FireSIGHT システムと RADIUS ユーザ認証用の ISE の統合

目次

概要

このドキュメントでは、Cisco FireSIGHT Management Center（FMC）または Firepower 管理対象デバイスを Remote Authentication Dial In User Service（RADIUS）ユーザ認証用の Cisco Identity Services Engine（ISE）と統合するために必要な設定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推奨されます。

- GUI またはシェルによる FireSIGHT システムおよび管理対象デバイスの初期設定
- 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くものです。

- Cisco ASA v9.2.1
- ASA FirePOWER モジュール v5.3.1
- ISE 1.2

本書の情報は、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、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

設定

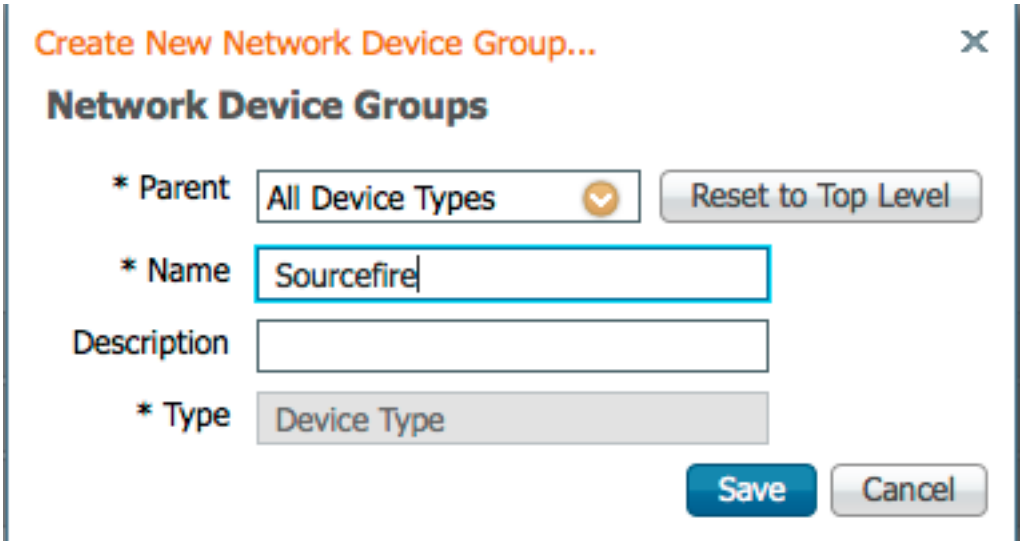
ISE 設定

> **ヒント**： ISE の認証ポリシーおよび認可ポリシーを、Sourcefire などのネットワーク アクセス デバイス（NAD）との統合をサポートするように設定する方法は複数あります。 次の例は、この統合を設定するための方法の 1 つです。 設定例は一種の評価基準であり、採用して特定の導入のニーズに合わせて変更させられます。 認可の設定は、2 つの手順のプロセスであることに注意してください。 1 つ以上の認可ポリシーを ISE で定義し、ISE に RADIUS 属性値のペア（av ペア）を FMC または管理対象デバイスに返させます。 これらの av ペアは、次に FMC システムの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されます。

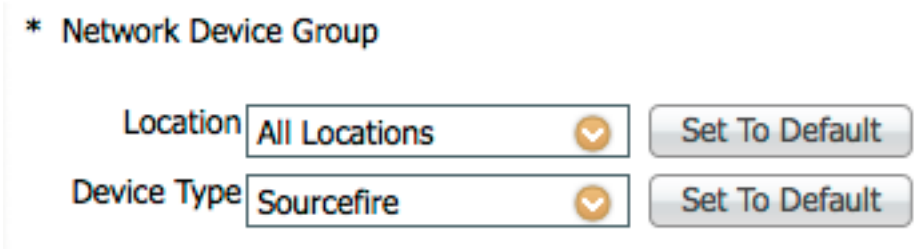
ネットワーク デバイスとネットワーク デバイス グループの設定

- ISE の GUI で、[Administration] > [Network Resources] > [Network Devices] に移動します。 [+Add] をクリックして、新しいネットワーク アクセス デバイス（NAD）を追加します。 このデバイスの説明になる名前とデバイスの IP アドレスを指定します。 次の例では、FMC が定義されています。

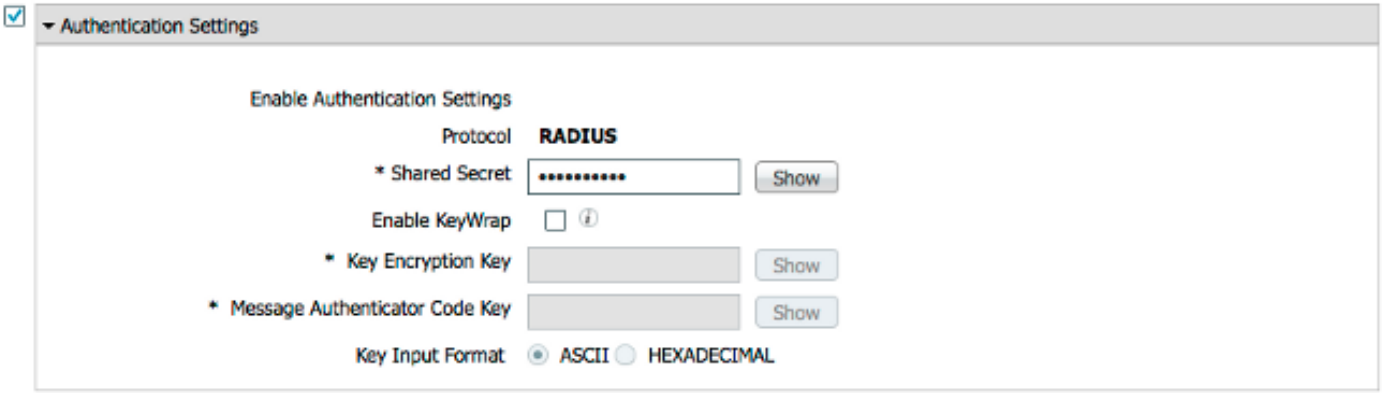
- [Network Device Groups] の下で、[All Device Types] の横の**オレンジ色の矢印**をクリックします。 アイコンを  クリックし、**新しいネットワーク デバイス グループを**『Create』 を選択 して下さい。 次のスクリーンショットの例では、[Device Type] の [Sourcefire] が設定されています。 この [Device Type] は、後の手順の認可ポリシーの規則の定義で参照されています。 [Save] をクリックします。



- **オレンジ色の矢印**を再度クリックし、上の手順で設定されたネットワーク デバイス グループを選択します



- [Authentication Settings] の横にあるチェックボックスをオンにします。 この NAD に使用する RADIUS 共有秘密キーを入力します。 同じ共有秘密キーが、後で FireSIGHT MC 上で RADIUS サーバを設定する際に再度使用されることに注意してください。 プレーン テキスト（非暗号化テキスト）のキー値を確認するには、[Show] ボタンをクリックします。 [Save] をクリックします。

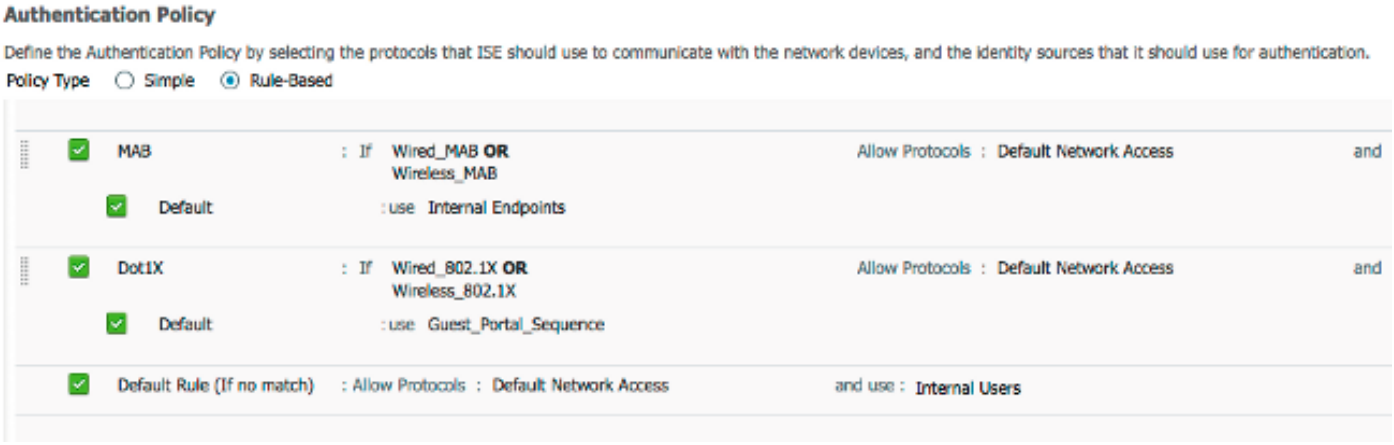


- GUI アクセスまたはシェル アクセスに RADIUS ユーザ認証または認可を必要とするすべての FireSIGHT MC と管理対象デバイスについて、上記の手順を繰り返します。

ISE 認証ポリシーの設定：

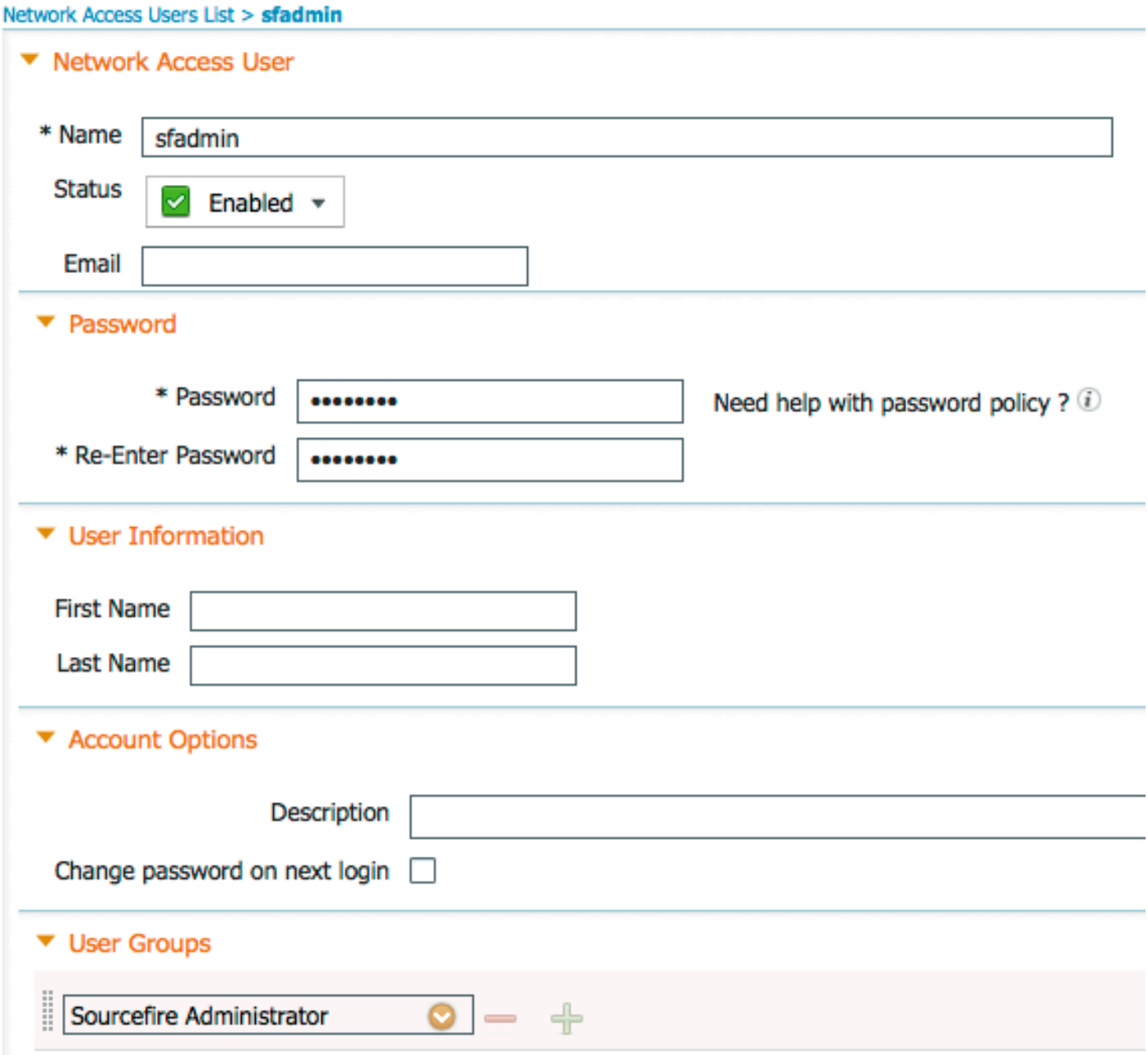
- ISE の GUI で、[Policy] > [Authentication] に移動します。 ポリシー セットを使用する場合、[Policy] > [Policy Sets] に移動します。 次の例は、デフォルトの認証ポリシー インターフェイスおよび認可ポリシー インターフェイスを使用する ISE 導入からのものです。 認証および認可規則のロジックは、設定方法に関係なく同じです。
- 使用中の方法が MAC 認証バイパス（MAB）または 802.1X でない NAD からの RADIUS 要求

を認証するために、[Default Rule（If no match）] が使用されます。 デフォルトで設定されているように、この規則では ISE のローカルの [Internal Users] ID ソース内のユーザ アカウントを検索します。 この設定は、[Administration] > [Identity Management] > [External Identity Sources] の下で定義される、Active Directory、LDAP などの外部 ID ソースを参照するように変更できます。 単純にして分かりやすくするために、次の例では ISE のローカルでユーザ アカウントを定義するため、認証ポリシーをさらに変更する必要はありません。



ISE へのローカル ユーザの追加

- [Administration] > [Identity Management] > [Identities] > [Users] の順に移動します。 [Add] をクリックします。 意味の分かりやすいユーザ名とパスワードを入力します。 [User Groups] の選択で、既存のグループ名を選択するか、または**緑の [+] 記号**をクリックして新しいグループを追加します。 次の例では、ユーザの「sfadmin」がカスタム グループの「Sourcefire Administrator」に割り当てられています。 このユーザ グループは、下の「**ISE 認可ポリシーの設定**」手順で定義される認可プロファイルにリンクされます。 [Save] をクリックします。

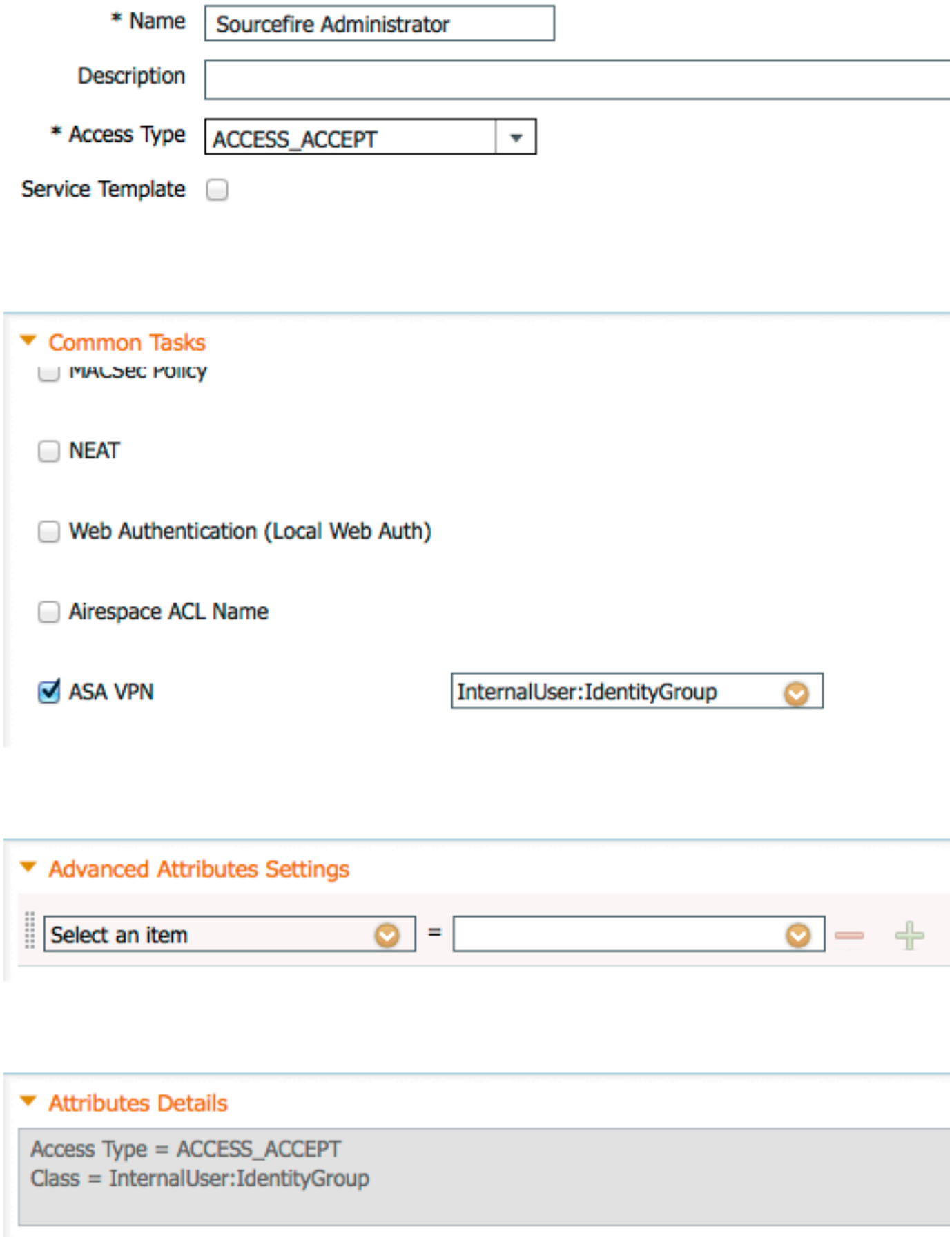


ISE 認可ポリシーの設定

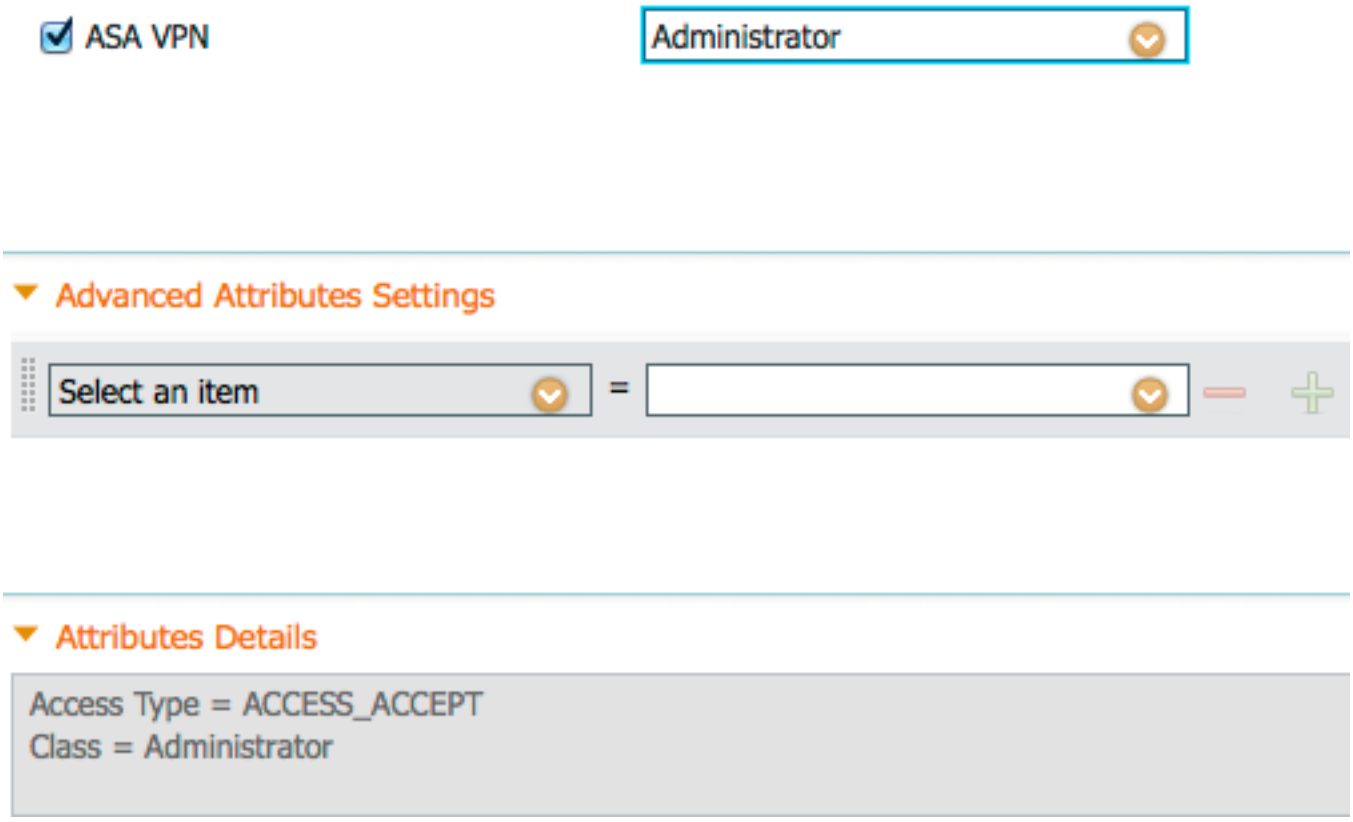
- [Policy] > [Policy Elements] > [Results] > [Authorization] > [Authorization Profiles] に移動します。 **緑の [+] 記号**をクリックして新しい認可プロファイルを追加します。
- Sourcefire Administrator のような意味の分かりやすい名前を [Name] に指定します。 [Access Type] で [ACCESS_ACCEPT] を選択します。 [Common Tasks] で、最下部までスクロールして [ASA VPN] の横のチェックボックスをオンにします。 **オレンジ色の矢印**をクリックして、[InternalUser: IdentityGroup] を選択します。 [Save] をクリックします。

  ヒント： この例では、ISE のローカルのユーザ ID ストアを使用するので、設定を単純化するために [InternalUser: IdentityGroup] グループ オプションが使用されています。 外部 ID ストアを使用する場合、ASA VPN の認可属性が引き続き使用されますが、Sourcefire デバイスに返す値は手動で設定します。 たとえば、[ASA VPN] ドロップダウン ボックスに Administrator と手動で入力すると、Sourcefire デバイスに送信される Class = Administrator という Class-25 の av ペア値が生成されます。 この値は、次にシステムのポリシー設定の一部として sourcefire のユーザ グループにマッピングできます。 内部ユーザの場合は、いずれの設定方法も許容されます。

内部ユーザの例



外部ユーザの例

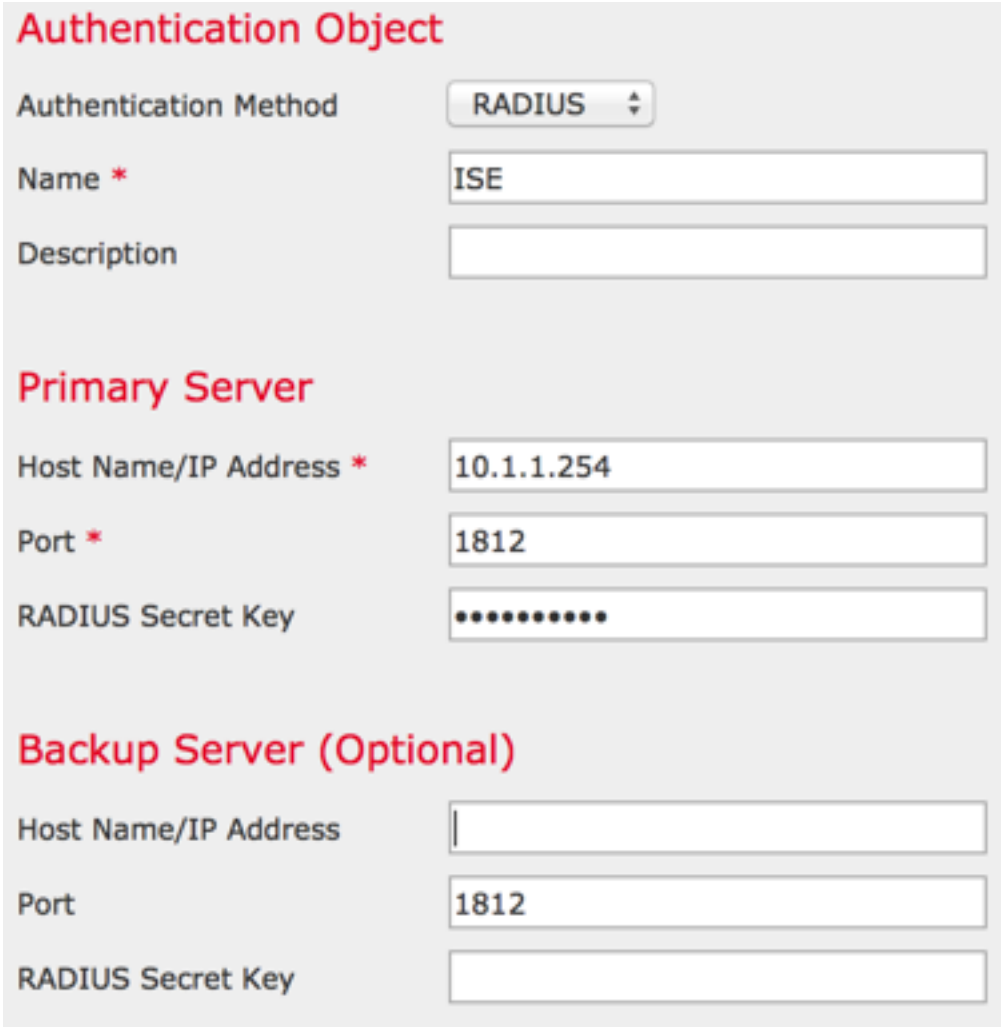


- [Policy] > [Authorization] に移動し、Sourcefire Administration のセッション用の新しい認可ポリシーを設定します。 次の例では、[DEVICE: Device Type] 条件を使用して、 上記の「**ネットワーク デバイスとネットワーク デバイス グループの設定**」セクションで設定したデバイス タイプに一致するようにしています。 このポリシーは、次に上で設定した Sourcefire Administrator 認可プロファイルに関連付けられます。 [Save] をクリックします。

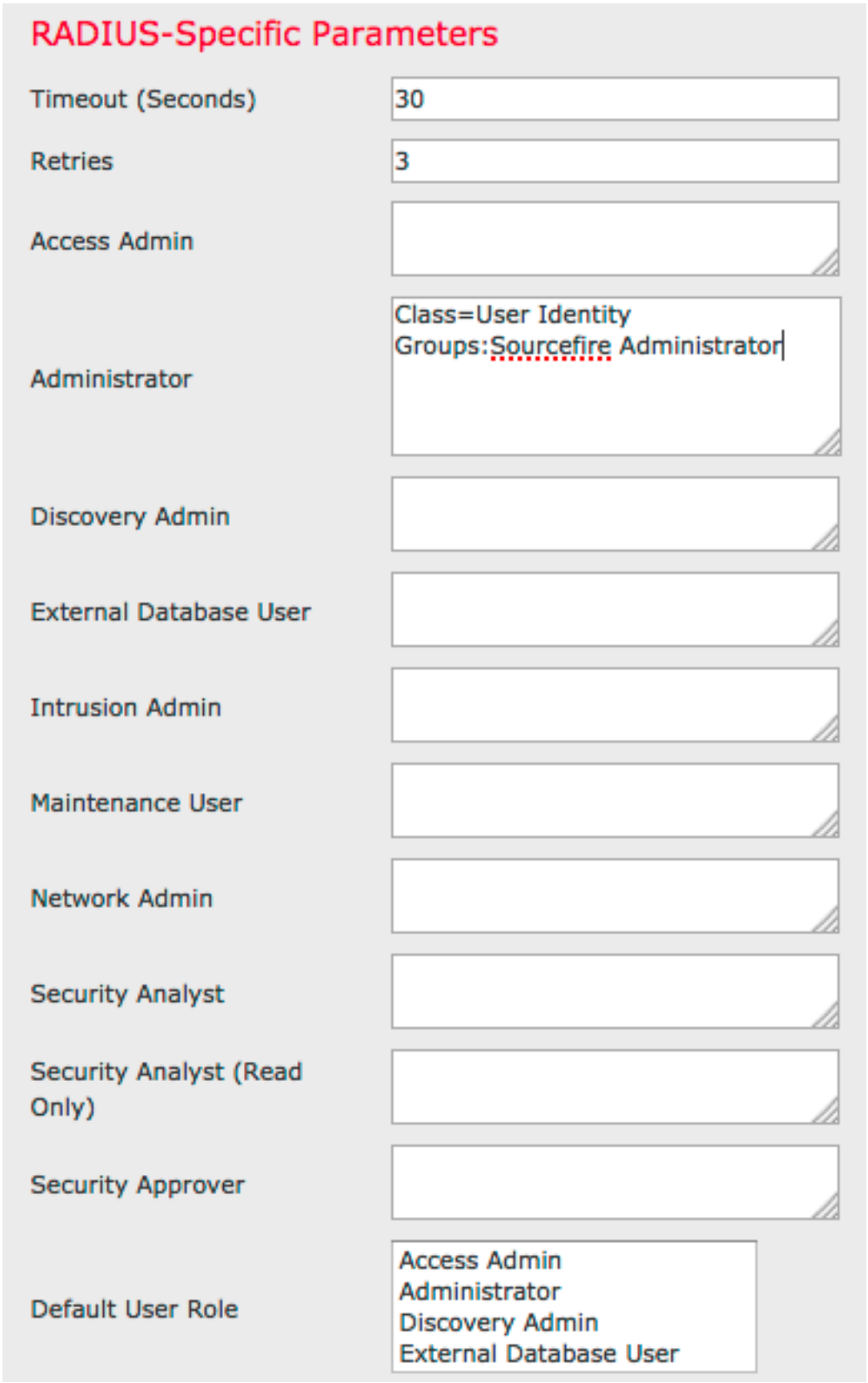
Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	Wireless Black List Default	if	**Blacklist** AND Wireless_Access	then	Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones
✓	Profiled Non Cisco IP Phones	if	Non_Cisco_Profiled_Phones	then	Non_Cisco_IP_Phones
✓	Sourcefire Administrator	if	DEVICE:Device Type EQUALS All Device Types#Sourcefire	then	Sourcefire Administrator
✓	CWA-PSN1	if	Network Access:ISE Host Name EQUALS ise12-psn1	then	CWA-PSN1
✓	CWA-PSN2	if	Network Access:ISE Host Name EQUALS ise12-psn2	then	CWA-PSN2

Sourcefire のシステム ポリシー設定

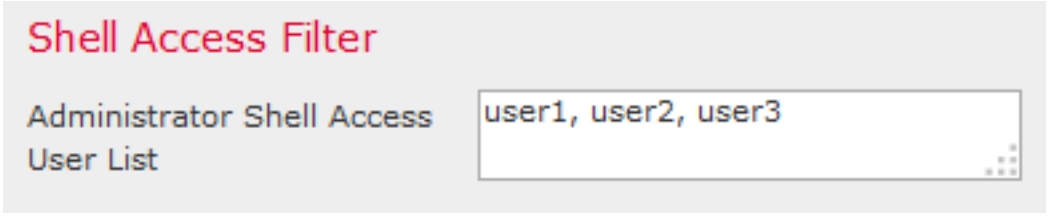
- FireSIGHT MC にログインして、[System] > [Local] > [User Management] に移動します。 [Login Authentication] タブをクリックします。 [+ Create Authentication Object] ボタンをクリックして、ユーザ認証または認可用の新しい RADIUS サーバを追加します。
- [Authentication Method] で [RADIUS] を選択します。 この RADIUS サーバの説明になる名前を入力します。 [Host Name/IP Address] と [RADIUS Secret Key] に入力します。 秘密キーは、前に ISE で設定したキーと一致している必要があります。 バックアップの ISE サーバが存在する場合は、[Host Name/IP Address] にオプションで入力します。



- [RADIUS-Specific Parameters] セクションで、GUI アクセスに一致する Sourcefire のローカル グループ名の横にあるテキスト ボックスに Class-25 の av ペアの文字列を入力します。 次の例では、Class=User Identity Groups: Sourcefire Administrator という値が Sourcefire Administrator グループにマッピングされます。 この値は、ISE が ACCESS-ACCEPT の一部として返す値です。 オプションで、Class-25 グループが割り当てられていない認証済みユーザ用の [Default User Role] を選択します。 [Save] をクリックして設定を保存するか、または ISE を使用して認証をテストするために下の「検証」セクションに進みます。



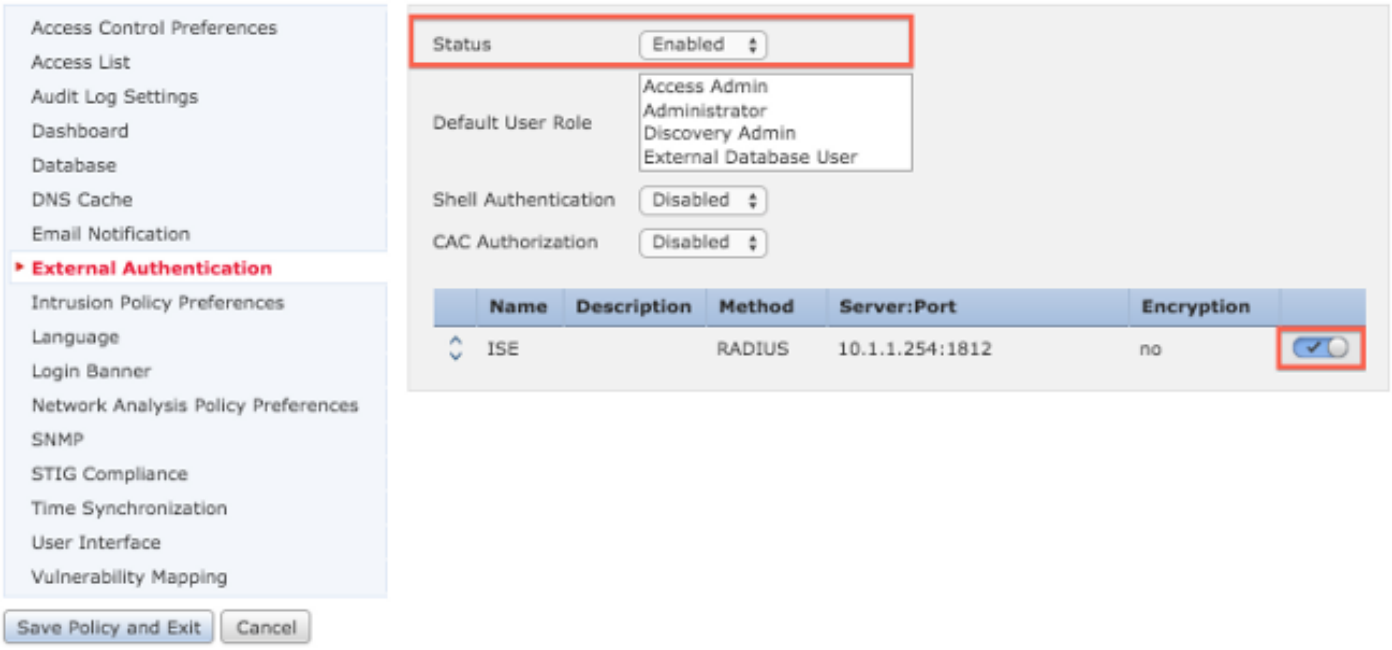
- [Shell Access Filter] で、シェル セッションまたは SSH セッションを制限するユーザのカンマ区切りリストを入力します。



外部認証の有効化

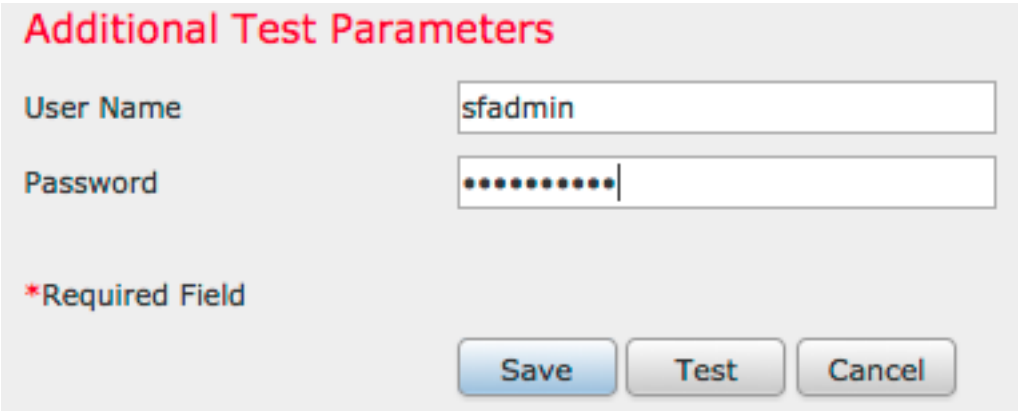
最後に以下の手順を実行して、FMC で外部認証を有効にします。

1. [System] > [Local] > [System Policy] に移動します。
2. 左側のパネルで [External Authentication] を選択します。
3. [Status] を [Enabled] に変更します（デフォルトは [Disabled]）。
4. 追加された ISE RADIUS サーバを有効にします。
5. ポリシーを保存し、アプライアンスにポリシーを再度適用します。



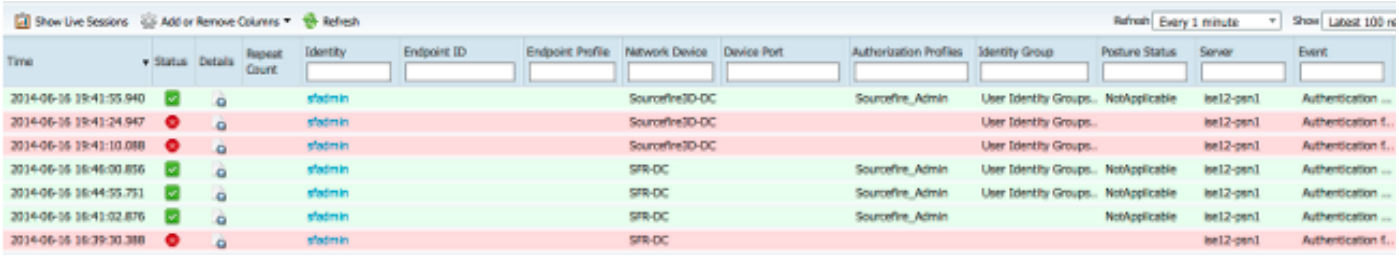
確認

- ISE に対してユーザ認証をテストするには、[Additional Test Parameters] セクションまでスクロールして、ISE ユーザのユーザ名とパスワードを入力します。 [Test] をクリックします。 テストに成功すると、**緑色の** Success: Test Complete というメッセージがブラウザ ウィンドウの先頭に表示されます。



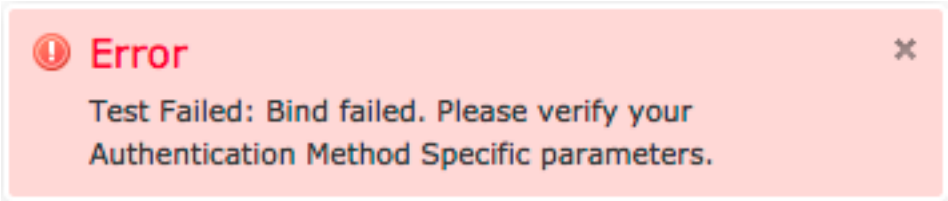
- テスト認証の結果を表示するには、[Test Output] セクションに移動して、[Show Details] の横にある**黒の**矢印をクリックします。 次のスクリーンショットの例では、「radiusauth - response: |Class=User Identity Groups: Sourcefire Administrator|」という ISE から受信した値に注目してください。 この値は、上で FireSIGHT MC 上で設定した Sourcefire ローカル グループに関連付けられた Class の値と一致するはずです。 [Save] をクリックします。

- ISE の管理 GUI で、[Operations] > [Authentications] に移動して、ユーザ認証テストの成功または失敗を検証します。

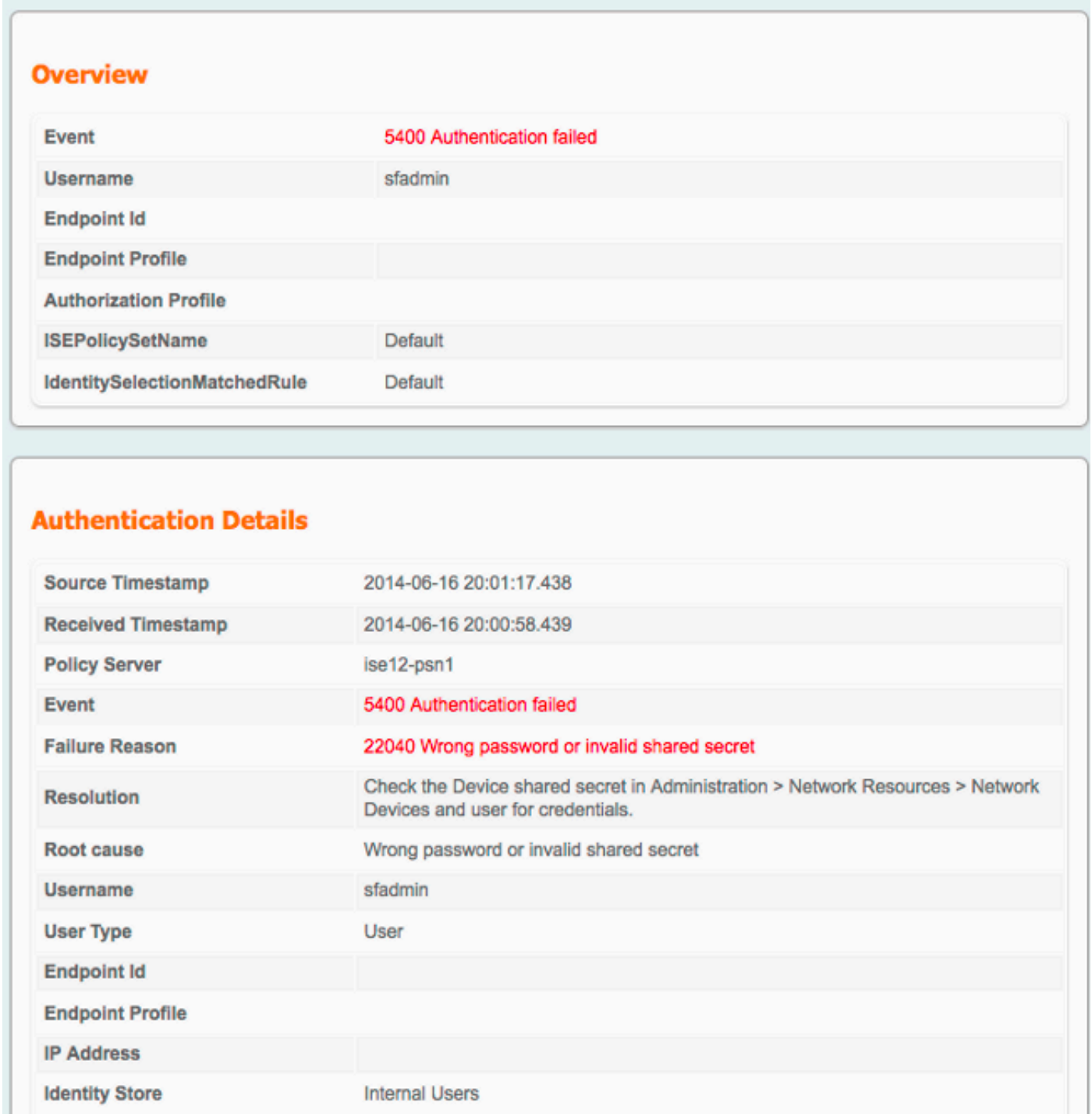


トラブルシューティング

- ISE に対してユーザ認証をテストした場合、次のエラーは RADIUS 秘密キーの不一致、あるいはユーザ名またはパスワードの誤りを示しています。



- ISE の管理 GUI で、[Operations] > [Authentications] に移動します。 **赤の**イベントは失敗を示し、**緑の**イベントは認証、認可、または認可変更の成功を表しています。 アイコンをクリックして認証イベントの詳細を確認します。



Overview

Event	5400 Authentication failed
Username	sfadmin
Endpoint Id	
Endpoint Profile	
Authorization Profile	
ISEPolicySetName	Default
IdentitySelectionMatchedRule	Default

Authentication Details

Source Timestamp	2014-06-16 20:01:17.438
Received Timestamp	2014-06-16 20:00:58.439
Policy Server	ise12-psn1
Event	5400 Authentication failed
Failure Reason	22040 Wrong password or invalid shared secret
Resolution	Check the Device shared secret in Administration > Network Resources > Network Devices and user for credentials.
Root cause	Wrong password or invalid shared secret
Username	sfadmin
User Type	User
Endpoint Id	
Endpoint Profile	
IP Address	
Identity Store	Internal Users

関連情報

テクニカル サポートとドキュメント – Cisco Systems