Cisco Secure Network Analytics

v7.4.2 TACACS+ 構成ガイド

目次

はじめに

Terminal Access Controller Access Control System（TACACS+）は、認証および許可サービスをサポートし、ユーザーが 1 つのクレデンシャルセットを使用して複数のアプリケーションにアクセスできるようにするプロトコルです。Cisco Secure Network Analytics（旧 Stealthwatch）で TACACS+ を設定するには、次の手順を実行します。

対象読者

このガイドは、Secure Network Analytics 製品のインストールおよび設定を担当するネットワーク管理者とその他の担当者を対象としています。

専門家によるインストールを希望する場合は、最寄りのシスコパートナーまたはシスコサポートに連絡してください。

用語

このガイドでは、Cisco Secure Network Analytics Flow Sensor Virtual Edition などの仮想製品を含むすべての Secure Network Analytics 製品に対して「**アプライアンス**」という用語を使用します。

「**クラスタ**」は、Cisco Secure Network Analytics Manager（旧 Stealthwatch Management Console または SMC）によって管理される Secure Network Analytics アプライアンスのグループです。

> v7.4.0 では、Cisco Stealthwatch Enterprise 製品のブランド名を Cisco Secure Network Analytics に変更しました。詳細なリストについては、リリース ノート を参照してください。このガイドでは、以前の製品名である Stealthwatch が必要に応じて明確さを維持するために使用され、Stealthwatch Management Console や SMC などの用語も使用されています。

互換

TACACS+ の認証および許可については、すべてのユーザーがマネージャ経由でログインしていることを確認してください。アプライアンス直接ログインしてアプライアンスの管理を使用するには、ローカルでログインします。

TACACS+ モードが有効になっている場合、FIPS およびコンプライアンスモードは使用できません。

[応答の管理（Response Management）]

応答管理は、マネージャで設定します。電子メールアラート、スケジュール設定されたレポートなどを受信するには、マネージャでユーザーをローカルユーザーとして設定する必要があります。手順については、[設定（Configure）] > [検出応答の管理（DETECTION Response Management）] に移動して、ヘルプを参照してください。

フェールオーバー

マネージャをフェールオーバーペアとして設定した場合は、次の点に注意してください。

- TACACS+ がプライマリ マネージャで設定されている場合、TACACS+ ユーザー情報はセカンダリ マネージャで利用できません。
- セカンダリ マネージャをプライマリに昇格する場合の流れは以下のとおりです。

  - セカンダリ マネージャで TACACS+ とリモート許可を有効にします。
  - 降格したプライマリ マネージャにログイン中の外部ユーザーはログアウトされます。
  - セカンダリ マネージャは、プライマリ マネージャからユーザーデータを引き継がないため、プライマリ マネージャに保存されていたデータは新しい（昇格された）プライマリ マネージャで利用できません。
  - リモートユーザーが新しいプライマリ マネージャに初めてログインすると、ユーザーディレクトリが作成され、これ以降はデータが保存されます。

- **フェールオーバー手順の確認**：詳細については、『Failover Configuration Guide』[英語] を参照してください。

準備

Cisco Secure Access Control System（ACS）または Cisco ISE（Identity Services Engine）で TACACS+ を設定できます。設定を開始するために必要なものがすべて揃っていることを確認します。

要件	詳細
Cisco Secure Access Control System（ACS） または Cisco ISE（Identity Services Engine）	**ACS**：お使いのモデルのインストールとアップグレードガイドに従って、Cisco Secure ACS サーバーをインストールします。 **ISE**：ご使用のエンジンの ISE マニュアルに記載されている手順に従って、ISE をインストールして設定します。
Cisco ISE（Identity Services Engine）	設定には、IP アドレス、ポート、および共有秘密キーが必要です。また、デバイス管理ライセンスも必要です。
TACACS+ サーバー	設定には、IP アドレス、ポート、および共有秘密キーが必要です。
Microsoft Internet Explorer 11（ACS のみ）	Cisco Secure Access Control System で TACACS+ を設定している場合は、このブラウザを使用します。
デスクトップ クライアント	この設定には デスクトップ クライアント を使用します。デスクトップ クライアント のインストール方法については、ご使用の Secure Network Analytics バージョンに一致する Cisco Secure Network Analytics システム コンフィギュレーション ガイド を参照してください。

ユーザーロールの概要

このガイドでは、リモート認証と許可のために TACACS+ ユーザーを設定する手順について説明します。設定を開始する前に、このセクションの詳細を確認して、ユーザーが正しく設定されていることを確認してください。

ユーザー名の設定

リモート認証と許可については、ACS または ISE でユーザーを設定します。ローカル認証と許可については、マネージャでユーザーを設定します。

- **リモート**：Cisco Secure ACS または ISE でユーザーを設定するには、このコンフィギュレーションガイドの手順に従います。
- **ローカル**：ユーザーをローカルでのみ設定するには、マネージャにログインします。メインメニューから、[設定（Configure）] > [グローバルユーザー管理（GLOBAL User Management）] を選択します。手順については、[ヘルプ（Help）] を選択してください。

ユーザー名の大文字と小文字を区別

リモートユーザーを設定する場合は、リモートサーバーで大文字と小文字の区別を有効化します。リモートサーバーで大文字と小文字の区別を有効にしない場合、ユーザーは Secure Network Analytics にログインしたときに自分のデータにアクセスできない可能性があります。

ユーザー名の重複

ユーザー名をリモート（ACS または ISE）で設定するか、ローカル（マネージャ）で設定するかにかかわらず、すべてのユーザー名が一意であることを確認してください。リモートサーバーと Secure Network Analytics 間で重複するユーザー名を使用することは推奨されません。

マネージャにログインしたユーザーと同じ名前が Secure Network Analytics ならびに ACS または ISE に設定されている場合、そのユーザーはローカルのマネージャ/Secure Network Analytics データ.にのみアクセスできます。ユーザー名が重複している場合、リモートの TACACS+ データにはアクセスできません。

以前のバージョン

以前のバージョンの Cisco Secure Network Analytics（Stealthwatch v7.1.1 以前）で TACACS+ を設定している場合には、v7.1.2 以降で一意の名前を持つ新しいユーザーを作成してください。以前のバージョンの Secure Network Analytics で使用していたユーザー名の使用や重複は推奨されません。

v7.1.1 以前で作成されたユーザー名を引き続き使用するには、プライマリ マネージャおよび デスクトップ クライアント でのみ**ローカル**に変更することを推奨します。手順についてはヘルプを参照してください。

ID グループとユーザーの設定

許可されたユーザーログインの場合は、シェルプロファイルをユーザーにマッピングします。各シェルプロファイルに対して、プライマリ管理者のロールを割り当てたり、管理者以外のロールの組み合わせを作成したりすることもできます。プライマリ管理者ロールをシェルプロファイルに割り当てると、追加のロールは許可されません。管理者以外のロールの組み合わせを作成する場合には、要件を満たしていることを確認してください。

プライマリ管理者ロール

プライマリ管理者は、すべての機能を表示し、あらゆる変更を行うことができます。プライマリ管理者ロールをシェルプロファイルに割り当てると、追加のロールは許可されません。

ロール	属性値
プライマリ Admin	cisco-stealthwatch-master-admin

非管理者ロールの組み合わせ

シェルプロファイルの非管理者ロールを組み合わせて作成する場合は、次のものが含まれていることを確認してください。

- 1 データロール（のみ）
- 1 つ以上の Web ロール
- 1 つ以上のデスクトップ クライアント ロール

詳しくは、「**属性値**」の表を参照してください。

> プライマリ管理者ロールをシェルプロファイルに割り当てると、追加のロールは許可されません。管理者以外のロールの組み合わせを作成する場合には、要件を満たしていることを確認してください。

属性値

ロールの各タイプの詳細については、[必要なロール（Required Roles）] 列のリンクをクリックしてください。

必要なロール	属性値
1 つのデータロール（のみ）	• cisco-stealthwatch-all-data-read-and-write • cisco-stealthwatch-all-data-read-only
1 つ以上の Web ロール	• cisco-stealthwatch-configuration-manager • cisco-stealthwatch-power-analyst • cisco-stealthwatch-analyst
1 つ以上のデスクトップ クライアント ロール	• cisco-stealthwatch-desktop-stealthwatch-power-user • cisco-stealthwatch-desktop-configuration-manager • cisco-stealthwatch-desktop-network-engineer • cisco-stealthwatch-desktop-security-analyst

ロールの概要

次の表に各ロールの概要が記載されています。Secure Network Analytics のユーザーロールの詳細については、ヘルプの [ユーザー管理(User Management)] ページを参照してください。

データロール

データロールは 1 つだけ選択してください。

データ ロール	権限
すべてのデータ(読み取り専用)	ユーザーは任意のドメインまたはホストグループ、あるいは任意のアプライアンスまたはデバイス内のデータを表示できますが、設定を行うことはできません。
すべてのデータ(読み取りおよび書き込み)	ユーザーは任意のドメインまたはホストグループ、あるいは任意のアプライアンスまたはデバイス内のデータを表示して、設定を行うことができます。

ユーザーが表示および設定できる機能(フロー検索、ポリシー管理、ネットワーク分類など)は、ユーザーの Web ロールによって決まります。

Web ロール

Web ロール	権限
パワーアナリスト(Power Analyst)	パワーアナリストは、トラフィックとフローに対する初期調査を行い、ポリシーとホストグループを設定できます。
設定マネージャ(Configuration Manager)	Configuration Manager は、設定に関する機能を表示できます。
アナリスト(Analyst)	アナリストは、トラフィックとフローに対する初期調査を実施できます。

デスクトップ クライアント ロール

Web ロール	権限
設定マネージャ(Configuration Manager)	Configuration Manager では、すべてのメニュー項目の表示と、すべてのアプライアンス、デバイス、およびドメインの設定が可能です。
ネットワークエンジニア(Network Engineer)	ネットワークエンジニアは、デスクトップ クライアント 内のすべてのトラフィック関連メニュー項目の表示、アラームとホストノートの追加、緩和を除くすべてのアラームアクションの実行が可能です。
セキュリティ アナリスト(Security Analyst)	セキュリティアナリストは、すべてのセキュリティ関連のメニュー項目の表示、アラームとホストノートの追加、緩和を含むすべてのアラームアクションの実行が可能です。

Stealthwatch（Secure Network Analytics）パワーユーザー	Stealthwatch（Secure Network Analytics）パワーユーザーは、すべてのメニュー項目の表示、アラームの確認、アラームとホストノートの追加が可能ですが、変更操作はできません。

プロセスの概要

Cisco ACS または ISE で TACACS+ を設定できます。TACACS+ を正しく設定し、Secure Network Analytics で TACACS+ を許可するには、次の手順が完了していることを確認してください。

1. ACS または ISE で TACACS+ を設定します。
2. Secure Network Analytics で TACACS+ 認証を有効にします。
3. TACACS+ のログインをテストします。

1a. ACS での TACACS+ の設定

Cisco Secure ACS に TACACS+ サービスを追加するには、次の手順を使用します。

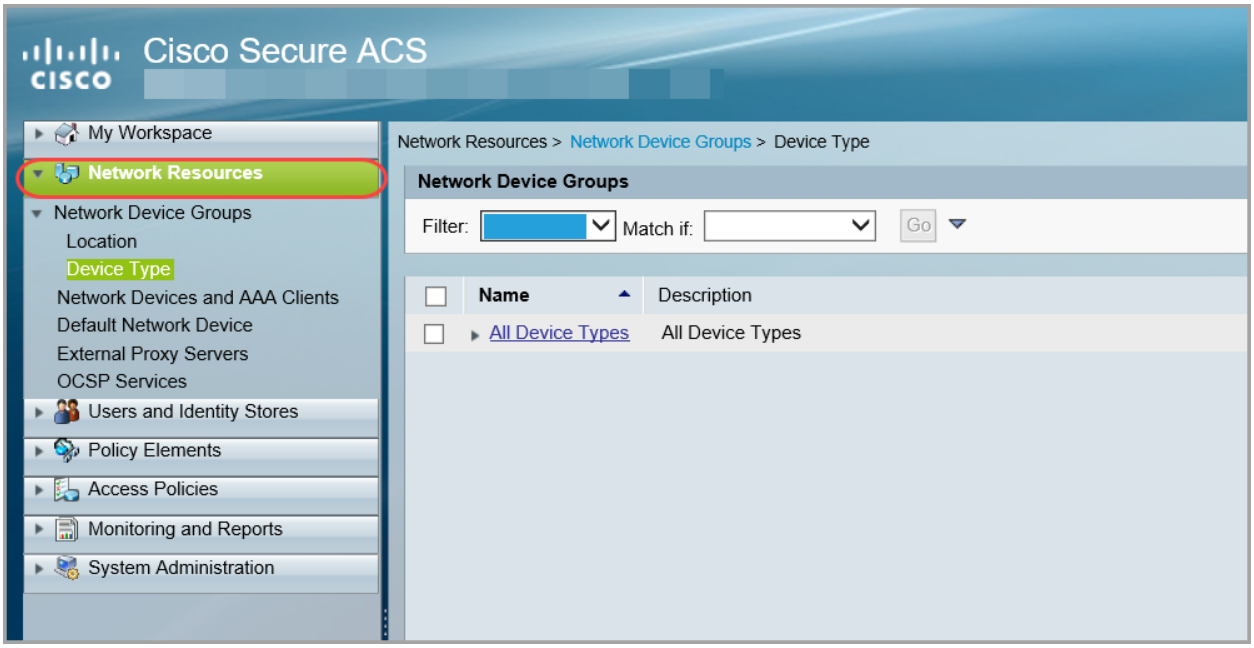
> ISE で TACACS+ を設定する方法については、「1b. ISE での TACACS+ の設定」を参照してください。

サービス名（Service Name）

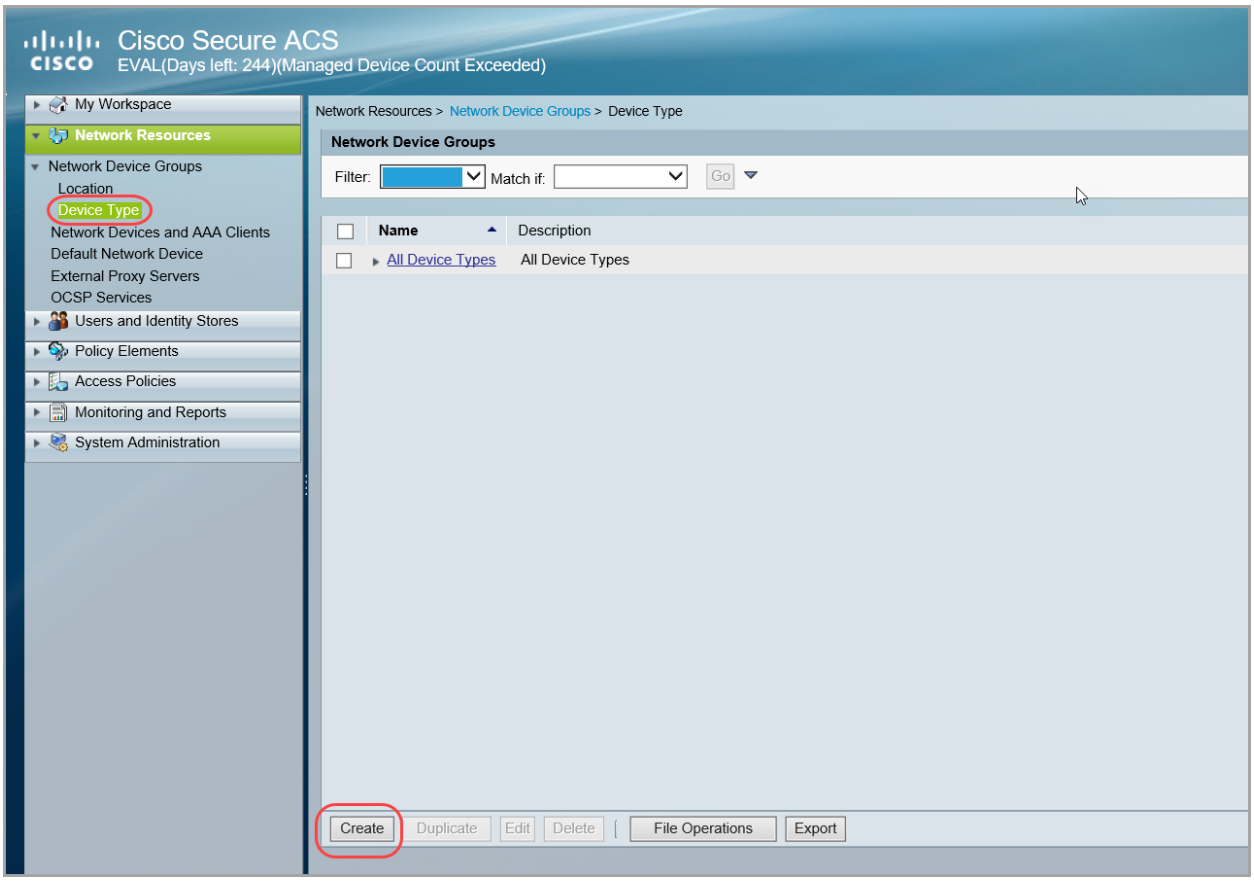
新しいサービス名を作成するときは、その他の手順でも必要になるため、その名前を記録しておいてください。

1. デバイスタイプの追加

1. Microsoft Internet Explorer 11 を起動します。
2. Cisco Secure ACS にログインします。
3. **[ネットワークリソース（Network Resources）]** メニューを選択します。



4. [ネットワーク デバイス グループ（Network Device Groups）] の下で、**[デバイスタイプ（Device Type）]** を選択します。
5. [作成（Create）] をクリックします。



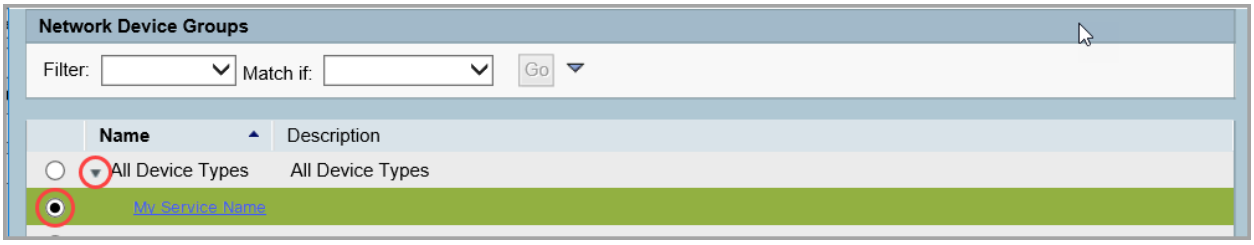
6. [名前（Name）] フィールドに、サービス名を入力します（例：Secure_Network_Analytics）。

   これは、TACACS+ のサービス名です。後の手順で TACACS+ を有効にするためにこの名前を使用します。

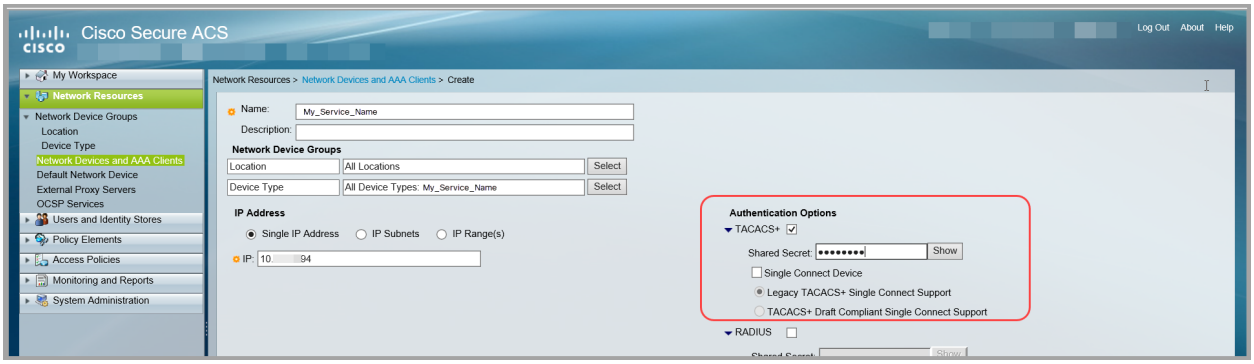
7. [送信（Submit）] をクリックします。

2. TACACS+ サーバーの追加

1. **[ネットワークデバイスとAAAクライアント(Network Devices and AAA Clients)]** メニューを選択します。
2. [作成(Create)] をクリックします。
3. [名前(Name)] フィールドに、次の手順で入力したサービス名を入力します(「**1. デバイスタイプの追加**」)。
4. [場所(Location)] フィールドで、**[すべての場所(All Locations)]** を選択します。
5. [デバイスタイプ(Device Type)] フィールドで、**[選択(Select)]** をクリックします。
    - [すべてのデバイスタイプ(All Device Types)] の横にある矢印をクリックします。
    - 作成したサービス名を選択します。
    - [OK] をクリックします。



6. [IPアドレス(IP Address)] セクションで、**[単一のIPアドレス(Single IP Address)]** を選択します。
7. [IP] フィールドに、TACACS+ サーバーの IP アドレスを入力します。
8. [認証オプション(Authentication Options)] セクションで、**[TACACS+]** チェックボックスをオンにします。
9. [共有秘密(Shared Secret)] フィールドに、サーバーのパスワードを入力します。

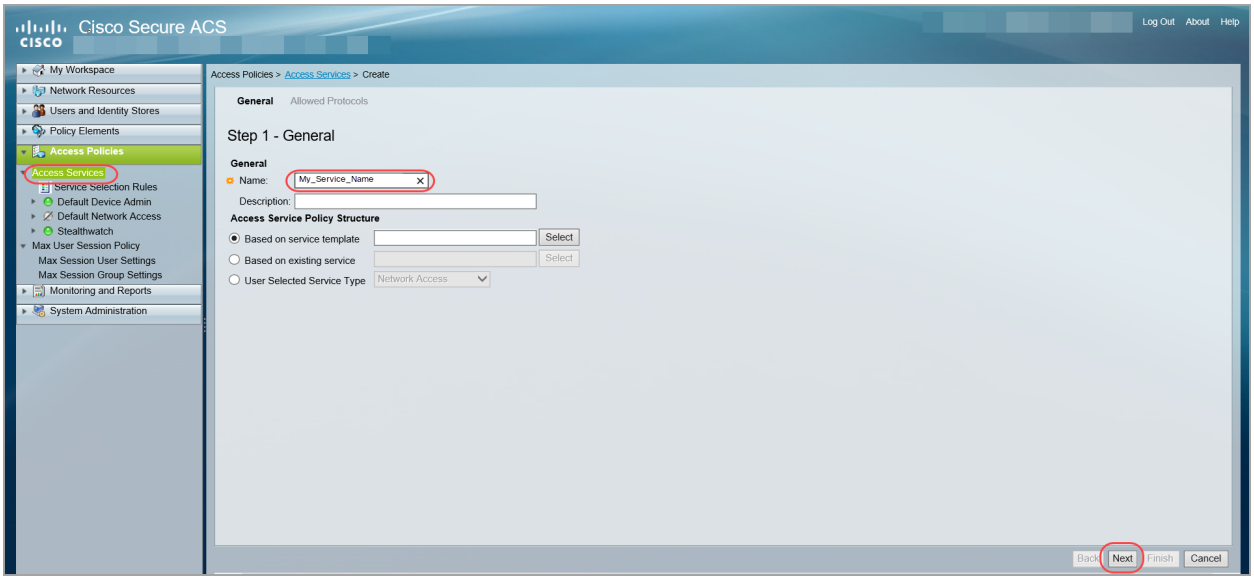


10. [送信(Submit)] をクリックします。

3. TACACS+ サービスの承認

Cisco Secure ACS で TACACS+ サービスを承認するには、次の手順を使用します。

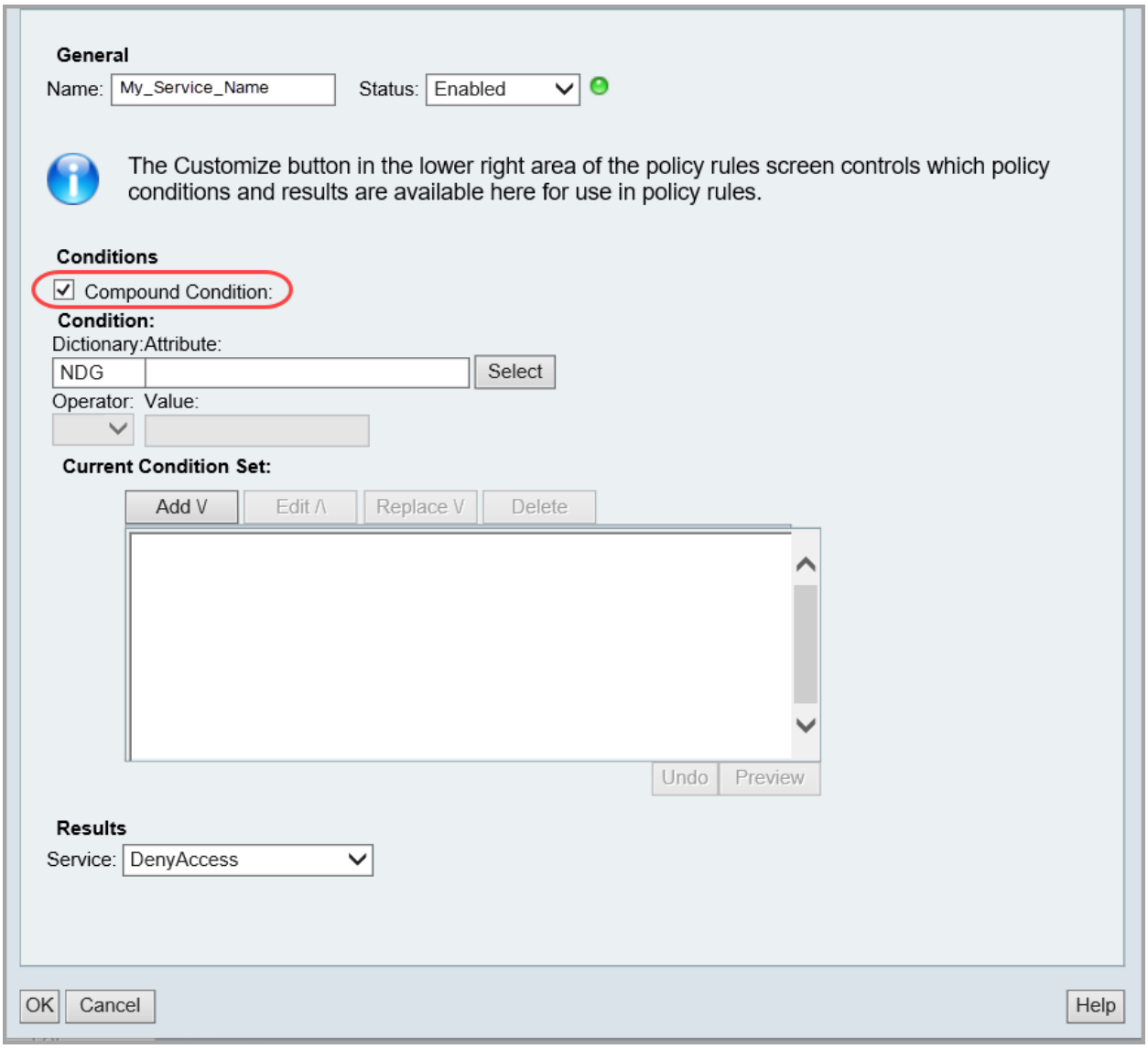
1. **[アクセスポリシー(Access Policies)]** メニューを選択します。
2. [アクセスサービス **Access Services**] メニューを選択します。
3. [作成(Create)] をクリックします。
4. [名前(Name)] フィールドに、以前の手順で入力したサービス名を入力します。



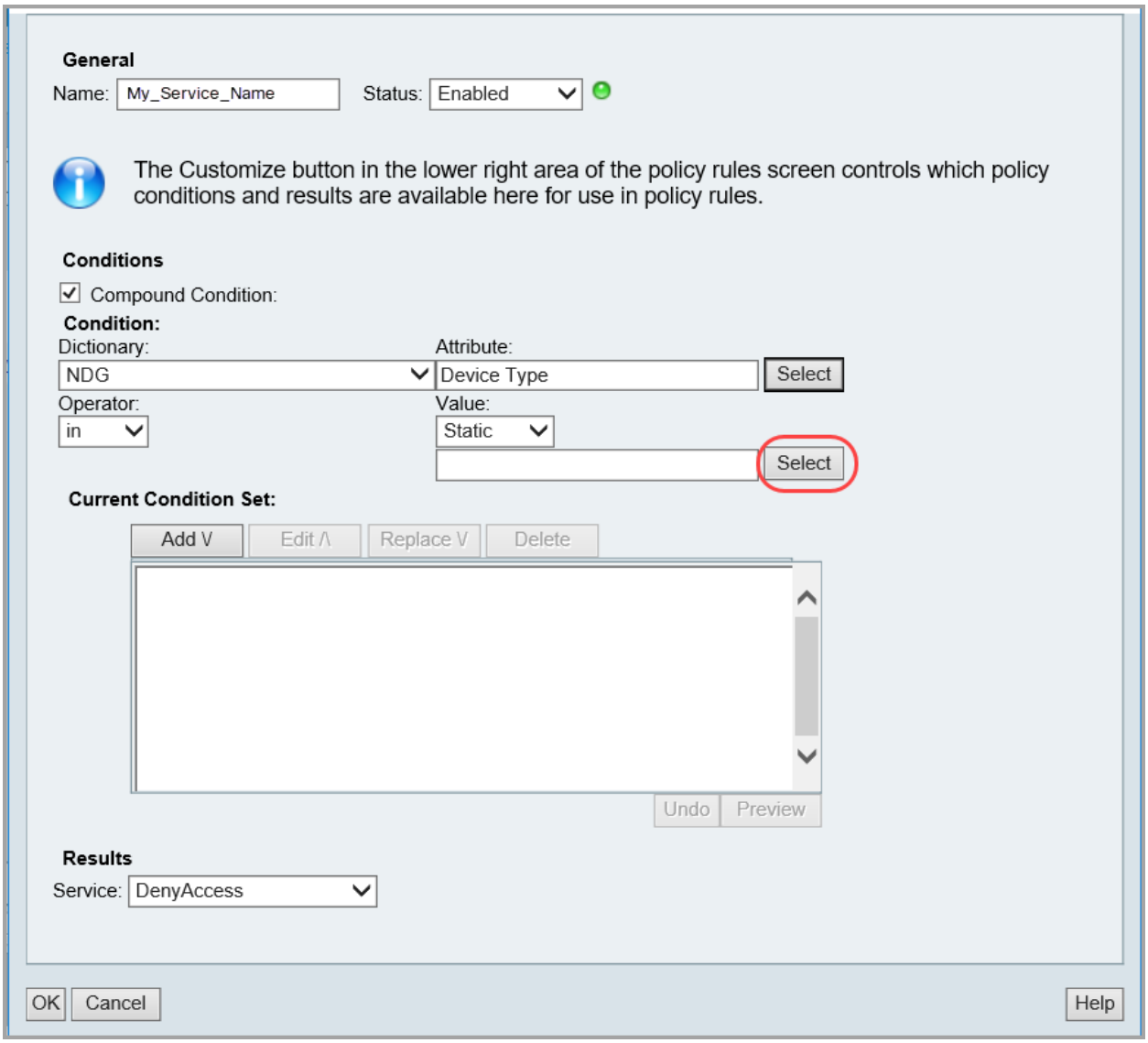
5. [アクセスサービスポリシー構造(Access Service Policy Structure)] で、**[サービステンプレートに基づく(Based on service template)]** を選択します。**[選択(Select)]** をクリックして、サービスポリシーを選択します。
6. [次へ(Next)] をクリックします。
7. プロトコルを選択するか、デフォルト値を使用します。
8. [終了(Finish)] をクリックします。
9. プロンプトが表示されたら、**[はい(Yes)]** をクリックしてサービス セレクション ポリシーを変更し、サービスをアクティブにします。

   次のメニューが開きます。[アクセスポリシー(Access Policies)] > [アクセスサービス(Access Services)] > [サービスセレクションルール(Service Selection Rules)]。

10. [作成(Create)] をクリックします。
11. [名前(Name)] フィールドに、サービス名を入力します。
12. [ステータス(Status)] フィールドで、**[使用する(Enabled)]** が選択されていることを確認します。
13. **[複合条件(Compound Condition)]** チェックボックスをオンにします。



14. [ディクショナリ(Dictionary)]フィールドで、**[NDG]**を選択します。
15. [属性(Attribute)]フィールドで、**[デバイスタイプ(Device Type)]**を選択します。
16. [演算子(Operator)]フィールドで、**[in]**を選択します。
17. [値(Value)]フィールドで、**[静的(Static)]**を選択します。
18. [値(Value)]の下の空白フィールドで、**[選択(Select)]**をクリックします。



19. [すべてのデバイスタイプ(All Device Types)] の横にある矢印をクリックします。
20. サービス名を選択します。
21. [OK] をクリックします。
22. [追加(Add)] をクリックします。
23. [サービス(Service)] フィールドで、サービス名を選択します。
24. [OK] をクリックします。

4. ACS サーバーへの ID グループの追加

ID グループを設定するには、次の手順を使用します。各 ID グループに対して、シェルプロファイルと許可アクセスを作成します。

ID グループ名（Identity Group Name）

新しいグループを作成して名前を付けるときは、対応するシェルプロファイルと許可アクセスに同じ名前を使用するようにしてください。

ユーザーロール

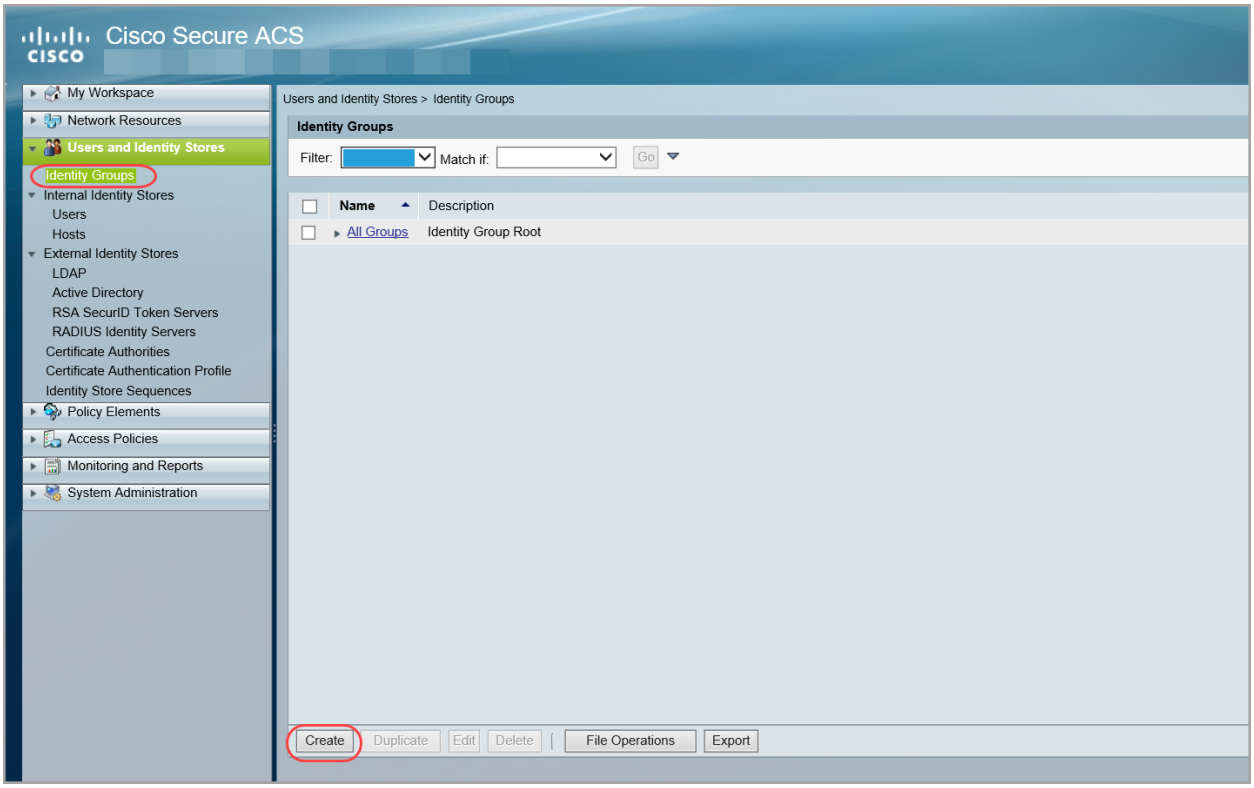
各シェルプロファイルに対して、プライマリ管理者のロールを割り当てたり、管理者以外のロールの組み合わせを作成したりすることもできます。

プライマリ管理者ロールをシェルプロファイルに割り当てると、追加のロールは許可されません。管理者以外のロールの組み合わせを作成する場合には、要件を満たしていることを確認してください。ユーザーロールの詳細については、「**ユーザーロールの概要**」を参照してください。

1. 新しい ID グループの作成

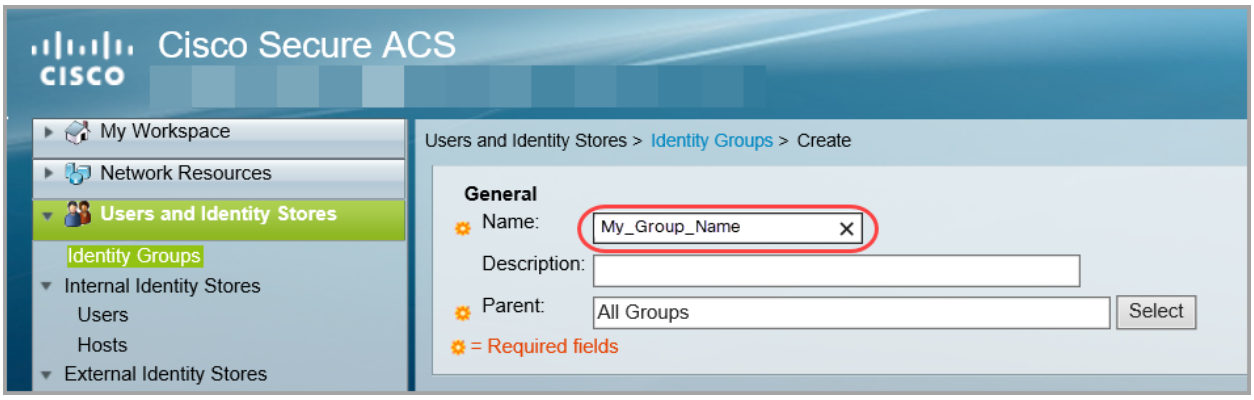
新しい ID グループを設定するには、次の手順を使用します。

1. **[ユーザーおよびIDストア（Users and Identity Stores）]** メニューを選択します。
2. **[IDグループ（Identity Groups）]** を選択します。
3. [作成（Create）] をクリックします。



4. **[名前（Name）]** フィールドにグループ名を入力します。

この先の手順では、対応するシェルプロファイルと許可アクセスに同じ名前を使用するようにしてください。

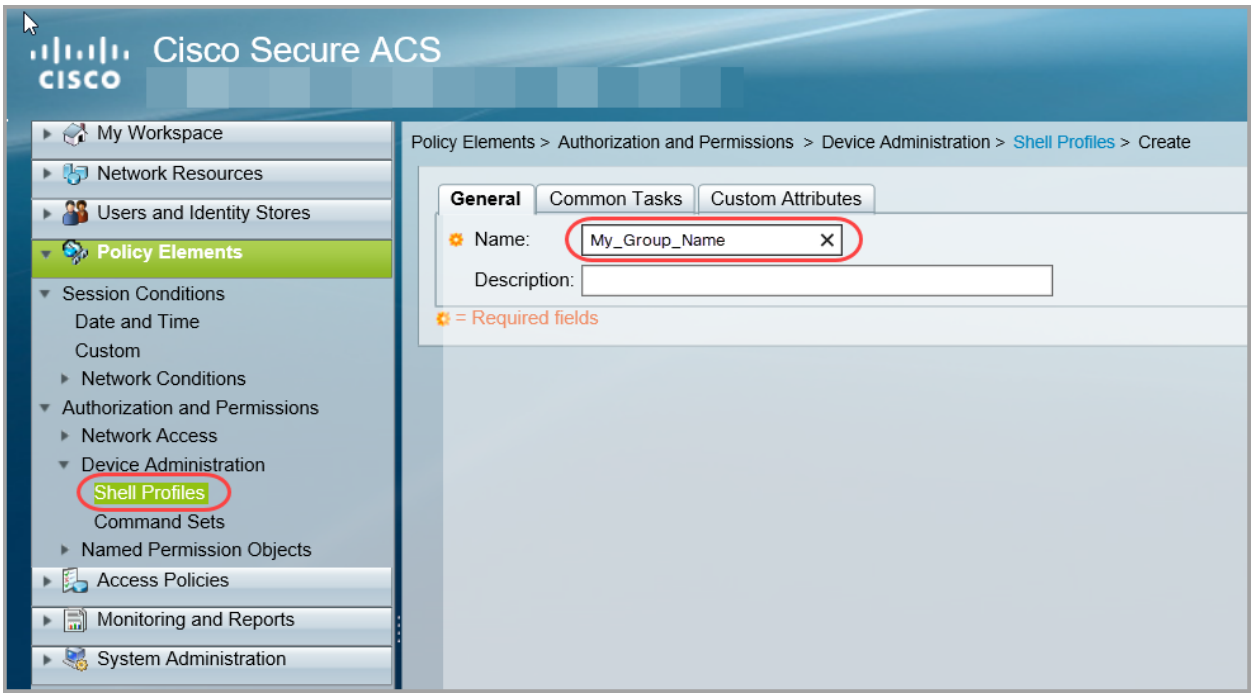


5. [送信(Submit)]をクリックします。

2. シェルプロファイルの作成

最後の手順で作成した ID グループのシェルプロファイルを作成するには、次の手順を使用します。また、これらの手順を使用して、必要なロールをシェルプロファイルに割り当てます。

1. **[ポリシー要素(Policy Elements)]**メニューを選択します。
2. [許可および権限(Authorization and Permissions)]>[デバイス管理(Device Administration)]の下で、**[シェルプロファイル(Shell Profiles)]**を選択します。



3. [作成(Create)]をクリックします。
4. [名前(Name)]フィールドに、「1. 新しい ID グループの作成」で作成した ID グループ名を入力します。

5. [Custom Attributes] タブを選択します。
6. 次のフィールドに入力します。

    - 属性：ロール
    - 要件：必須
    - 属性値：Static

7. [属性値（Attribute Value）] の下にある空白のフィールドにプライマリ管理者の値を入力するか、非管理者ロールの組み合わせを作成します。

    プライマリ管理者ロールをシェルプロファイルに割り当てると、追加のロールは許可されません。管理者以外のロールの組み合わせを作成する場合には、要件を満たしていることを確認してください。

プライマリ管理者ロール

プライマリ管理者は、すべての機能を表示し、あらゆる変更を行うことができます。プライマリ管理者ロールをシェルプロファイルに割り当てると、追加のロールは許可されません。

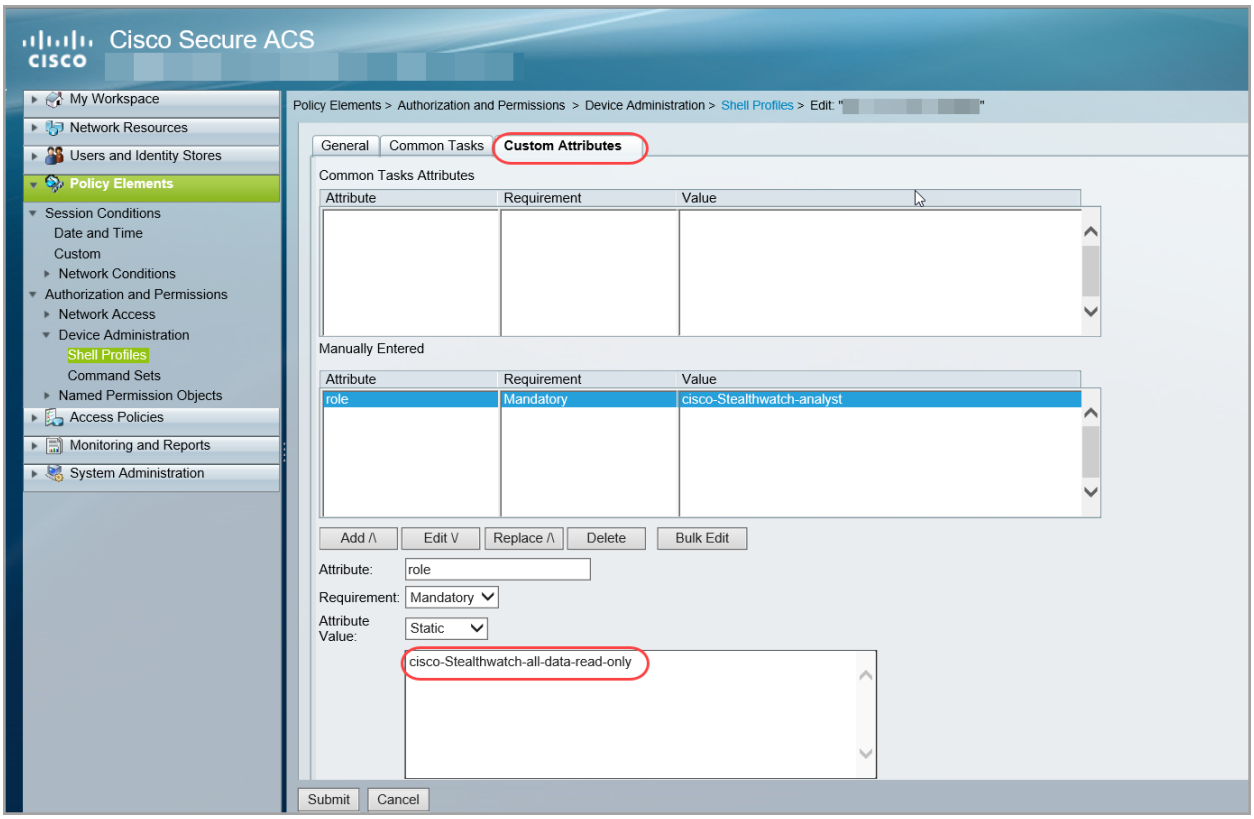
ロール	属性値
プライマリ Admin	cisco-stealthwatch-master-admin

非管理者ロールの組み合わせ

シェルプロファイルの非管理者ロールを組み合わせて作成する場合は、次のものが含まれていることを確認してください。

- 1 データロール（のみ）：1 つのデータロールのみを選択するようにしてください
- 1 つ以上の Web ロール
- 1 つ以上のデスクトップ クライアント ロール

必要なロール	属性値
1 つのデータロール（のみ）	• cisco-stealthwatch-all-data-read-and-write • cisco-stealthwatch-all-data-read-only
1 つ以上の Web ロール	• cisco-stealthwatch-configuration-manager • cisco-stealthwatch-power-analyst • cisco-stealthwatch-analyst
1 つ以上のデスクトップ クライアント ロール	• cisco-stealthwatch-desktop-stealthwatch-power-user • cisco-stealthwatch-desktop-configuration-manager • cisco-stealthwatch-desktop-network-engineer • cisco-stealthwatch-desktop-security-analyst



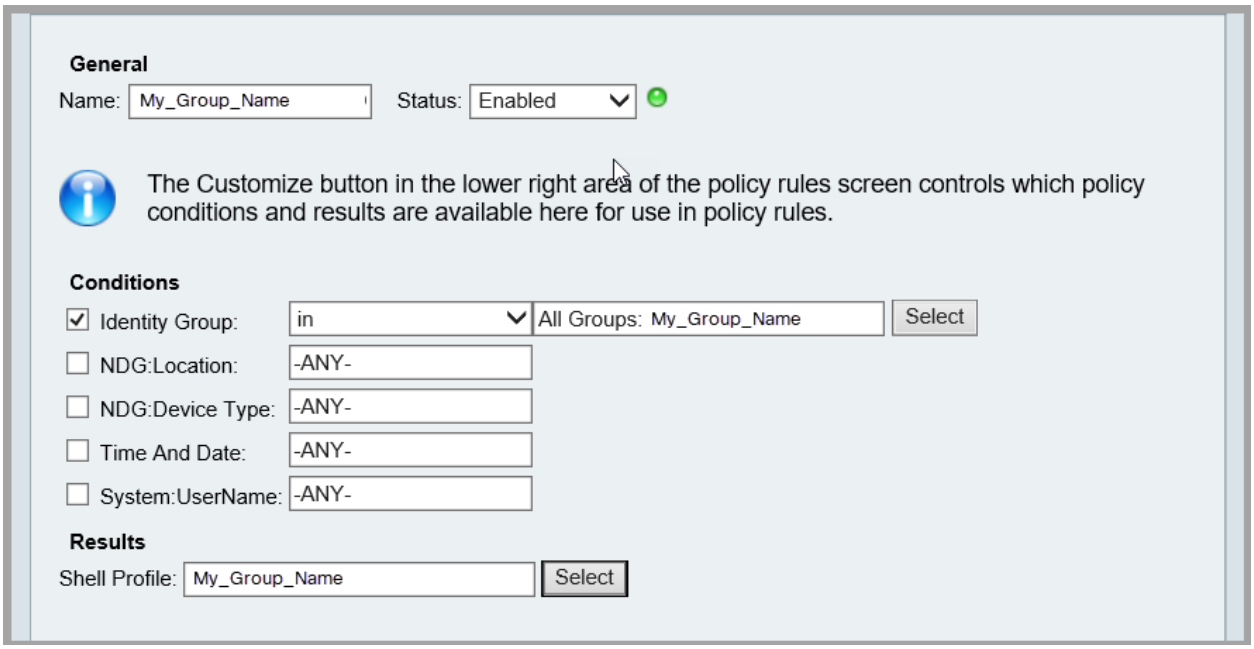
プライマリ管理者ロールをシェルプロファイルに割り当てると、追加のロールは許可されません。管理者以外のロールの組み合わせを作成する場合には、要件を満たしていることを確認してください。

8. [追加(Add)]をクリックします。
9. 必要なすべてのロールをシェルプロファイルに追加し終わるまで、手順 6 ～ 8 を繰り返します。
10. [送信(Submit)]をクリックします。

3. ID グループベースの許可の設定

1. **[アクセスポリシー(Access Policies)]**メニューを選択します。
2. [アクセスサービス(Access Services)]> お使いのサービス名 >[許可(Authorization)]の順に選択します。
3. [作成(Create)]をクリックします。
4. [名前(Name)]フィールドに、「**1. 新しい ID グループの作成**」で作成した ID グループ名を入力します。
5. [ステータス(Status)]フィールドで、**[使用する(Enabled)]**が選択されていることを確認します。
6. **[IDグループ(Identity Group)]**チェックボックスをオンにします。
7. [選択]をクリックします。
8. [すべてのグループ(All Groups)]の横にある矢印をクリックします。

9. リストから ID グループ名を選択します。
10. [OK] をクリックします。
11. [シェルプロファイル（Shell Profile）] フィールドで、**[選択（Select）]** をクリックします。
12. リストから ID グループ名を選択します。



13. [OK] をクリックします。
14. セクション「4. ACS サーバーへの ID グループの追加」の手順を繰り返して別の ID グループを作成し、シェルプロファイルを設定して、許可を割り当てます。

5. ユーザーへの ID グループの割り当て

Secure Network Analytics の ID グループの設定が完了したら、ID グループを Secure Network Analytics ユーザーに割り当てます。

ユーザ名

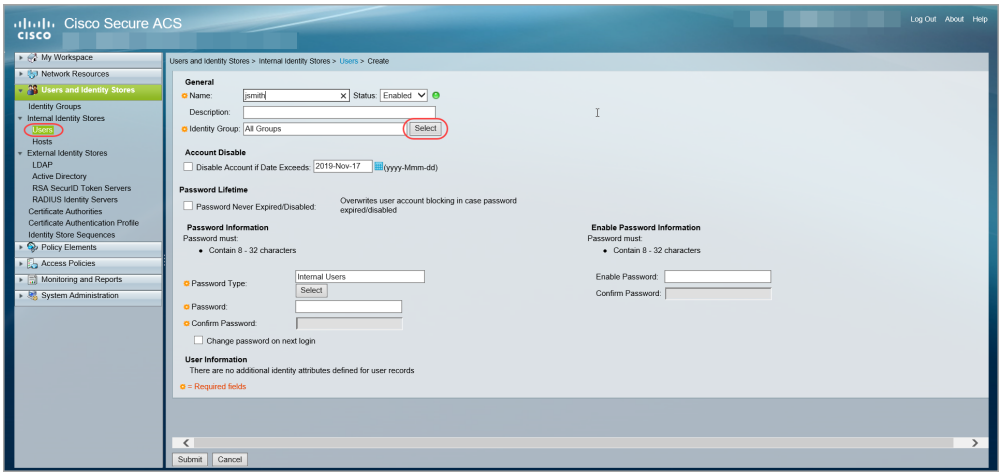
ユーザー名をリモート（ACS または ISE）で設定するか、ローカル（マネージャ）で設定するかにかかわらず、すべてのユーザー名が一意であることを確認してください。リモートサーバーと Secure Network Analytics 間で重複するユーザー名を使用することは推奨されません。

重複するユーザー名：マネージャにログインしたユーザーと同じ名前が Secure Network Analytics ならびに ACS または ISE に設定されている場合、そのユーザーはローカルのマネージャ/Secure Network Analytics データにのみアクセスできます。ユーザー名が重複している場合、リモートの TACACS+ データにはアクセスできません。

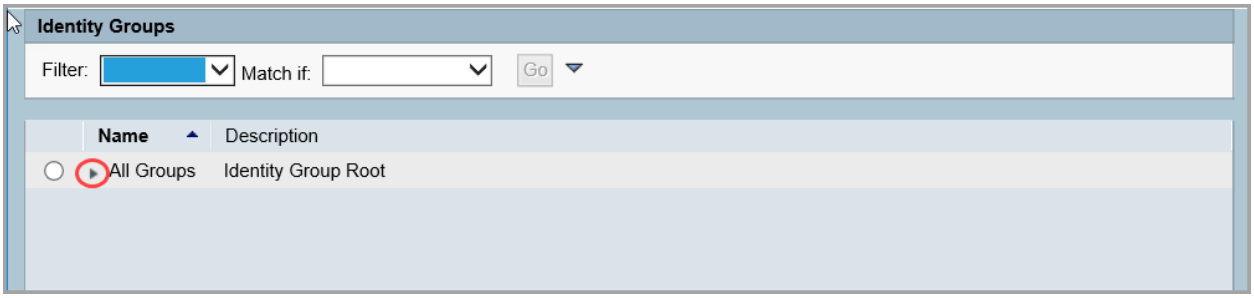
ユーザー名の大文字と小文字を区別：リモートユーザーを設定する場合は、リモートサーバーで大文字と小文字の区別を有効にします。リモートサーバーで大文字と小文字の区別を有効にしない場合、ユーザーは Secure Network Analytics にログインしたときに自分のデータにアクセスできない可能性があります。

ユーザーへの ID グループの割り当て

1. **[ユーザーおよび ID ストア(Users and Identity Stores)]** メニューを選択します。
2. [内部IDストア(Internal Identity Stores)] の下で、**[ユーザー(Users)]** を選択します。
3. リストからユーザー名を選択するか、**[作成(Create)]** をクリックして新しいユーザーを作成します。
4. [IDグループ(Identity Group)] フィールドで、**[選択(Select)]** をクリックします。



5. [すべてのグループ(All Groups)] の横にある矢印をクリックします。



6. ID グループ名を選択します。
7. [OK] をクリックします。
8. ユーザー設定を終了します。[Submit] をクリックして変更を保存します。
9. 「**5. ユーザーへの ID グループの割り当て**」の手順を必要に応じて繰り返します。
10. 「**2. Secure Network Analytics での TACACS+ 認証の有効化**」に進みます。

1b. ISE での TACACS+ の設定

ISE で TACACS+ を設定するには、次の手順を実行します。この設定により、ISE で TACACS+ のリモートユーザーが Secure Network Analytics にログインできるようになります。

> ACS で TACACS+ を設定する方法については、「**1a. ACS での TACACS+ の設定**」を参照してください。

始める前に

以下の手順を開始する前に、ご使用のエンジンの ISE マニュアルに記載されている手順に従って、ISE をインストールして設定します。これには、証明書が正しく設定されているかどうかの確認も含まれます。

ユーザ名

ユーザー名をリモート（ACS または ISE）で設定するか、ローカル（マネージャ）で設定するかにかかわらず、すべてのユーザー名が一意であることを確認してください。リモートサーバーと Secure Network Analytics 間で重複するユーザー名を使用することは推奨されません。

重複するユーザー名：マネージャにログインしたユーザーと同じ名前が Secure Network Analytics ならびに ACS または ISE に設定されている場合、そのユーザーはローカルのマネージャ/Secure Network Analytics データにのみアクセスできます。ユーザー名が重複している場合、リモートの TACACS+ データにはアクセスできません。

ユーザー名の大文字と小文字を区別：リモートユーザーを設定する場合は、リモートサーバーで大文字と小文字の区別を有効にします。リモートサーバーで大文字と小文字の区別を有効にしない場合、ユーザーは Secure Network Analytics にログインしたときに自分のデータにアクセスできない可能性があります。

ユーザーロール

ISE の各 TACACS+ プロファイルに対して、プライマリ管理者のロールを割り当てることも、管理者以外のロールの組み合わせを作成することもできます。

プライマリ管理者ロールをシェルプロファイルに割り当てると、追加のロールは許可されません。管理者以外のロールの組み合わせを作成する場合には、要件を満たしていることを確認してください。ユーザーロールの詳細については、「**ユーザーロールの概要**」を参照してください。

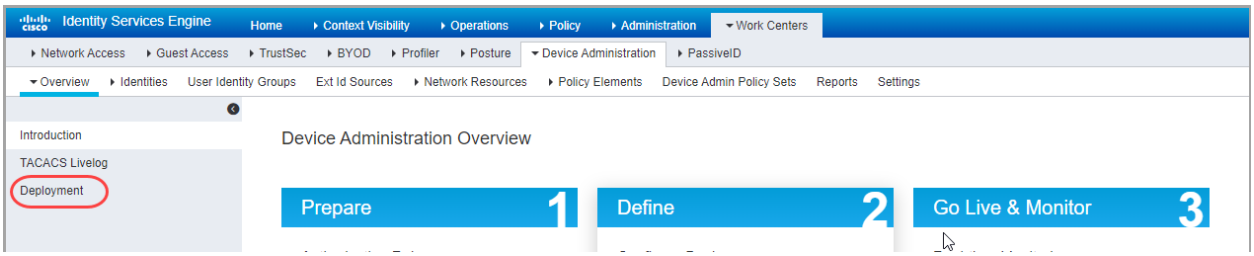
1. ISE でのデバイス管理の有効化

ISE で TACACS+ サービスを追加するには、次の手順を実行します。

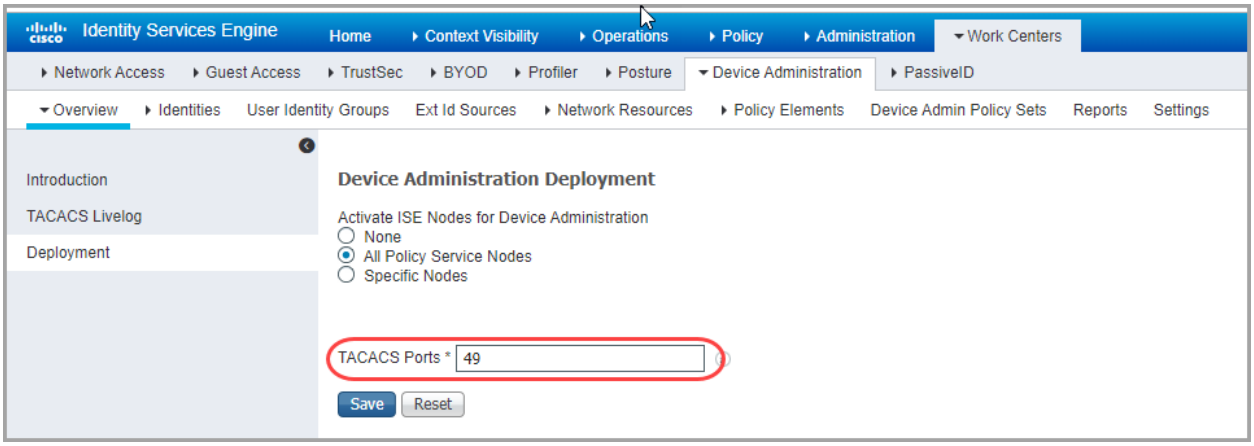
1. 管理者として ISE にログインします。
2. **[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[概要（Overview）]** の順に選択します。

   ワークセンターにデバイス管理が表示されない場合は、**[管理（Administration）]** > **[システム（System）]** > **[ライセンス（Licensing）]** の順に移動します。[ライセンス（Licensing）] セクションに、デバイス管理ライセンスが表示されていることを確認します。表示されていない場合は、アカウントにライセンスを追加します。

3. **[導入（Deployment）]** を選択します。



4. **[すべてのポリシーサービスノード（All Policy Service Nodest）]** または **[特定のノード（Specific Nodest）]** を選択します。
5. [TACACSポート（TACACS Ports）] フィールドに、**49** と入力します。



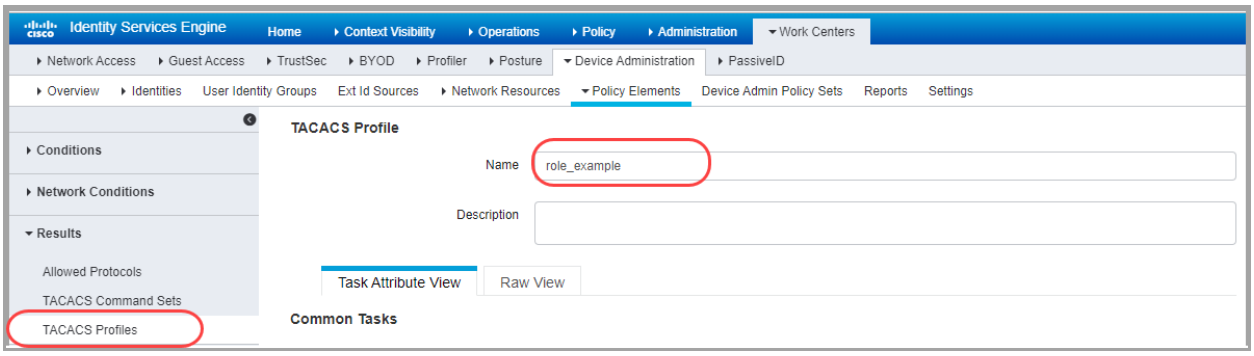
6. [保存（Save）] をクリックします。

2. TACACS+ プロファイルの作成

ISE で TACACS+ シェルプロファイルを追加するには、次の手順を実行します。また、これらの手順を使用して、必要なロールをシェルプロファイルに割り当てます。

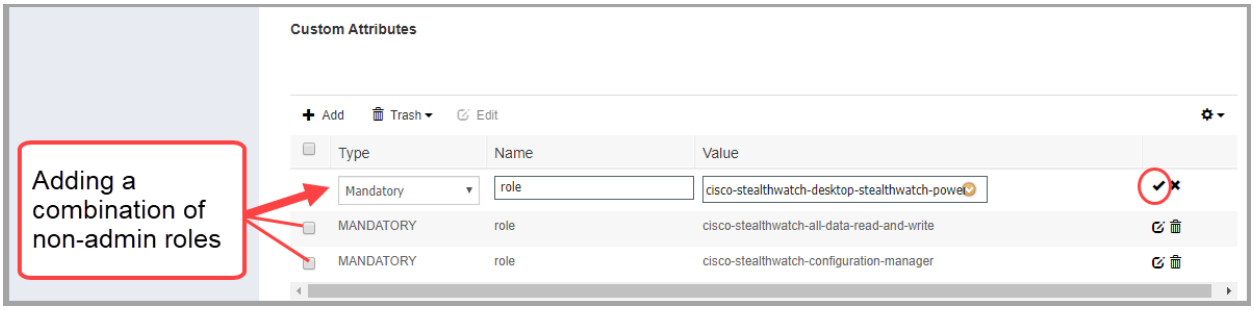
1. **[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[ポリシー要素（Policy Elements）]** を選択します。
2. **[結果（Results）]** > **[TACACSプロファイル（TACACS Profiles）]** を選択します。
3. **[+ 追加（+Add）]** をクリックします。
4. [名前（Name）] フィールドに、一意のユーザー名を入力します。

   ユーザー名の詳細については、「**ユーザーロールの概要**」を参照してください。



5. [一般的なタスクタイプ（Common Task Type）] ドロップダウンリストで、**[シェル（Shell）]** を選択します。
6. [カスタム属性（Custom Attributes）] セクションで、**[追加（+Add）]** をクリックします。
7. [タイプ（Type）] フィールドで、**[必須（Mandatory）]** を選択します。
8. [名前（Name）] フィールドに、**ロール**を入力します。
9. [値（Value）] フィールドにプライマリ管理者の属性値を入力するか、非管理者ロールの組み合わせを構築します。

   - **保存**：保存するロールの ✔ チェックマークアイコンをクリックします。
   - **非管理者ロールの組み合わせ**：非管理者ロールの組み合わせを作成する場合は、必要なロール（データロール、Web ロール、および デスクトップ クライアント ロール）ごとに行が追加されるまで、手順 5 ～ 8 を繰り返します。



プライマリ管理者ロール

プライマリ管理者は、すべての機能を表示し、あらゆる変更を行うことができます。プライマリ管理者ロールをシェルプロファイルに割り当てると、追加のロールは許可されません。

ロール	属性値
プライマリ Admin	cisco-stealthwatch-master-admin

非管理者ロールの組み合わせ

シェルプロファイルの非管理者ロールを組み合わせて作成する場合は、次のものが含まれていることを確認してください。

- 1 データロール（のみ）：1 つのデータロールのみを選択するようにしてください
- 1 つ以上の Web ロール
- 1 つ以上のデスクトップ クライアント ロール

必要なロール	属性値
1 つのデータロール（のみ）	• cisco-stealthwatch-all-data-read-and-write • cisco-stealthwatch-all-data-read-only
1 つ以上の Web ロール	• cisco-stealthwatch-configuration-manager • cisco-stealthwatch-power-analyst • cisco-stealthwatch-analyst
1 つ以上のデスクトップ クライアント ロール	• cisco-stealthwatch-desktop-stealthwatch-power-user • cisco-stealthwatch-desktop-configuration-manager • cisco-stealthwatch-desktop-network-engineer • cisco-stealthwatch-desktop-security-analyst

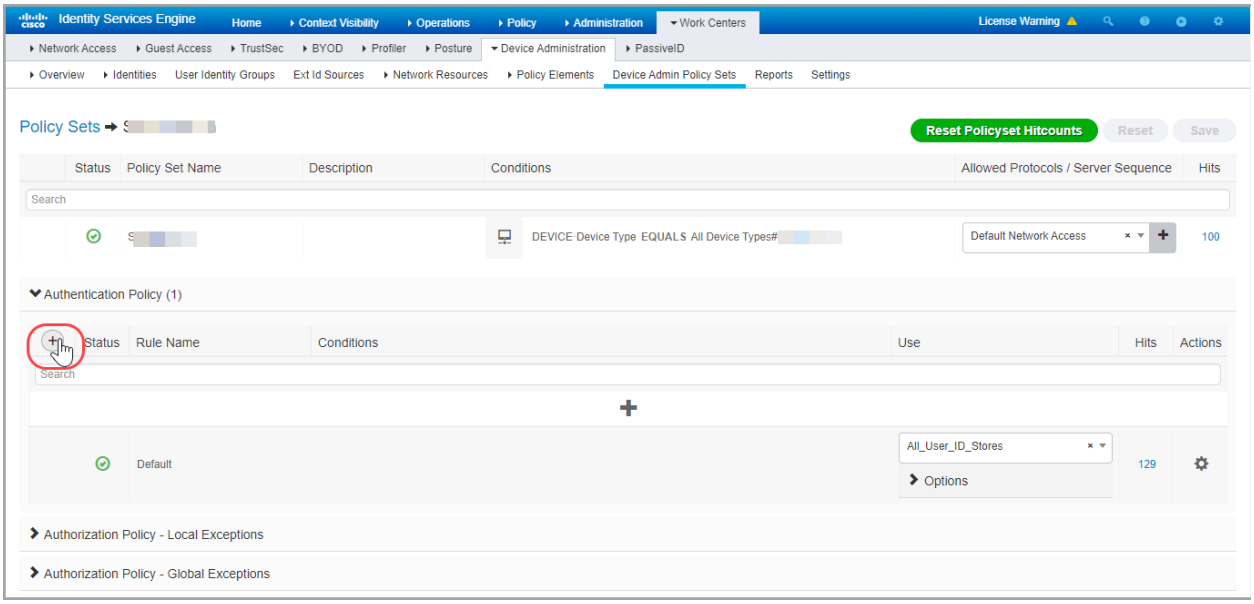
プライマリ管理者ロールをシェルプロファイルに割り当てると、追加のロールは許可されません。管理者以外のロールの組み合わせを作成する場合には、要件を満たしていることを確認してください。

10. [保存（Save）] をクリックします。
11. 「**2. TACACS+ プロファイルの作成**」の手順を繰り返して、追加の TACACS+ シェルプロファイルを ISE に追加します。

3. グループまたはユーザーへのシェルプロファイルのマッピング

次の手順を使用して、許可ルールにシェルプロファイルをマッピングします。

1. **[ワークセンター(Work Centers)]** > **[デバイス管理(Device Administration)]** > **[デバイス管理ポリシーセット(Device Admin Policy Sets)]** の順に選択します。
2. ポリシーセット名を見つけます。 > 矢印アイコンをクリックします。
3. 許可ポリシーを見つけます。 > 矢印アイコンをクリックします。
4. プラス記号(+)アイコンをクリックします。



5. [条件(Conditions)] フィールドで、プラス記号(+)アイコンをクリックします。ポリシー条件を設定します。

   ヘルプ:[条件スタジオ(Conditions Studio)] の手順については、?[ヘルプ] アイコンをクリックしてください。

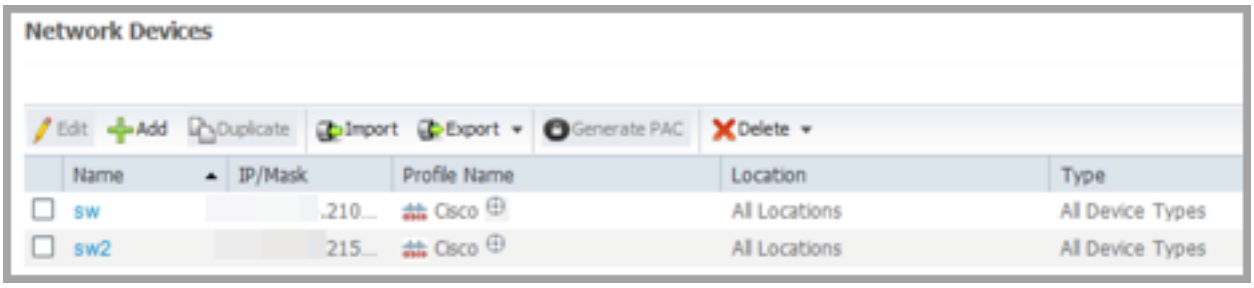
6. [シェルプロファイル(Shell Profiles)] フィールドで、「**2. TACACS+ プロファイルの作成**」で作成したシェルプロファイルを追加します。
7. 認証ルールにすべてのシェルプロファイルがマッピングされるまで、「**3. グループまたはユーザーへのシェルプロファイルのマッピング**」の手順を繰り返します。

4. Secure Network Analytics をネットワークデバイスとして追加

1. **[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Devices）]** を選択します。
2. [ネットワークデバイス（Network Devices）] を選択し、**[+追加（+Add）]** をクリックします。
3. プライマリ マネージャの次の情報を入力します。フィールドは以下のとおりです。

    - [名前（Name）]：マネージャの名前を入力します。
    - [IPアドレス（IP Address）]：マネージャの IP アドレスを入力します。
    - [共有秘密（Shared Secret）]：共有秘密キーを入力します。

4. [保存（Save）] をクリックします。
5. ネットワークデバイスが [ネットワークデバイス（Network Devices）] リストに保存されていることを確認します。



6. 「2. Secure Network Analytics での TACACS+ 認証の有効化」に進みます。

2. Secure Network Analytics での TACACS+ 認証の有効化

Secure Network Analytics に TACACS+ サーバーを追加し、リモート許可を有効にするには、次の手順を使用します。

> Secure Network Analytics に TACACS+ サーバーを追加できるのは、プライマリ管理者だけです。

1. プライマリ マネージャにログインします。
2. メインメニューから、[設定(Configure)] > [グローバルユーザー管理(GLOBAL User Management)] を選択します。
3. **[認証と許可(Authentication and Authorization)]** タブをクリックします。
4. [作成(Create)] をクリックします。**[認証サービス(Authentication Service)]** を選択します。
5. [認証サービス(Authentication Service)] ドロップダウンをクリックします。[TACACS+] を選択します。
6. 各フィールドに入力します。

フィールド	(注)
名前(Name)	一意の名前を入力して、サーバーを識別します。
説明(Description)	サーバーの使用方法または理由を指定する説明を入力します。
キャッシュタイムアウト(秒) (Cache Timeout(秒))	Secure Network Analytics が情報の再入力を要求するまでに、ユーザー名またはパスワードが有効と見なされる時間(秒単位)。
プレフィックス(Prefix)	このフィールドは任意です。プレフィックス文字列は、名前が RADIUS または TACACS+ サーバーに送信されるときにユーザー名の先頭に付きます。たとえば、ユーザー名が *zoe* でレルムプレフィックスが *DOMAIN-A¥* の場合、ユーザー名 DOMAIN-A¥zoe がサーバーに送信されます。[プレフィックス(Prefix)] フィールドを設定しない場合は、ユーザー名のみがサーバーに送信されます。

サフィックス	このフィールドは任意です。サフィックス文字列は、ユーザー名の末尾に付きます。たとえば、サフィックスが *@mydomain.com* の場合、ユーザー名 *zoe@mydomain.com* が TACACS+ サーバーに送信されます。[サフィックス(Suffix)] フィールドを設定しない場合は、ユーザー名のみがサーバーに送信されます。

8. [サーバー(Servers)] セクションで、**[新規追加(Add New)]** をクリックします。
9. 次のフィールドに入力します。

フィールド	**(注)**
IP アドレス(IP Address)	認証サービスを構成する場合は、IPv4 アドレスまたは IPv6 アドレスを使用します。
ポート(Port)	適用可能なポートに対応する 0 ～ 65535 の任意の番号を入力します。
秘密キー(Secret Key)	適用可能なサーバー用に設定された秘密キーを入力します。

10. [追加(Add)] をクリックします。
11. [保存(Save)] をクリックします。
12. 新しい TACACS+ サーバーがリストに表示されていることを確認します。
13. TACACS+ サーバーの **[アクション(Actions)]** メニューをクリックします。
14. ドロップダウンメニューから、**[リモート許可の有効化(Enable Remote Authorization)]** を選択します。
15. 画面に表示される指示に従って、TACACS+ を有効にします。

3. リモート TACACS+ ユーザーのログインテスト

マネージャにログインするには、次の手順を実行します。TACACS+ のリモート許可については、すべてのユーザーがマネージャ経由でログインしていることを確認してください。

> アプライアンス直接ログインしてアプライアンスの管理を使用するには、ローカルでログインします。

1. ブラウザのアドレスフィールドに、次のように入力します。

   https:// の後にマネージャの IP アドレスを指定します。

2. リモート TACACS+ ユーザーのユーザー名とパスワードを入力します。
3. [サインイン（Sign In）] をクリックします。

   ユーザーがマネージャにログインできない場合は、「**トラブルシューティング**」を確認してください。

トラブルシューティング

これらのトラブルシューティング シナリオのいずれかが発生した場合は、管理者に連絡して、ここで提供するソリューションで設定を確認してください。管理者が問題を解決できない場合は、シスコサポートに連絡してください。

シナリオ

シナリオ	注記
特定の TACACS+ ユーザーがログインできない	• **不正なマッピング**または**ロールの無効な組み合わせ**によるユーザーログイン失敗の監査ログを確認します。この問題は、ID グループのシェルプロファイルにプライマリ管理者と追加のロールが含まれている場合、または管理者以外のロールの組み合わせが要件を満たしていない場合に発生する可能性があります。詳細については、「**ユーザーロールの概要**」を参照してください。 • TACACS+ のユーザー名がローカル（Secure Network Analytics）のユーザー名と同じでないことを確認してください。詳細については、「**ユーザーロールの概要**」を参照してください。

すべての TACACS+ ユーザーがログインできない	• Secure Network Analytics で TACACS+ の設定を確認します。
	• TACACS+ サーバーの設定を確認します。
	• TACACS+ サーバーが動作していることを確認します。
	• Secure Network Analytics で TACACS+ サービスが有効になっていることを確認します。
	  • 複数の認証サーバーを定義することはできますが、許可のために有効にできるのは 1 つだけです。詳細については、「**2. Secure Network Analytics での TACACS+ 認証の有効化**」を参照してください。
	  • 特定の TACACS+ サーバーの認証を有効にする方法については、「**2. Secure Network Analytics での TACACS+ 認証の有効化**」を参照してください。

ユーザーがログインすると、マネージャにはローカルでのみアクセスできます。	Secure Network Analytics（ローカル）と TACACS+ サーバー（リモート）に同じ名前を持つユーザーが存在する場合、ローカルログインによってリモートログインがオーバーライドされます。詳細については、「**ユーザーロールの概要**」を参照してください。

サポートへの問い合わせ

テクニカル サポートが必要な場合は、次のいずれかを実行してください。

- 最寄りのシスコ パートナーにご連絡ください。
- シスコサポートの連絡先
- Web でケースを開く場合：http://www.cisco.com/c/en/us/support/index.html
- 電子メールでケースを開く場合：tac@cisco.com
- 電話でサポートを受ける場合：800-553-2447（米国）
- ワールドワイド サポート番号：
  https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

変更履歴

マニュアルのバージョン	公開日	説明
1_0	2023 年 3 月 3 日	最初のバージョン。

著作権情報