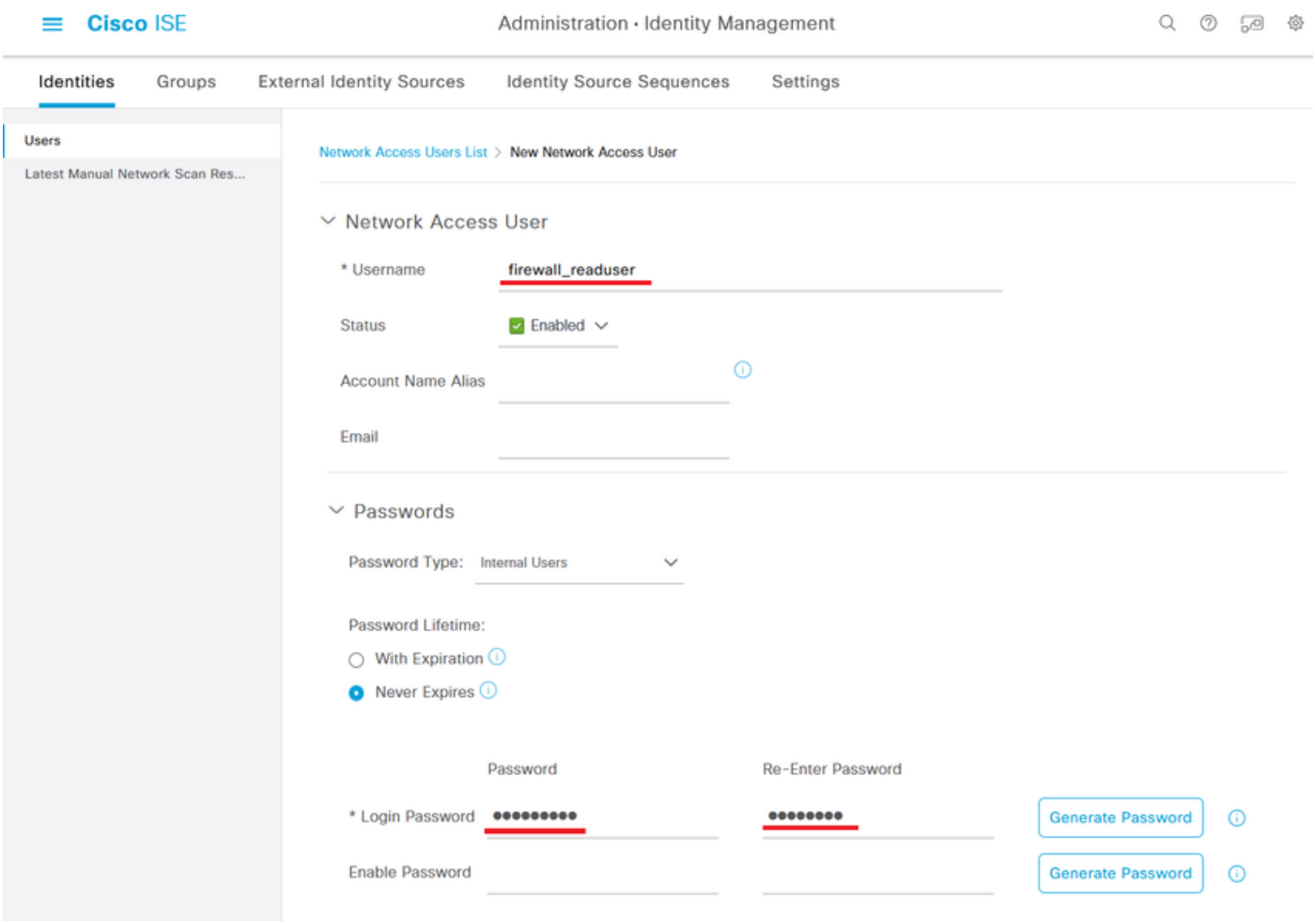


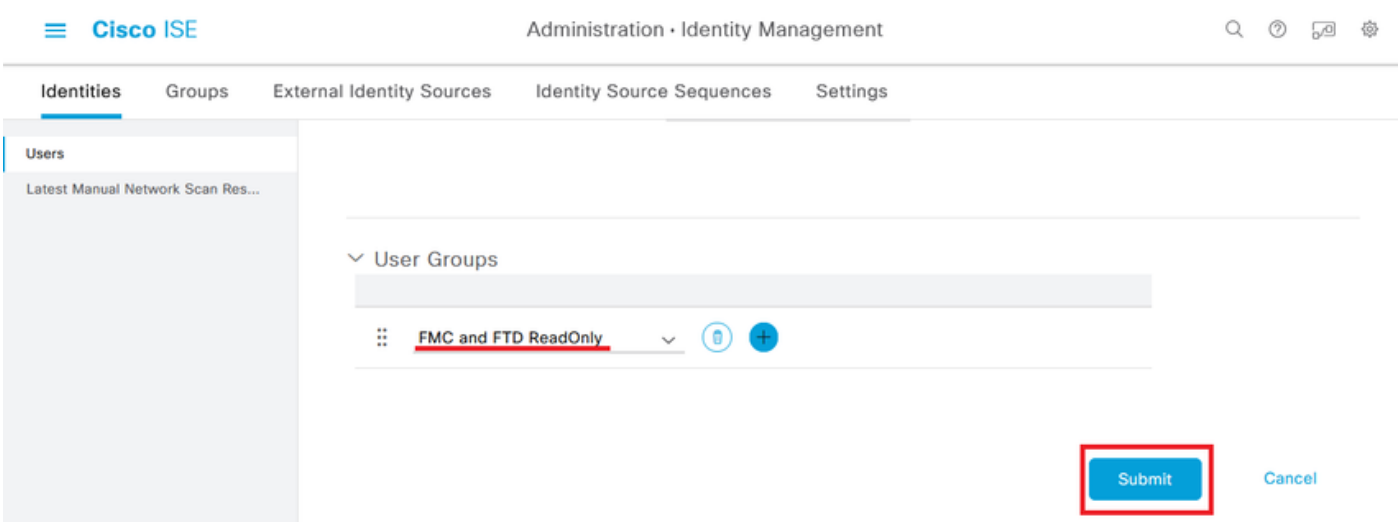
ステップ 5.1：まず、管理者権限を持つユーザを作成します。名前、パスワード、およびFMCとFTDの管理者グループを割り当てます。





ステップ 5.2：読み取り専用権限を持つユーザを追加します。名前、パスワード、およびFMCとFTDのReadOnlyグループを割り当てます。

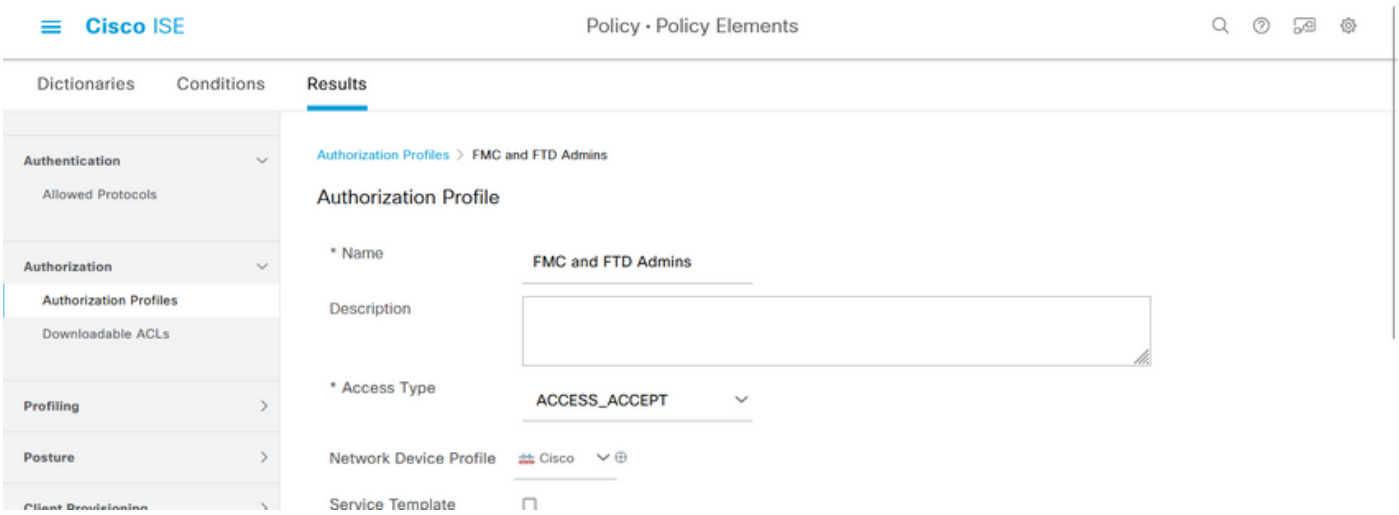


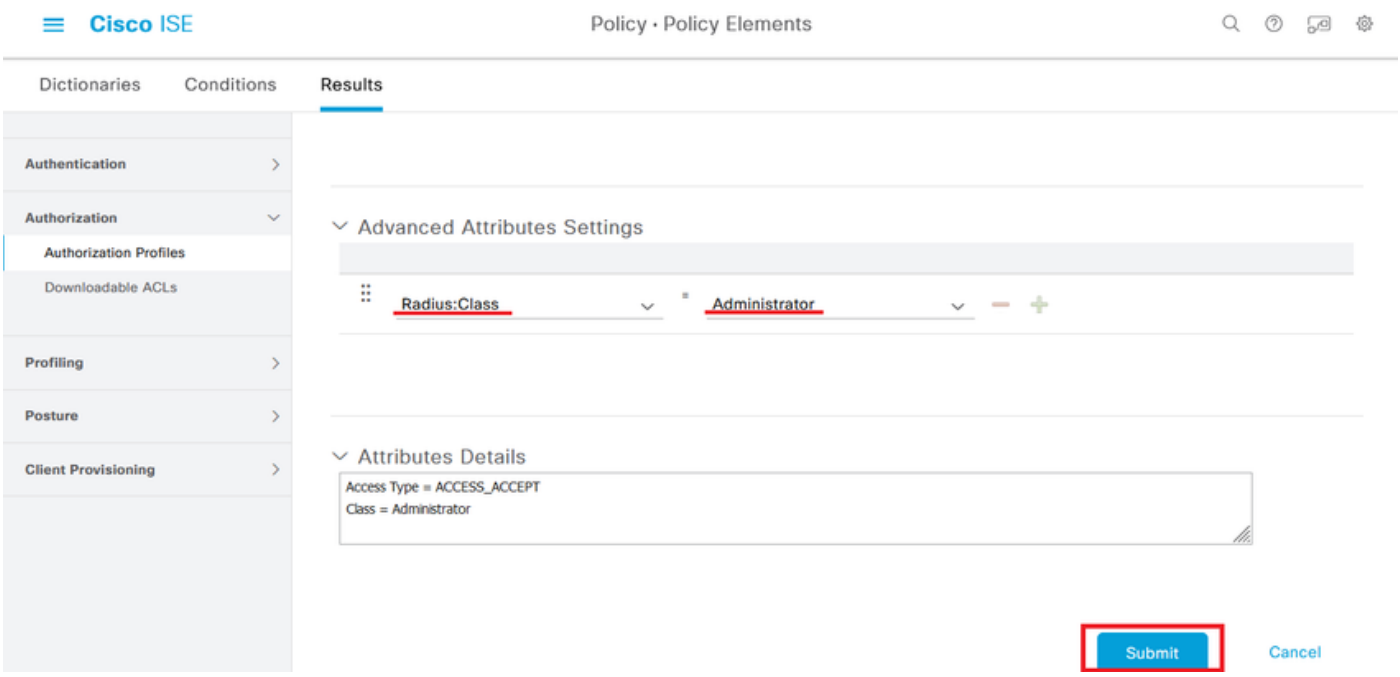


手順 6：管理者ユーザの認可プロファイルを作成します。

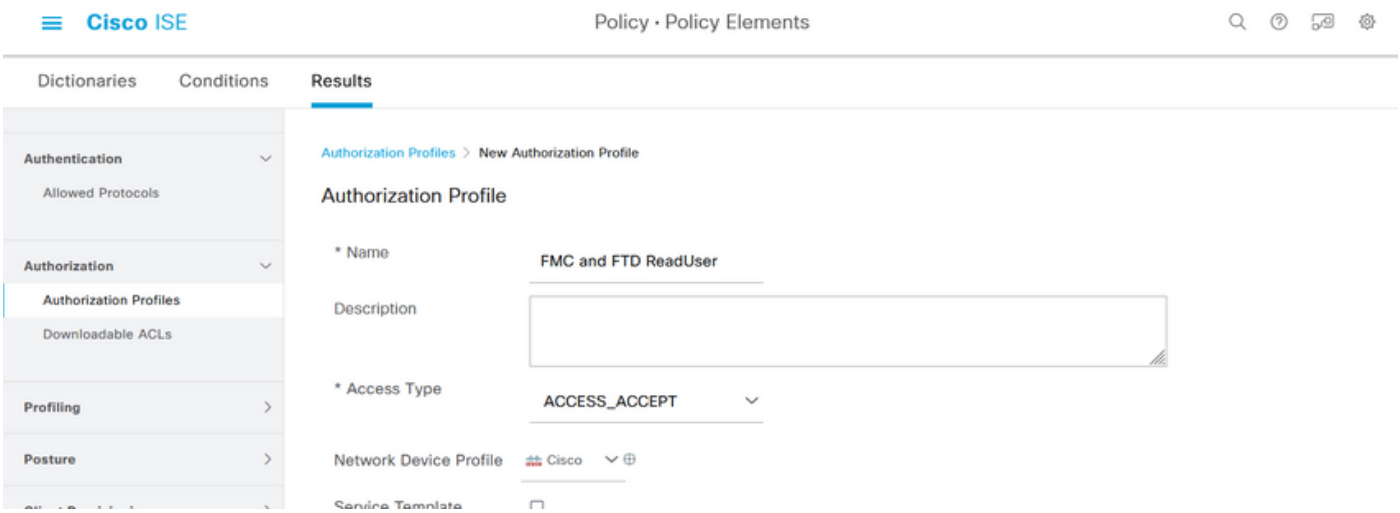
> Policy > Policy Elements > Results > Authorization > Authorization Profiles > +Addの順に移動します。

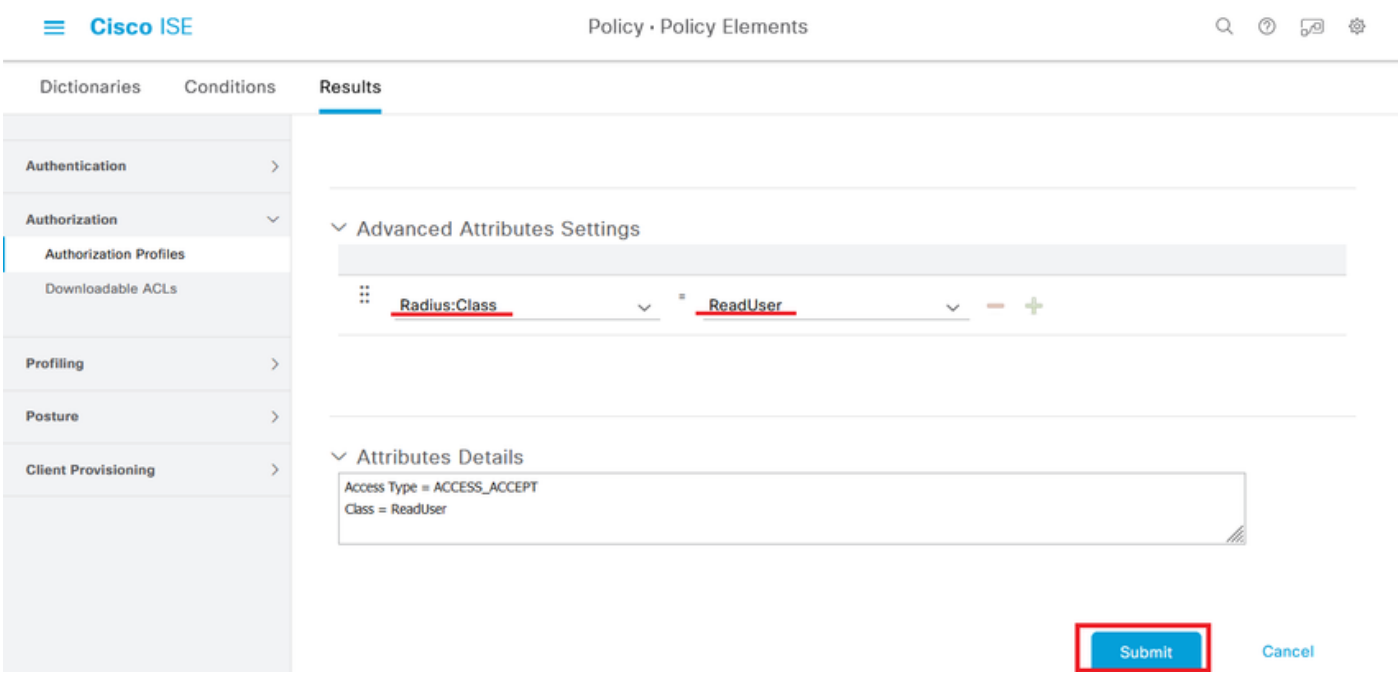
許可プロファイルの名前を定義し、Access TypeをACCESS_ACCEPTのままにして、Advanced Attributes Settingsで値Administratorを指定してRadius > Class—[25]を追加し、Submitをクリックします。





手順 7：前の手順を繰り返して、ReadOnlyユーザの許可プロファイルを作成します。今回はAdministratorではなく、ReadUserの値でRadiusクラスを作成します。

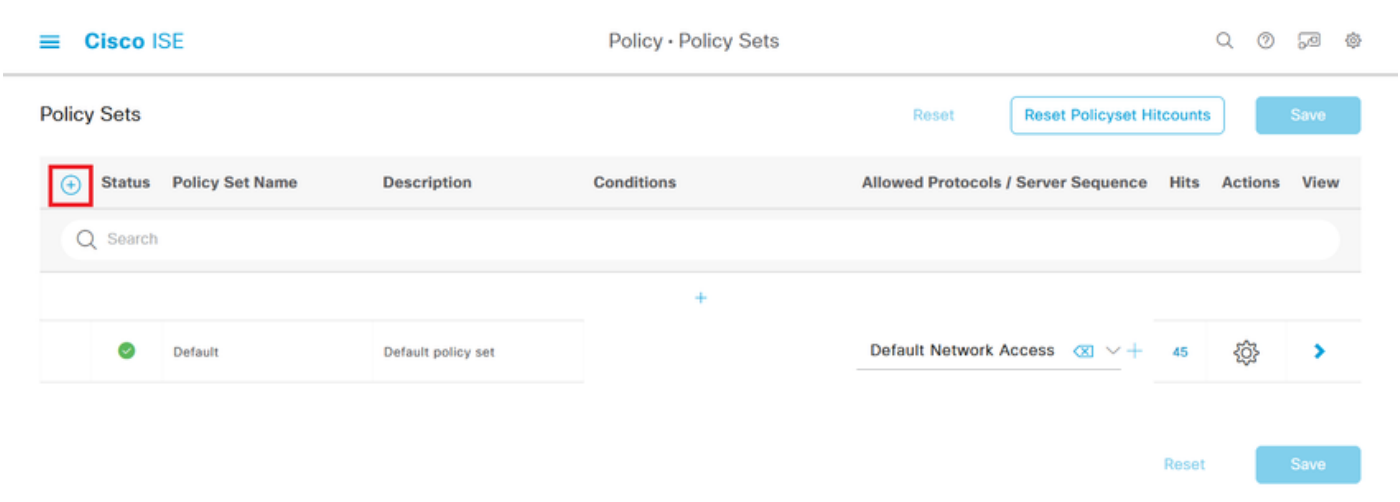




ステップ 8：FMCのIPアドレスに一致するポリシーセットを作成します。これは、他のデバイスがユーザにアクセス権を付与するのを防ぐためです。

左上隅にある
> Policy > Policy Sets >

アイコンに移動します。

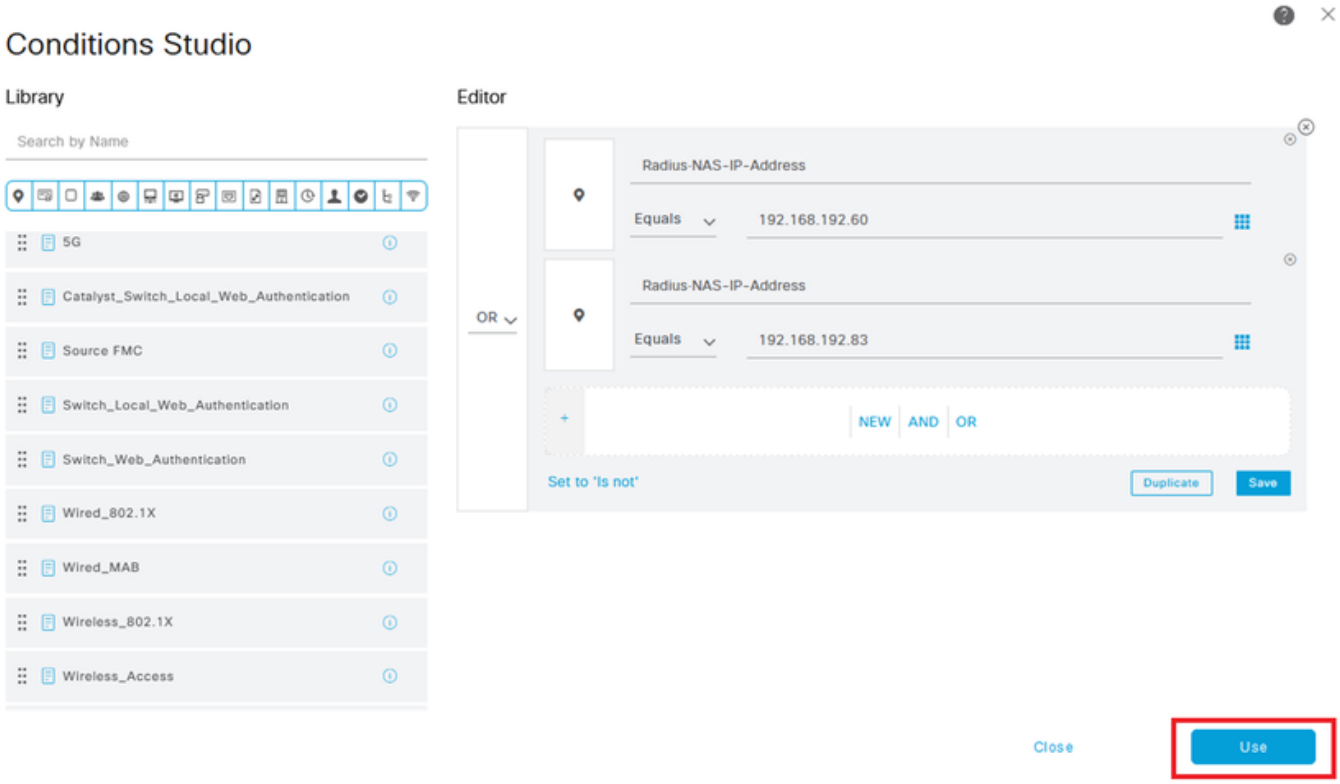

Cisco ISE
Policy · Policy Sets
Policy Sets
Reset
Reset Policyset Hitcounts
Save
Status
Policy Set Name
Description
Conditions
Allowed Protocols / Server Sequence
Hits
Actions
View
Search
Default
Default policy set
Default Network Access
45
Reset
Save

ステップ 8.1：新しい品目がポリシーセットの最上部に配置されます。

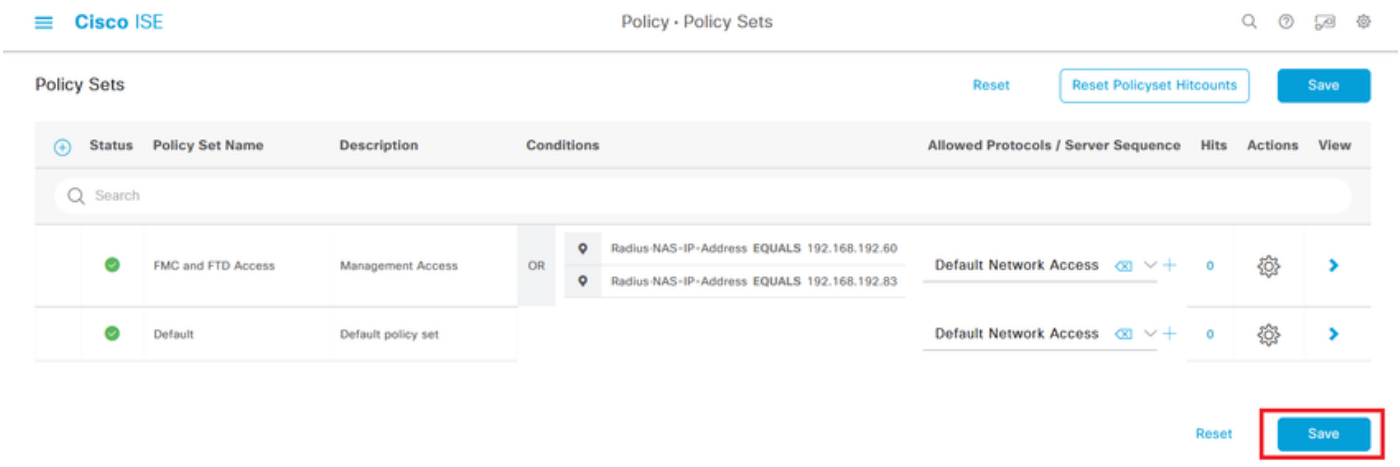
新しいポリシーに名前を付け、FMC IPアドレスに一致するRADIUS NAS-IP-Address属性の上位条件を追加します。

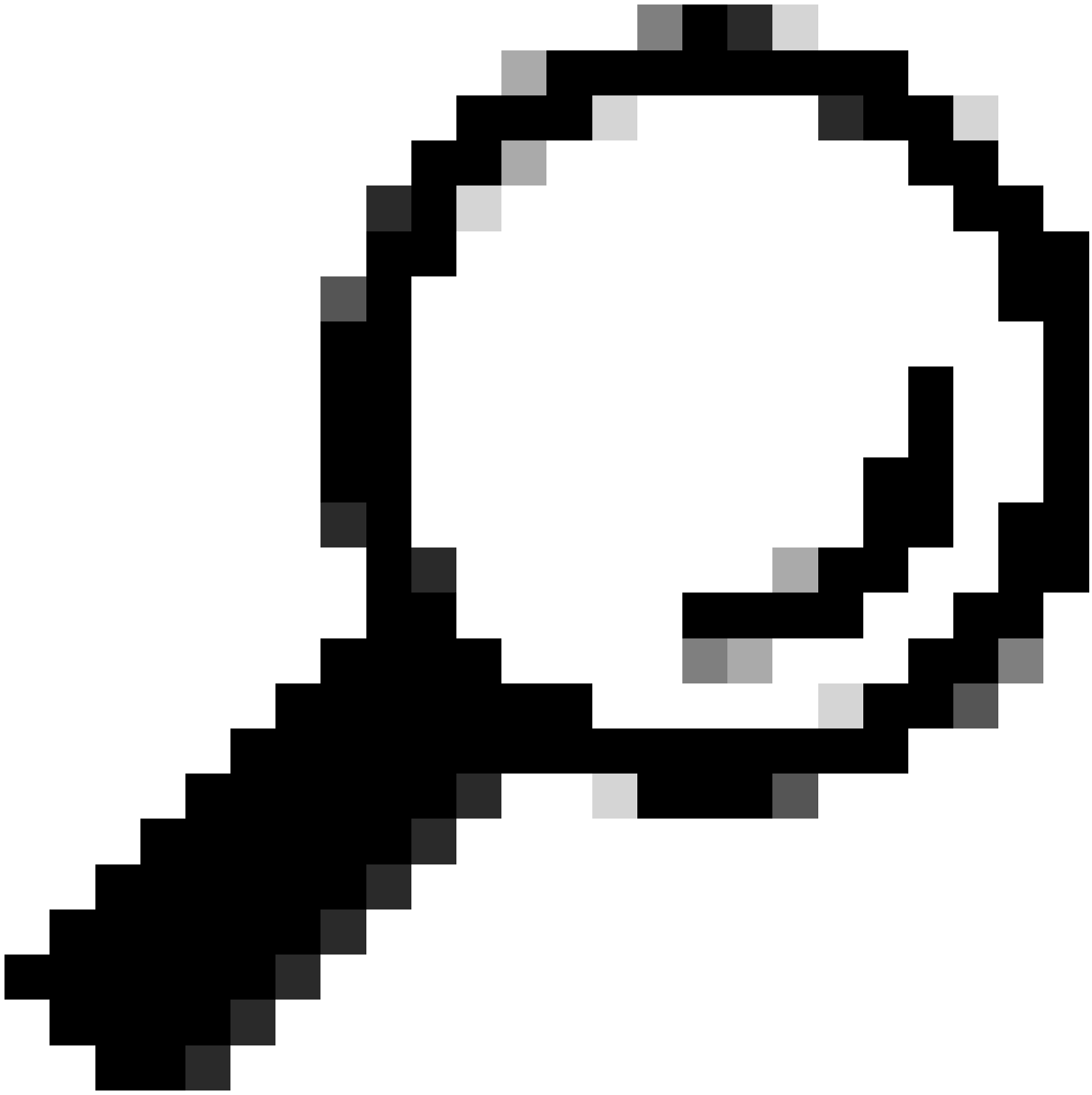
ORを一緒に使用して2番目の条件を追加し、FTDのIPアドレスを含めます。

Useをクリックして変更を保存し、エディタを終了します。



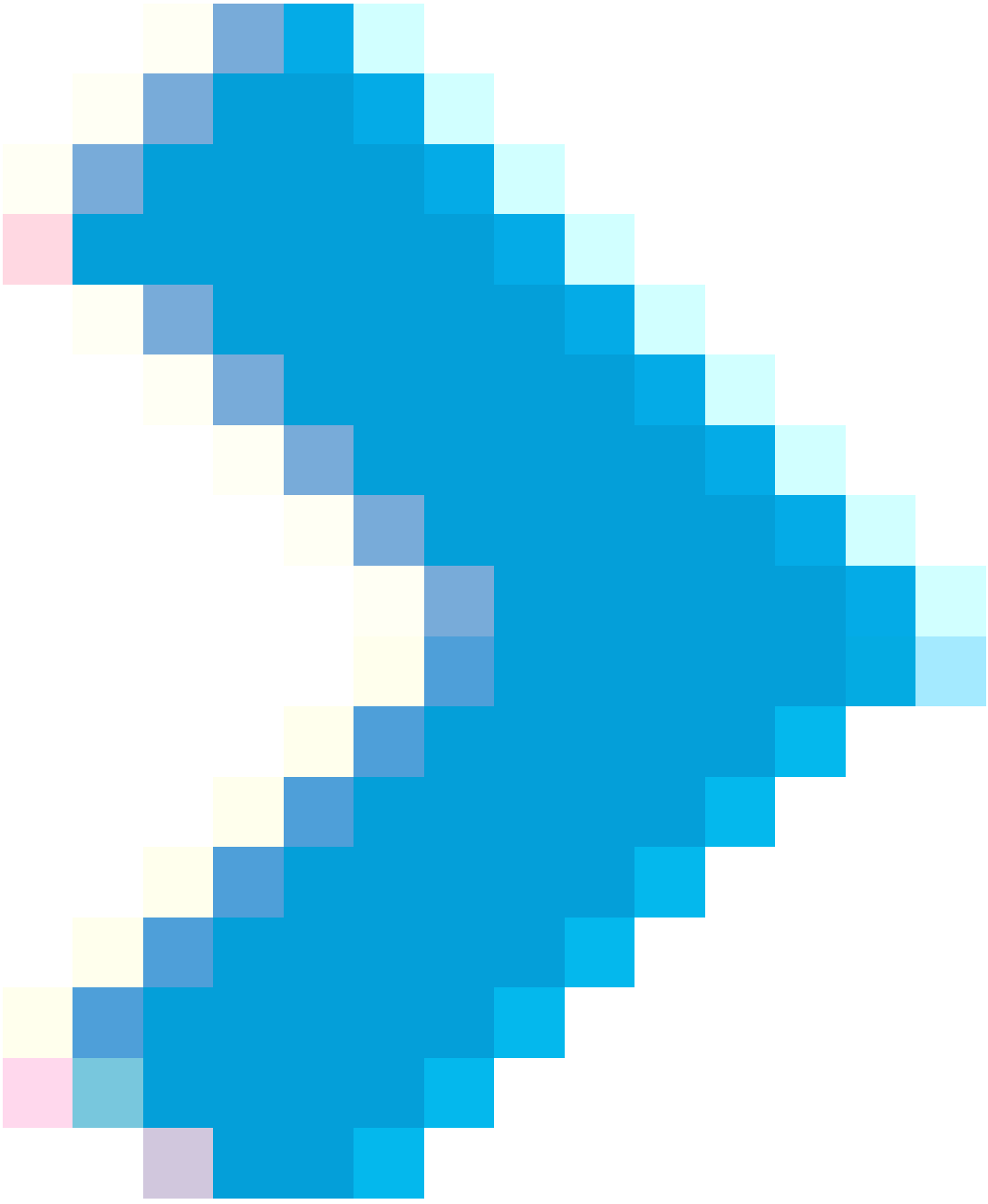
ステップ 8.2：完了したら、Saveを押します。





ヒント：この演習では、デフォルトのNetwork Access Protocolsリストを許可しています。新しいリストを作成し、必要に応じてリストを絞り込むことができます。

ステップ 9：行の最後にある



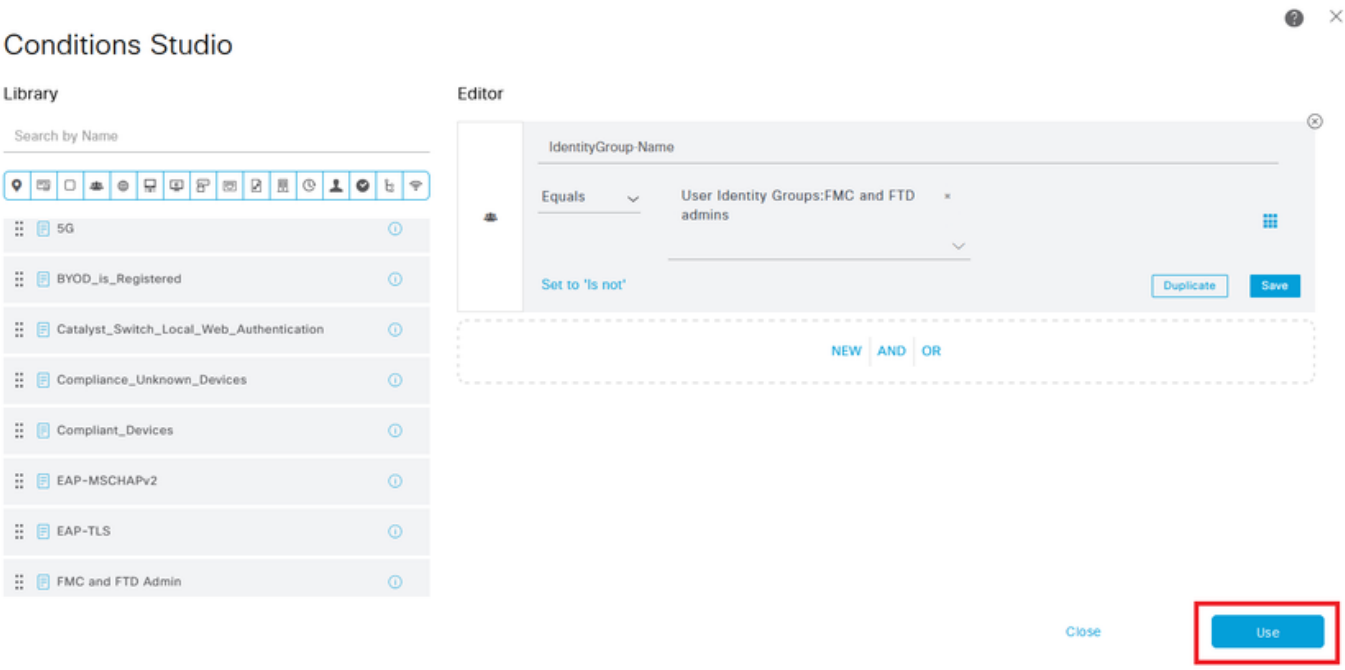
アイコンをクリックして、新しいポリシーセットを表示します。

Authorization Policyメニューを展開し、

のアイコンを押して、管理者権限を持つユーザにアクセスを許可する新しいルールを追加します。

名前を指定します。

条件を設定して、Identity GroupとName Equals User Identity Groups: FMC and FTD admins（ステップ4で作成したグループ名）という属性を持つディクショナリを照合し、Useをクリックします。

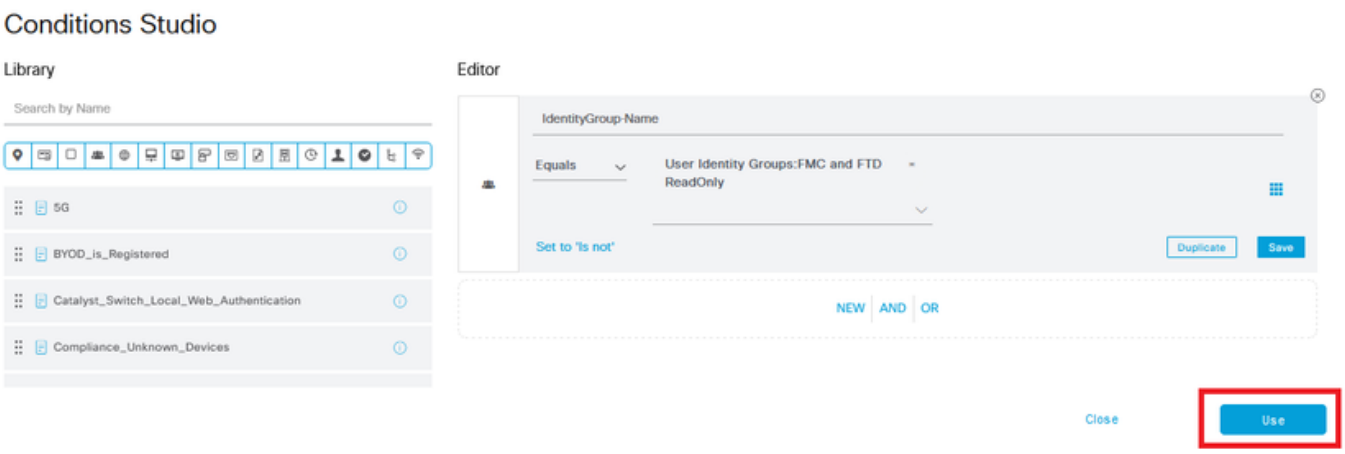


ステップ 10：読み取り専用権限を持つユーザにアクセスを許可する2番目のルールを追加するには、

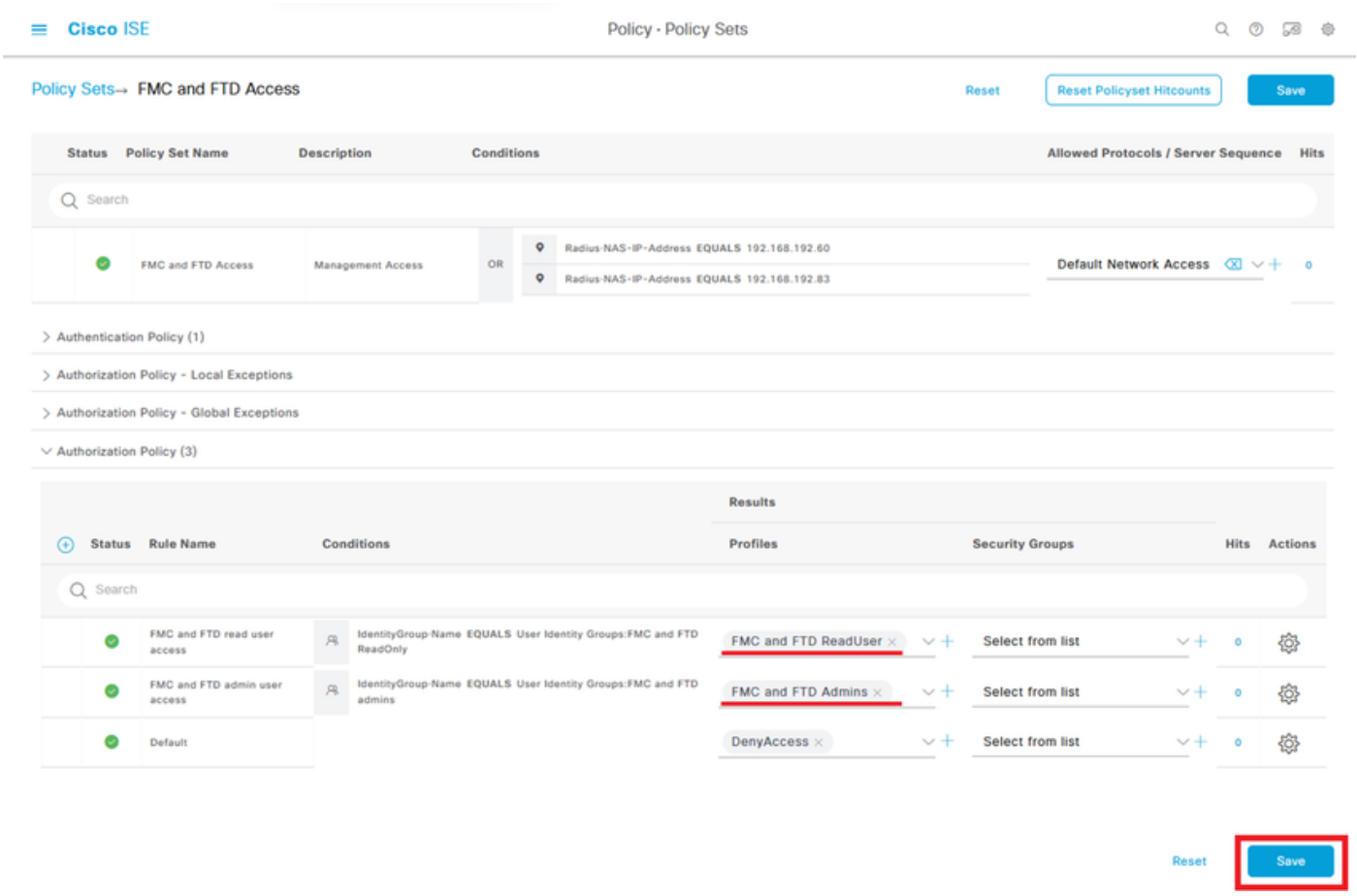
アイコンをクリックします。

名前を指定します。

条件を設定して、Identity Groupというディクショナリと Name Equals User Identity Groups: FMCおよびFTD ReadOnly（手順4で作成したグループ名）を照合し、Useをクリックします。

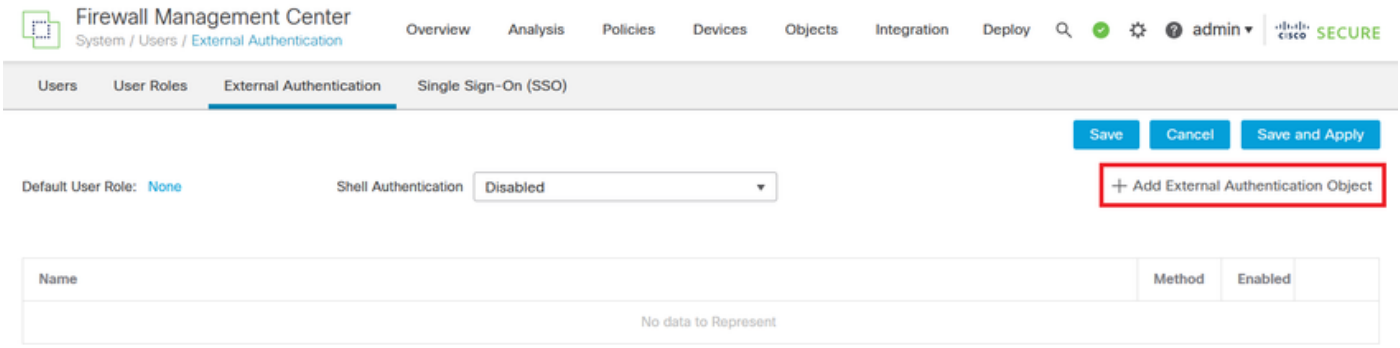


ステップ 11各ルールの認可プロファイルをそれぞれ設定し、Saveをクリックします。



FMCの設定

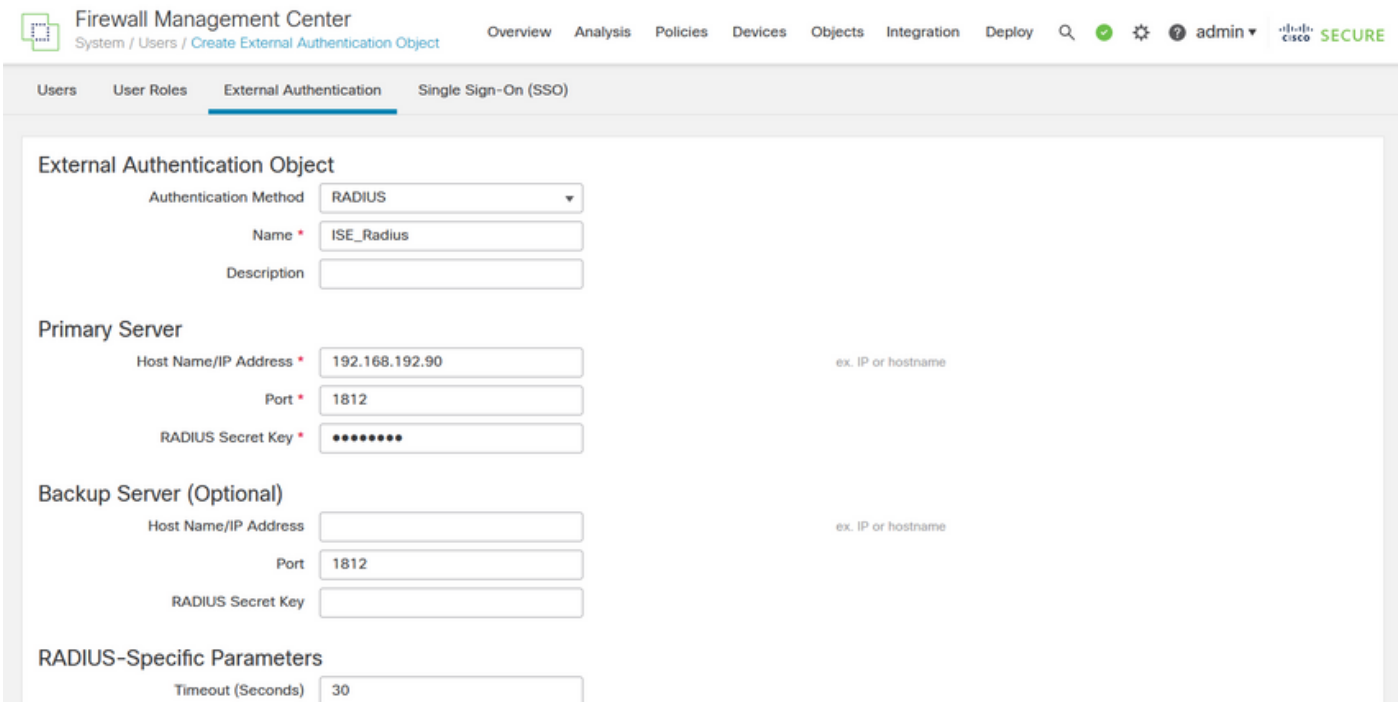
ステップ 1：System > Users > External Authentication > + Add External Authentication Objectの順に選択し、外部認証オブジェクトを作成します。



ステップ 2：認証方式としてRADIUSを選択します。

External Authentication Objectで、新しいオブジェクトにNameを指定します。

次に、プライマリサーバ設定で、ISE IPアドレスと、ISE設定のステップ2で使用したものと同じRADIUS秘密鍵を挿入します。

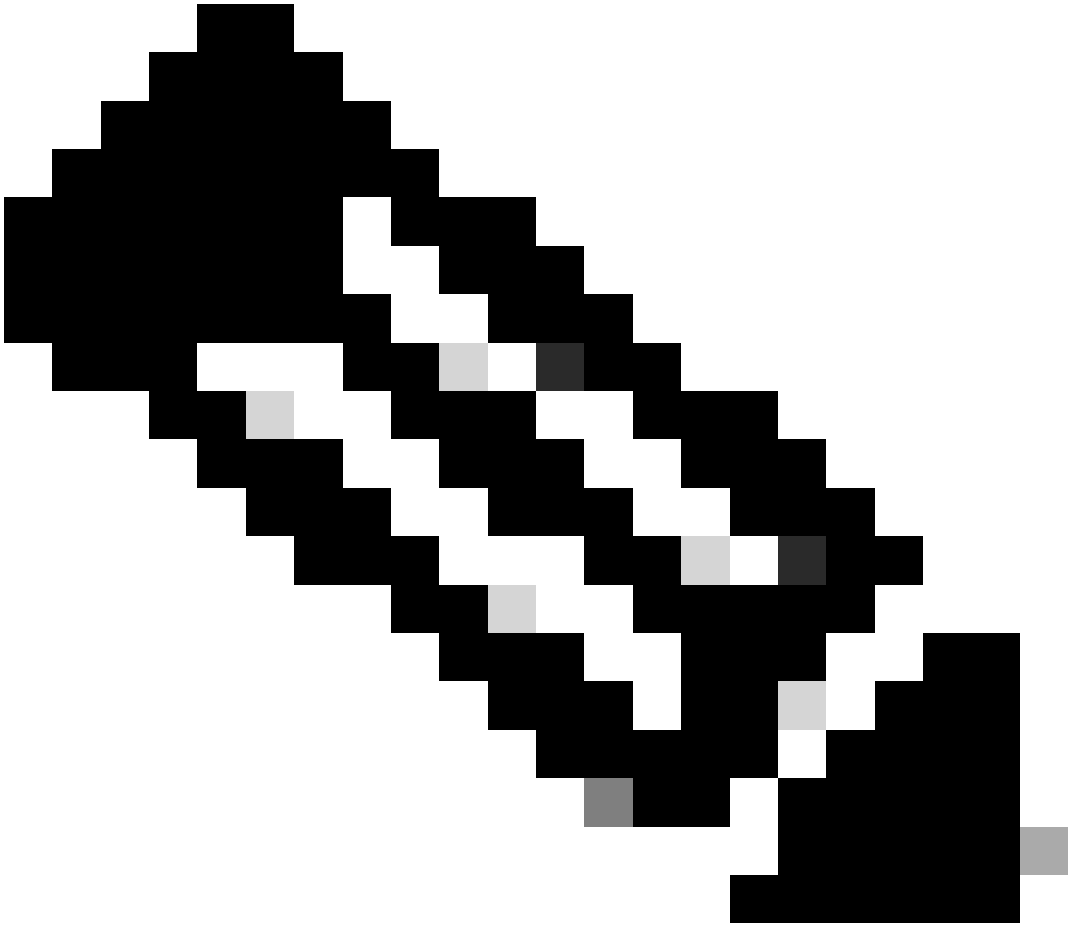


ステップ 3：ISE設定のステップ6と7で設定したRADIUS Class属性の値（firewall_adminにはAdministrator、firewall_readuserにはReadUser）を挿入します。

RADIUS-Specific Parameters

Timeout (Seconds)	30
Retries	3
Access Admin	
Administrator	Class=Administrator
Discovery Admin	
External Database User	
Intrusion Admin	
Maintenance User	
Network Admin	
Security Analyst	
Security Analyst (Read Only)	Class=ReadUser
Security Approver	
Threat Intelligence Director (TID) User	
Default User Role	Access Admin Administrator Discovery Admin External Database User

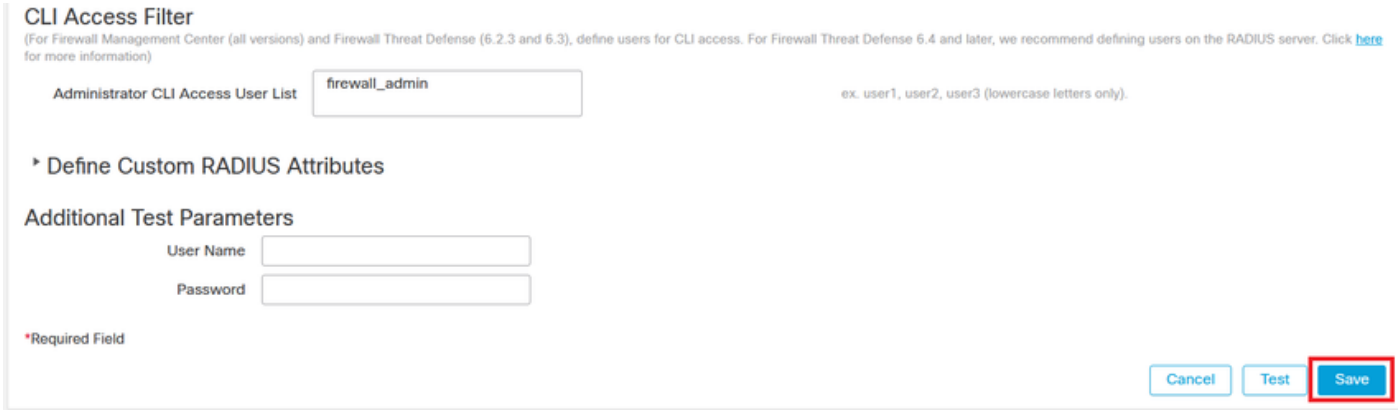
To specify the default user role if user is not found in any group



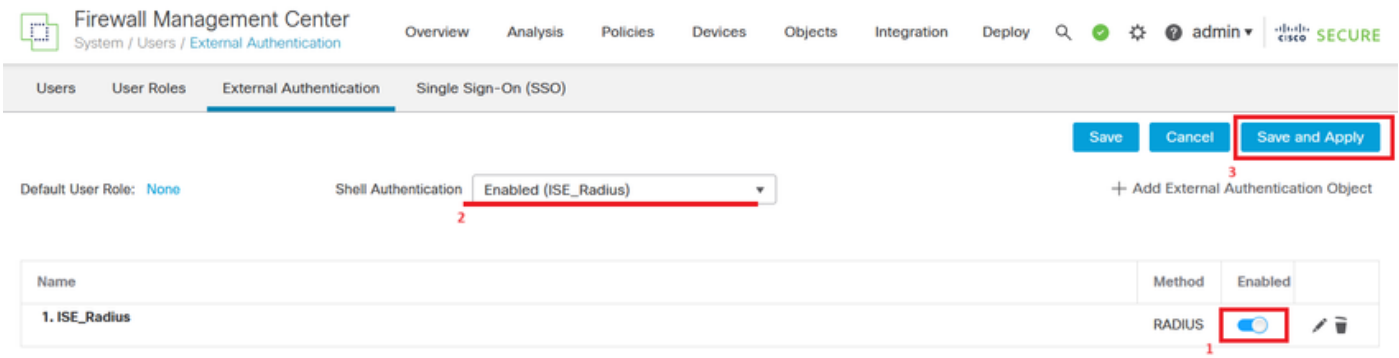
注：タイムアウトの範囲はFTDとFMCとで異なります。そのため、オブジェクトを共有する場合にデフォルト値の30秒を変更するときは、FTDデバイスのタイムアウトの範囲を小さく（1 ~ 300秒）設定することを忘れないでください。タイムアウトを大きい値に設定すると、脅威対策のRADIUS設定が機能しません。

ステップ 4：CLIアクセスフィルタの下にあるAdministrator CLI Access User Listに、CLIアクセスを許可されるユーザ名を入力します。

完了したら、Saveをクリックします。

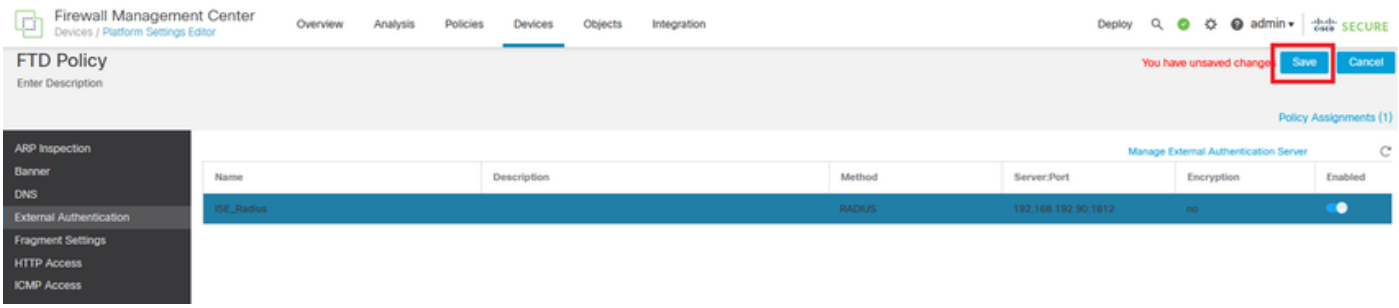


ステップ 5：新規オブジェクトを有効にします。これをFMCのシェル認証方式として設定し、Save and Applyをクリックします。

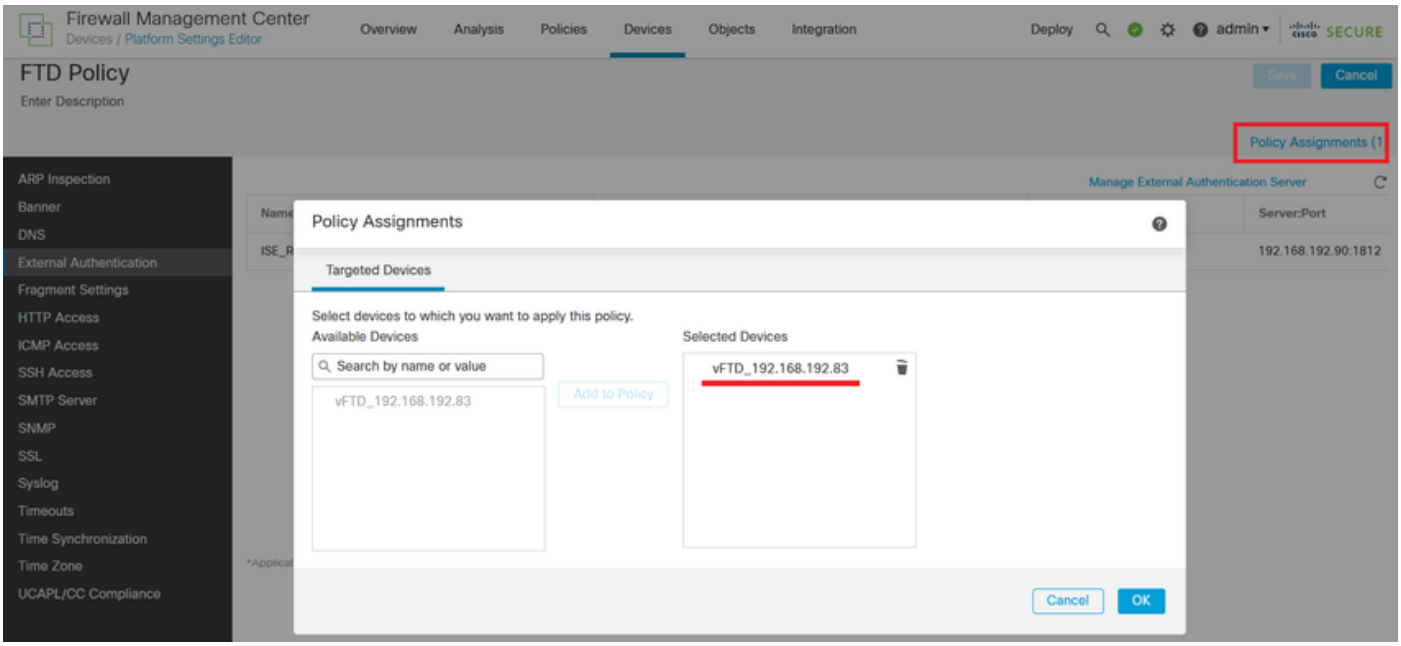


FTD の設定

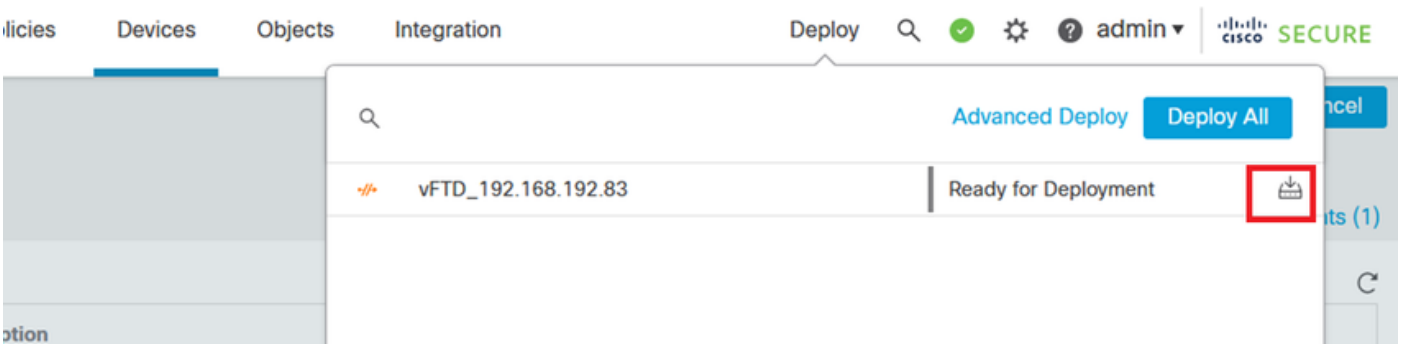
ステップ 1：FMC GUIで、Devices > Platform Settingsの順に移動します。アクセスするFTDが割り当てられていない場合は、現在のポリシーを編集するか、新しいポリシーを作成します。External Authenticationの下のRADIUSサーバをイネーブルにし、Saveをクリックします。



ステップ 2：アクセスする必要があるFTDがPolicy Assignments as a Selected Deviceの下に表示されていることを確認します。

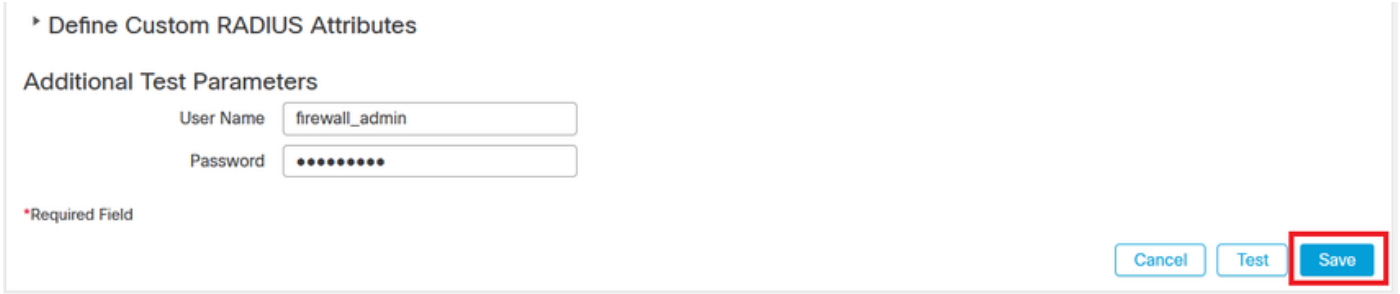


ステップ 3：変更を展開します。

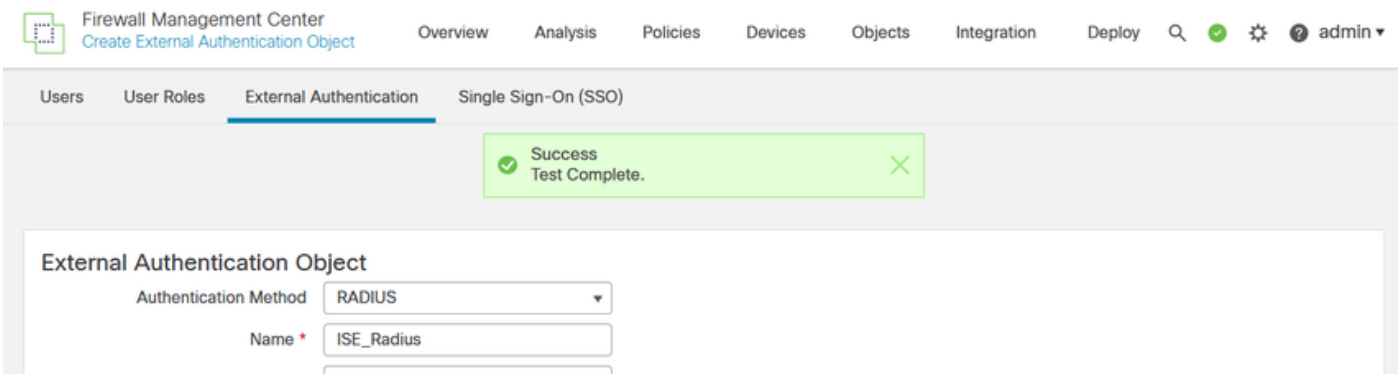


確認

- 新しい展開が正常に動作していることをテストします。
- FMCのGUIで、RADIUSサーバの設定に移動し、Additional Test Parametersセクションまでスクロールダウンします。
- ISEユーザのユーザ名とパスワードを入力し、Testをクリックします。



- テストに成功すると、ブラウザウィンドウの上部に「Success Test Complete」というメッセージが緑色で表示されます。



- 詳細は、テスト出力の下のDetailsを展開すると表示されます。

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。