RADIUSサーバとしてISEを使用したSWA外部認証の設定

内容

はじめに

このドキュメントでは、Cisco ISEをRADIUSサーバとして使用して、Secure Web Access(SWA)で外部認証を設定する手順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 Web Applianceの基礎知識。
- ISEでの認証および認可ポリシー設定に関する知識。
- RADIUS の基礎知識.

次の情報も含めることをお勧めします。

- SWAおよびISE管理アクセス。
- 互換性のあるWSAおよびISEバージョン。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- SWA 14.0.2-012
- ISE 3.0.0

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

SWAの管理ユーザの外部認証を有効にすると、デバイスは外部認証設定で指定されている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。

Network Topology

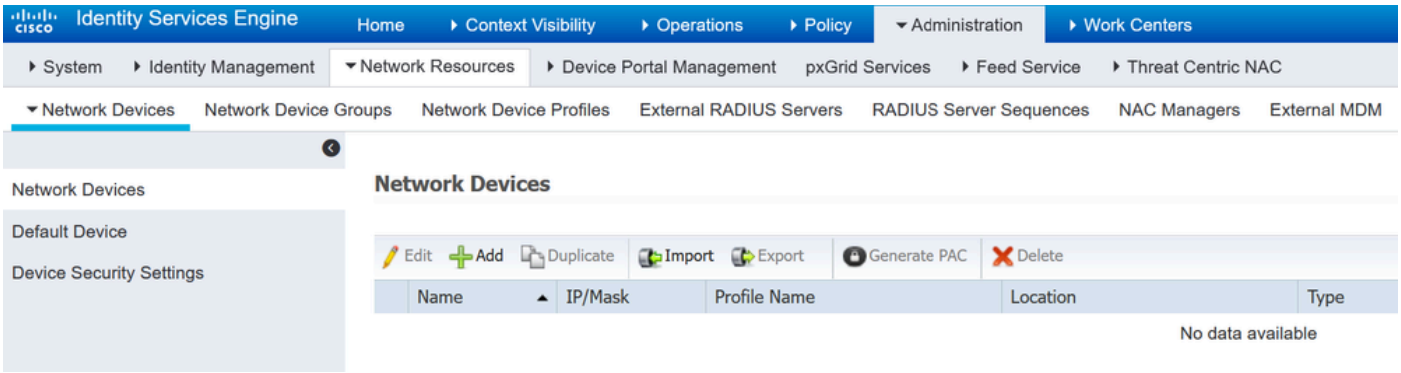
ネットワークトポロジ図

管理ユーザは、クレデンシャルを使用してポート443でSWAにアクセスします。SWAがRADIUSサーバでクレデンシャルを確認します。

設定

ISE 設定

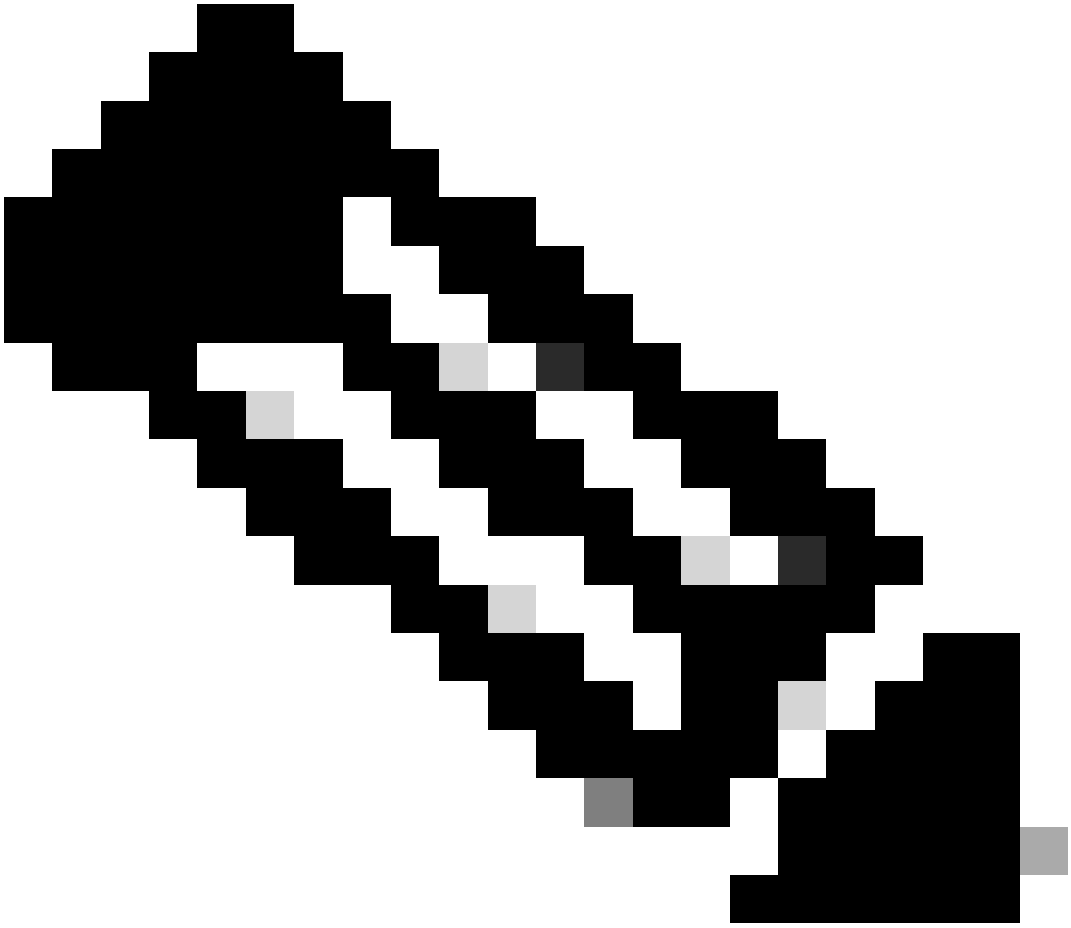
ステップ 1： 新しいネットワークデバイスを追加します。Administration > Network Resources > Network Devices > +Addの順に移動します。



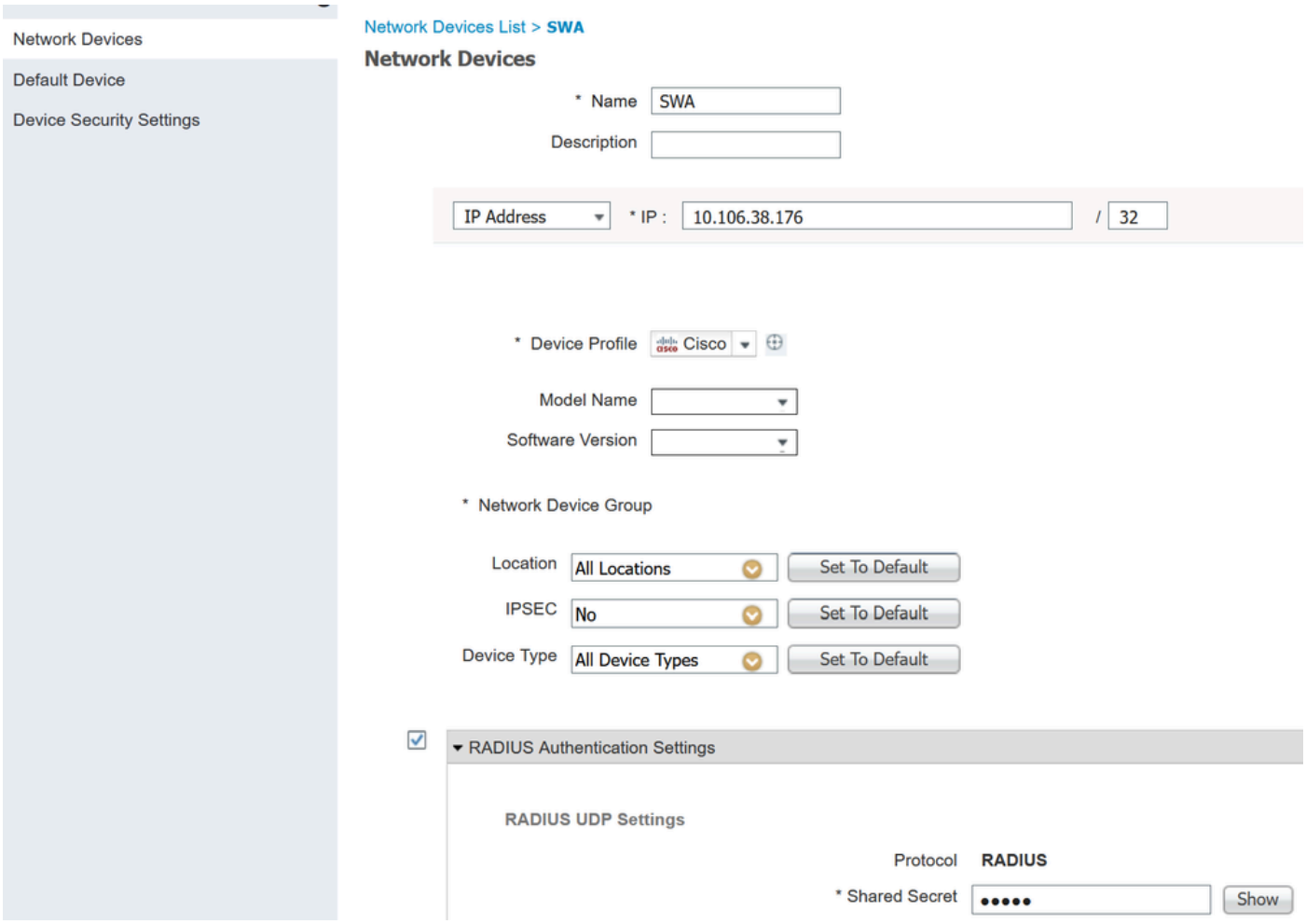
ISEのネットワークデバイスとしてのSWAの追加

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、SWA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。

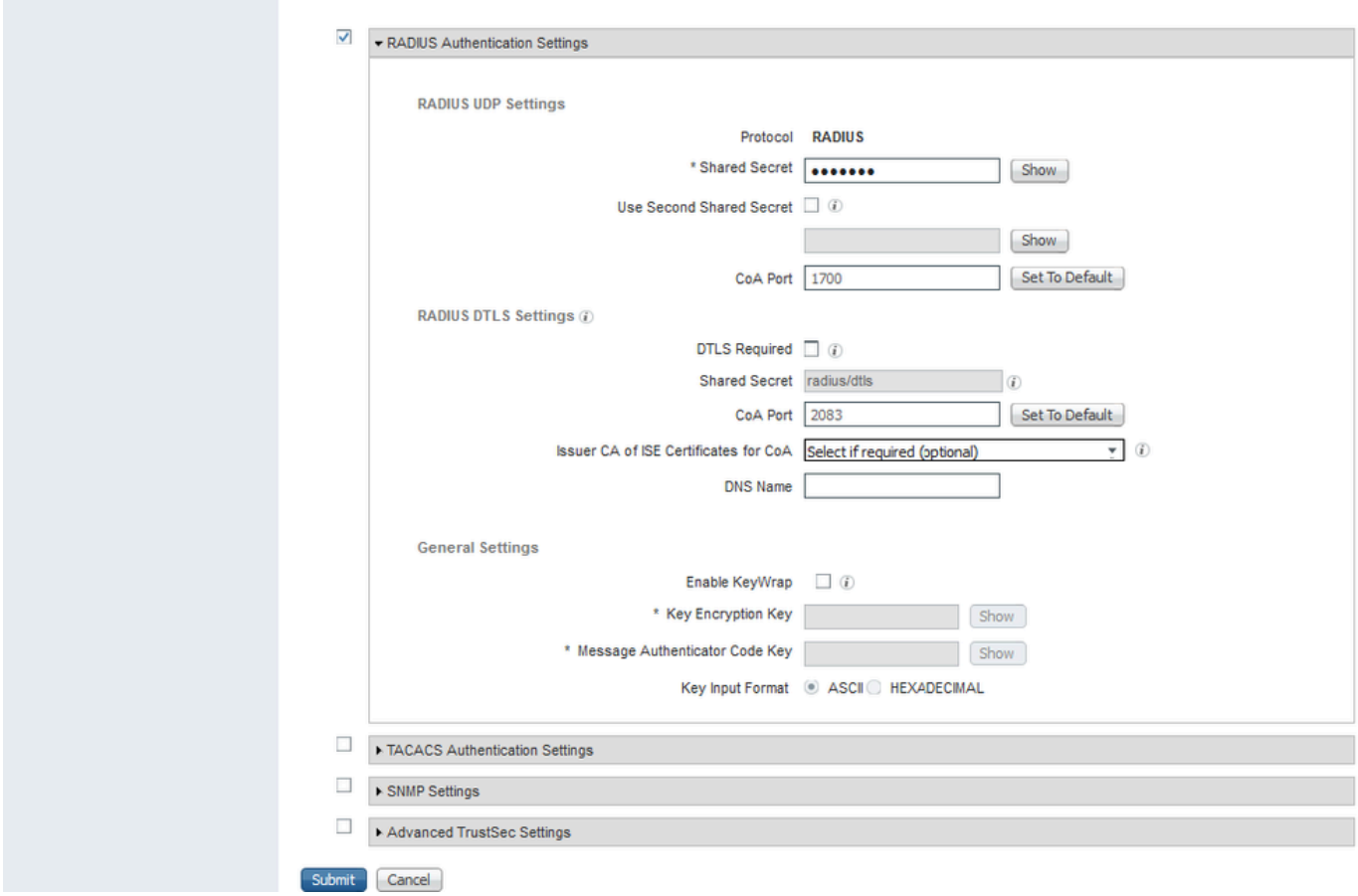


注：後でSWAにRADIUSサーバを設定するときにも、同じキーを使用する必要があります。



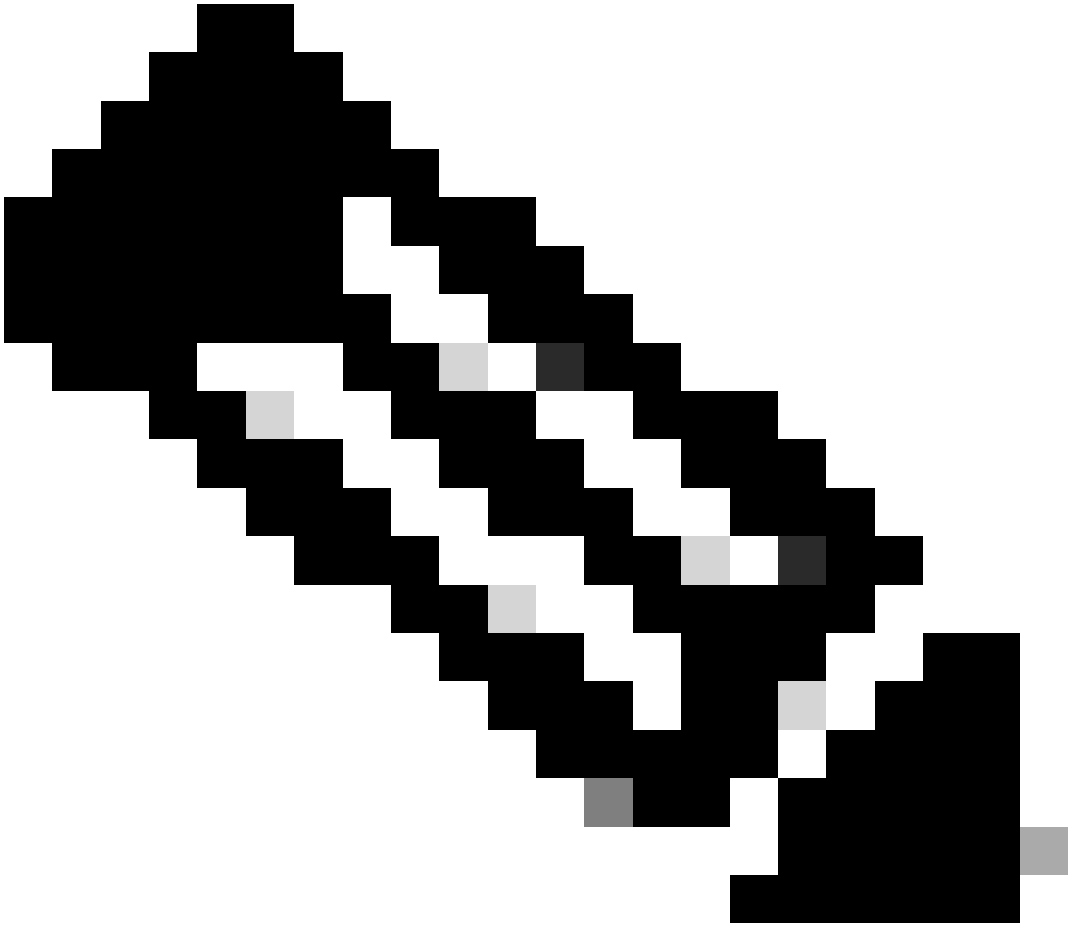
SWAネットワークデバイスの共有キーの設定

ステップ 2.1：[Submit] をクリックします。

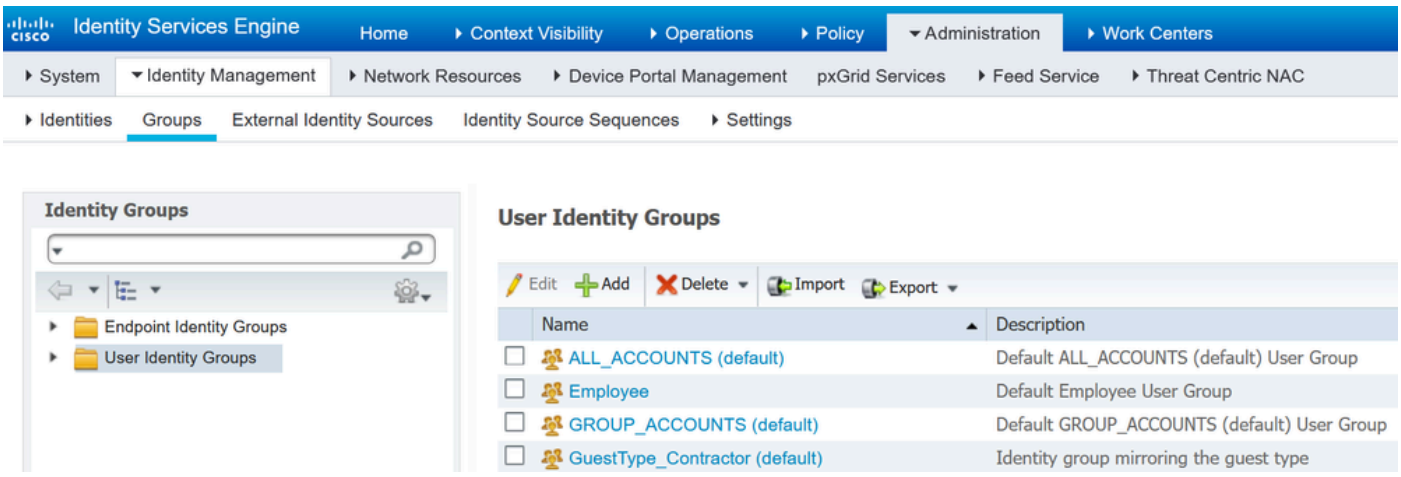


ネットワークデバイス設定の送信

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。



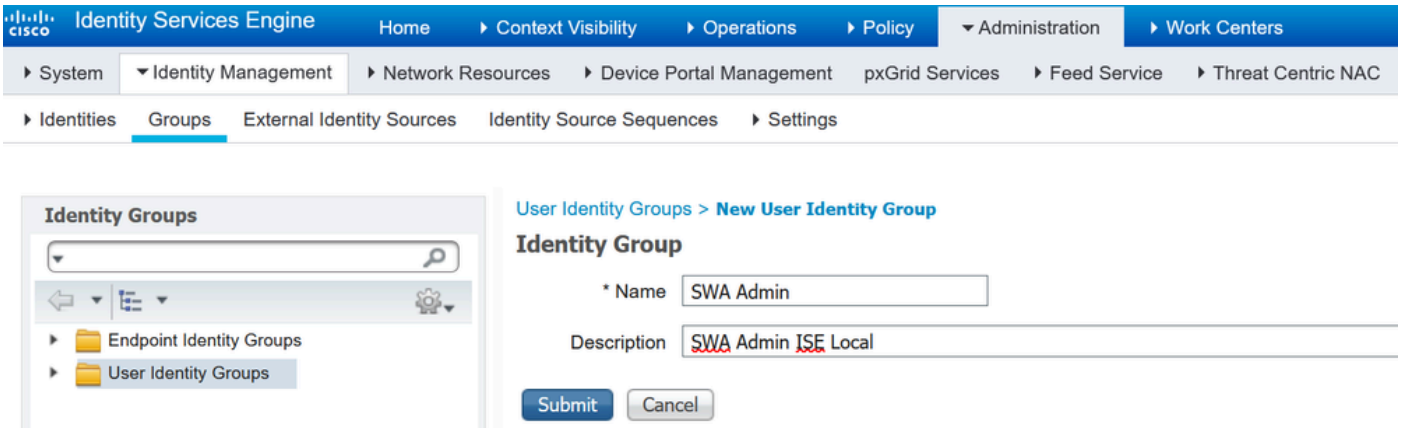
注：異なるユーザタイプに一致させるには、異なるユーザグループを設定する必要があります。



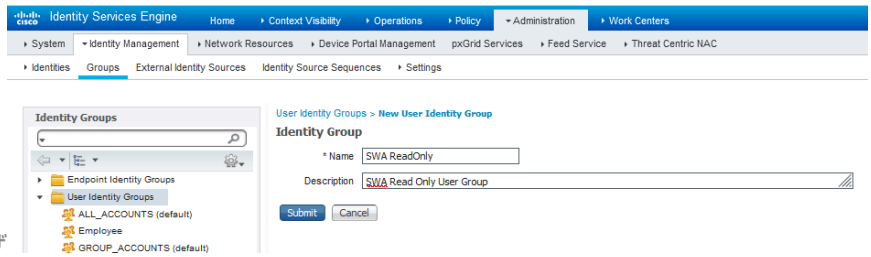
ユーザIDグループの追加

ステップ 4：グループ名、説明（オプション）、および送信を入力します。グループごとにこれ

らの手順を繰り返します。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。



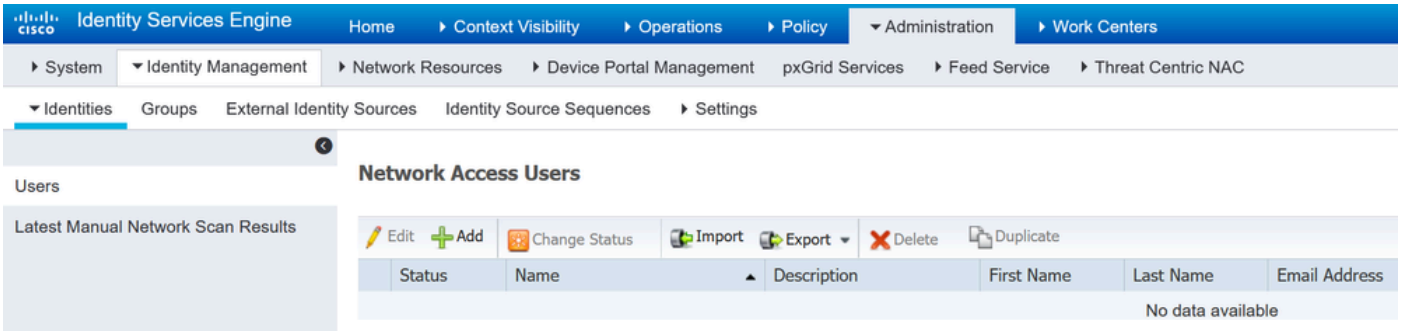
ユーザID



グループの追加SWA読み取り専用ユーザのユーザIDグループの追加

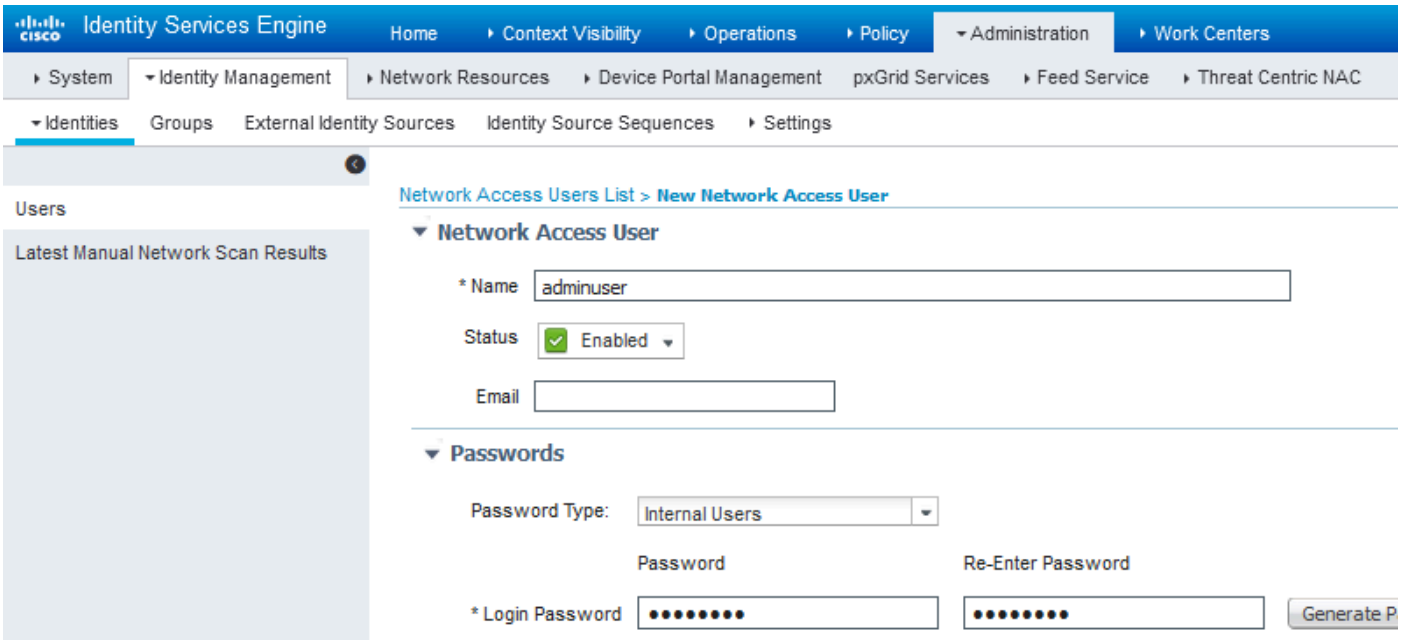
ステップ 5：SWAで設定されたユーザ名と一致するネットワークアクセスユーザを作成する必要があります。

ネットワークアクセスユーザを作成し、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。



ISEでのローカルユーザの追加

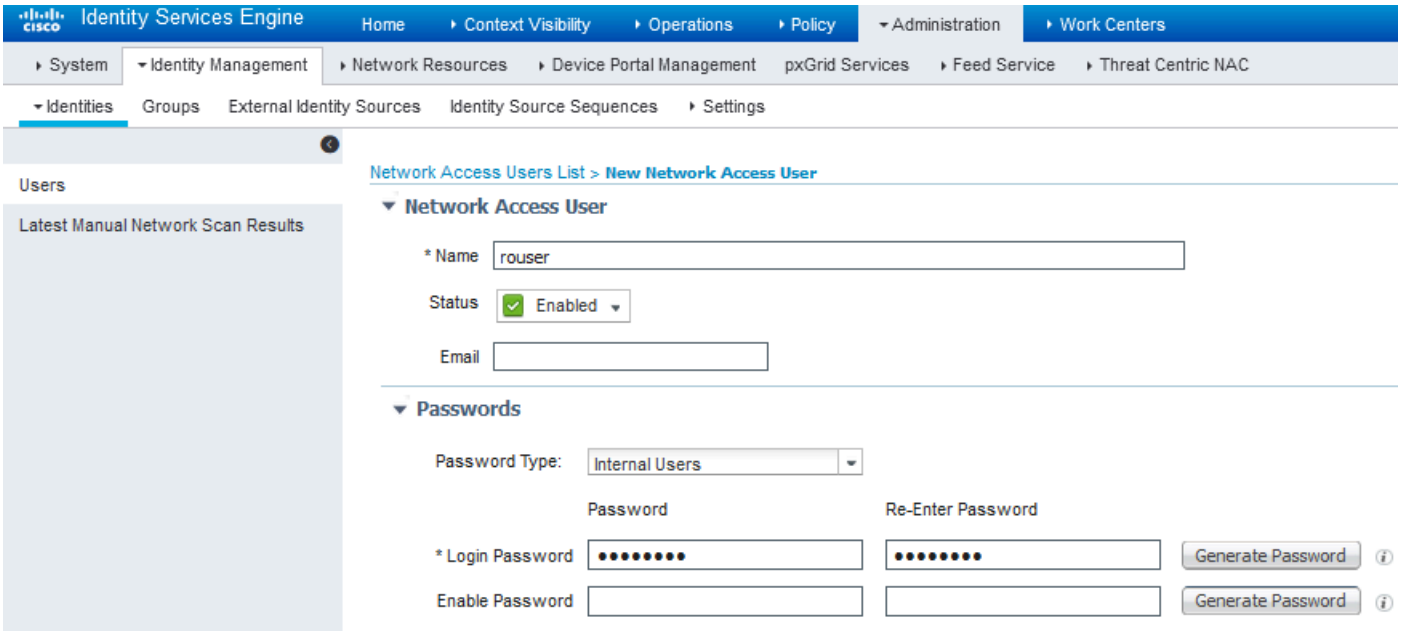
ステップ 5.1：管理者権限を持つネットワークアクセスユーザを作成する必要があります。名前とパスワードを割り当てます。



管理者ユーザの追加

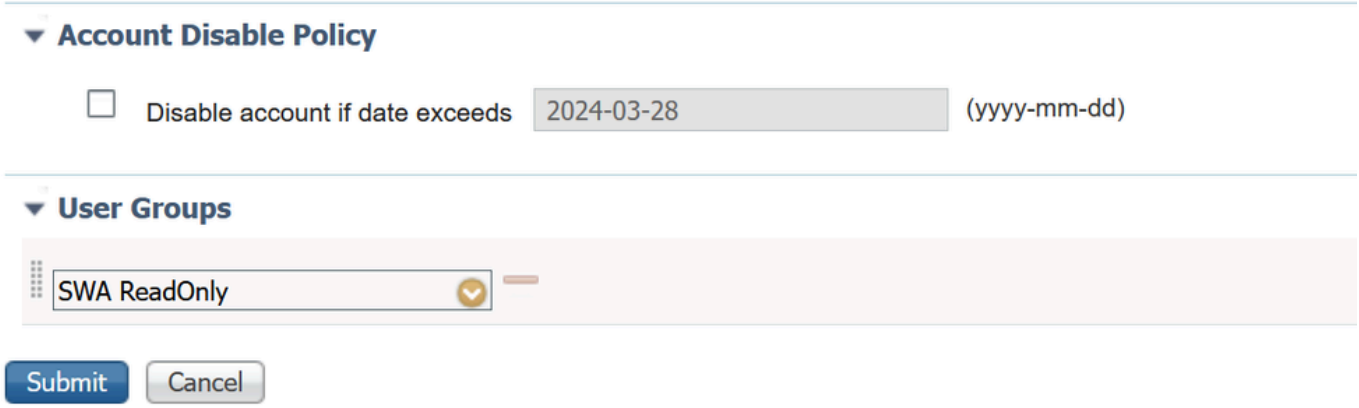
ステップ 5.2：User GroupsセクションでSWA Adminを選択し、Admin UserにAdmin Groupを割り当てます。

ステップ 5.3：読み取り専用権限を持つユーザを作成する必要があります。名前とパスワードを割り当てます。



読み取り専用ユーザの追加

ステップ 5.4：User GroupsセクションでSWA ReadOnlyを選択します。

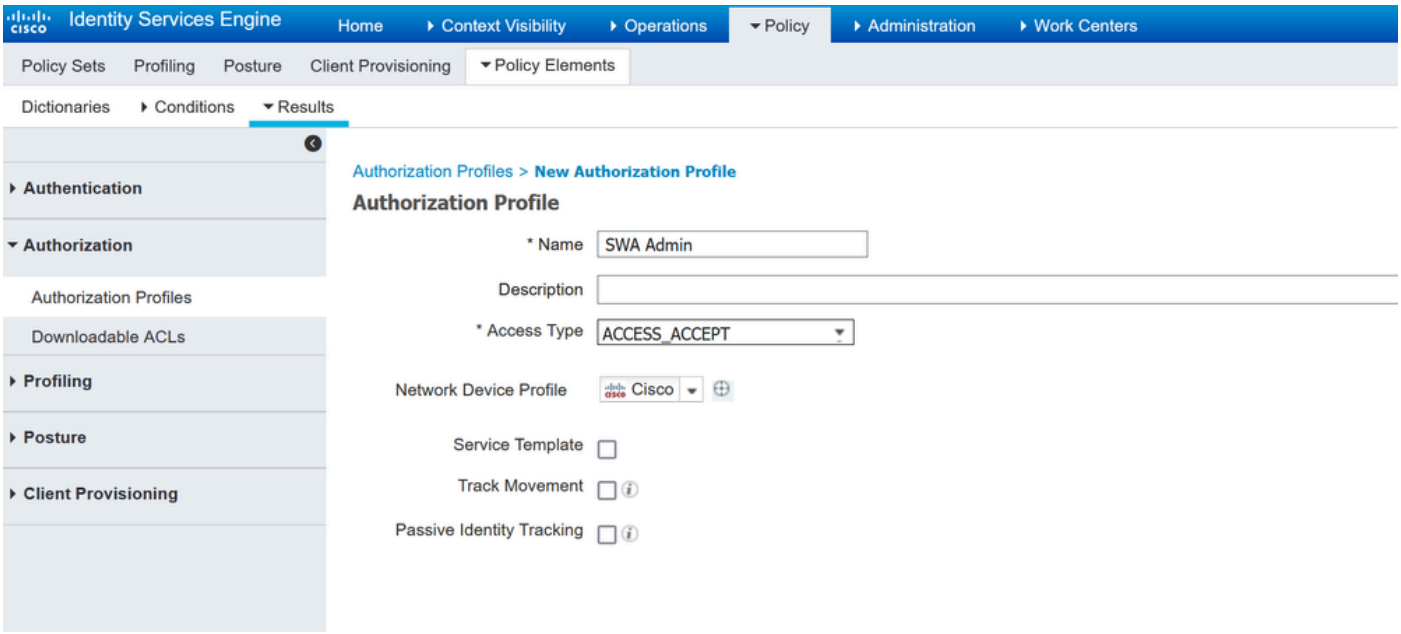


読み取り専用ユーザグループの読み取り専用ユーザへの割り当て

手順 6： 管理者ユーザの許可プロファイルを作成します。

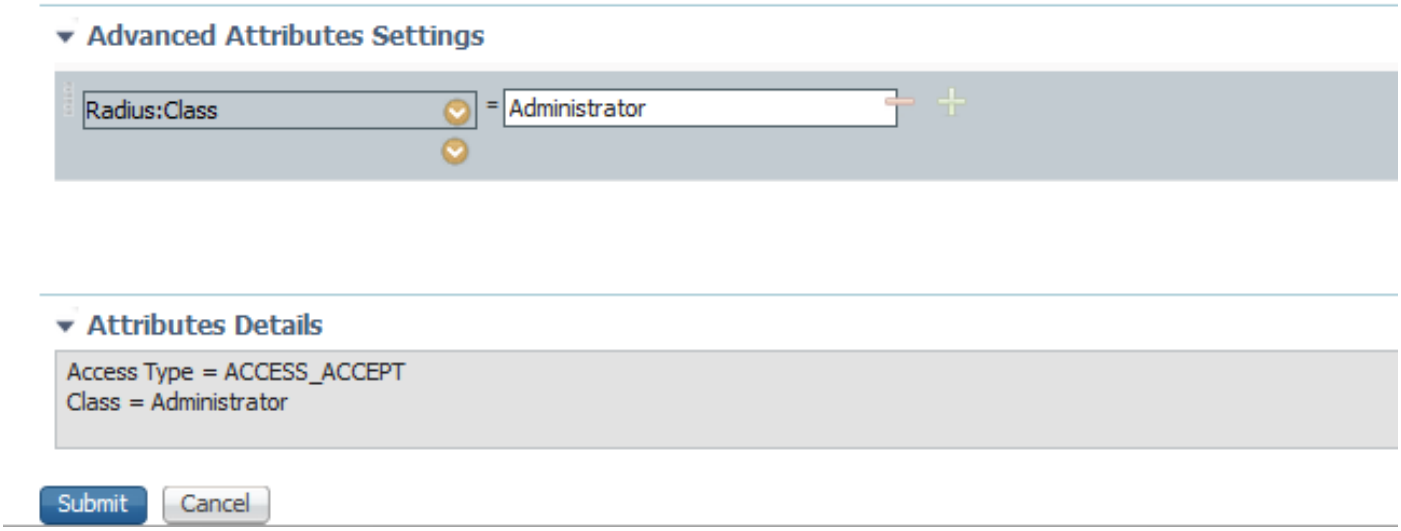
Policy > Policy Elements > Results > Authorization > Authorization Profiles > +Addの順に移動します。

許可プロファイルの名前を定義し、アクセスタイプがACCESS_ACCEPTに設定されていることを確認します。



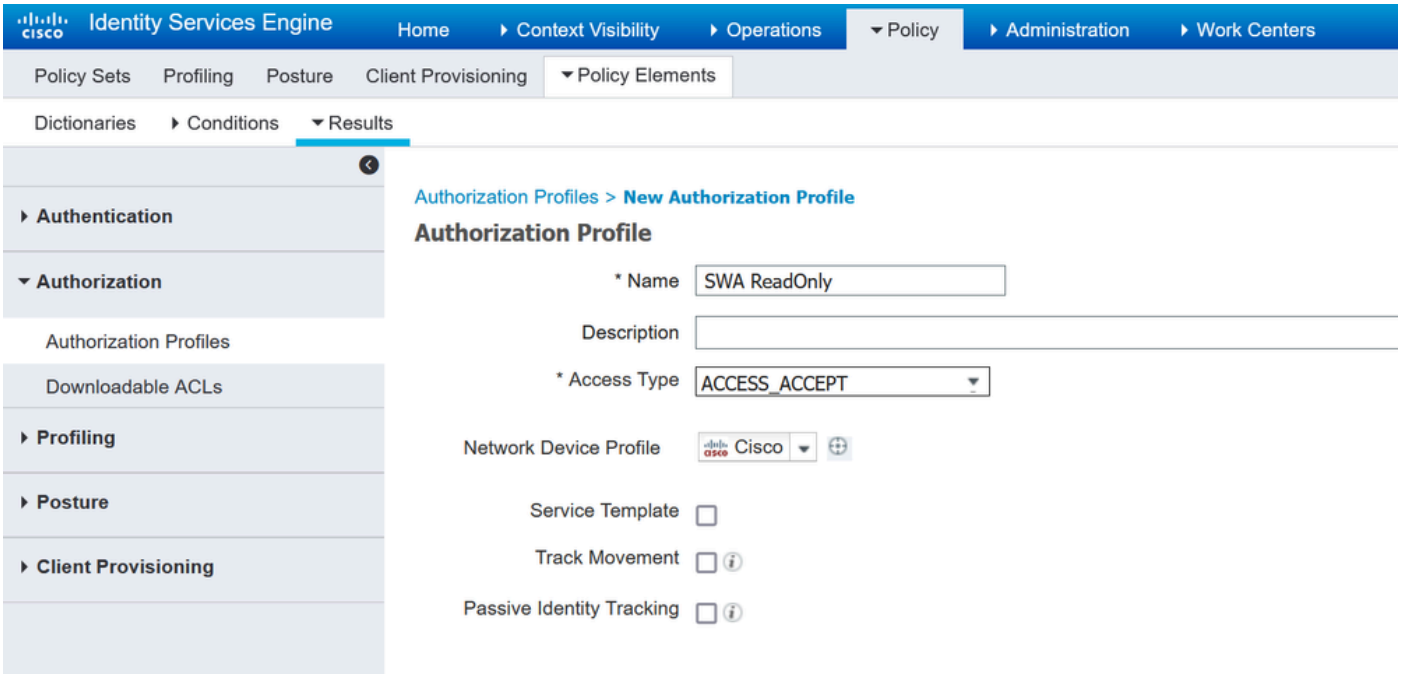
管理者ユーザの許可プロファイルの追加

ステップ 6.1：Advanced Attributes Settingsで、Radius > Class—[25]に移動し、値Administratorを入力してSubmit.



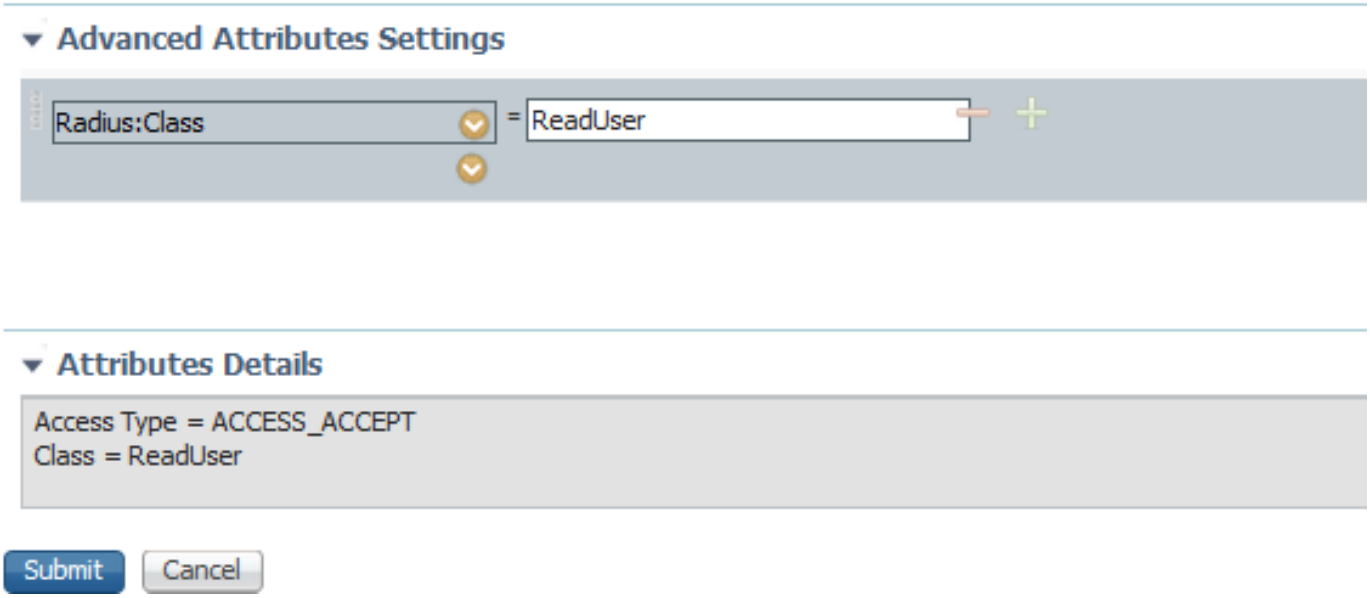
Add Authorization Profile for Admin Usersをクリックします

手順 7： ステップ6を繰り返して、読み取り専用ユーザの許可プロファイルを作成します。



読み取り専用ユーザの許可プロファイルの追加

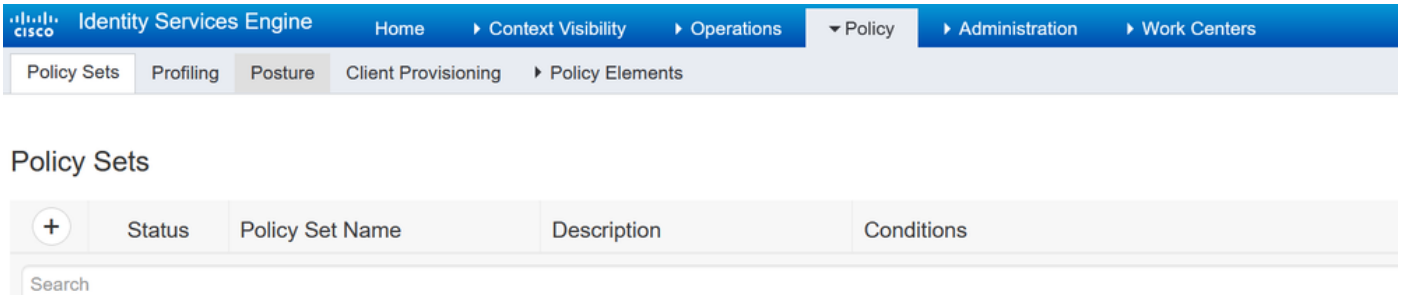
ステップ 7.1：今回はAdministratorではなくReadUserの値でRadius:Classを作成します。



読み取り専用ユーザの許可プロファイルの追加

ステップ 8： SWA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、これらのユーザクレデンシャルを使用して他のデバイスにアクセスするのを防ぐためです。

Policy > PolicySetsに移動し、左上隅にある+アイコンをクリックします。

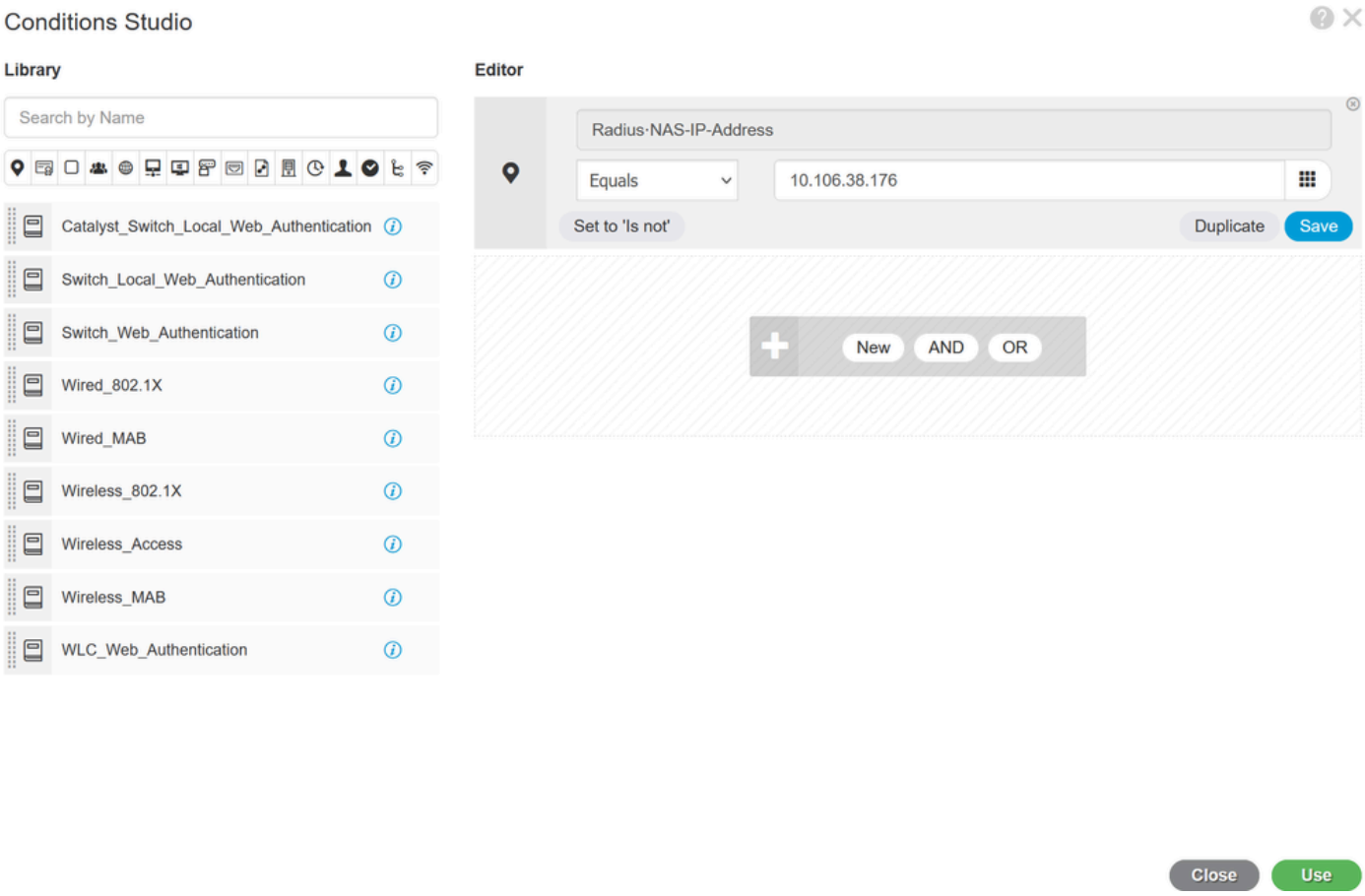


ISEでのポリシーセットの追加

ステップ 8.1： 新しい行がポリシーセットの先頭に配置されます。

新しいポリシーに名前を付け、SWAのIPアドレスと一致するようにRADIUS NAS-IP-Address属性の条件を追加します。

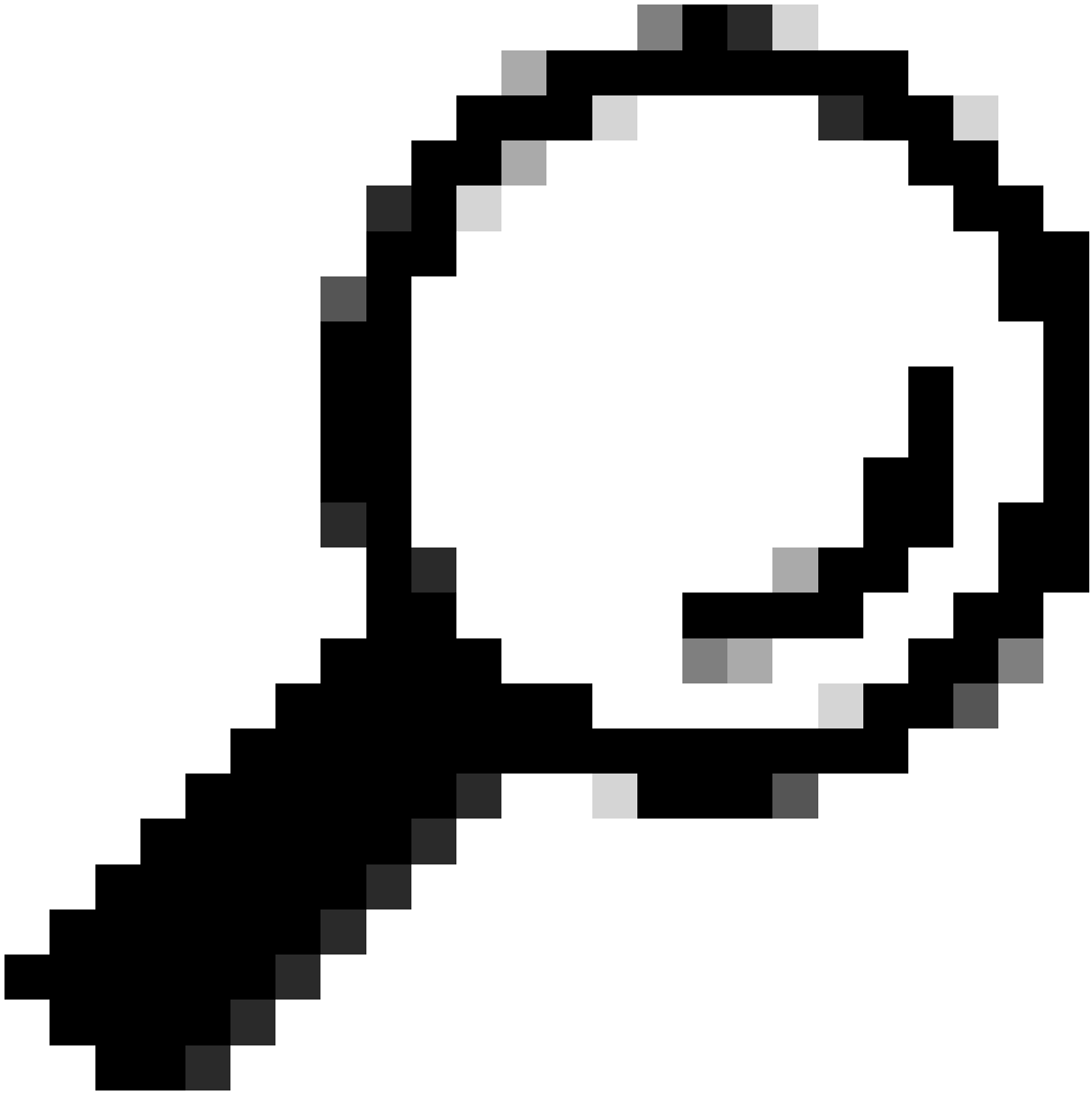
Useをクリックして変更を保存し、エディタを終了します。



マップSWAネットワークデバイスへのポリシーの追加

ステップ 8.2：[Save] をクリックします。

ポリシーの保存



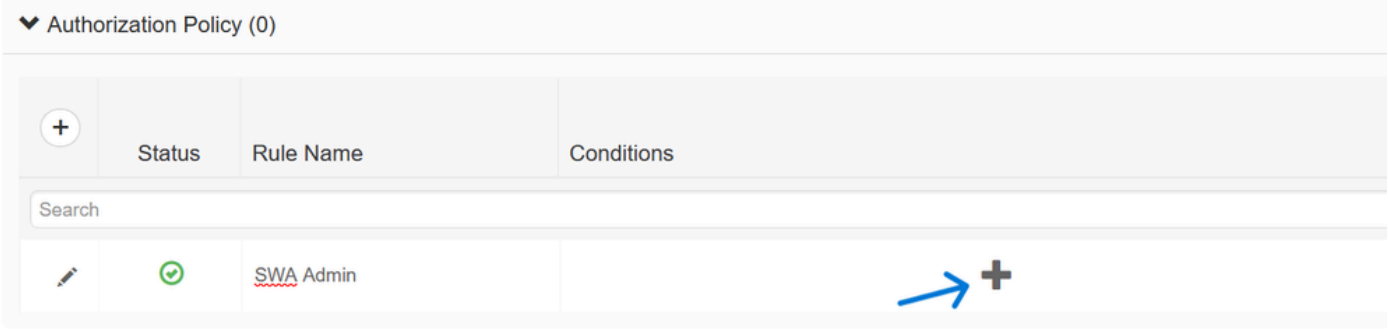
ヒント：この記事では、デフォルトのネットワークアクセスプロトコルリストが許可されています。新しいリストを作成し、必要に応じて絞り込むことができます。

ステップ 9：新しいポリシーセットを表示するには、表示列の>アイコンをクリックします。Authorization Policyメニューを展開し、+アイコンをクリックして、管理者権限を持つユーザへのアクセスを許可する新しいルールを追加します。

名前を設定します。

ステップ 9.1：管理者ユーザグループに一致する条件を作成するには、+アイコンをクリックします。

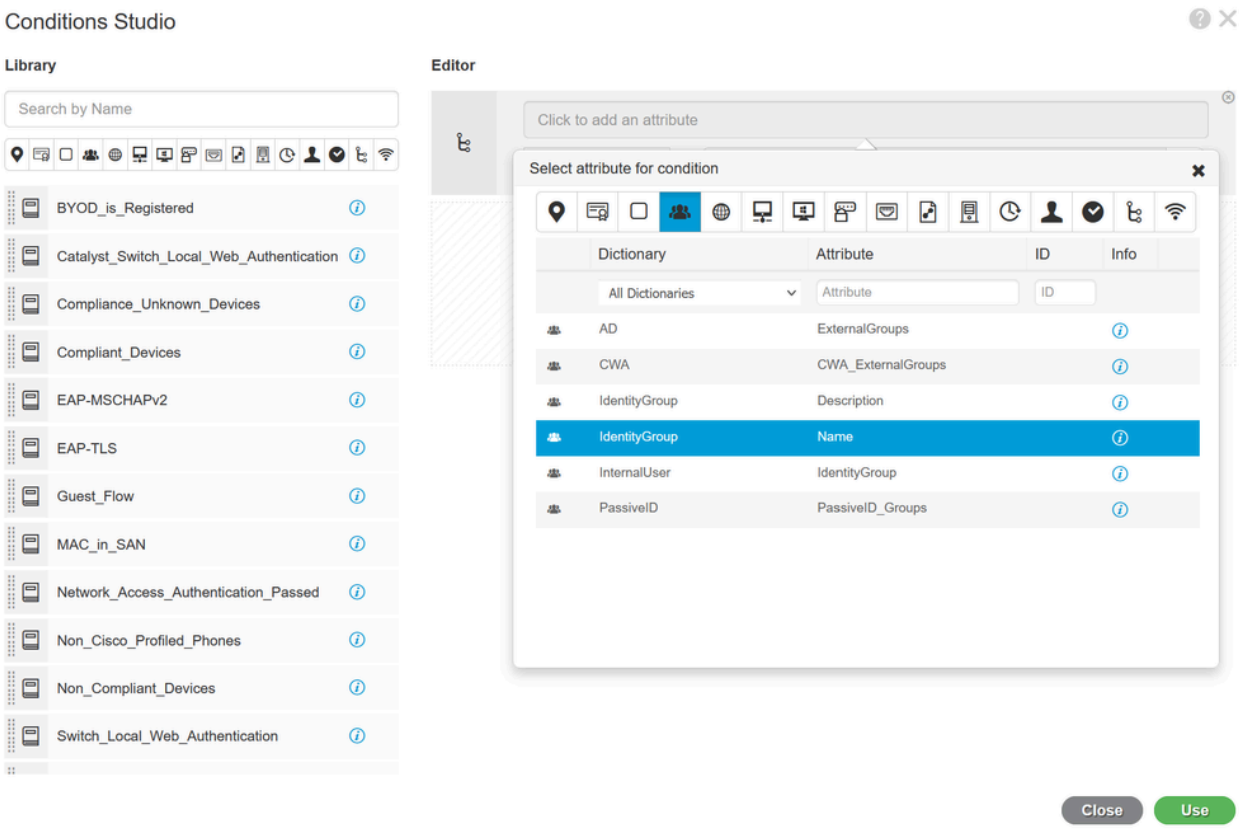
許可ポリシー条件の追



加

ステップ 9.2：条件を、Dictionary Identity Group with Attribute Name Equals User Identity Groups: SWA admin.

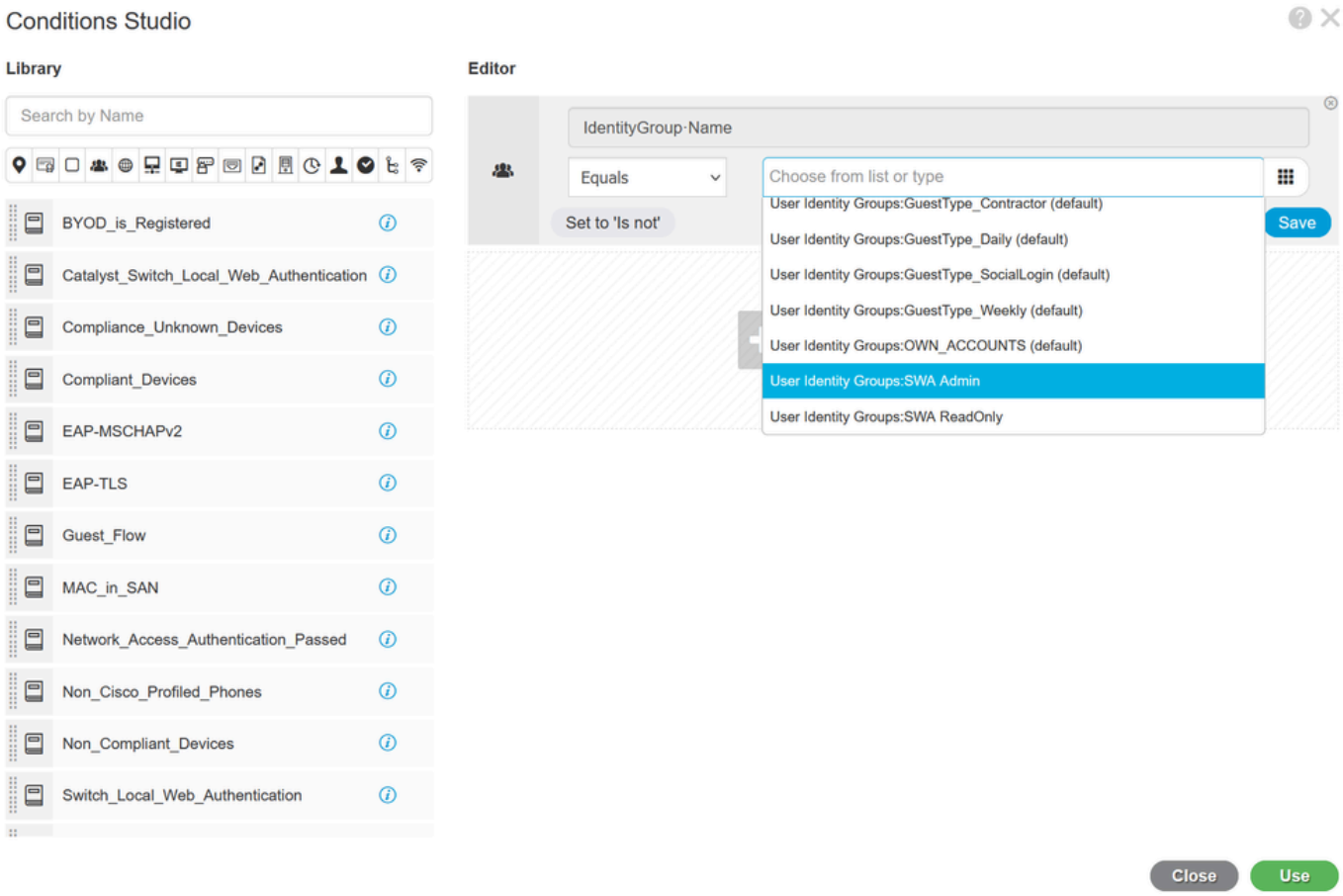
Select Identity Group as Condition



に設定します。

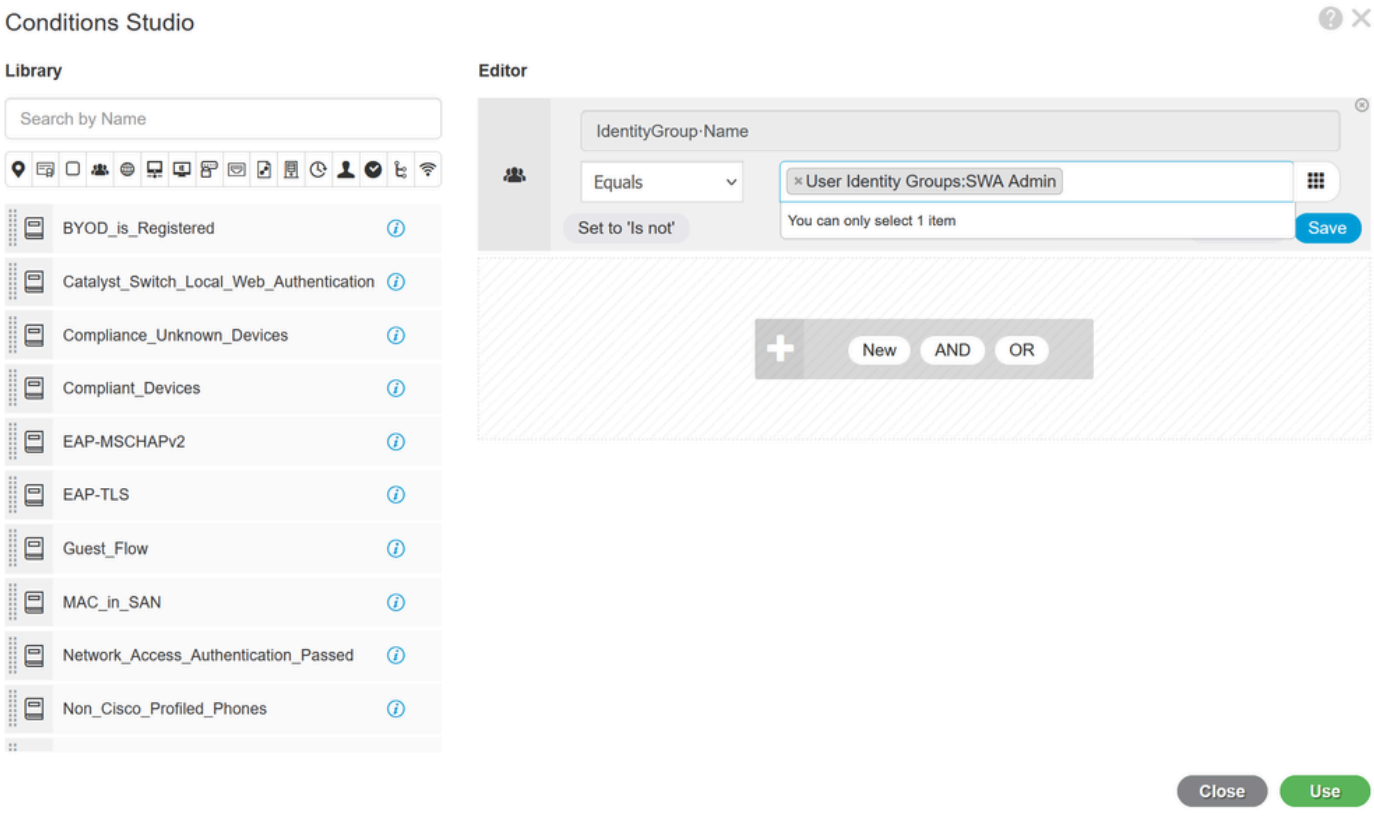
ステップ 9.3：下にスクロールしてUser Identity Groups: SWA adminを選択します。

下にスクロールして



Identity Group Nameを選択します。

ステップ 9.4：Useをクリックします。

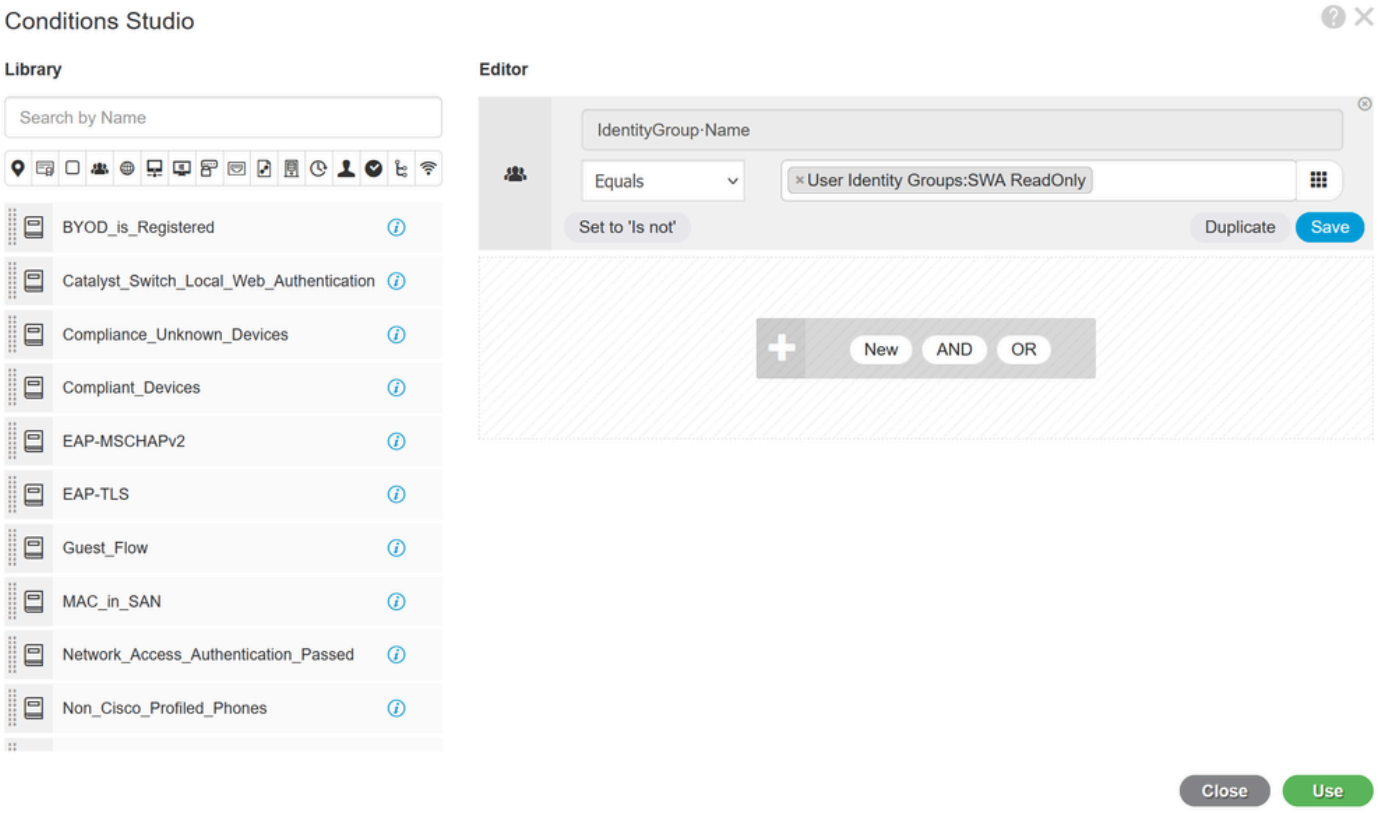


SWA管理ユーザグループの許可ポリシーの選択

ステップ 10： +アイコンをクリックして、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します。

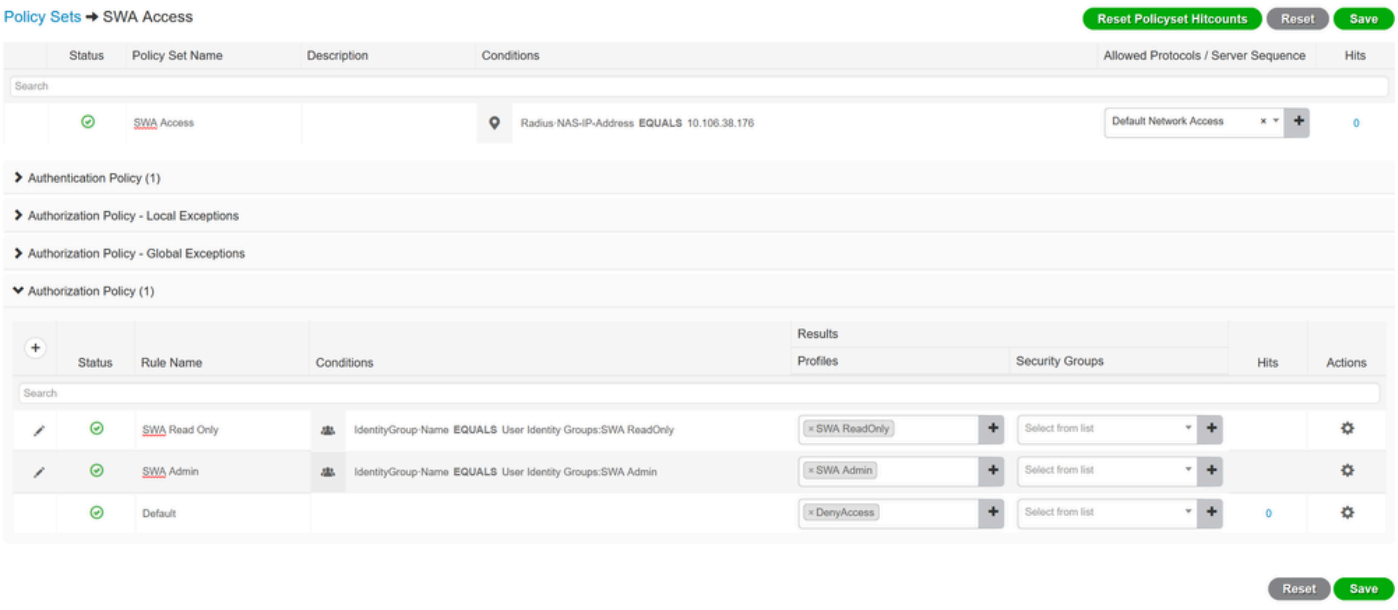
名前を設定します。

条件を、Dictionary Identity Group with Attribute Name Equals User Identity Groups: SWA ReadOnlyに一致するように設定し、Useをクリックします。



読み取り専用ユーザグループの許可ポリシーの選択

ステップ 11 ルールごとに許可プロファイルを設定し、Saveをクリックします。

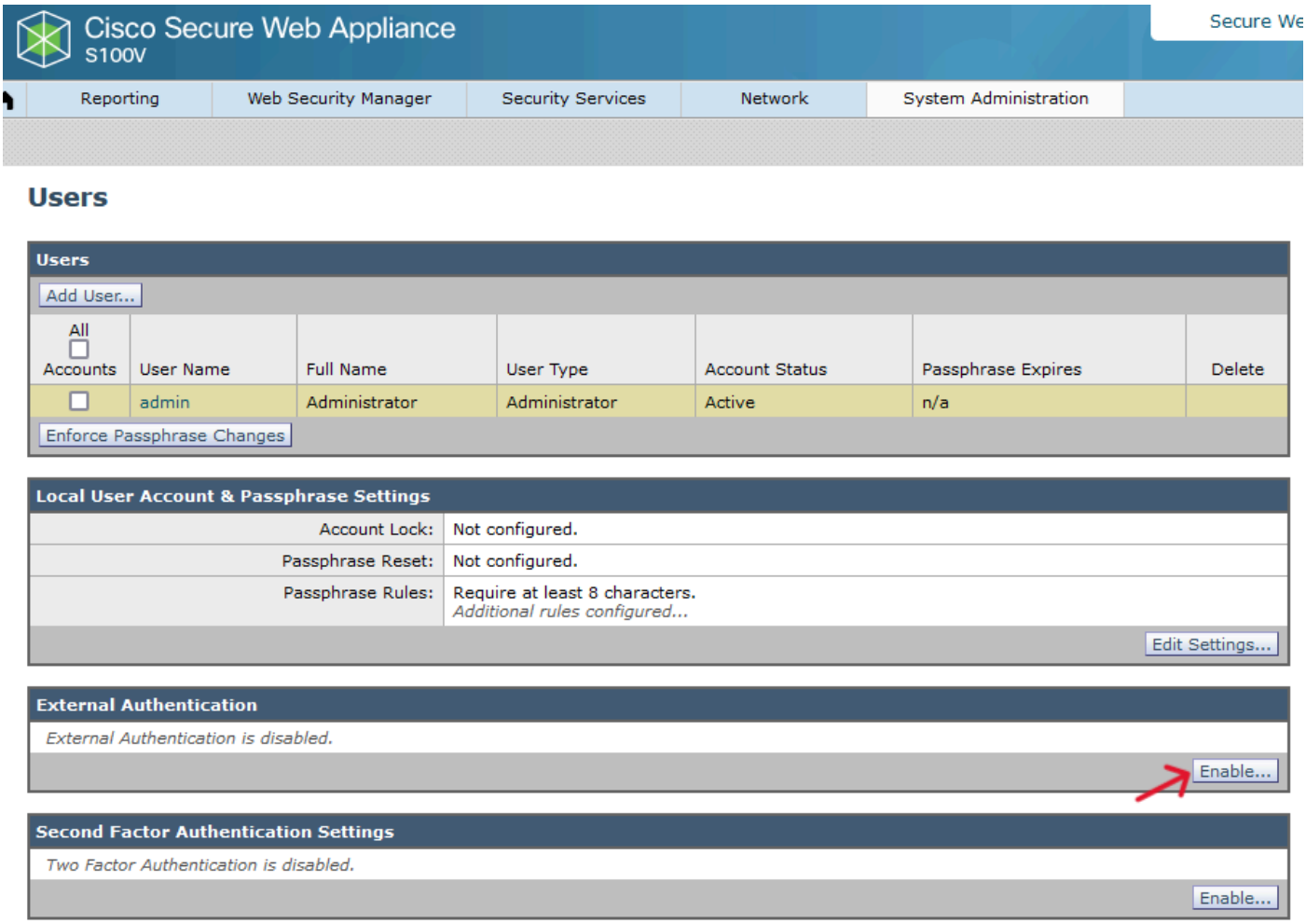


許可プロファイルの選択

SWAの設定

ステップ 1：SWAのGUIで、System Administrationに移動し、Usersをクリックします。

ステップ 2：External AuthenticationでEnableをクリックします。



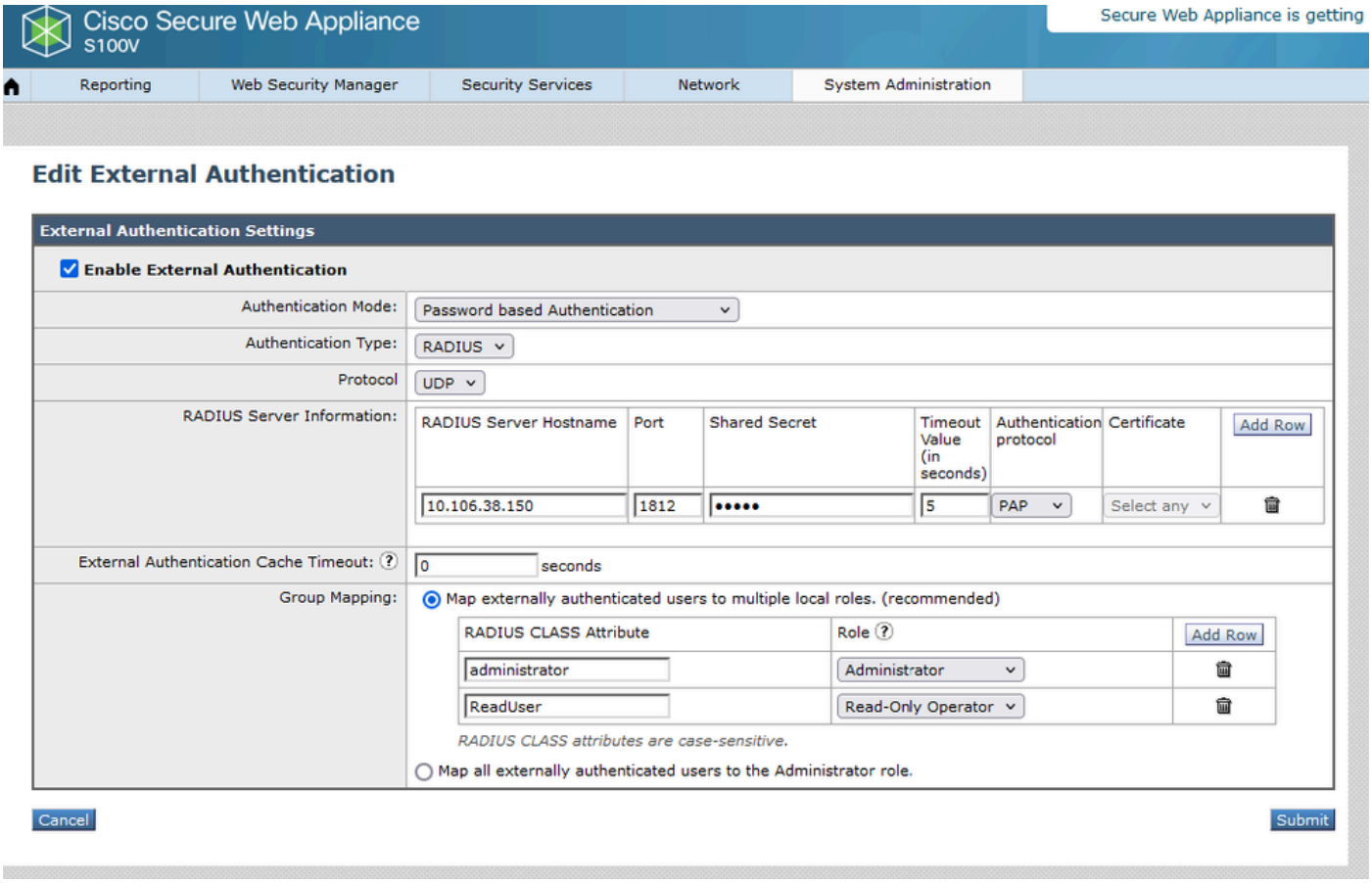
SWAでの外部認証の有効化

ステップ 3：RADIUSサーバホスト名フィールドにISEのIPアドレスまたはFQDNを入力し、ステップ2のISE設定で設定したのと同じ共有秘密を入力します。

ステップ 4：Map externally authenticated users to multiple local roles in Group Mappingを選択します。

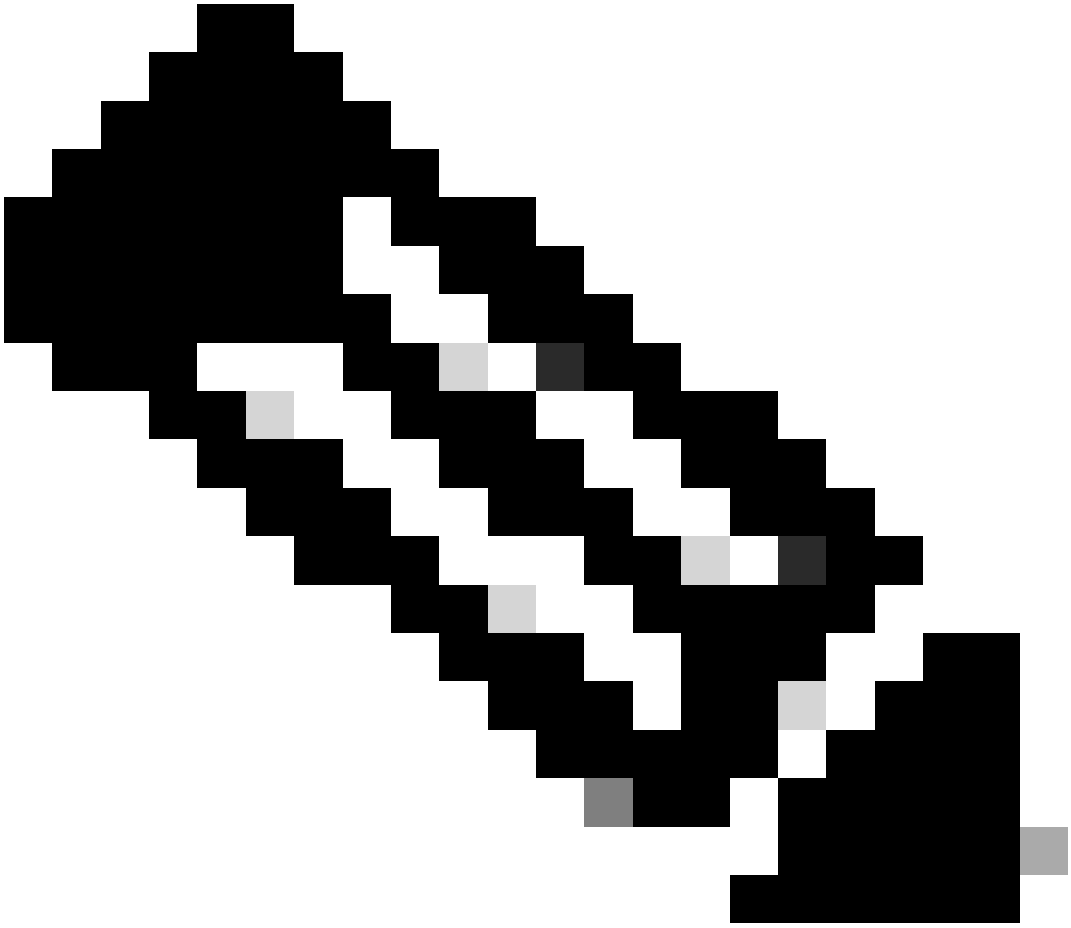
ステップ 4.1：RADIUS CLASS Attributeフィールドに Administratorと入力し、Role Administratorを選択します。

ステップ 4.2：RADIUS CLASS AttributeフィールドにReadUserと入力し、Role Read-Only Operatorを選択します。



RADIUSサーバの外部認証設定

ステップ5:SWAでユーザを設定するには、ユーザの追加をクリックします。ユーザ名を入力し、目的のロールに必要なユーザタイプを選択します。パスフレーズと再入力：パスフレーズを入力します。これは、アプライアンスが外部RADIUSサーバに接続できない場合にGUIアクセスに必要です。



注：アプライアンスが外部サーバに接続できない場合、アプライアンスはユーザをセキュアWebアプライアンスで定義されているローカルユーザとして認証しようとします。

Users

Users

Add User...

** When RADIUS external authentication is enabled, all local user accounts except "admin" are disabled. If all RADIUS services fail, local user accounts will be used for authentication.*

All Accounts	User Name	Full Name	User Type*	Account Status	Passphrase Expires	Delete
☐	adminuser	Admin User	*Administrator*	Active	n/a	🗑
☐	rouser	RO User	*Read-Only Operator*	Active	n/a	🗑

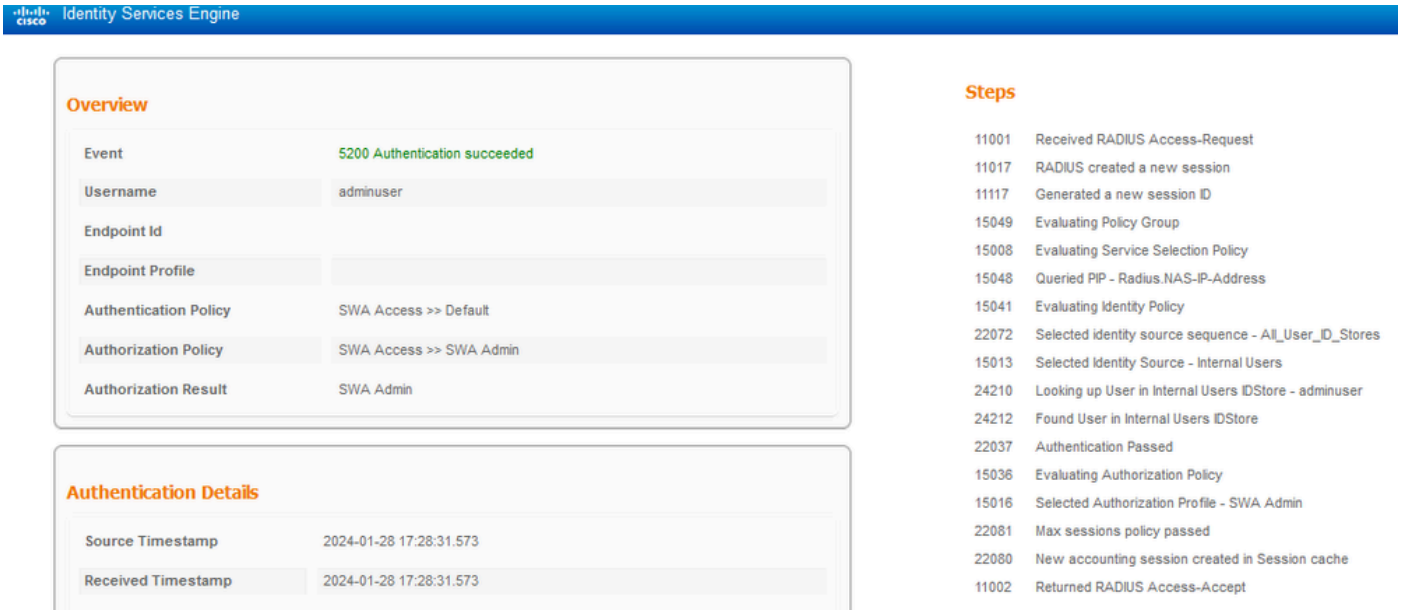
SWAでのユーザ設定

ステップ6:Submitをクリックして、変更を確定します。

確認

設定されたユーザクレデンシャルでSWA GUIにアクセスし、ISEのライブログを確認します。

ISEのライブログを確認するには、Operations > Live Logsの順に移動します。



ユーザログインISEの確認

関連情報

- AsyncOS 14.0 for Cisco Secure Web Applianceユーザガイド
- ISE 3.0管理ガイド
- セキュアWebアプライアンスのISE互換性マトリックス
- シスコのテクニカルサポートとダウンロード

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。