RADIUSサーバとしてISEを使用したSWAの第2因子認証の設定

内容

はじめに

このドキュメントでは、RADIUSサーバとしてCisco Identity Service Engine(ISE)を使用して、セキュアWebアプライアンスで2番目の要素認証を設定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。

- SWA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。

- セキュアWebアプライアンス(SWA)およびCisco Identity Service Engine(ISE)管理アクセス
- ISEがActive DirectoryまたはLDAPに統合されます。
- SWAのデフォルトの「admin」アカウントを認証するために、Active Directoryまたは LDAPにユーザ名「admin」が設定されています。
- 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上の管理ユーザに対して2番目の要素認証を有効にすると、デバイスは、SWAで設定されたクレデンシャルを確認した後、2回目にユーザクレデンシャルをRADIUSサーバで確認します。

Network Topology

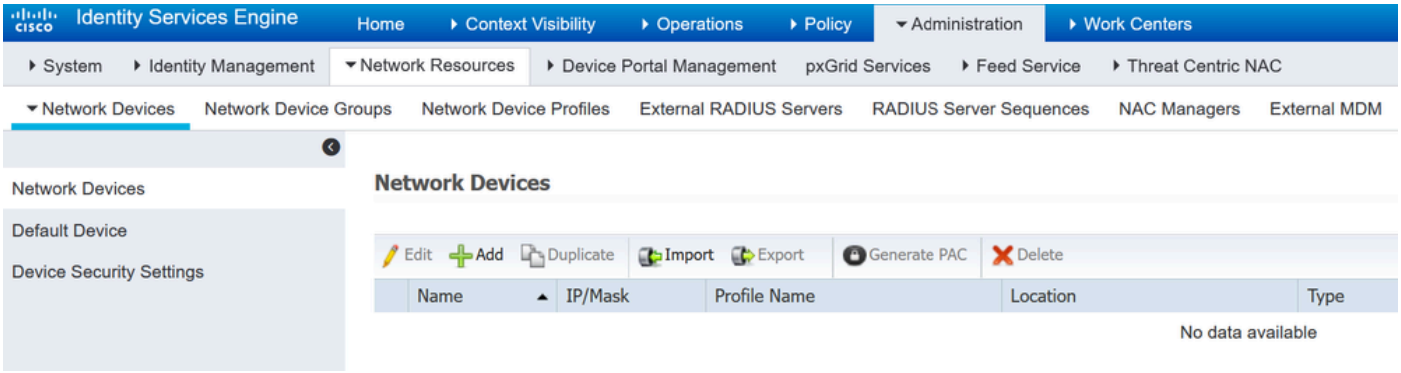
イメージ：ネットワークトポロジ図

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は、第2要素認証のためにRADIUSサーバでクレデンシャルを確認します。

設定手順

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。



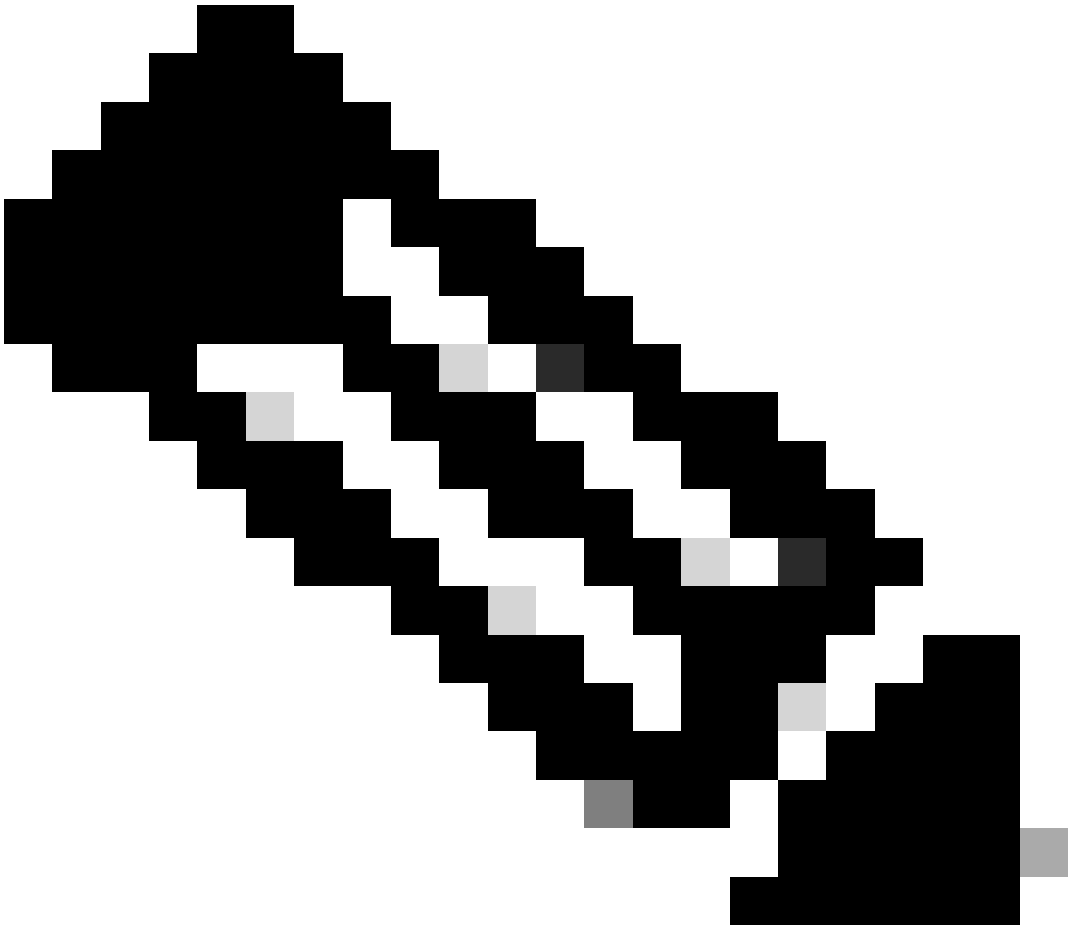
ステップ 2：ISEでネットワークデバイスを設定します。

ステップ 2.1：ネットワークデバイスオブジェクトに名前を割り当てます。

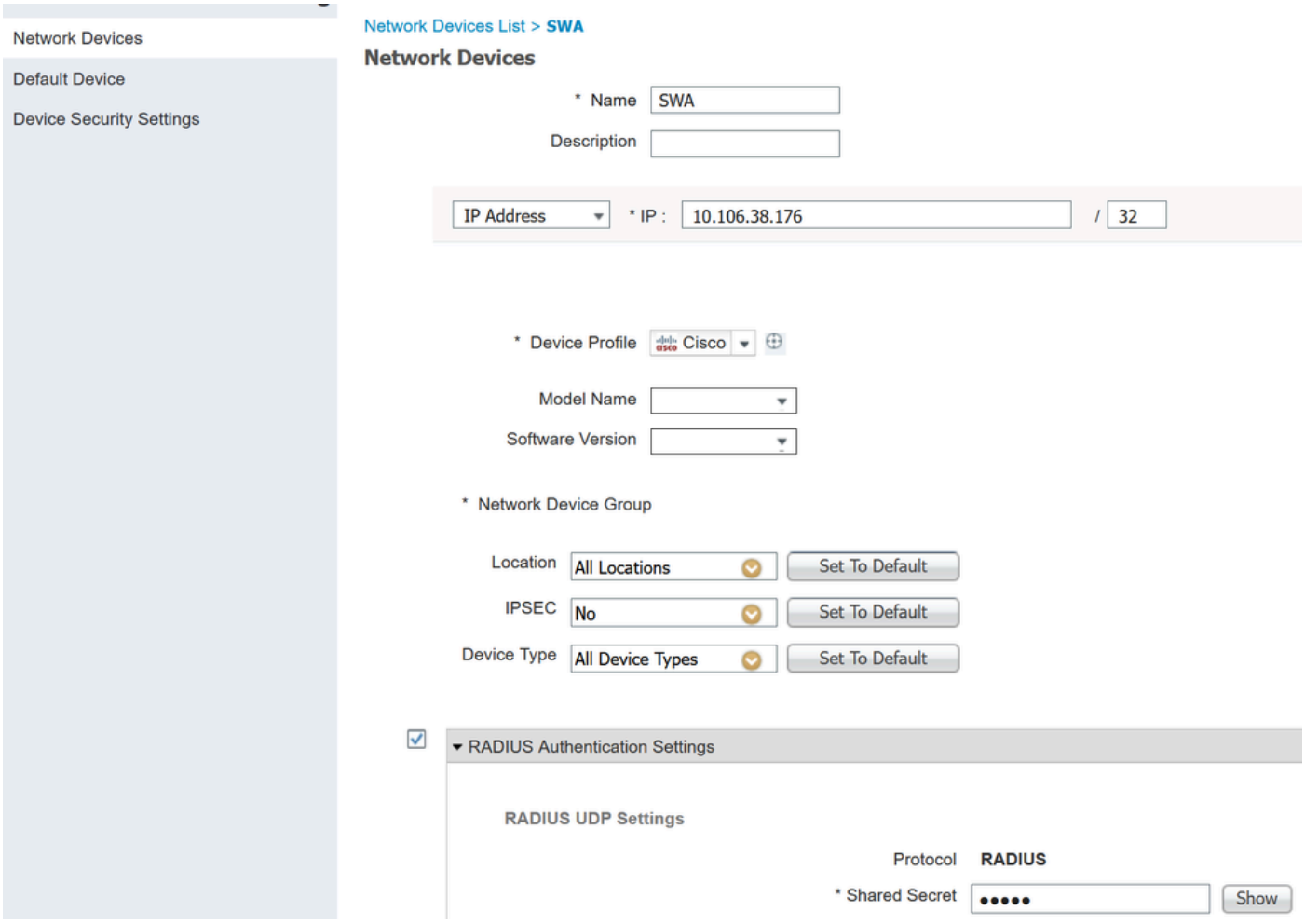
ステップ 2.2：SWAのIPアドレスを挿入します。

ステップ 2.3：RADIUSチェックボックスをオンにします。

ステップ 2.4：共有秘密を定義します。

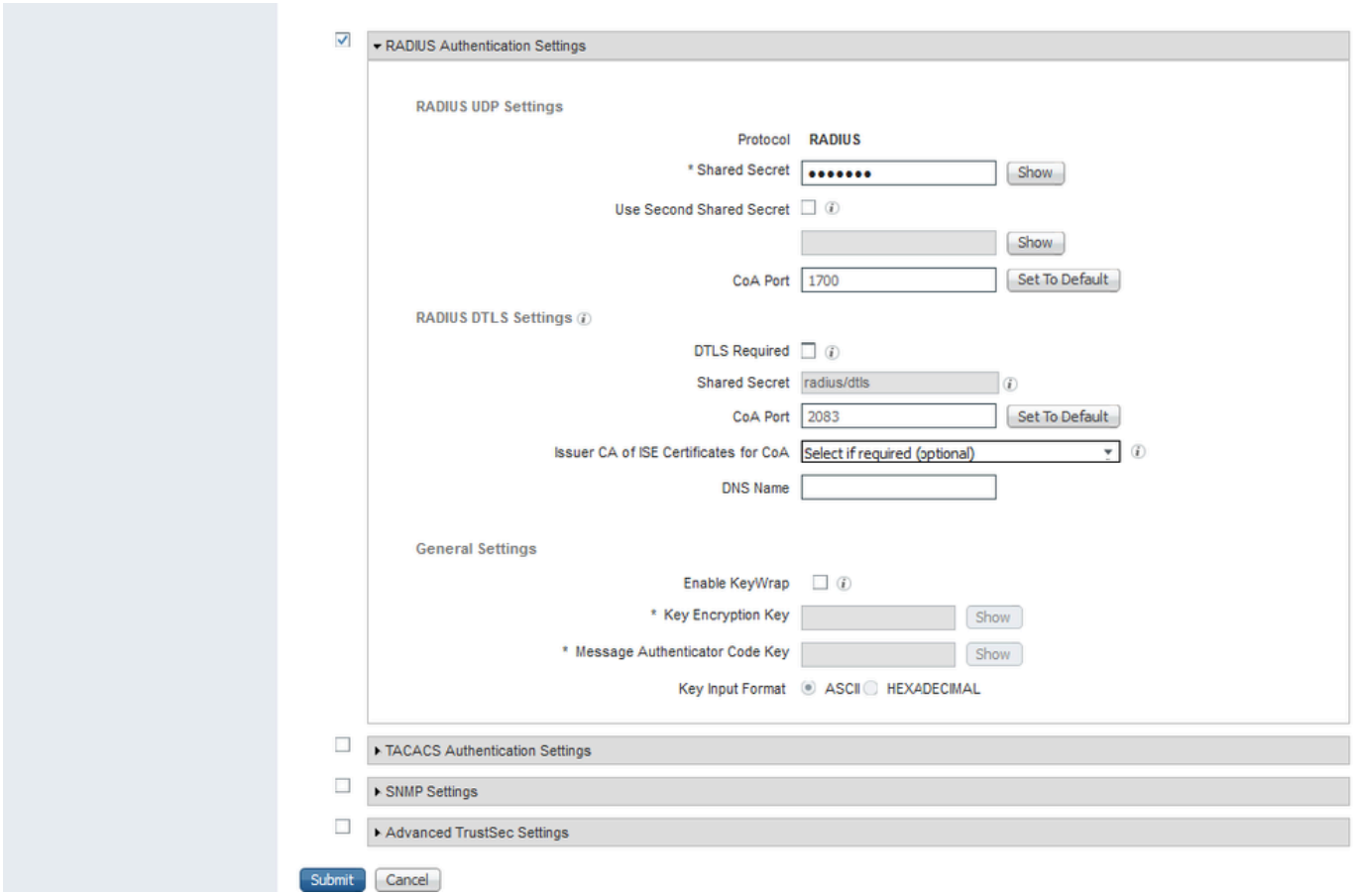


注：後でSWAを設定するときに同じキーを使用する必要があります。



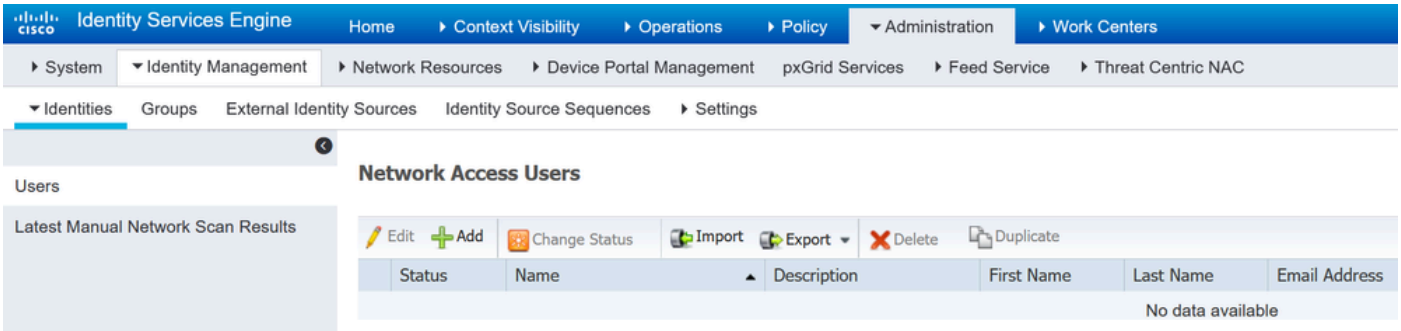
SWAネットワークデバイスの共有キーの設定

ステップ 2.5：[Submit] をクリックします。



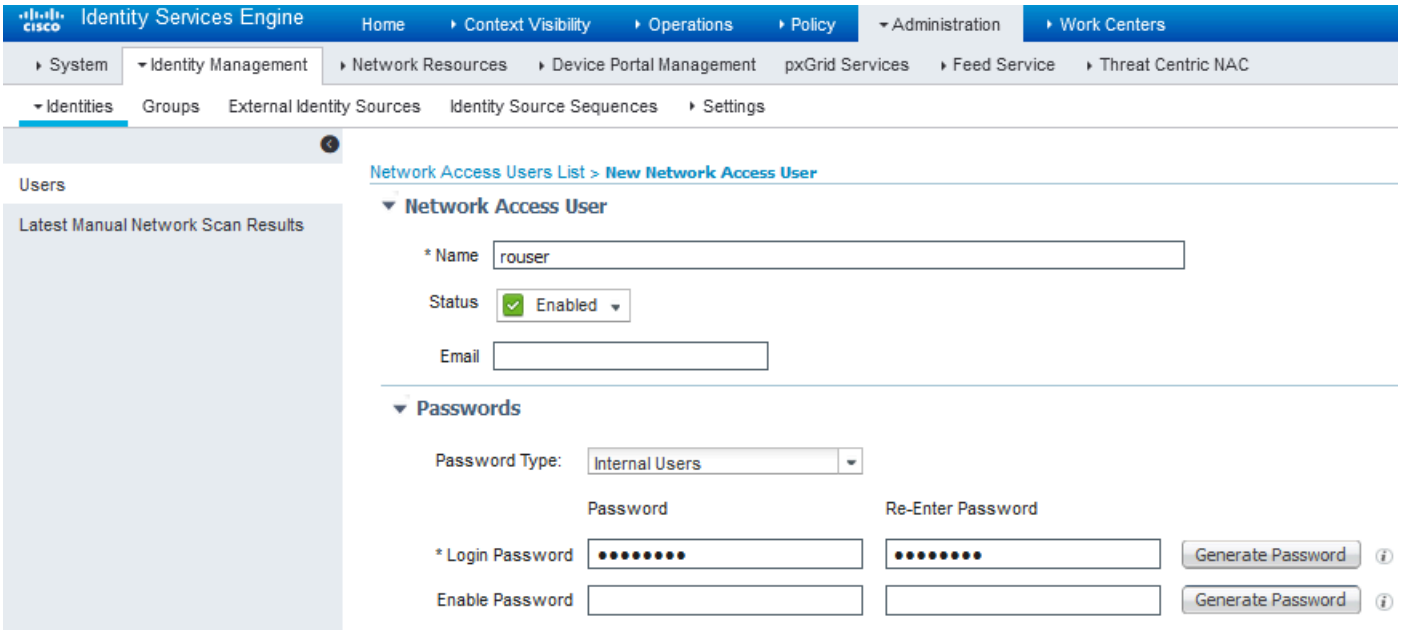
ネットワークデバイス設定の送信

ステップ 3：SWAで設定し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。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

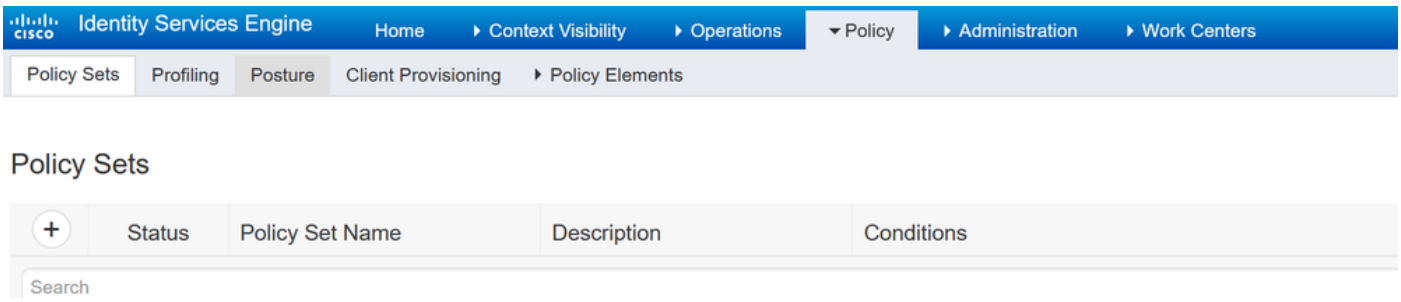
ステップ 3.1：名前を割り当てます。
ステップ3.2:（オプション）ユーザの電子メールアドレスを入力します。
ステップ 3.3：パスワードの設定.
ステップ 3.4：[Save] をクリックします。



ISEでのローカルユーザの追加

ステップ 4：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。

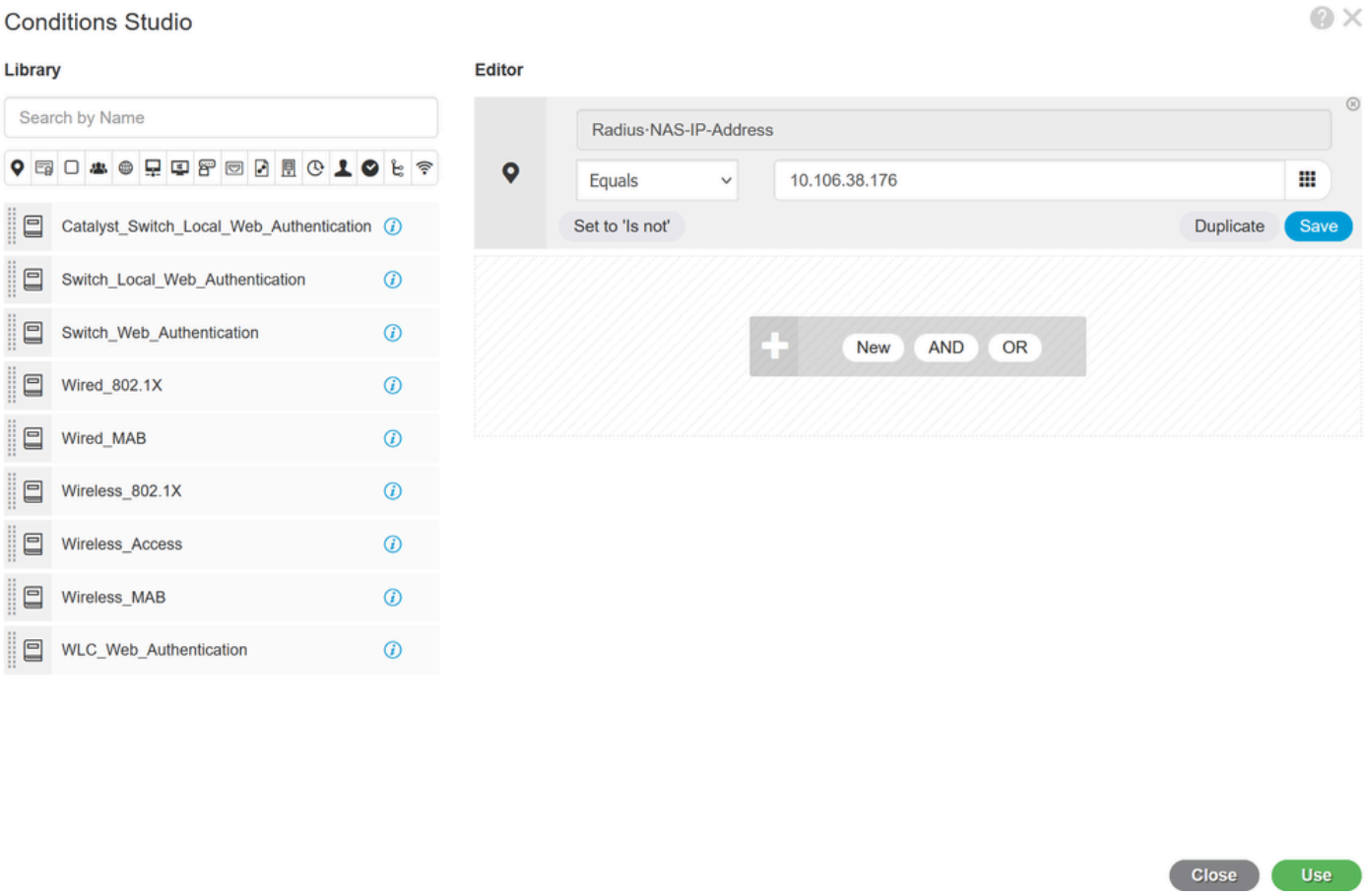


ISEでのポリシーセットの追加

ステップ 4.1： 新しい行がポリシーセットの先頭に配置されます。新しいポリシーの名前を入力します。

ステップ 4.2：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。

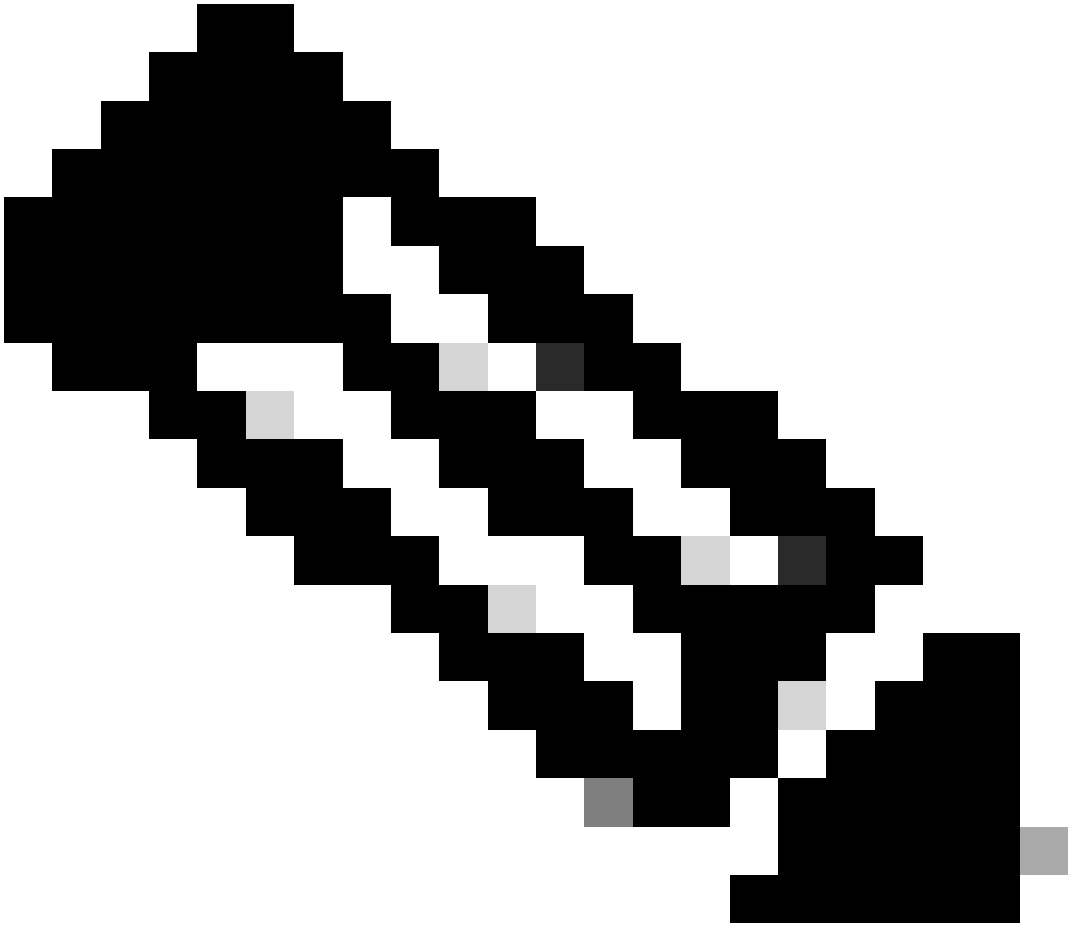
ステップ 4.3：Useをクリックして変更を保存し、エディタを終了します。



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 4.4：[Save] をクリックします。

ポリシーの保存



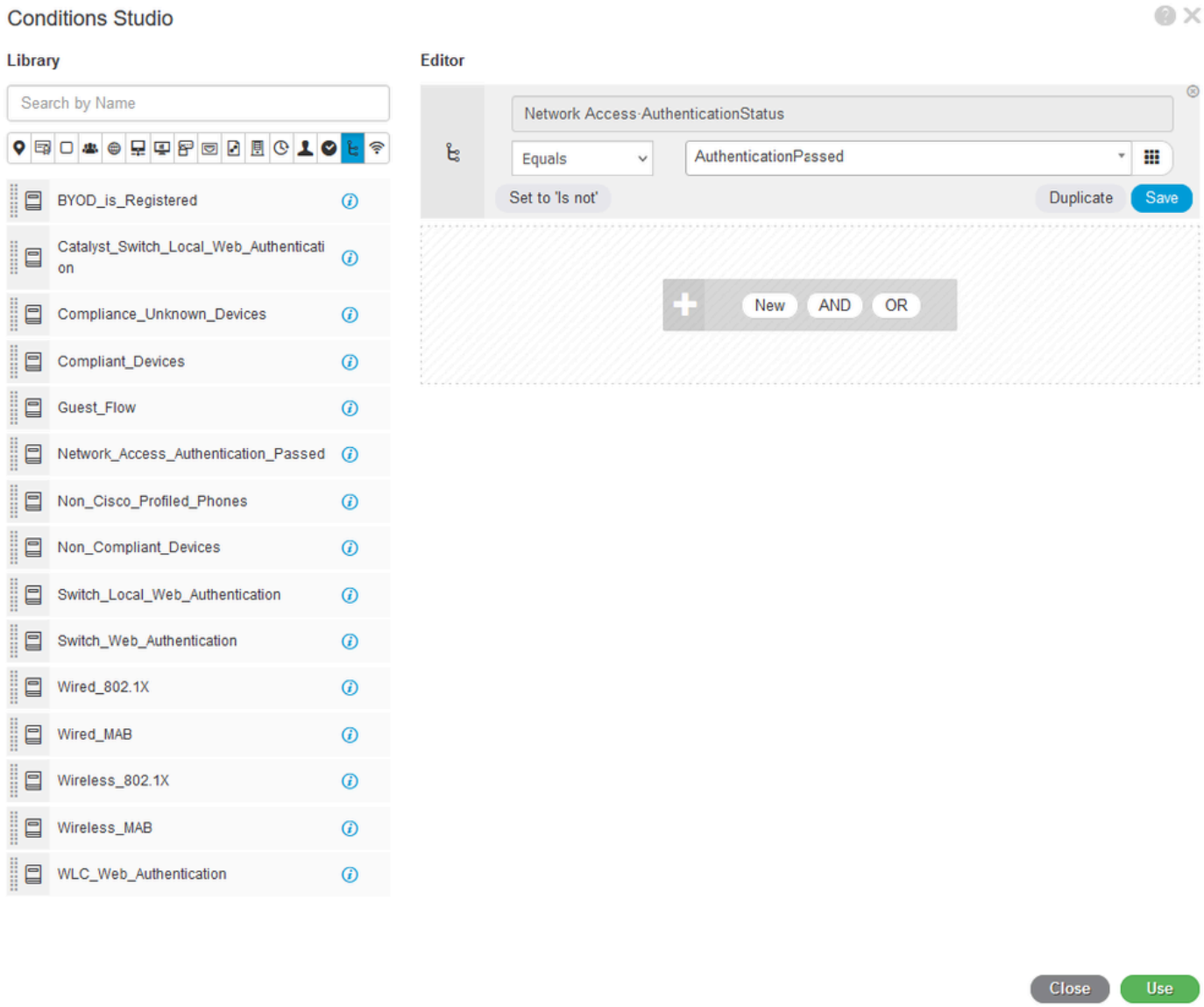
注：この例では、Default Network Access Protocolsリストを使用できます。新しいリストを作成し、必要に応じてリストを絞り込むことができます。

ステップ 5：新しいポリシーセットを表示するには、表示列の> (右矢印) アイコンをクリックします。

ステップ 5.1：Authorization Policyメニューを展開し、+アイコンをクリックして、認証されたすべての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。

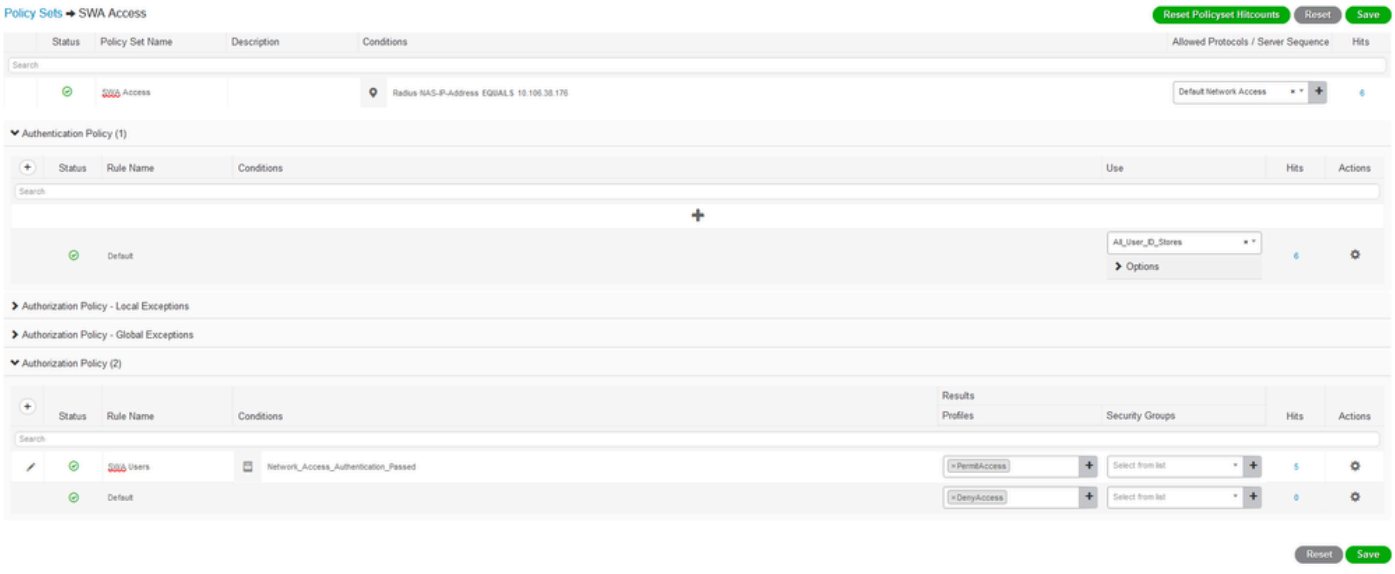
ステップ 5.2：名前を設定します。

ステップ 5.3：条件を設定して、Network Accessディクショナリと属性AuthenticationStatus Equals AuthenticationPassedが一致するようにします。次に、Useをクリックします。



許可条件の選択

手順 6： 許可プロファイルとしてデフォルトのPermitAccessを設定し、Saveをクリックします。

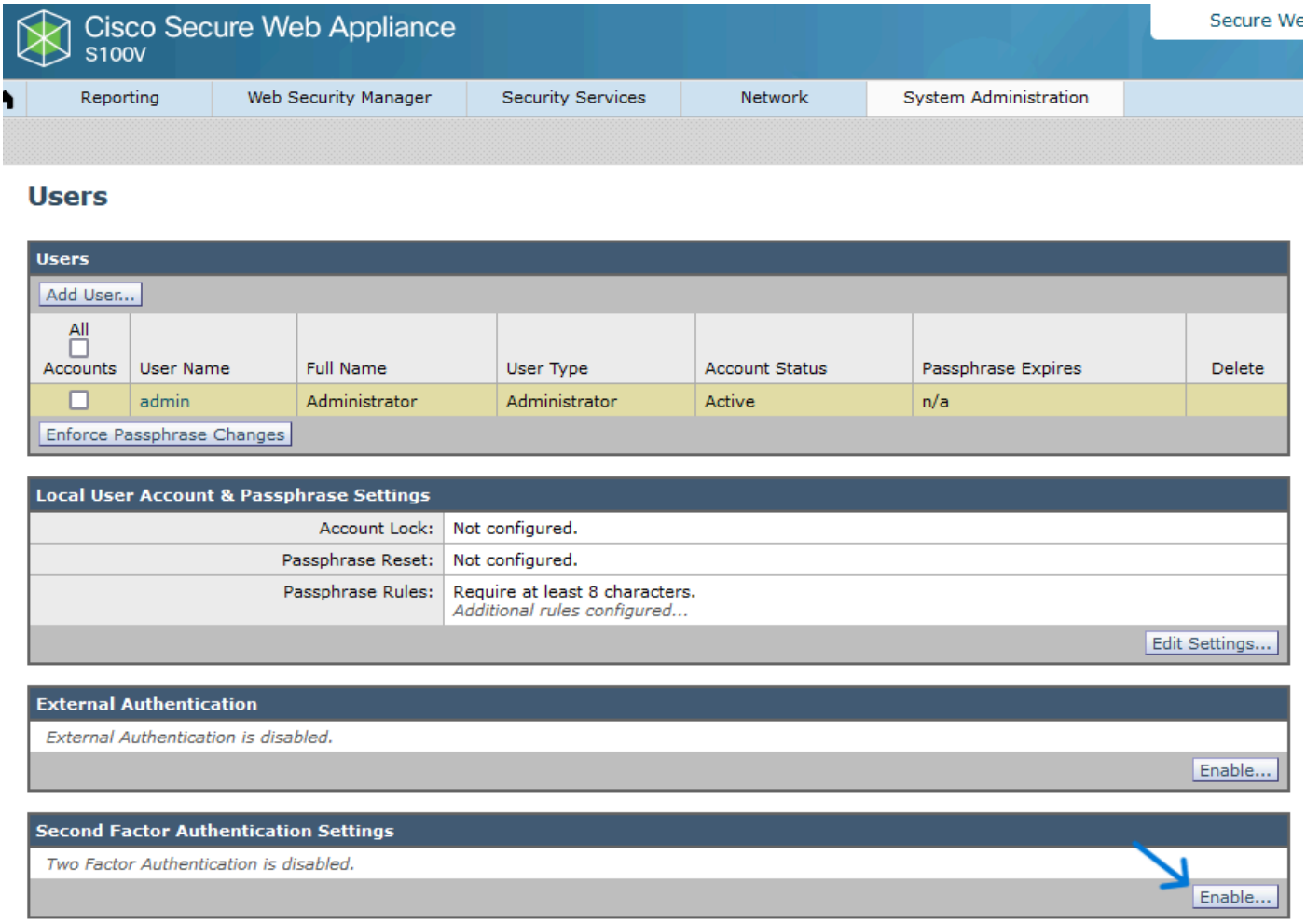


許可プロファイルの選択

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。

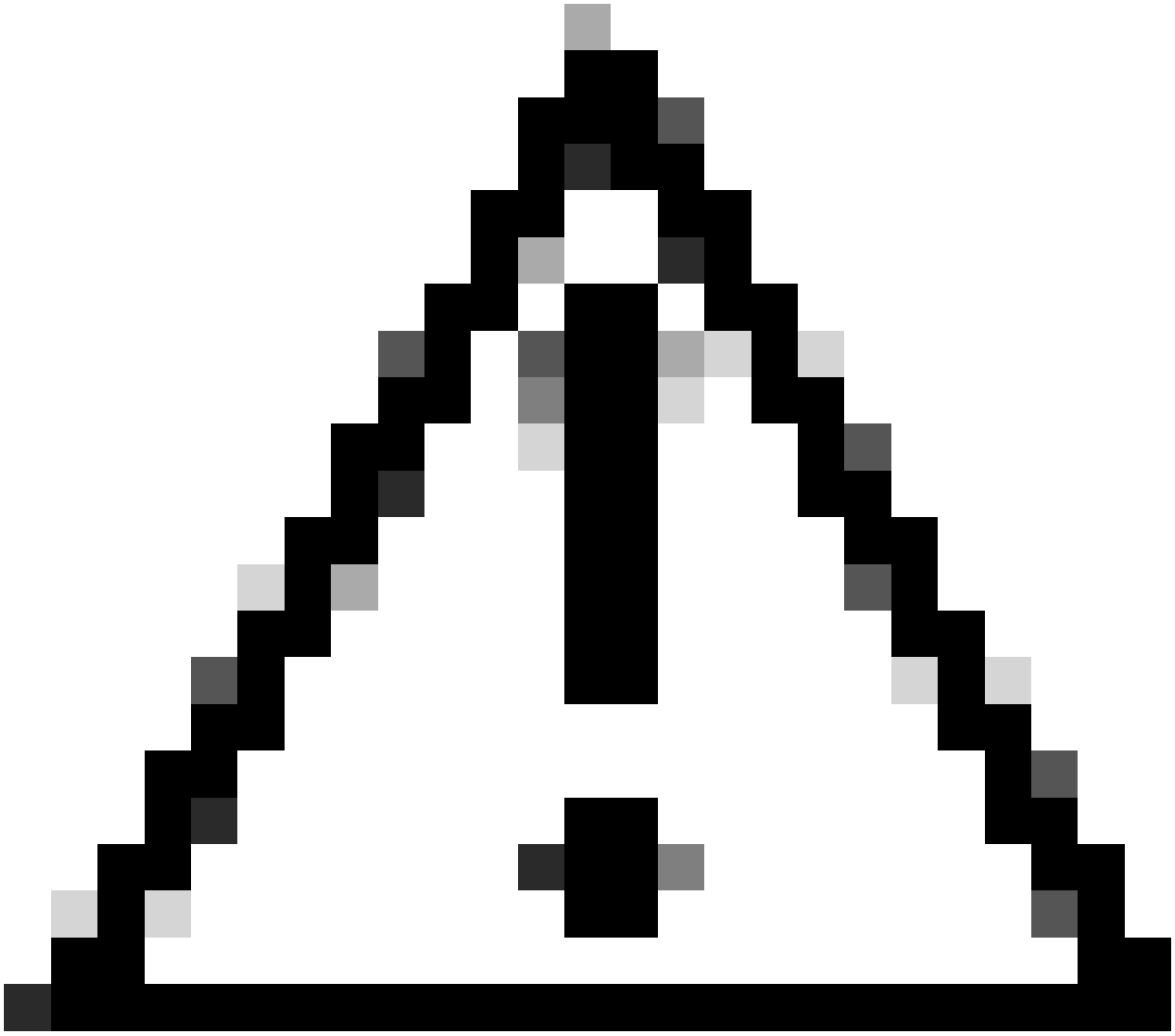
ステップ 2：Second Factor Authentication SettingsでEnableをクリックします。



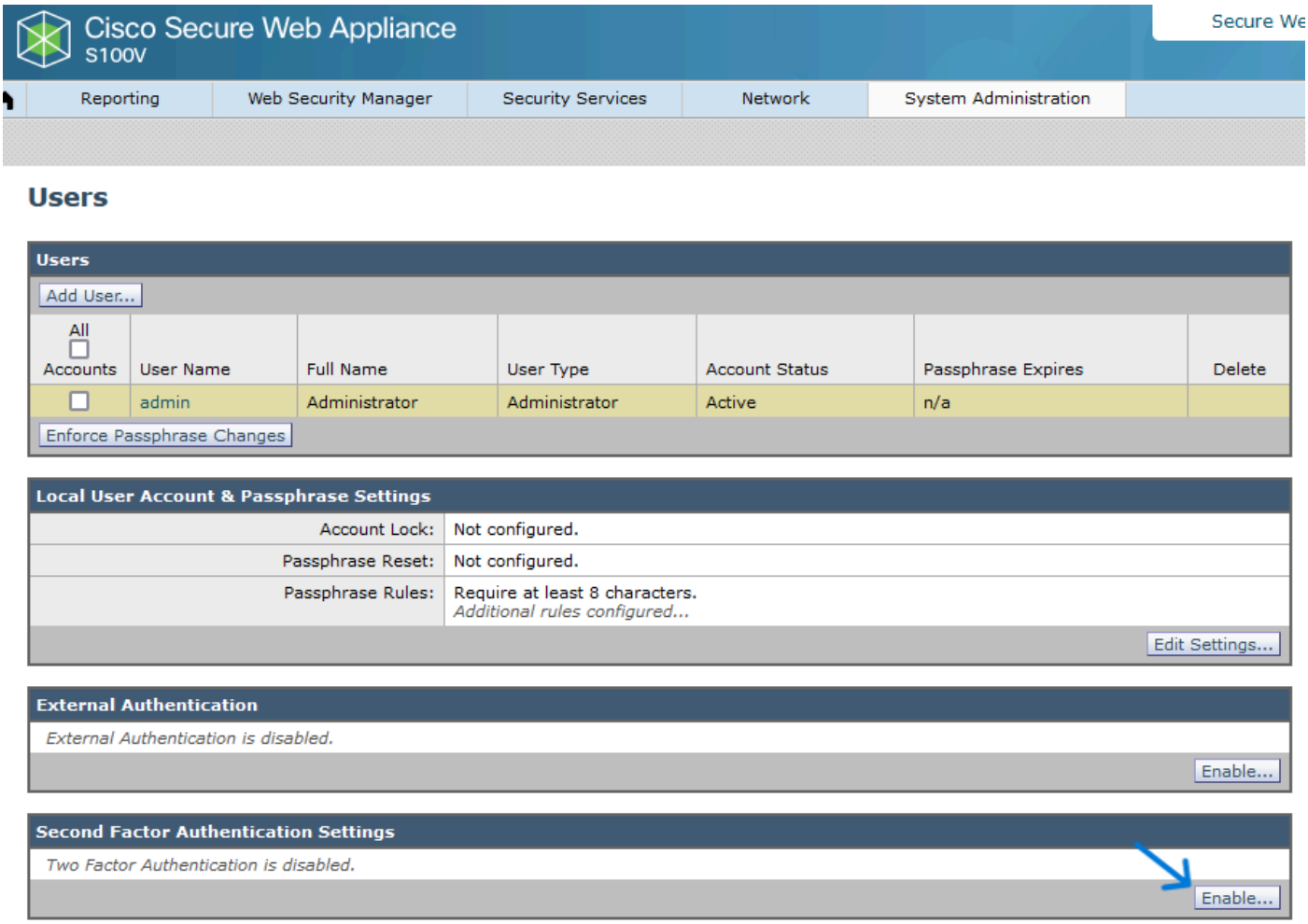
SWAで第2因子認証を有効にする

ステップ 3： RADIUS Server HostnameフィールドにISEのIPアドレスを入力し、「ISE設定」のステップ2で設定した共有秘密を入力します。

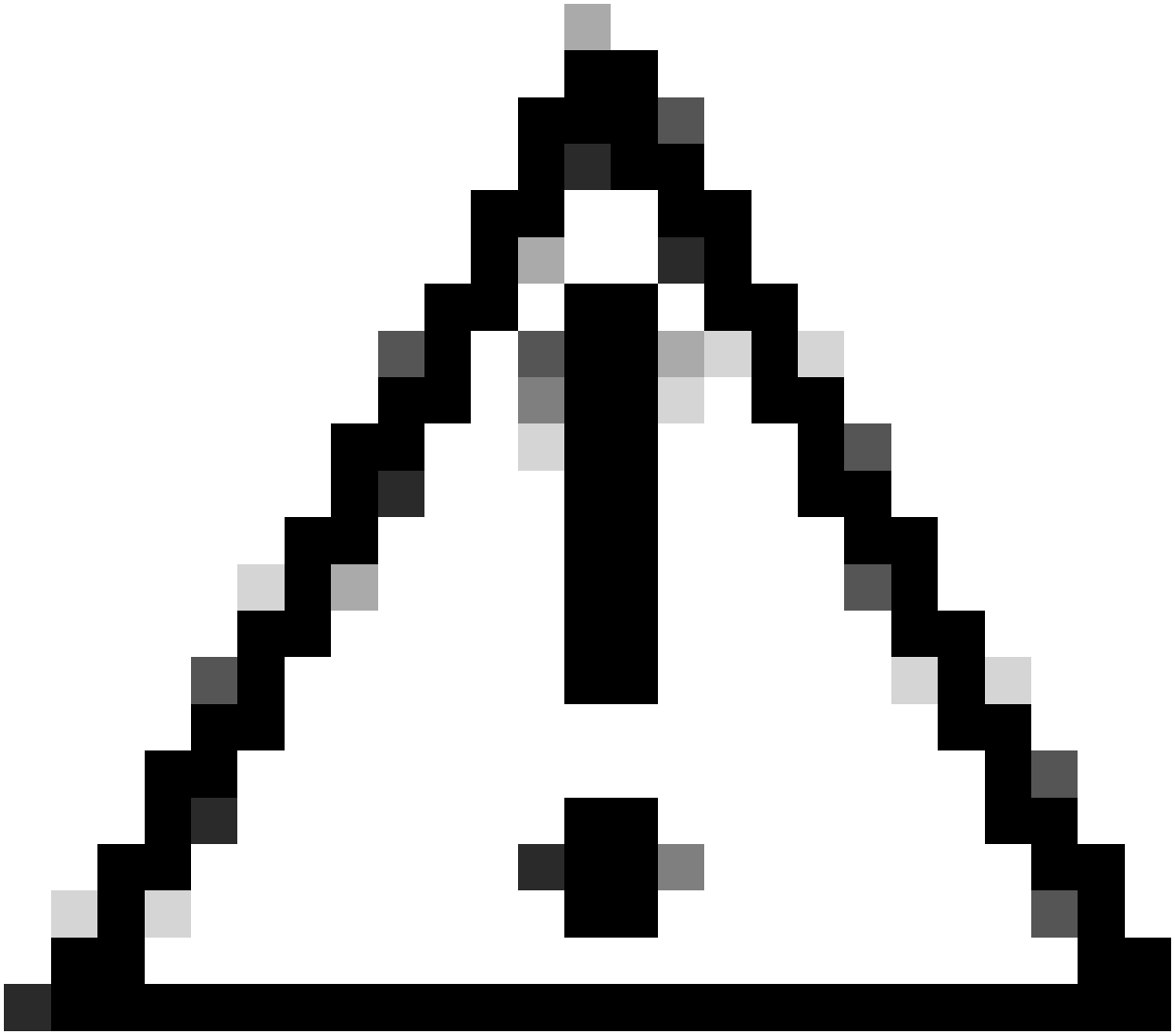
ステップ 4： Second Factor Enforcementを有効にする必要がある必須の定義済みロールを選択します。



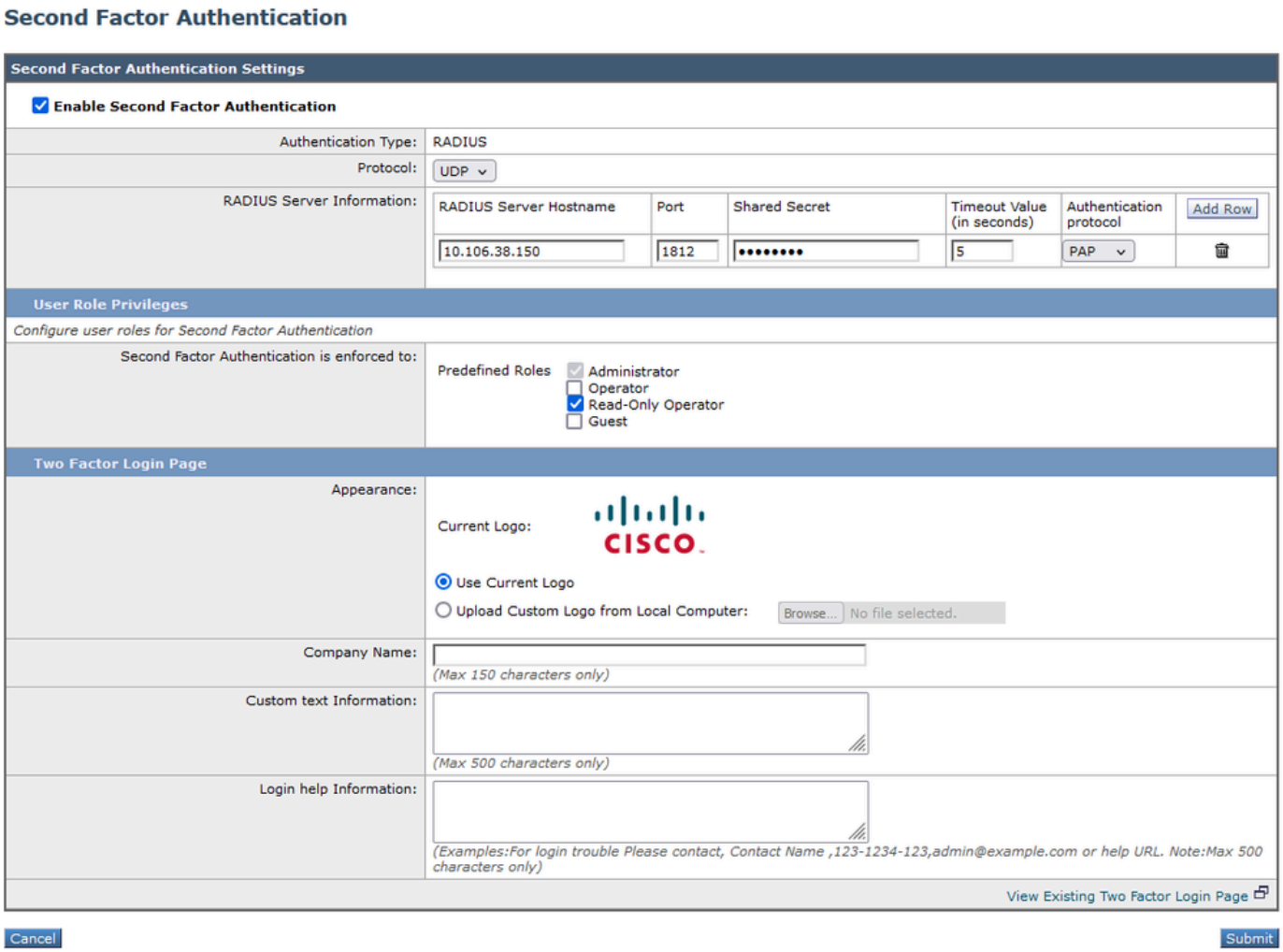
注意:SWAで2番目の要素の認証を有効にすると、デフォルトの「admin」アカウントも2番目の要素の適用により有効になります。ISEではネットワークアクセスユーザとして「admin」を設定できないため、ISEをLDAPまたはActive Directory(AD)と統合して「admin」クレデンシャルを認証する必要があります。



SWAで第2因子認証を有効にする

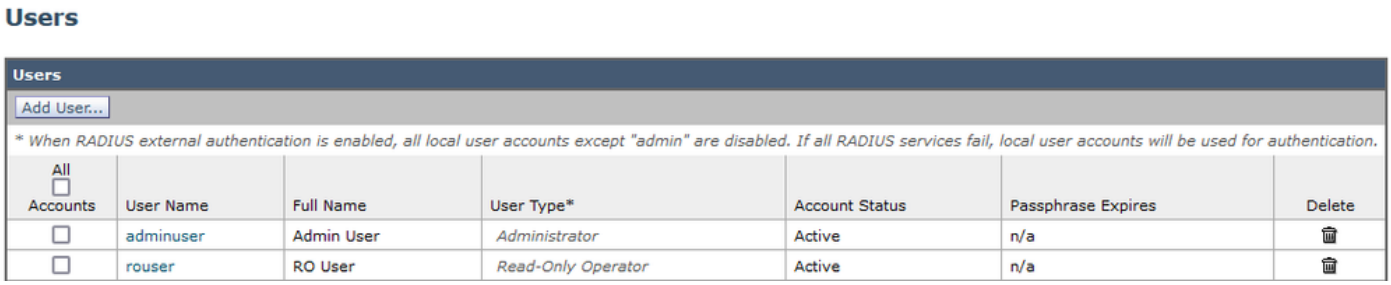


注意:SWAで2番目の要素の認証を有効にすると、デフォルトの「admin」アカウントも2番目の要素の適用により有効になります。ISEではネットワークアクセスユーザとして「admin」を設定できないため、ISEをLDAPまたはActive Directory(AD)と統合して「admin」クレデンシャルを認証する必要があります。



第2因子認証の設定

ステップ5:SWAでユーザを設定するには、Add User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。Passphraseと入力して、Passphraseを再入力します。

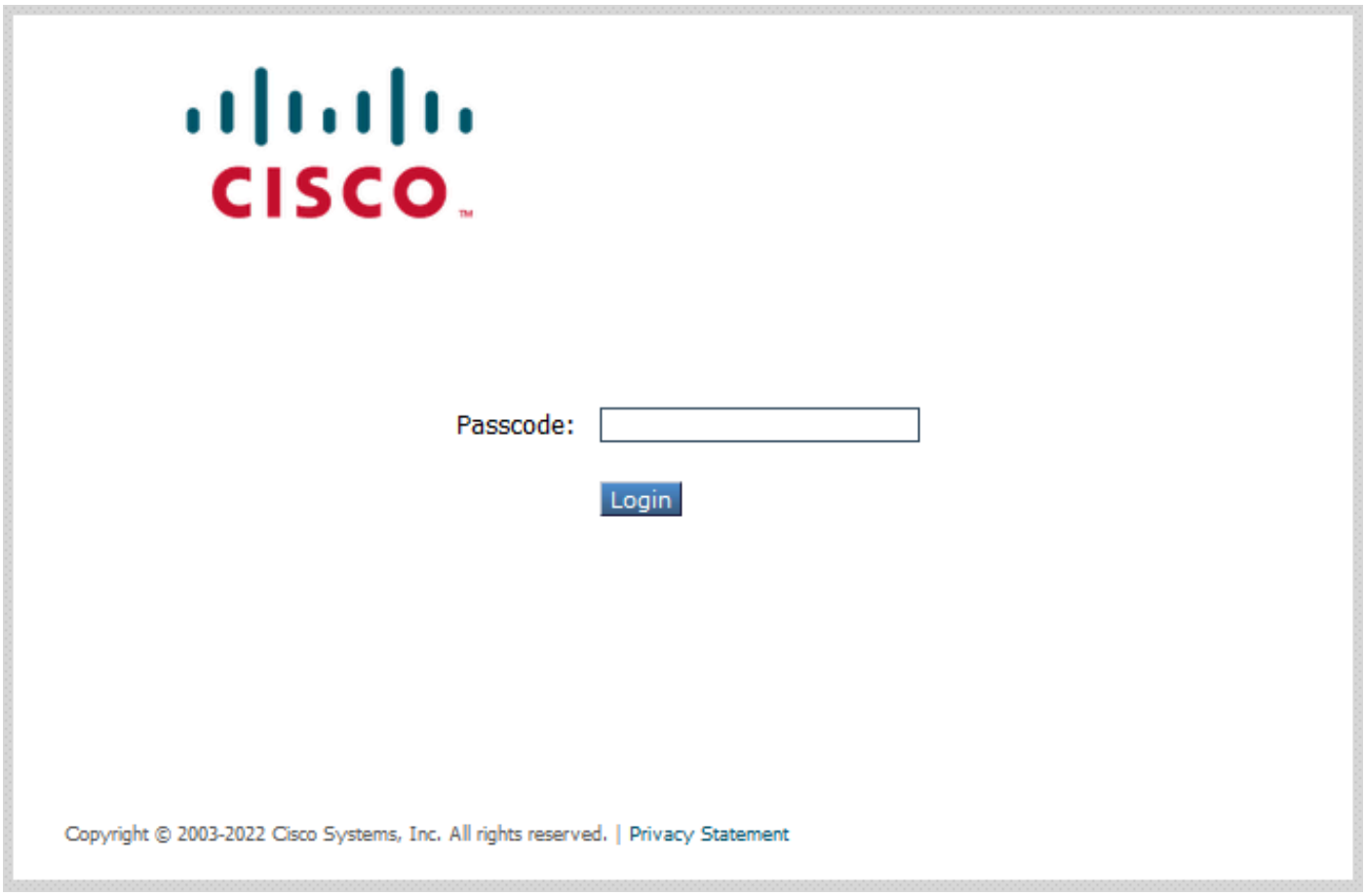


SWAでのユーザ設定

ステップ6:Submitをクリックして、変更を確定します。

確認

設定済みのユーザクレデンシャルを使用してSWA GUIにアクセスします。認証に成功すると、セカンダリ認証ページにリダイレクトされます。ここでは、ISEで設定したセカンダリ認証クレデンシャルを入力する必要があります。



2番目の要素のログインの確認

参考資料

- 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
- ISE GUIおよびCLIログイン用のADの統合

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。