ISE 2.0: ASA CLI TACACS+ 認証およびコマンド認可の設定例

目次

概要

このドキュメントでは、Identity Service Engine（ISE）2.0 以降を搭載した Cisco 適応型セキュリティ アプライアンス（ASA）に TACACS+ 認証およびコマンド許可を設定する方法について説明します。 ISE は、ユーザ、マシン、グループ、エンドポイントなどのリソースを保存するためにローカル ID ストアを使用します。

前提条件

要件

次の項目に関する知識が推奨されます。

- ASA ファイアウォールが完全に機能していること
- ASA と ISE 間の接続
- ISE サーバがブートストラップされていること

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 Identity Service Engine 2.0
- Cisco ASA ソフトウェア リリース 9.5(1)

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。

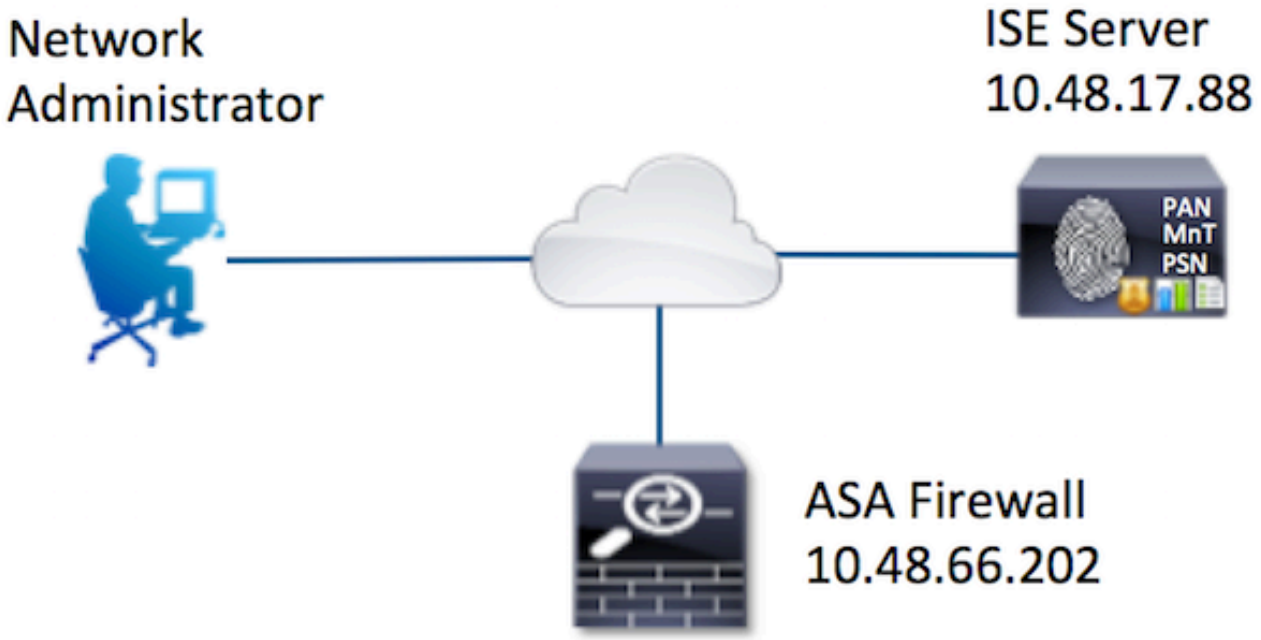
ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

この設定の目標は次のとおりです。

- 内部 ID ストアを介して ssh ユーザを認証する
- ssh ユーザを認可して、ユーザがログイン後に特権 EXEC モードに入るようにする
- 検証のため ISEに、実行されたコマンドを確認し、送信する

ネットワーク図



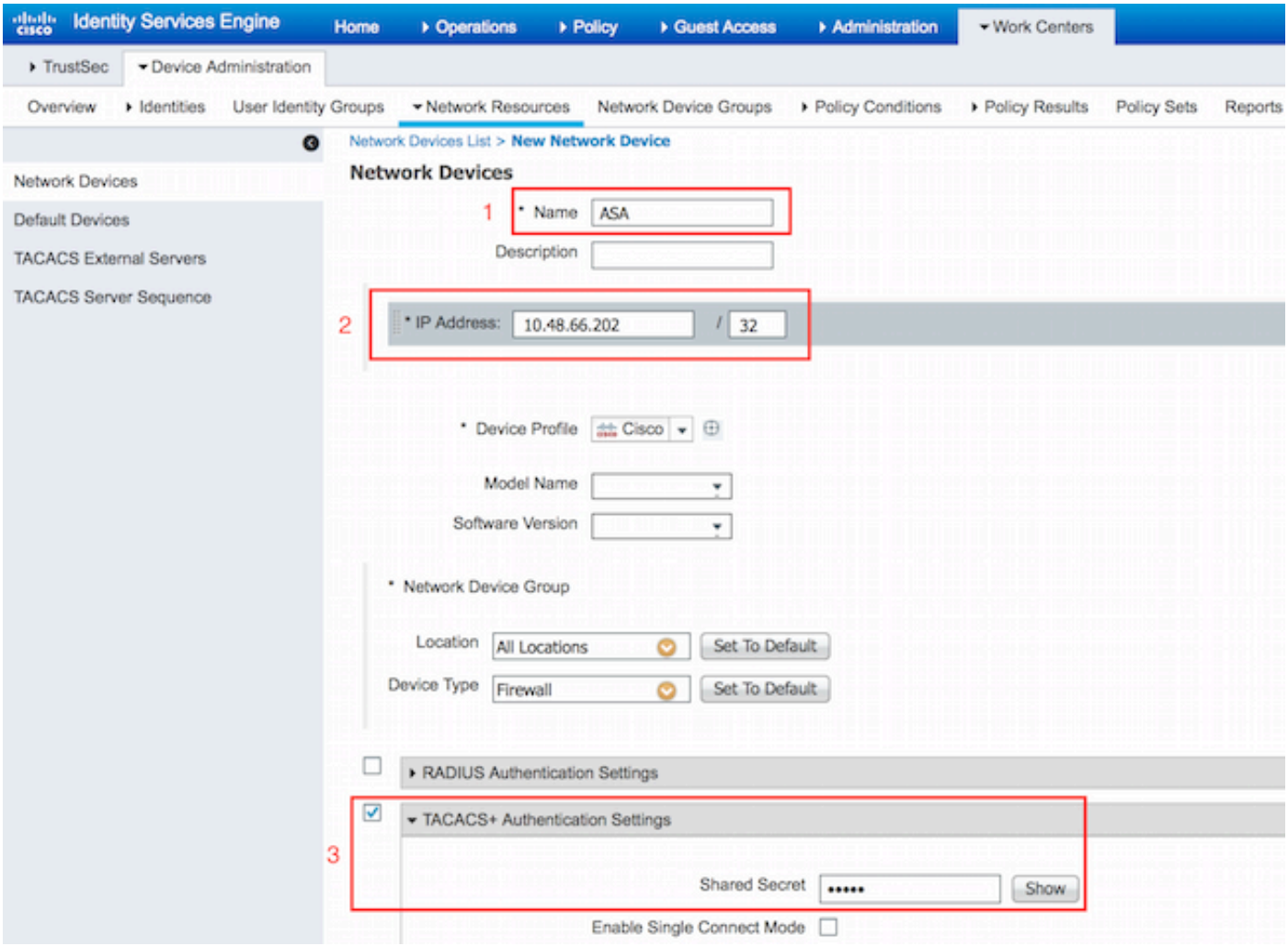
設定

認証および認可のための ISE の設定

2 種類のユーザが作成されます。 **administrator** ユーザは、ISE の **Network Admins** ローカル ID グループのメンバーです。 このユーザはすべての CLI 権限を持っています。 **user** ユーザは、ISE の **Network Maintenance Team** ローカル ID グループのメンバーです。 このユーザは、show コマンドと ping のみを実行できます。

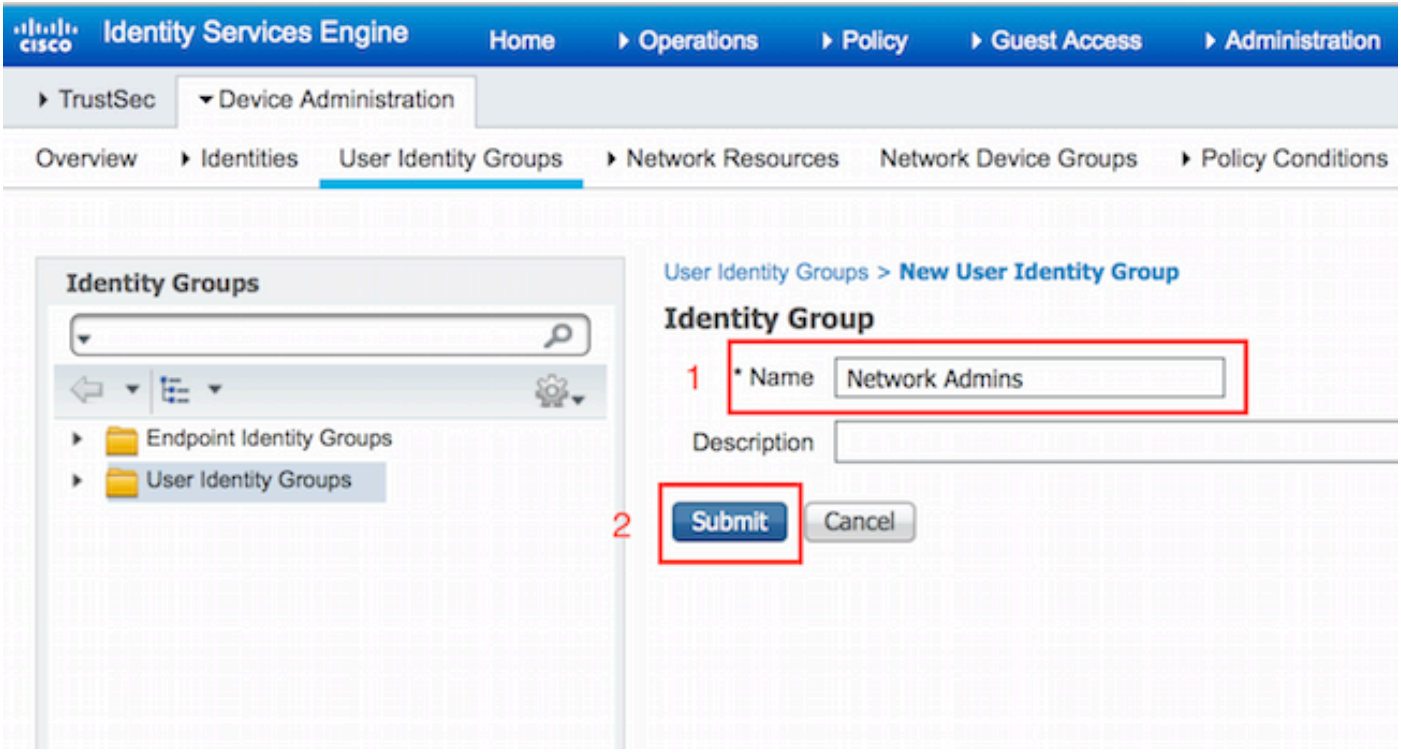
ネットワーク デバイスの追加

[Work Centers] > [Device Administration] > [Network Resources] > [Network Devices] を選択します。 [Add] をクリックします。 [Name] と [IP Address] を入力し、[TACACS+ Authentication Settings] チェックボックスをオンにして、[Shared Secret] に共有秘密キーを入力します。 （任意）デバイスのタイプ/ロケーションを指定できます。



ユーザ ID グループの設定

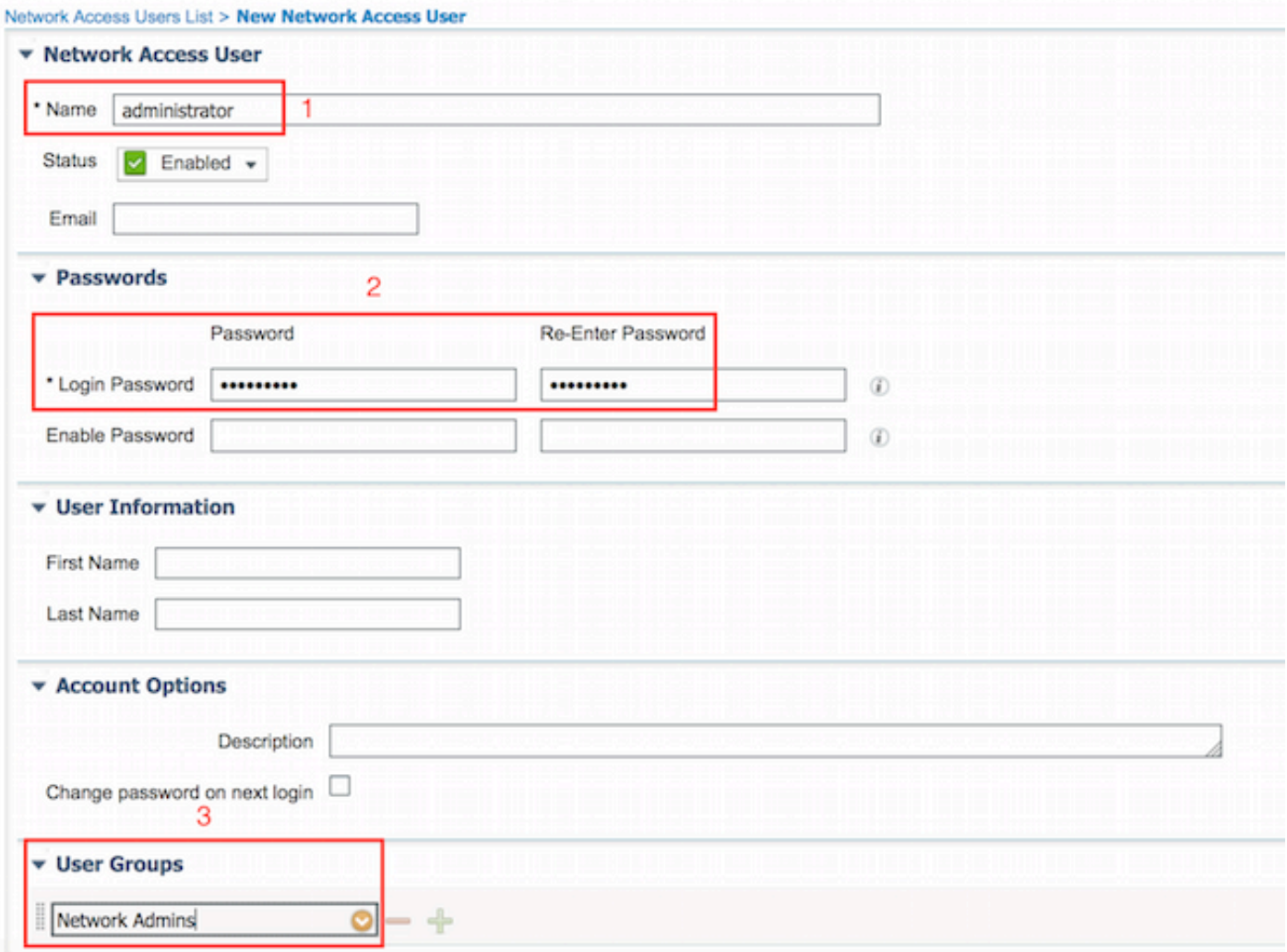
[Work Centers] > [Device Administration] > [User Identity Groups] に移動します。 [Add] をクリックします。 [Name] を入力し、[Submit] をクリックします。



同じ手順を繰り返して、**Network Maintenace Team** ユーザ ID グループを設定します。

ユーザの設定

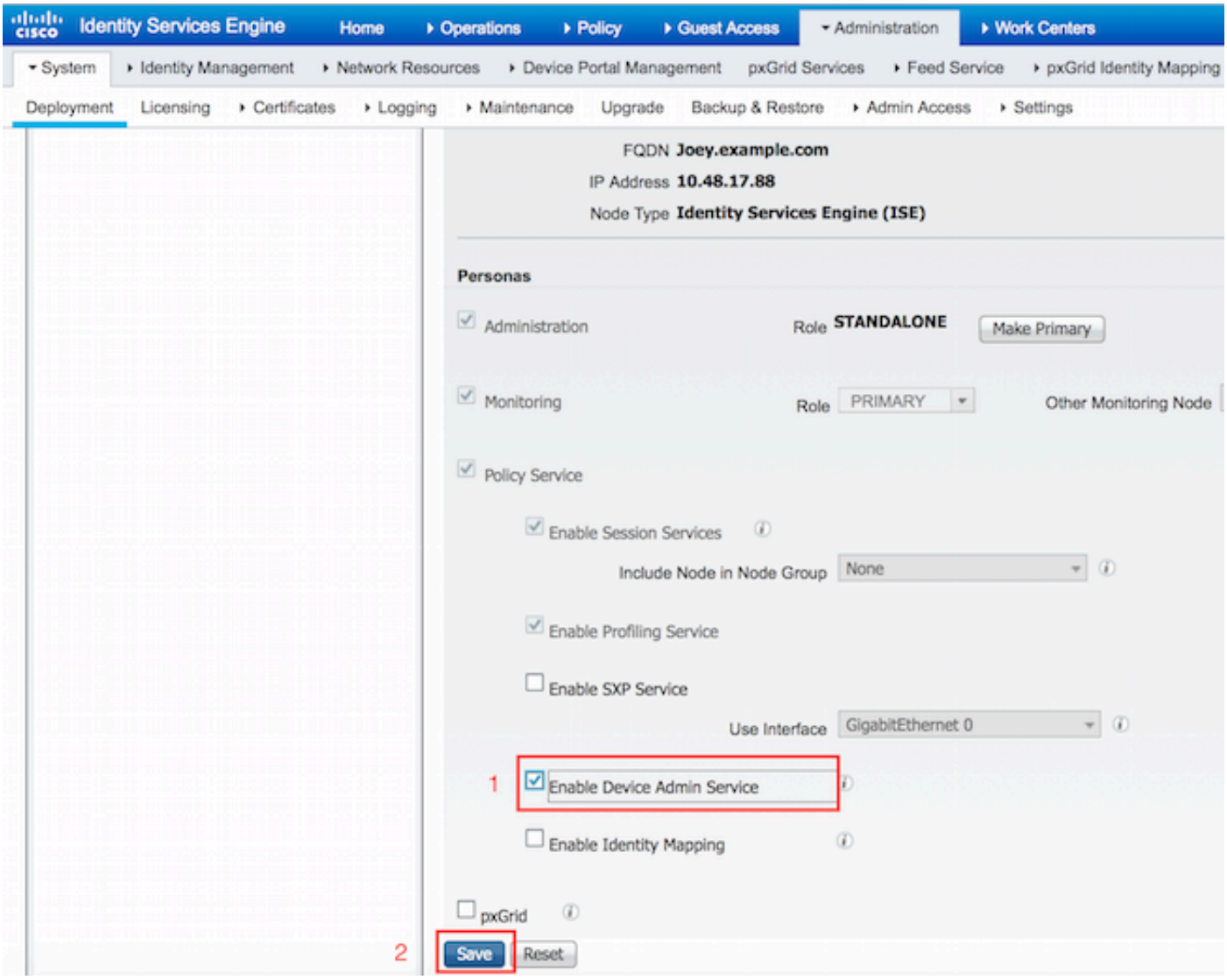
[Work Centers] > [Device Administration] > [Identities] > [Users] に移動します。 [Add] をクリックします。 [Name] と [Login Password] を入力し、[User Group] を指定して、[Submit] をクリックします。



手順を繰り返して、**user** ユーザを設定し、**Network Maintenace Team** ローカル ID グループを割り当てます。

Enable Device Admin Service

[Administration] > [System] > [Deployment] を選択します。 必要なノードを選択します。 [Enable Device Admin Service] チェックボックスを選択し、[Save] をクリックします

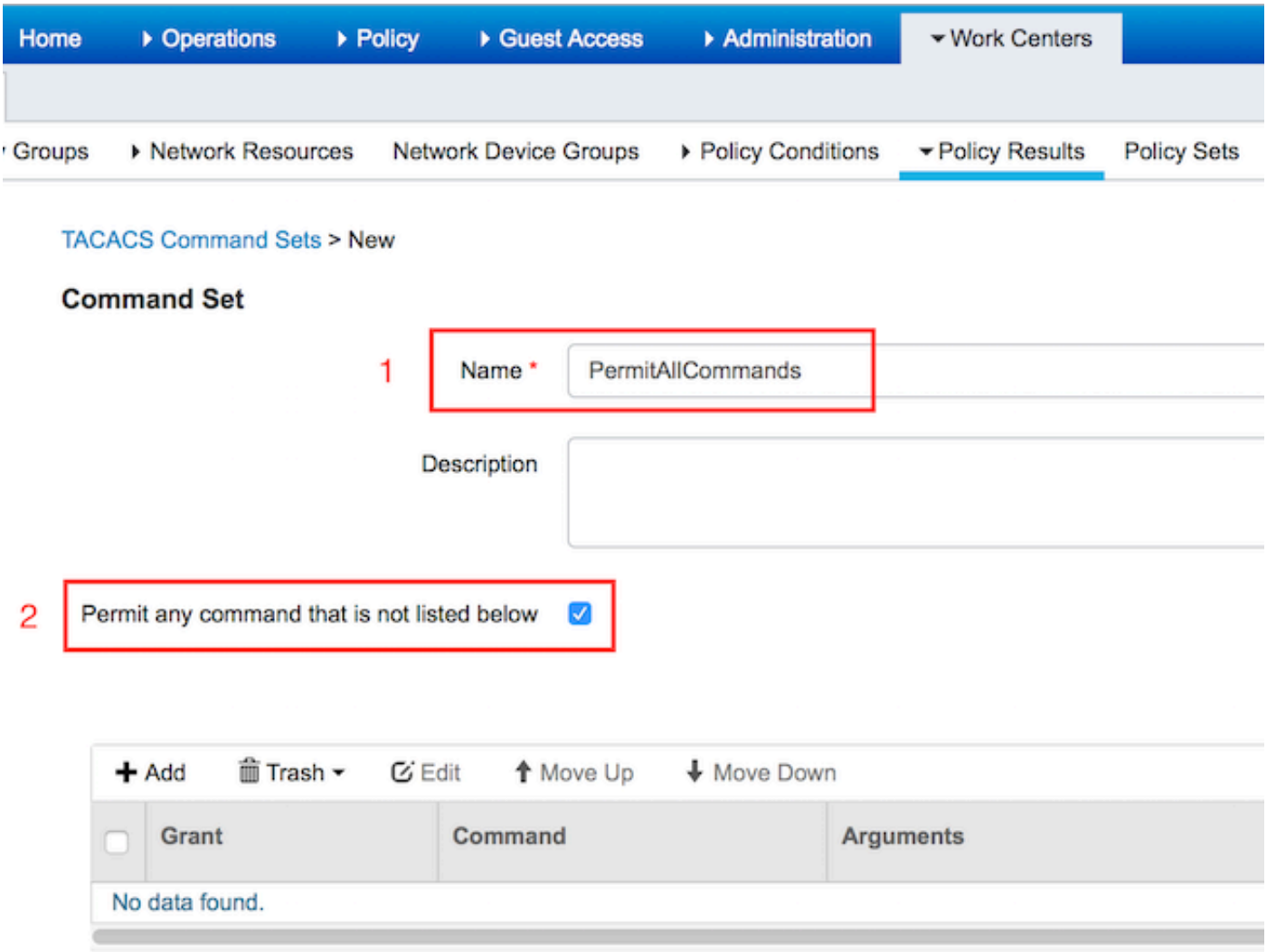


注: TACACS 用に、別のライセンスをインストールする必要があります。

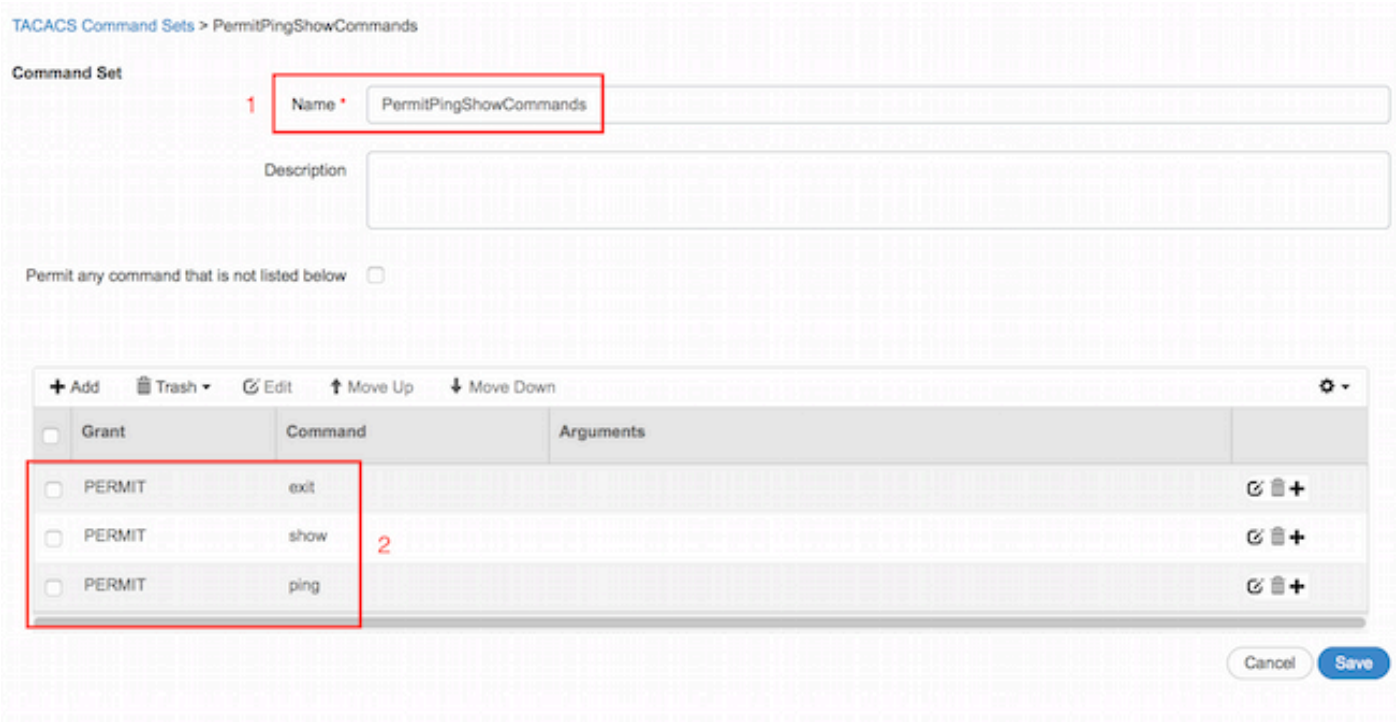
TACACS コマンド セットの設定

2 つの コマンド セットを設定します。 1 つ目は **administrator** ユーザ用の **PermitAllCommands** で、デバイスのすべてのコマンドを許可します。 2 つ目は **user** ユーザ用の **PermitPingShowCommands** で、show および ping コマンドのみを許可します。

1. [Work Centers] > [Device Administration] > [Policy Results] > [TACACS Command Sets] を選択します。 [Add] をクリックします。 [Name] に「PermitAllCommands」と入力し、[Permit any command that is not listed below] チェックボックスをオンにして、[Submit] をクリックします。

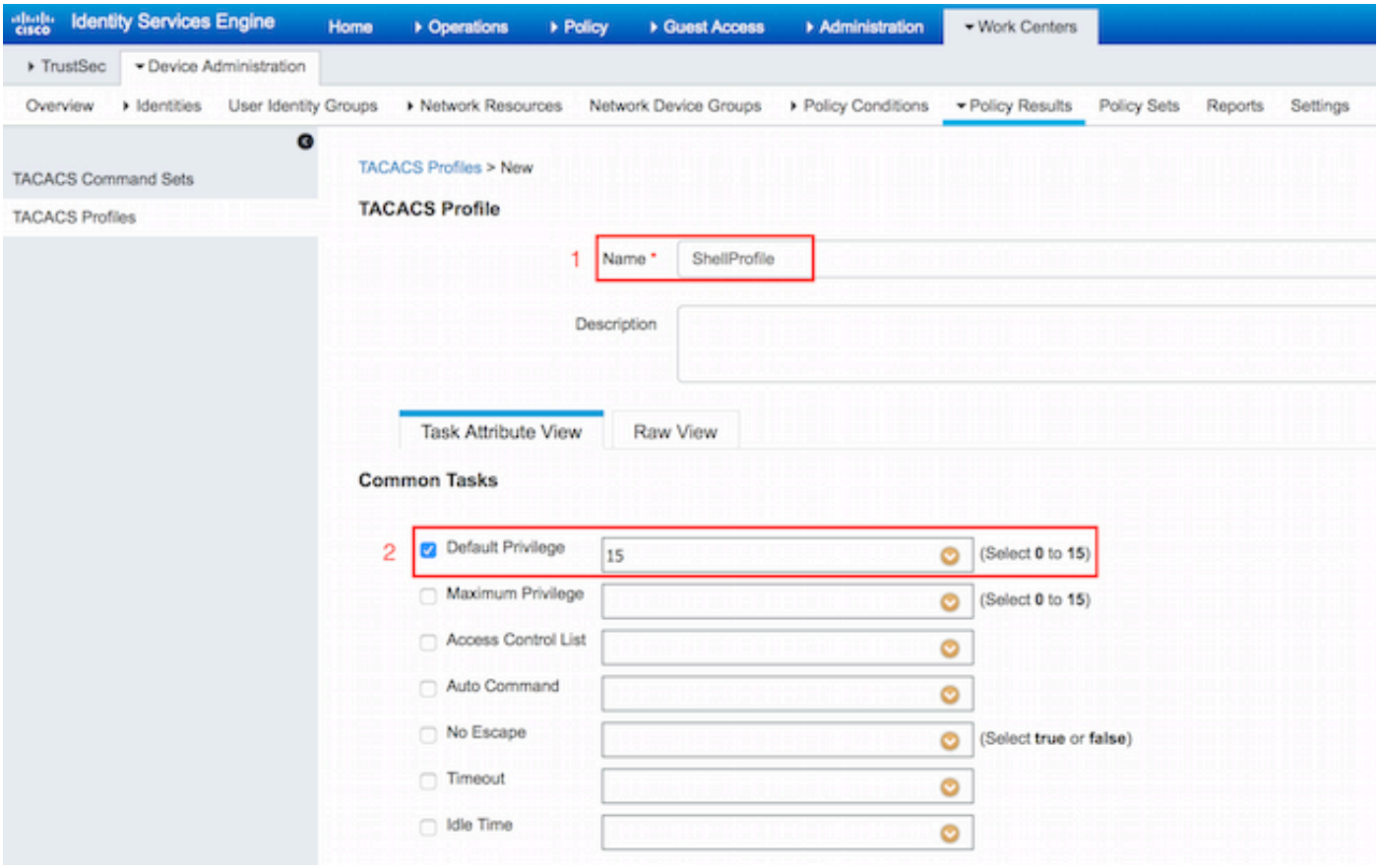


2. [Work Centers] > [Device Administration] > [Policy Results] > [TACACS Command Sets] を選択します。 [Add] をクリックします。 [Name] に「PermitPingShowCommands」と入力し、[Add] をクリックして **show**、**ping** および **exit** コマンドを許可します。 デフォルトでは、[Arguments] を空白のままにするとすべての引数が含まれます。 [Submit] をクリックします。



TACACS プロファイルの設定

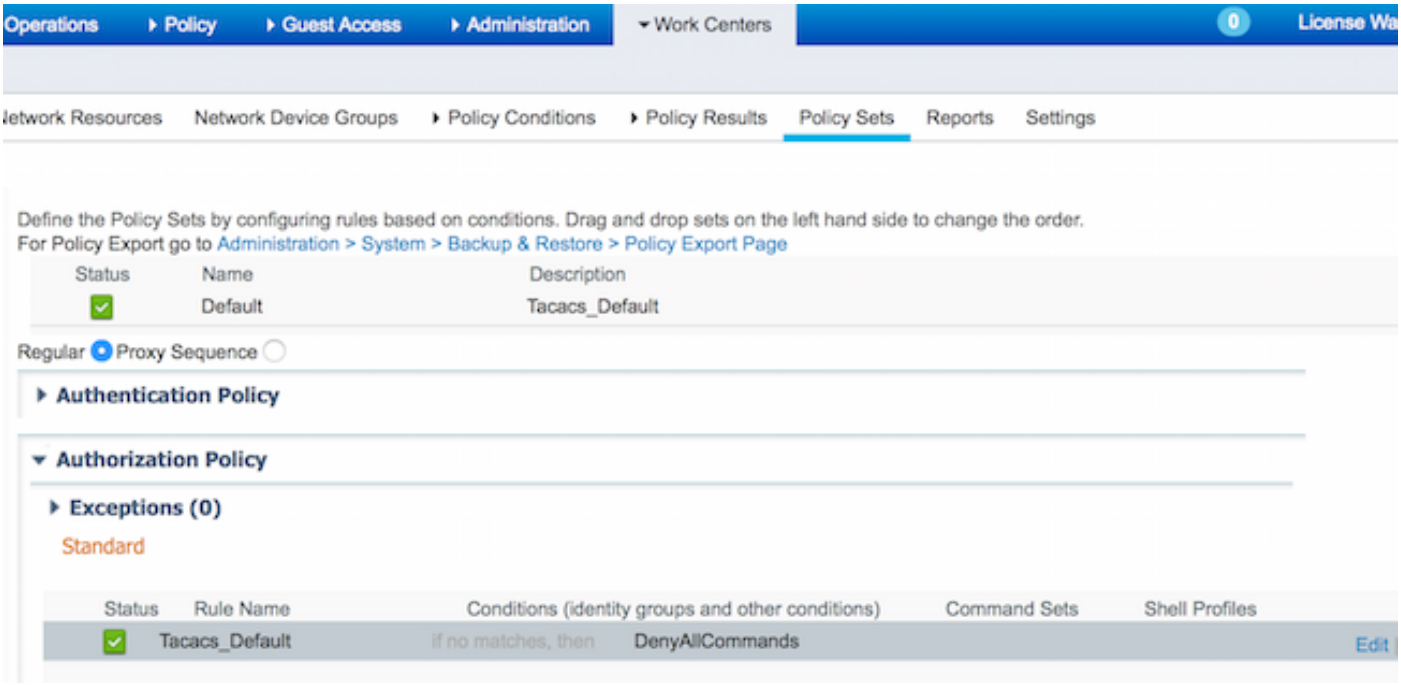
1 つの TACACS プロファイルが設定されます。 実際のコマンドの適用は、コマンド セットを通じて行います。 [Work Centers] > [Device Administration] > [Policy Results] > [TACACS Profiles] を選択します。 [Add] をクリックします。 [Name] に「ShellProfile」と入力し、[Default Privilege] チェックボックスをオンにして、値 15 を入力します。 [Submit] をクリックします。



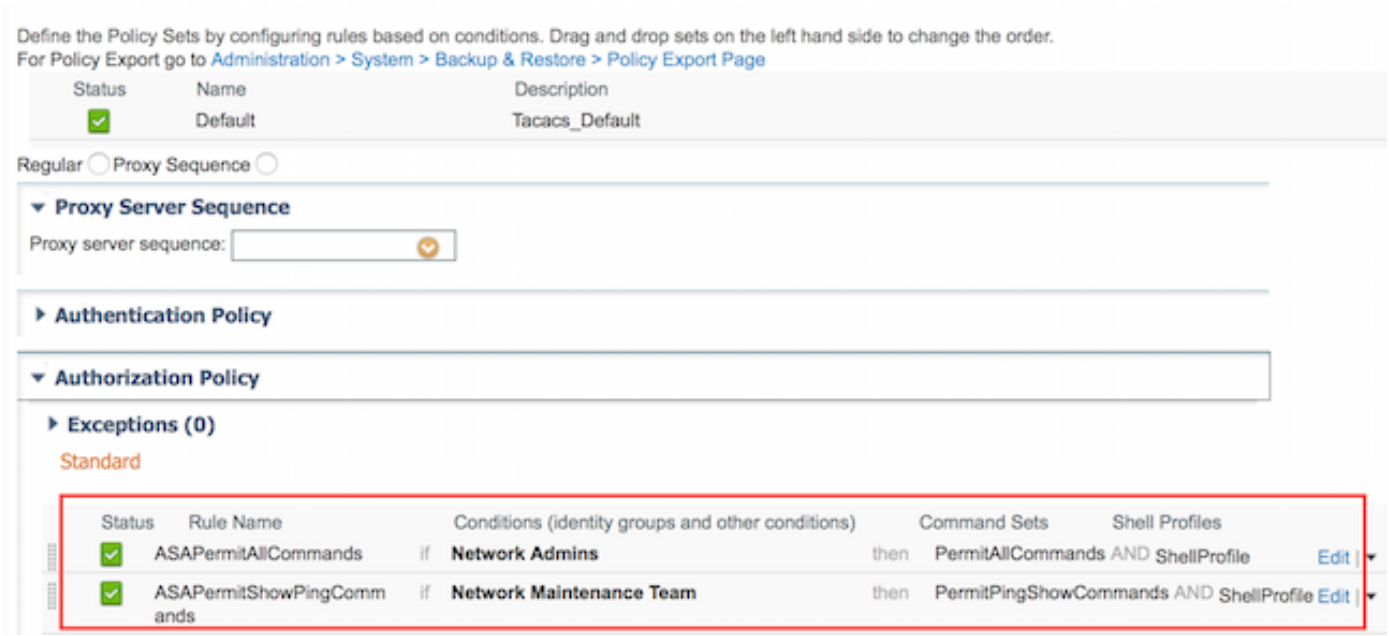
TACACS 認可ポリシーの設定

デフォルトでは、[Authentication Policy] は All_User_ID_Stores を指します。これにはローカル ストアも含まれているので、未変更のままにします。

[Work Centers] > [Device Administration] > [Policy Sets] > [Default] > [Authorization Policy] > [Edit] > [Insert New Rule Above] を選択します。



2 つの認可ルールを設定します。1 つ目のルールは、TACACS プロファイル **ShellProfile** とコマンド セット **PermitAllCommands** を、**Network Admins** ユーザ ID グループのメンバーシップに基づいて割り当てます。 2 つ目のルールは、TACACS プロファイル **ShellProfile** とコマンド セット **PermitPingShowCommands** を、**Network Maintenance Team** ユーザ ID グループのメンバーシップに基づいて割り当てます。



認証および認可のための Cisco ASA ファイアウォールの設定

1. 次に示すように、**username** コマンドを使用して、フォールバックに対する全権限を持つローカル ユーザを作成します。

```
ciscoasa(config)# username cisco password cisco privilege 15
```

2. TACACS サーバの ISE を定義し、インターフェイス、プロトコル IP アドレス、tacacs キーを指定します。

```
ciscoasa(config)# username cisco password cisco privilege 15
```

注: サーバ キーは ISE サーバで以前指定したものと一致している必要があります。

3. 次に示すように、**aaa コマンド** により、TACACS サーバの到達可能性をテストします。

```
ciscoasa# test aaa authentication ISE host 10.48.17.88 username administrator Krakow123
INFO: Attempting Authentication test to IP address <10.48.17.88> (timeout: 12 seconds)
INFO: Authentication Successful
```

前のコマンドの出力では、TACACS サーバが到達可能であり、ユーザが正常に認証されたことを示しています。

4. 次に示すように、ssh に対する認証、EXEC 認可、コマンド許可を設定します。 **aaa authorization exec authentication-server auto-enable** により、自動的に特権 EXEC モードに入ります。

```
ciscoasa# test aaa authentication ISE host 10.48.17.88 username administrator Krakow123
INFO: Attempting Authentication test to IP address <10.48.17.88> (timeout: 12 seconds)
INFO: Authentication Successful
```

注: 上記のコマンドによって、ISE で認証が実行され、ユーザが直接に特権モードに入り、コマンド認可が行われます。

5. mgmt インターフェイスでの shh を許可します。

```
ciscoasa# test aaa authentication ISE host 10.48.17.88 username administrator Krakow123
INFO: Attempting Authentication test to IP address <10.48.17.88> (timeout: 12 seconds)
INFO: Authentication Successful
```

確認

Cisco ASA ファイアウォールの確認

1. フル アクセスできるユーザ ID グループに属す **administrator** として、ASA ファイアウォールに ssh します。 **Network Admins** グループが、ISE で **ShellProfile** と **PermitAllCommands** コマンド セットにマッピングされます。 フル アクセスを確認するコマンドを実行します。

```
EKORNEYC-M-K04E:~ ekorneyc$ ssh administrator@10.48.66.202
administrator@10.48.66.202's password:
Type help or '?' for a list of available commands.
ciscoasa#
ciscoasa# configure terminal
ciscoasa(config)# crypto ikev1 policy 10
ciscoasa(config-ikev1-policy)# encryption aes
ciscoasa(config-ikev1-policy)# exit
```

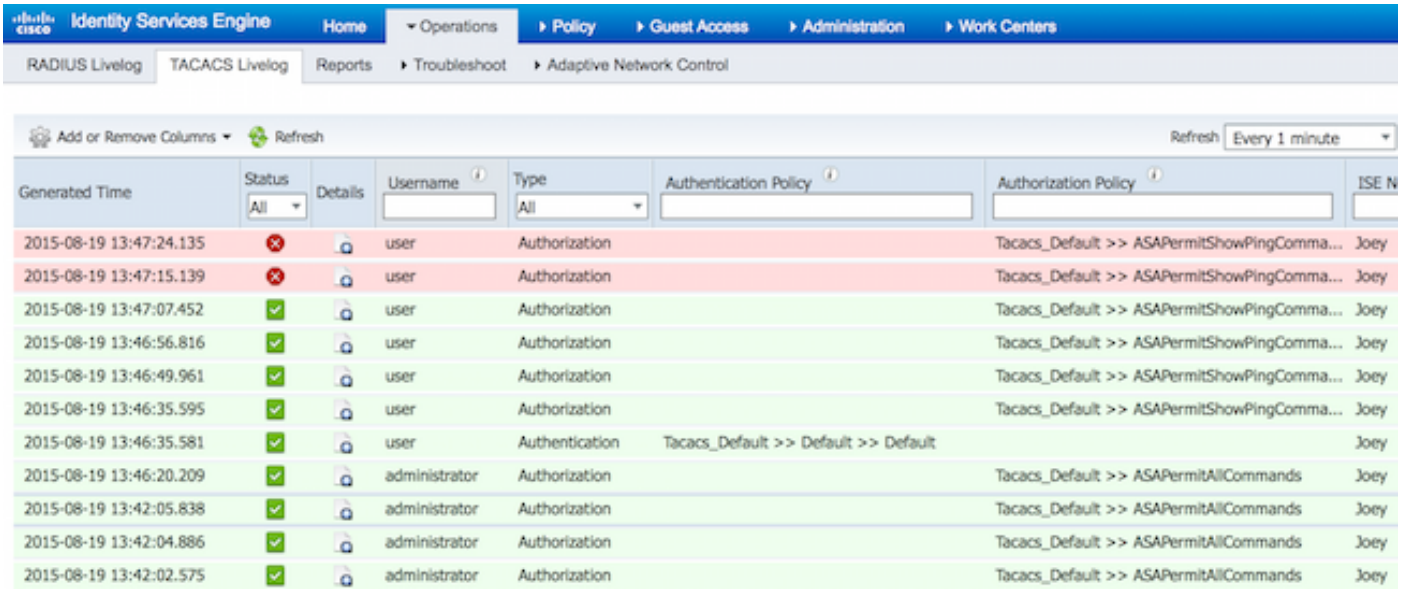
```
ciscoasa(config)# exit
ciscoasa#
```

2. アクセス制限があるユーザ ID グループに属す **user** として、ASA ファイアウォールに ssh します。 **Network Maintenance** グループが、ISE で **ShellProfile** と **PermitPingShowCommands** コマンドセットにマッピングされます。 任意のコマンドを実行して、show と ping コマンドのみが発行されることを確認します。

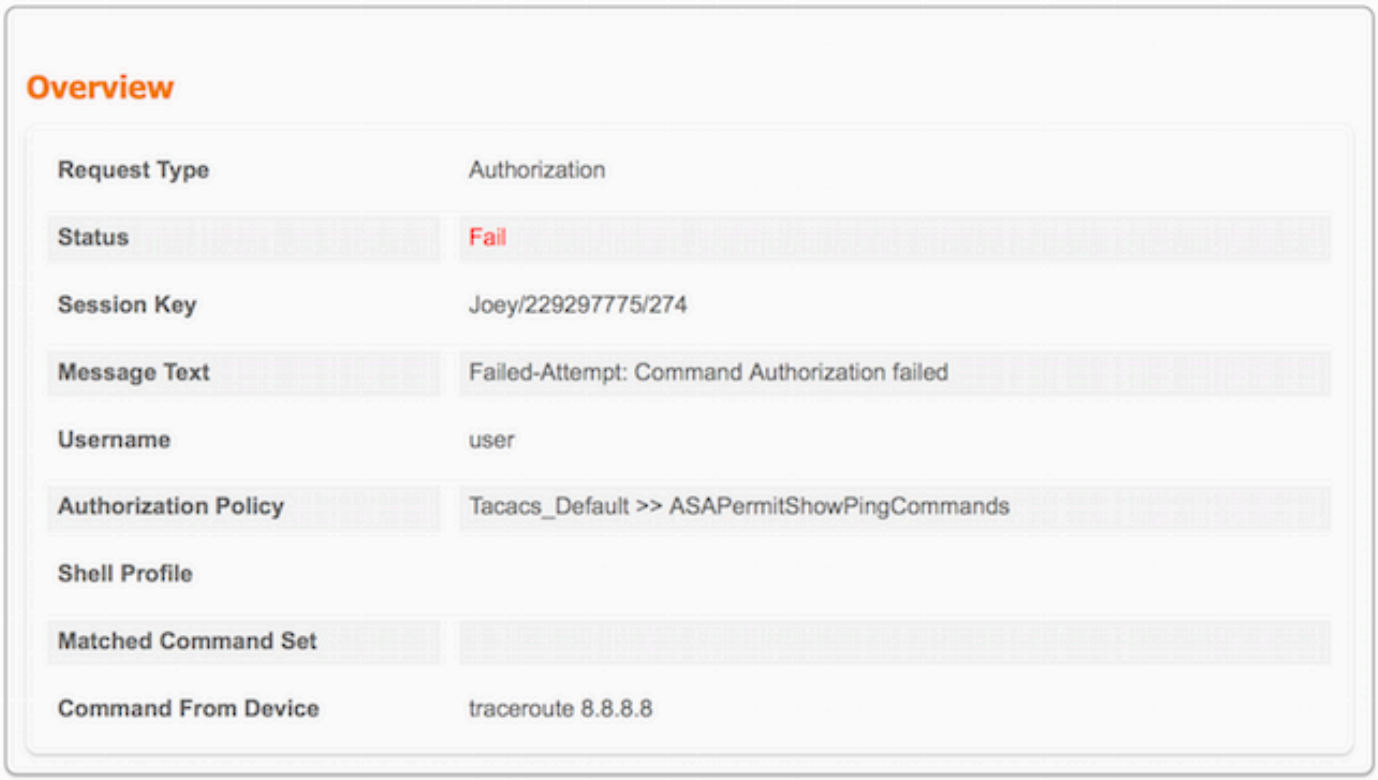
```
EKORNEYC-M-K04E:~ ekorneyc$ ssh user@10.48.66.202
administrator@10.48.66.202's password:
Type help or '?' for a list of available commands.
ciscoasa#
ciscoasa# show version | include Software
Cisco Adaptive Security Appliance Software Version 9.5(1)
ciscoasa# ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/24/30 ms
ciscoasa# configure terminal
Command authorization failed
ciscoasa# traceroute 8.8.8.8
Command authorization failed
```

ISE 2.0 の検証

1. [Operations] > [TACACS Livelog] を選択します。 上記で行った試行が表示されていることを確認します。



2. 赤色のレポートの [details] をクリックすると、以前実行して失敗したコマンドが表示されます。



トラブルシューティング

Error: Failed-Attempt: Command Authorization failed

SelectedCommandSet 属性を調べて、認可ポリシーで予想どおりのコマンド セットが選択されていることを確認します。

関連情報

テクニカル サポートとドキュメント – Cisco Systems

ISE 2.0 リリース ノート

ISE 2.0 ハードウェア インストール ガイド

ISE 2.0 アップグレード ガイド

ACS から ISE への移行ツール ガイド

ISE 2.0 Active Directory 統合ガイド"

ISE 2.0 エンジン管理者ガイド