ISE 2.0 TACACS+認証コマンド許可の設定

内容

概要

このドキュメントでは、Microsoft Active Directory(AD)グループメンバーシップに基づいて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。

背景説明

Identity Service Engine(ISE)2.0以降を搭載したユーザのMicrosoft Active Directory(AD)グループメンバーシップに基づいてTACACS+認証およびコマンド許可を設定するために、ISEはADを外部IDストアとして使用し、ユーザ、マシン、グループ、属性などのリソースを格納します。

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 IOSルータが完全に動作している

- ルータと ISE 間の接続。
- ISE サーバがブートストラップされ、Microsoft AD に接続できる

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いています。

- Cisco Identity Service Engine 2.0
- Cisco IOS® ソフトウェア リリース 15.4(3)M3
- Microsoft Windows Server 2012 R2

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、初期（デフォルト）設定の状態から起動しています。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。

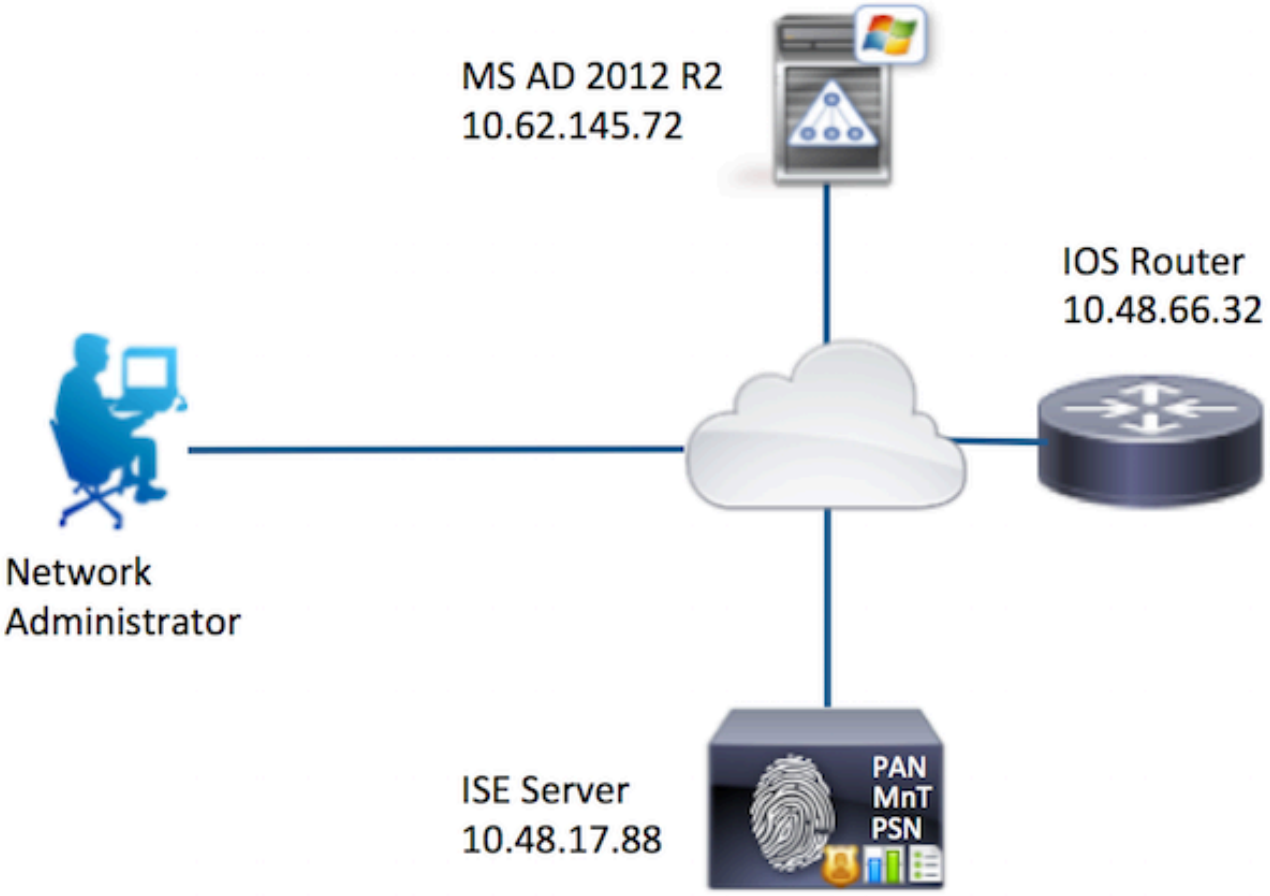
ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

この設定の目標は次のとおりです。

- AD 経由の telnet ユーザを認証する
- Telnet ユーザを認可し、ログイン後に特権 EXEC モードを与える
- 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

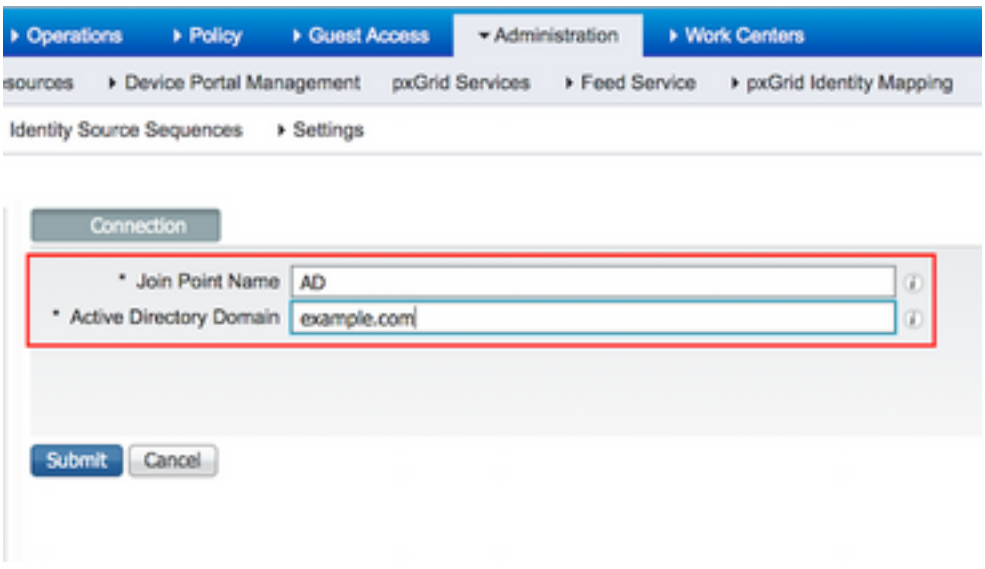


設定

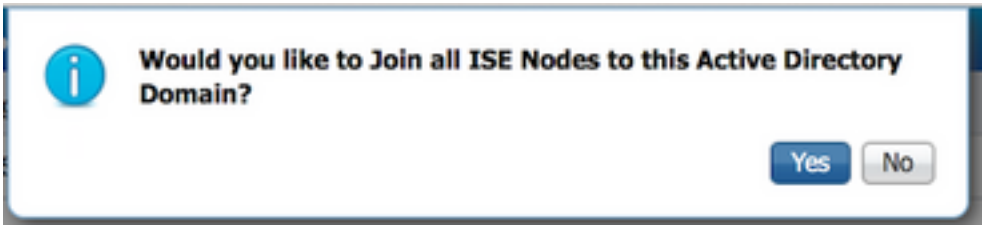
認証および認可のための ISE の設定

ISE 2.0 の Active Directory への参加

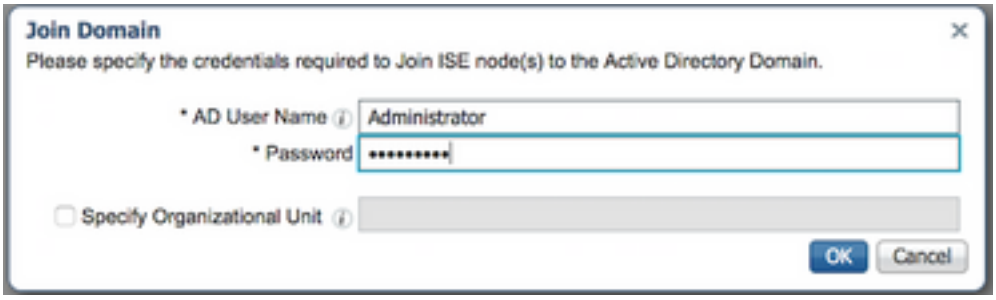
1. [Administration] > [Identity Management] > [External Identity Stores] > [Active Directory] > [Add] に移動します。[Join Point Name] と [Active Directory Domain] に入力し、[Submit] をクリックします。



2. [Join all ISE Nodes to this Active Directory Domain]プロンプトが表示されたら、[**Yes**]をクリックします。



3. ADユーザ名とパスワードを入力し、**OK**をクリックします。

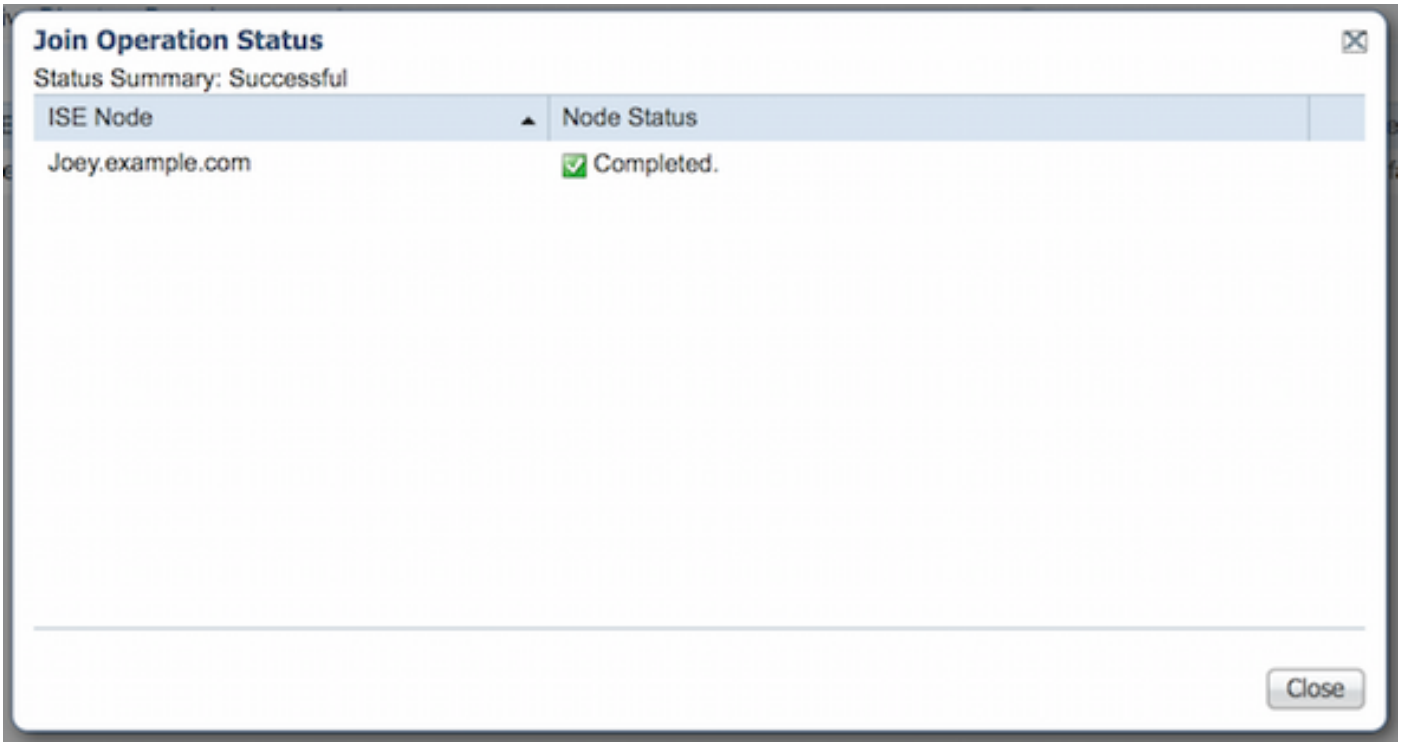


ISEのドメインアクセスに必要なADアカウントは、次のいずれかを持つことができます。

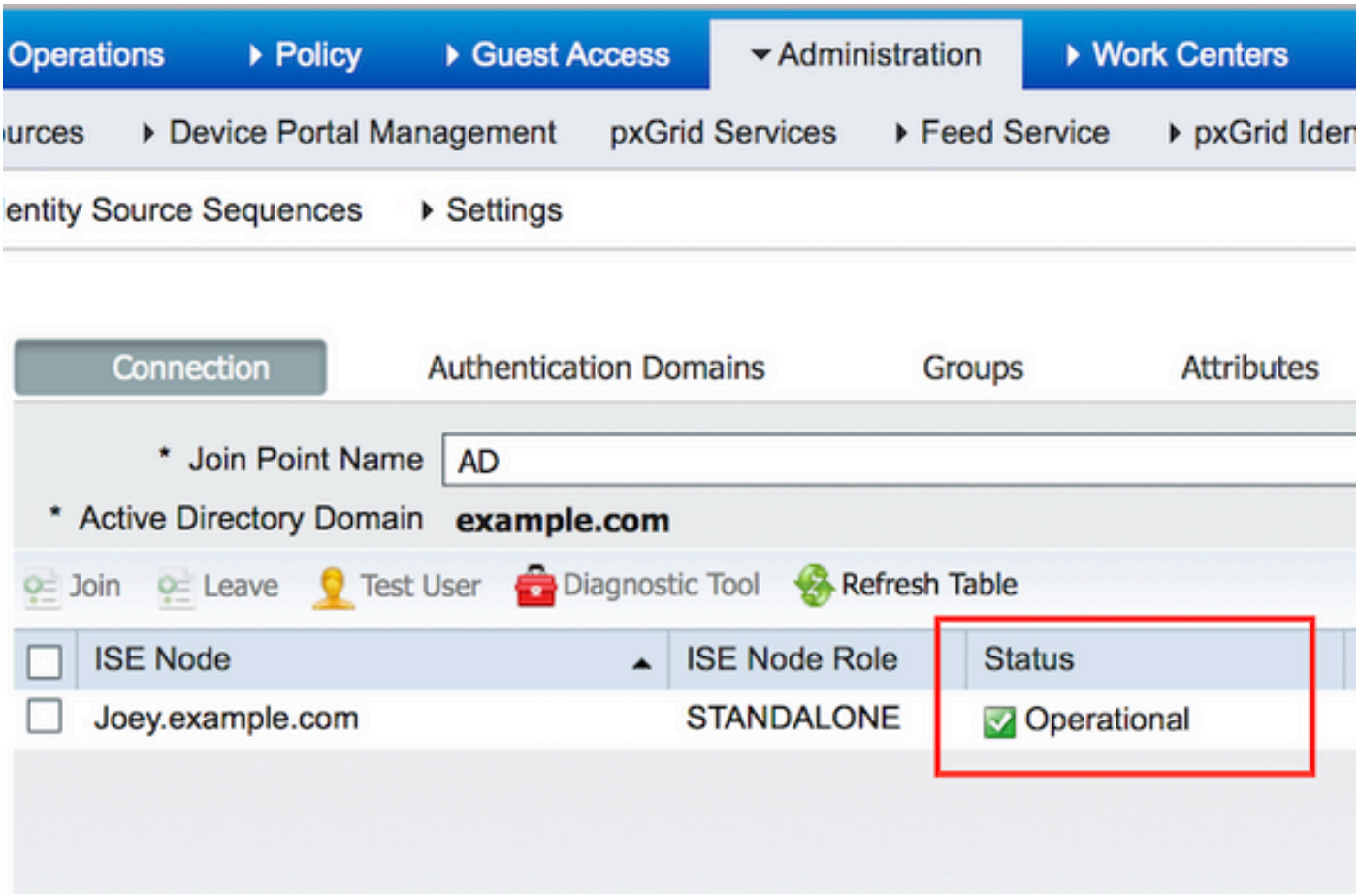
- 各ドメインのドメインユーザ権限にワークステーションを追加する
- ISEマシンをドメインに結合する前にISEマシンのアカウントが作成される各コンピュータコンテナに対するコンピュータオブジェクトの作成またはコンピュータオブジェクトの削除の権限

  注：ISE アカウントのロックアウト ポリシーを無効にし、不正なパスワードがこのアカウントに使用された場合に、管理者にアラートを送信するように AD インフラストラクチャを設定することを推奨します。誤ったパスワードを入力すると、ISEは必要に応じてマシンアカウントを作成または変更しないため、すべての認証を拒否する可能性があります。

4.運用ステータスの確認[ノードステータス(Node Status)]が[完了(Completed)]と表示されている必要があります。[Close] をクリックします。



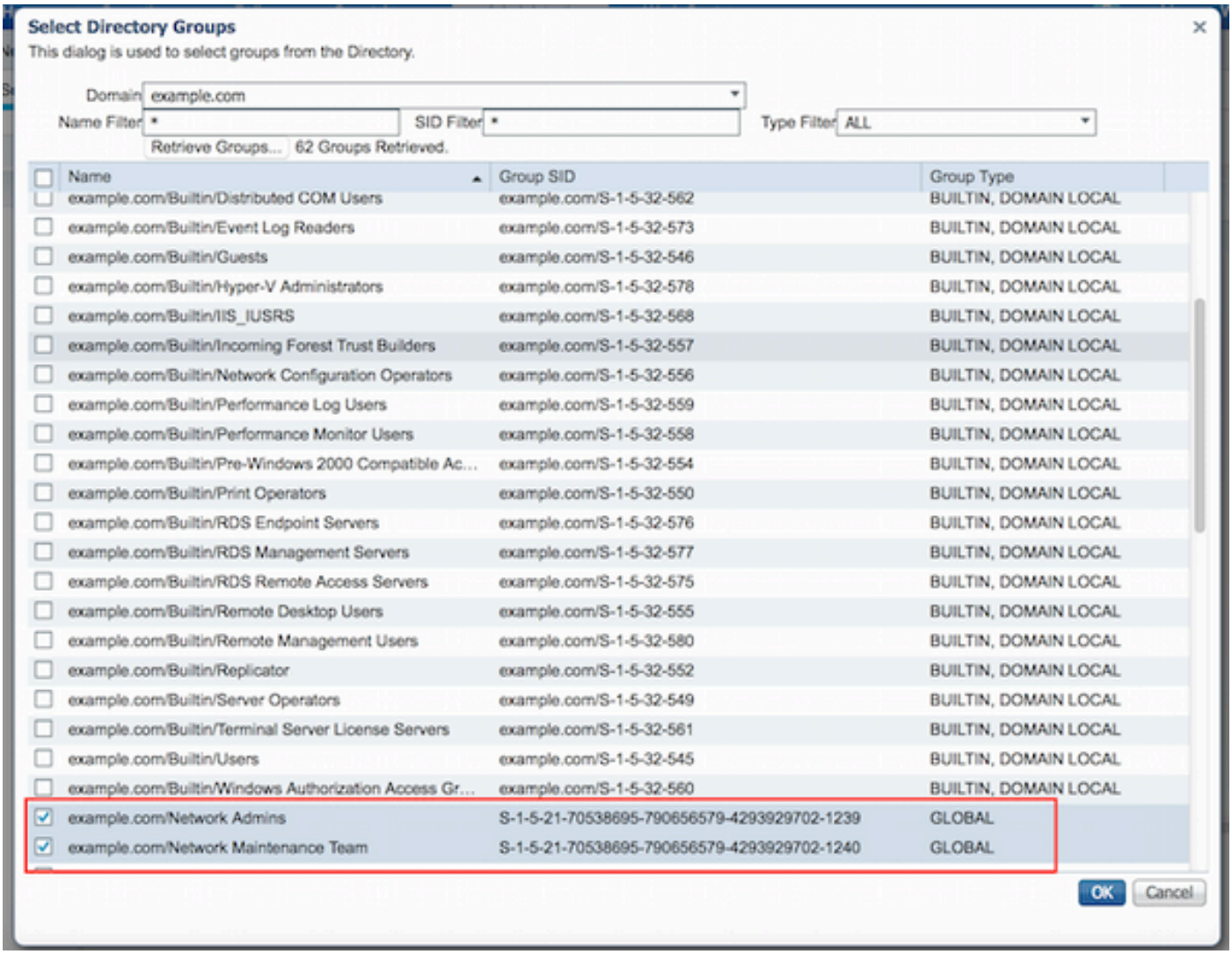
5. ADのステータスは[Operational]です。



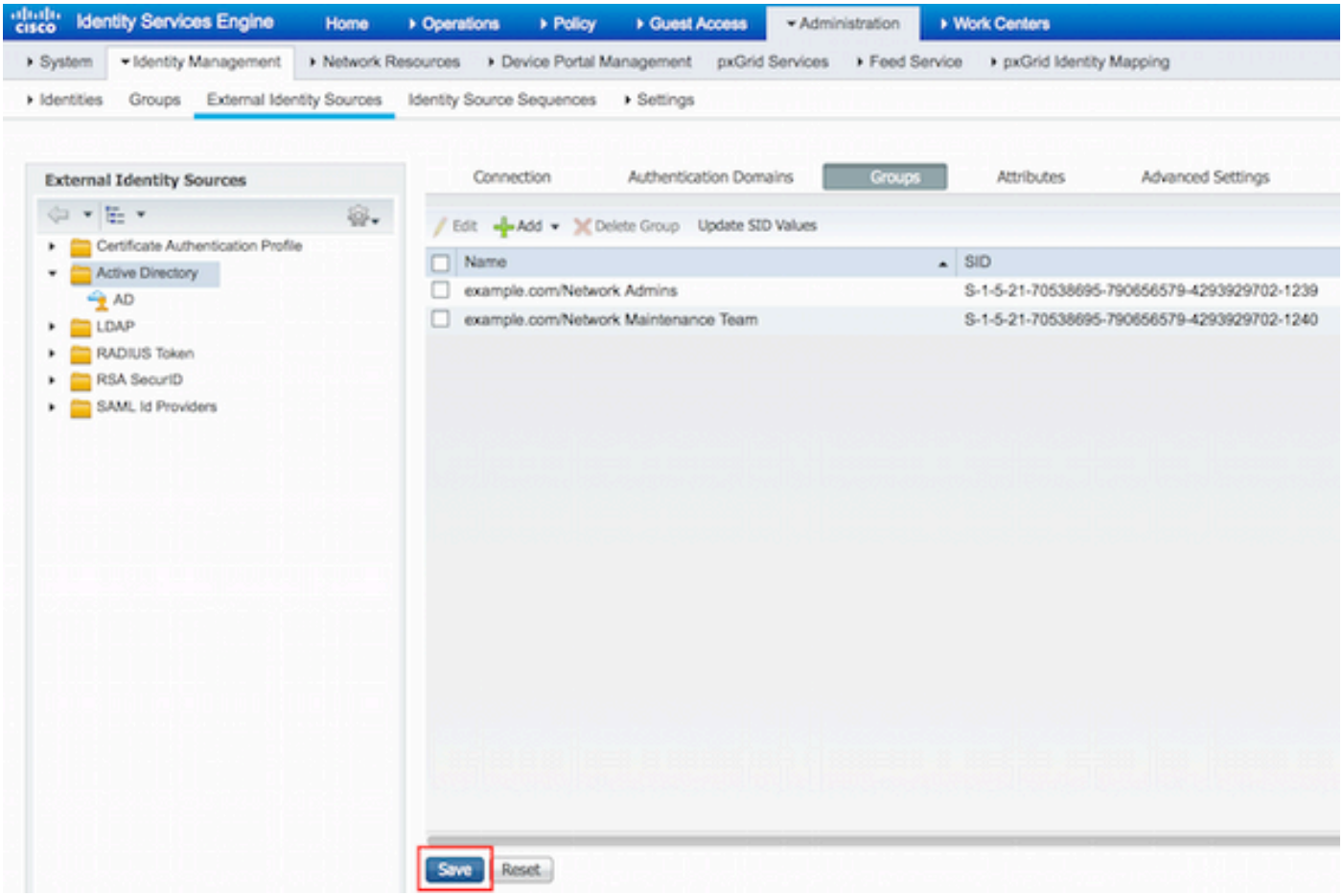
6. [Groups] > [Add] > [Select Groups From Directory] > [Retrieve Groups] に移動します。次の図に示すように、[Network Admins] AD グループと [Network Maintenance Team] AD グループのチェックボックスをオンにします。

注：ユーザ admin は、Network Admins AD グループのメンバーです。このユーザにはフルアクセス権限があります。このユーザは、Network Maintenance Team ADグループのメン

バーです。このユーザは show コマンドだけを実行できます。

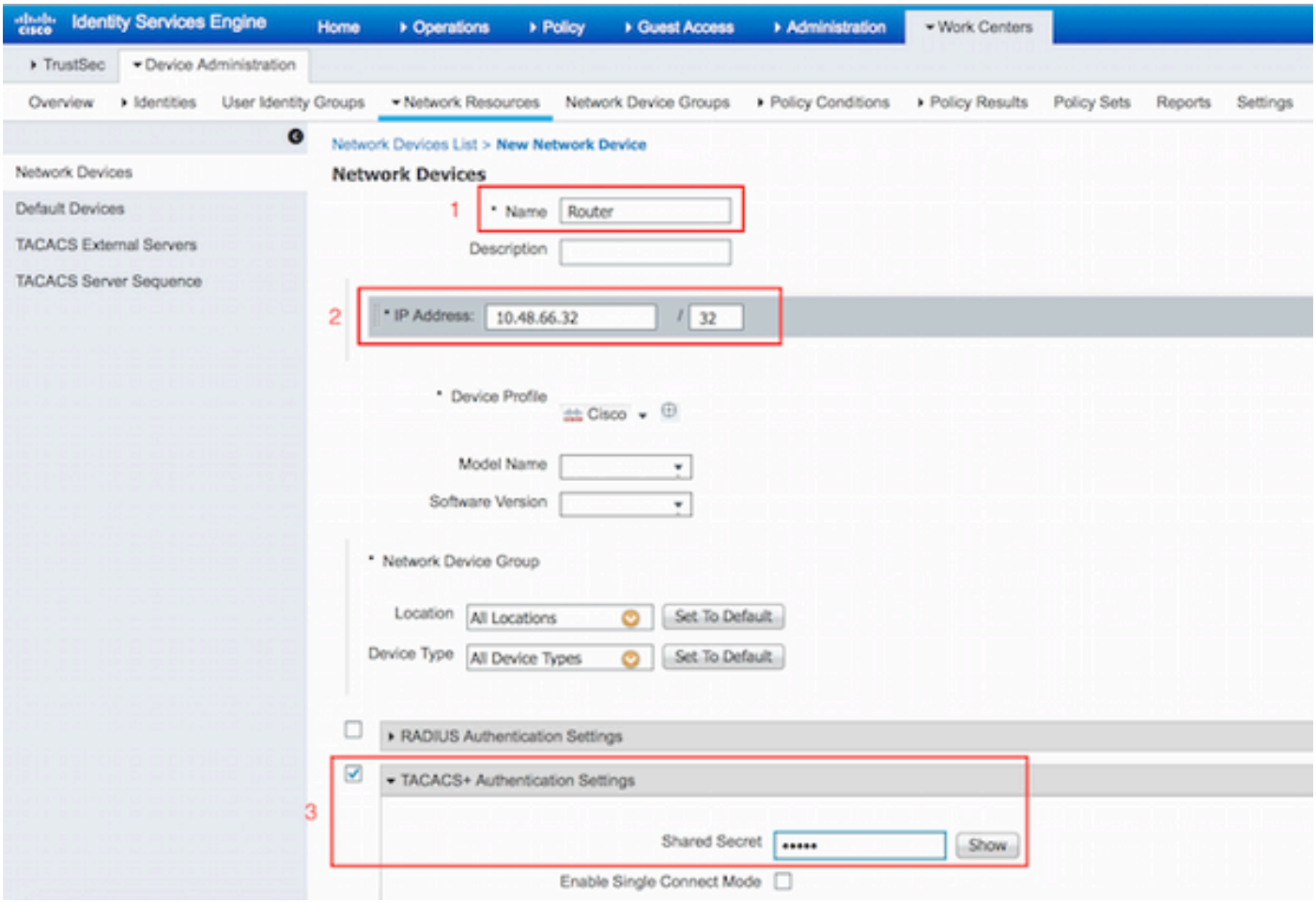


7. [Save] をクリックして、取得したADグループを保存します。



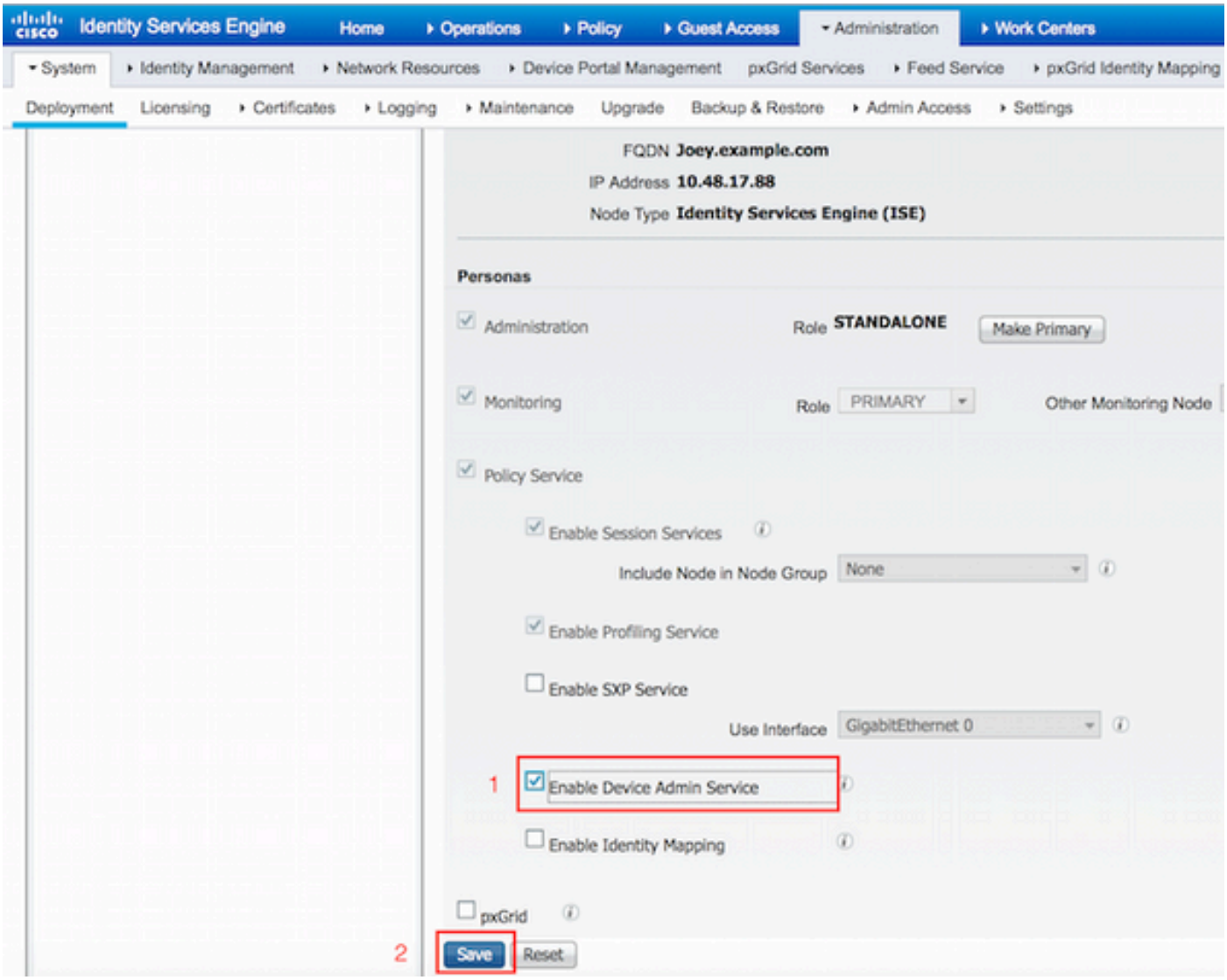
ネットワーク デバイスの追加

[Work Centers] > [Device Administration] > [Network Resources] > [Network Devices] **に移動します。**[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。



[デバイス管理サービスを有効にする（Enable Device Admin Service）]

[Administration] > [System] > [Deployment] に移動します。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。

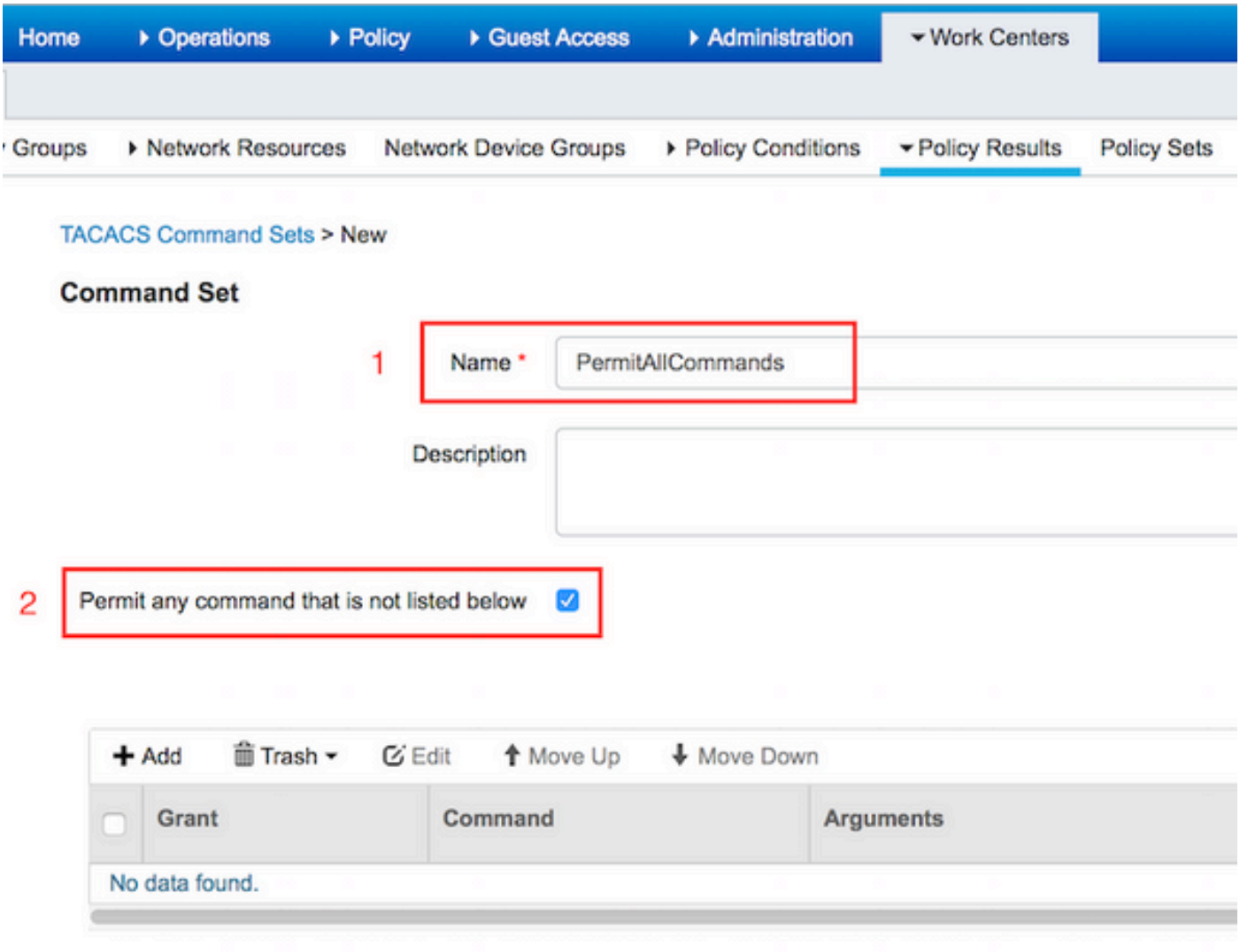


注：TACACSの場合は、個別のライセンスをインストールする必要があります。

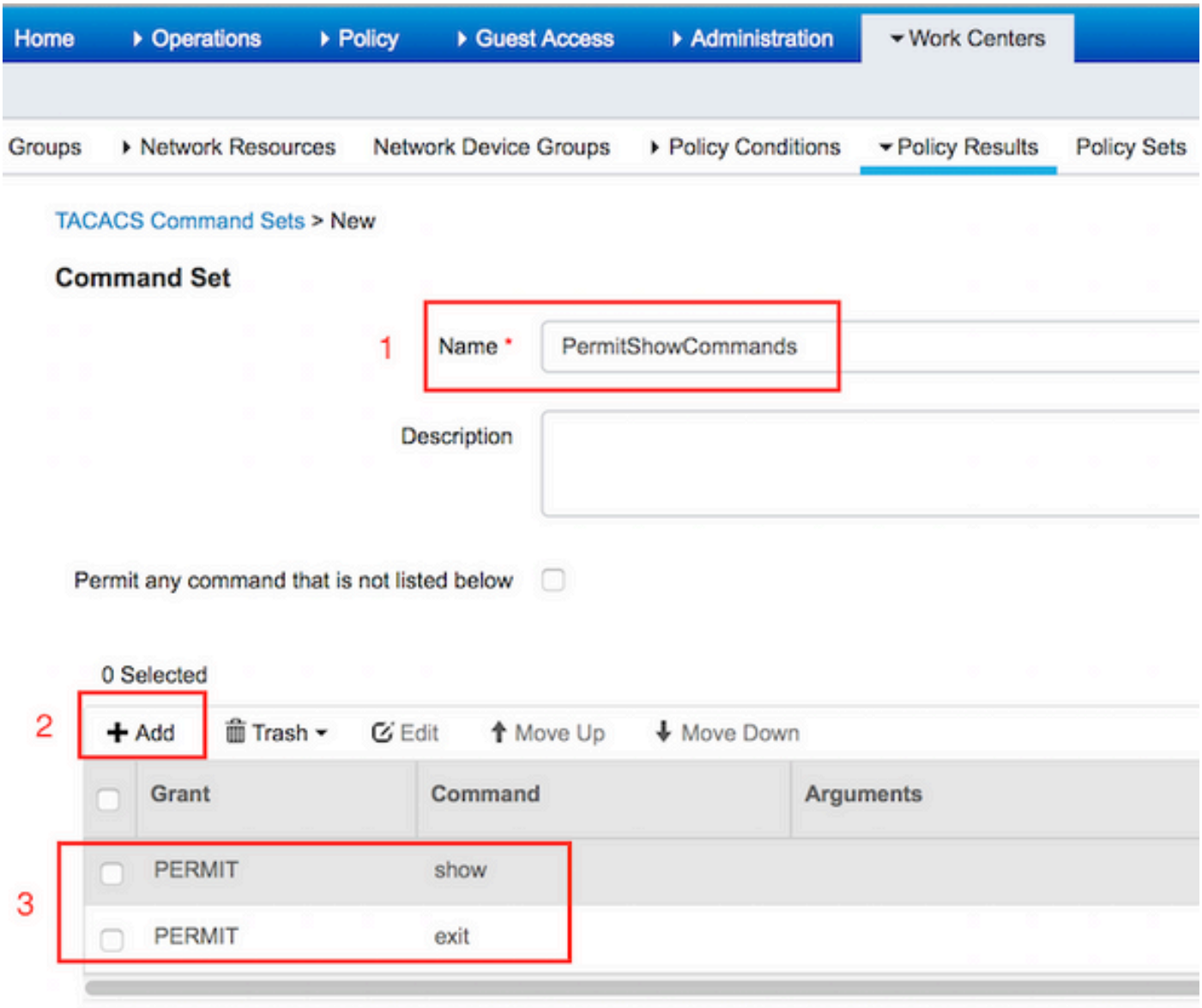
TACACSコマンドセットの設定

2 つの コマンド セットを設定します。ユーザadminに対する最初の**PermitAllCommands**は、デバイス上のすべてのコマンドを許可します。2つ目の**PermitShowCommands**は、showコマンドだけを許可するuser user用です。

1. [Work Centers] > [Device Administration] > [Policy Results] > [TACACS Command Sets] に移動します。[Add] をクリックします。[Name] に[PermitAllCommands]を入力し、リストされていない[Permit any command] チェックボックスを選択して、[Submit] をクリックします。

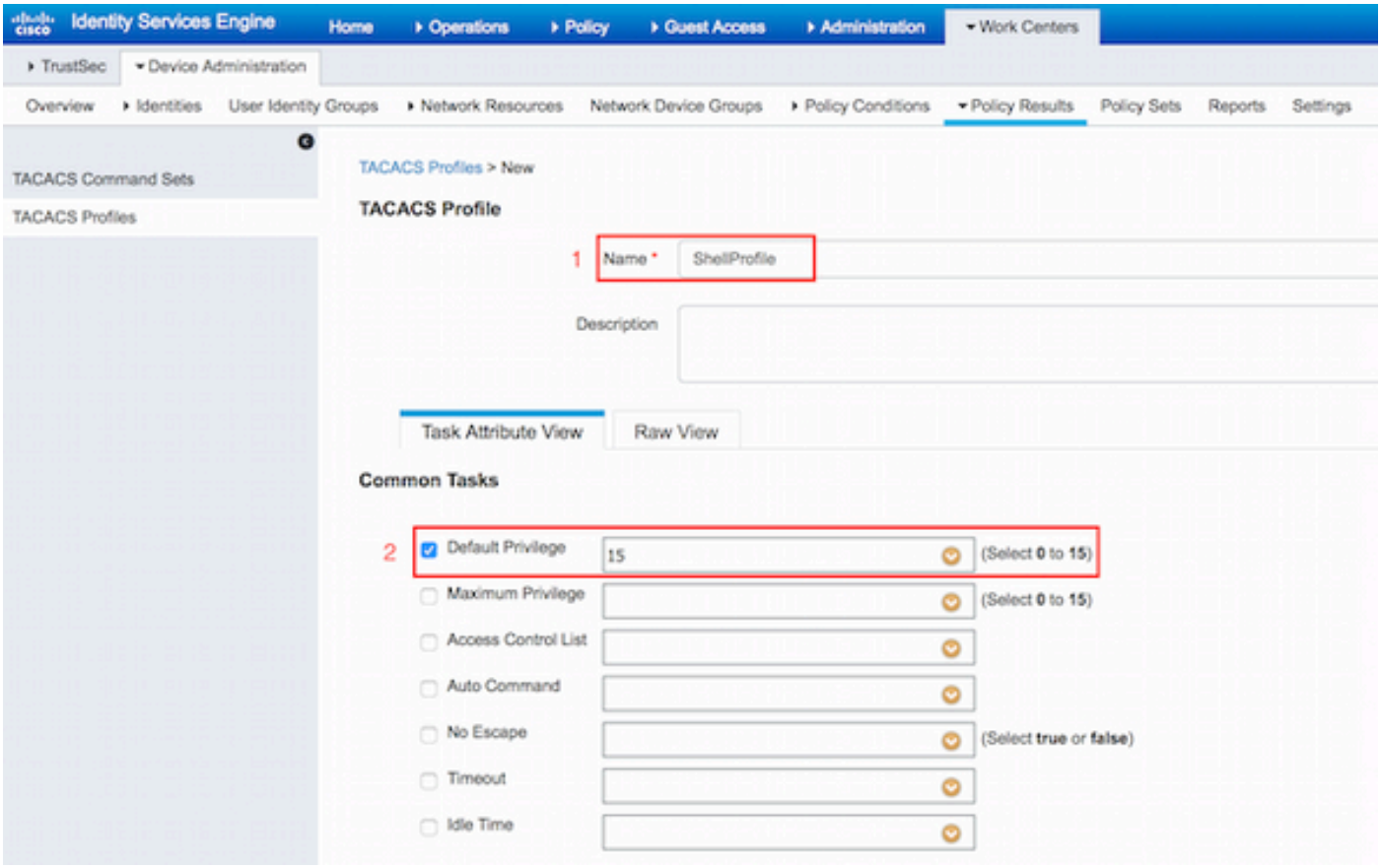


2. [Work Centers] > [Device Administration] > [Policy Results] > [TACACS Command Sets] に移動します。[Add] をクリックします。[Name] に [PermitShowCommands] を入力し、[Add] をクリックし、**show** および exit コマンドを許可します。デフォルトで引数が空白のままの場合、すべての引数が含まれます。[Submit] をクリックします。



TACACSプロファイルの設定

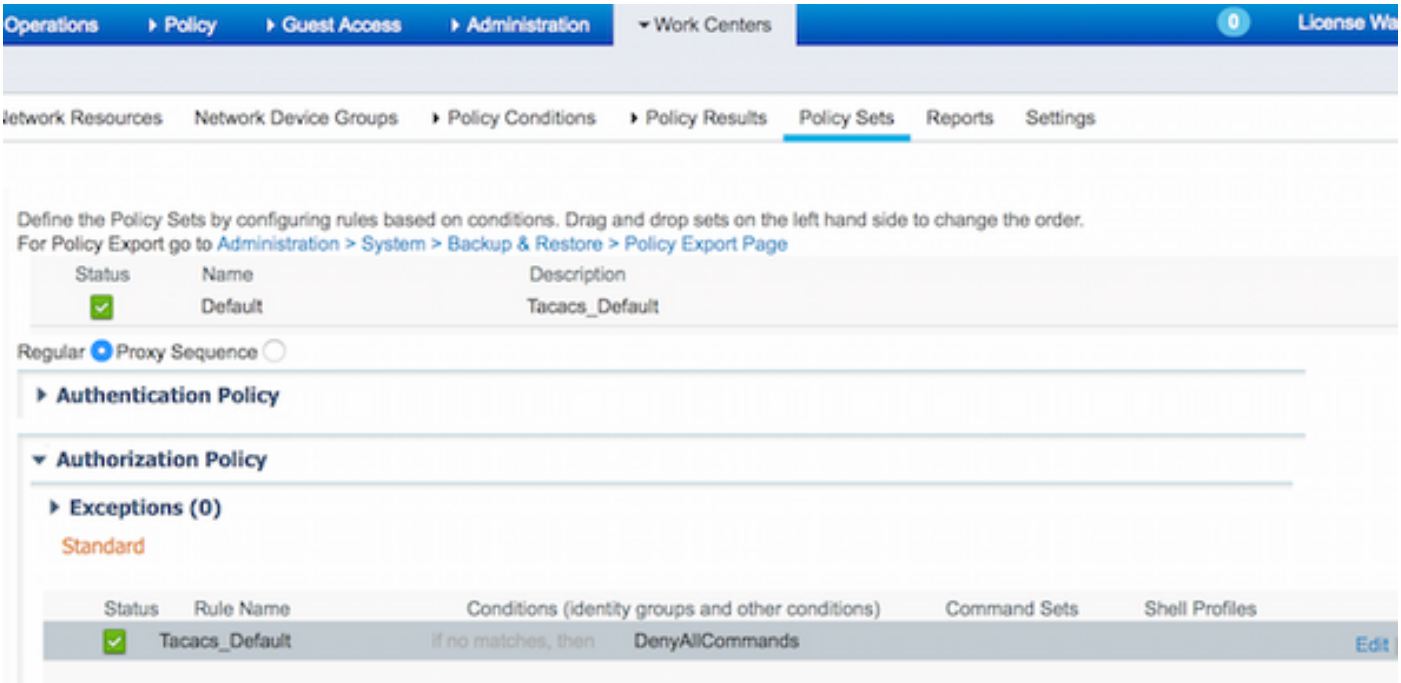
1 つの TACACS プロファイルを設定します。TACACS プロファイルは、ACS のシェル プロファイルと同じ概念です。実際のコマンドの適用は、コマンド セットを通じて行います。[Work Centers] > [Device Administration] > [Policy Results] > [TACACS Profiles] を選択します。[Add] をクリックします。[Name]に[ShellProfile]と入力し、[Default Privilege] チェックボックスをオンにして値15を入力します。[Submit]をクリックします。



TACACS認可ポリシーの設定

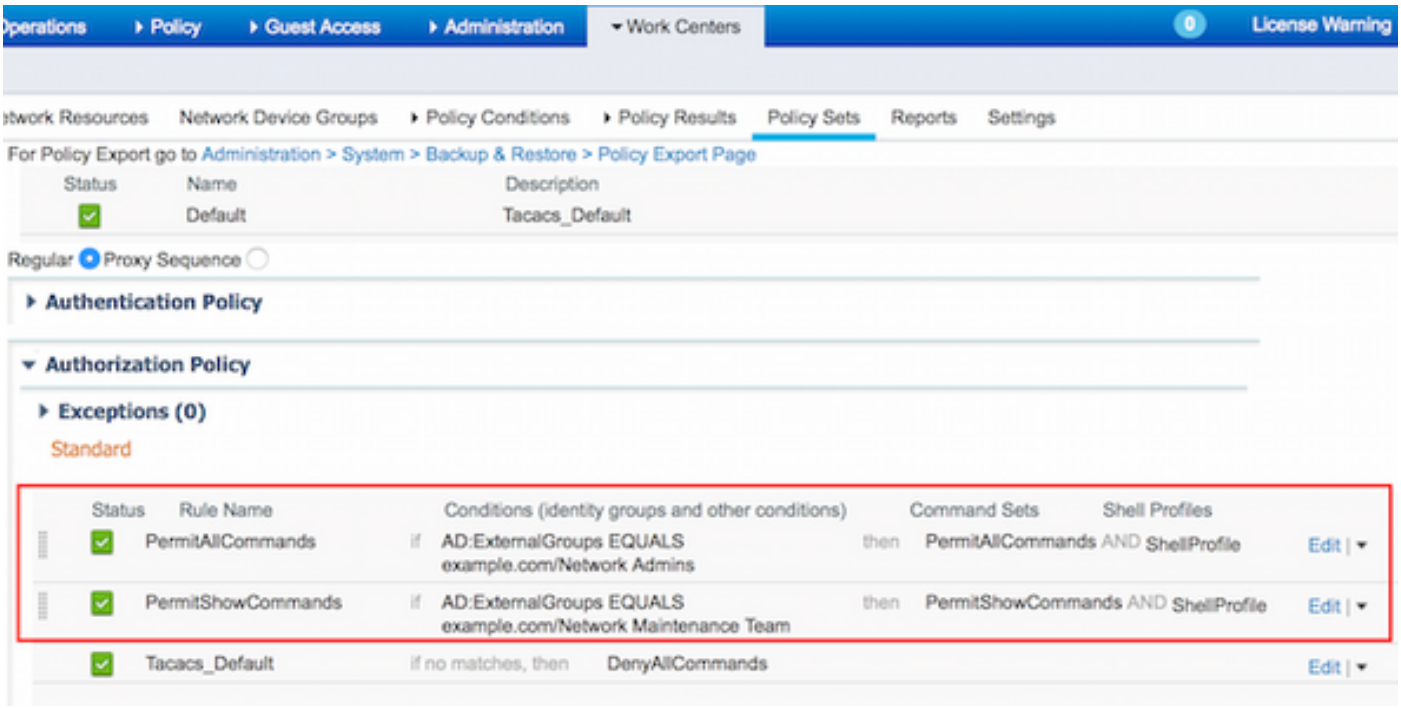
デフォルトで認証ポリシーは All_User_ID_Stores を指し、これは AD を含むため、未変更のままにします。

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



2つの認可ルールが設定されます。最初のルールは、Network Admins ADグループメンバーシップに基づいて、TACACSプロファイルShellProfileとコマンドセットPermitAllCommandsを割り当て

ます。2 つ目のルールは、TACACS プロファイルの ShellProfile とコマンド セットの PermitShowCommands を、Network Maintenance Team AD グループ 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 IOS ルータの設定

認証と認可のために Cisco IOS ルータを設定するには、次の手順を実行します。

1.次に示すように、**username**コマンドを使用して、フォールバックの完全な権限を持つローカルユーザを作成します。

```
username cisco privilege 15 password cisco
```

2. aaa new-modelを有効にします。TACACS サーバ ISE を指定し、ISE_GROUP グループに配置します。

```
aaa new-model

tacacs server ISE
 address ipv4 10.48.17.88
 key cisco
aaa group server tacacs+ ISE_GROUP
 server name ISE
```

注：サーバキーは、以前にISEサーバで定義されたものと一致します。

3.次に示すようにtest **aaa**コマンドを使用して、TACACSサーバの到達可能性をテストします。

```
Router#test aaa group tacacs+ admin Krakow123 legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.
```

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.ログインを設定し、認証を有効にしてから、次に示すようにexecおよびコマンドの認可を使用します。

```
aaa authentication login AAA group ISE_GROUP local
aaa authentication enable default group ISE_GROUP enable
aaa authorization exec AAA group ISE_GROUP local
aaa authorization commands 0 AAA group ISE_GROUP local
aaa authorization commands 1 AAA group ISE_GROUP local
aaa authorization commands 15 AAA group ISE_GROUP local
aaa authorization config-commands
```

> **注：**作成された方式リストはAAAという名前で、後で回線vtyに割り当てるときに使用されます。

5.回線vty 0 4に方式リストを割り当てます。

```
line vty 0 4
 authorization commands 0 AAA
 authorization commands 1 AAA
 authorization commands 15 AAA
 authorization exec AAA
 login authentication AAA
```

確認

Cisco IOS ルータ の検証

1. ADのフルアクセスグループに属するadminとしてCisco IOSルータにTelnet接続します。Network Admins グループは、ISE で設定される ShellProfile と PermitAllCommands コマンド セットにマッピングされる AD グループです。フル アクセスを確認するコマンドを実行します。

```
Username:admin
Password:

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#encryption aes
Router(config-isakmp)#exit
Router(config)#exit
Router#
```

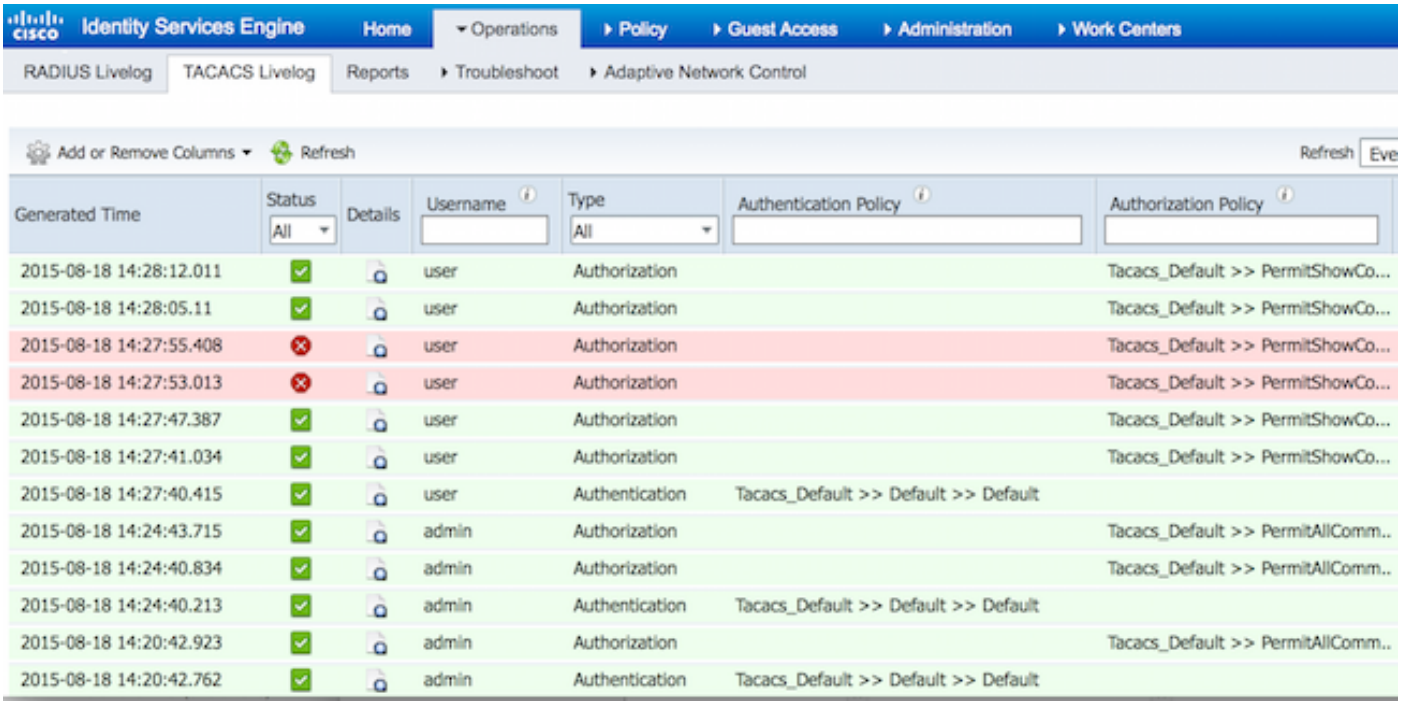
2. ADの制限付きアクセスグループに属するユーザとしてCisco IOSルータにTelnet接続します。Network Maintenance Team グループは、ISE で設定される ShellProfile と PermitShowCommands コマンド セットにマッピングされる AD グループです。show コマンドのみ発行されることを確認するコマンドを実行します。

```
Username:user
Password:

Router#show ip interface brief | exclude unassigned
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         10.48.66.32     YES NVRAM  up                    up
```

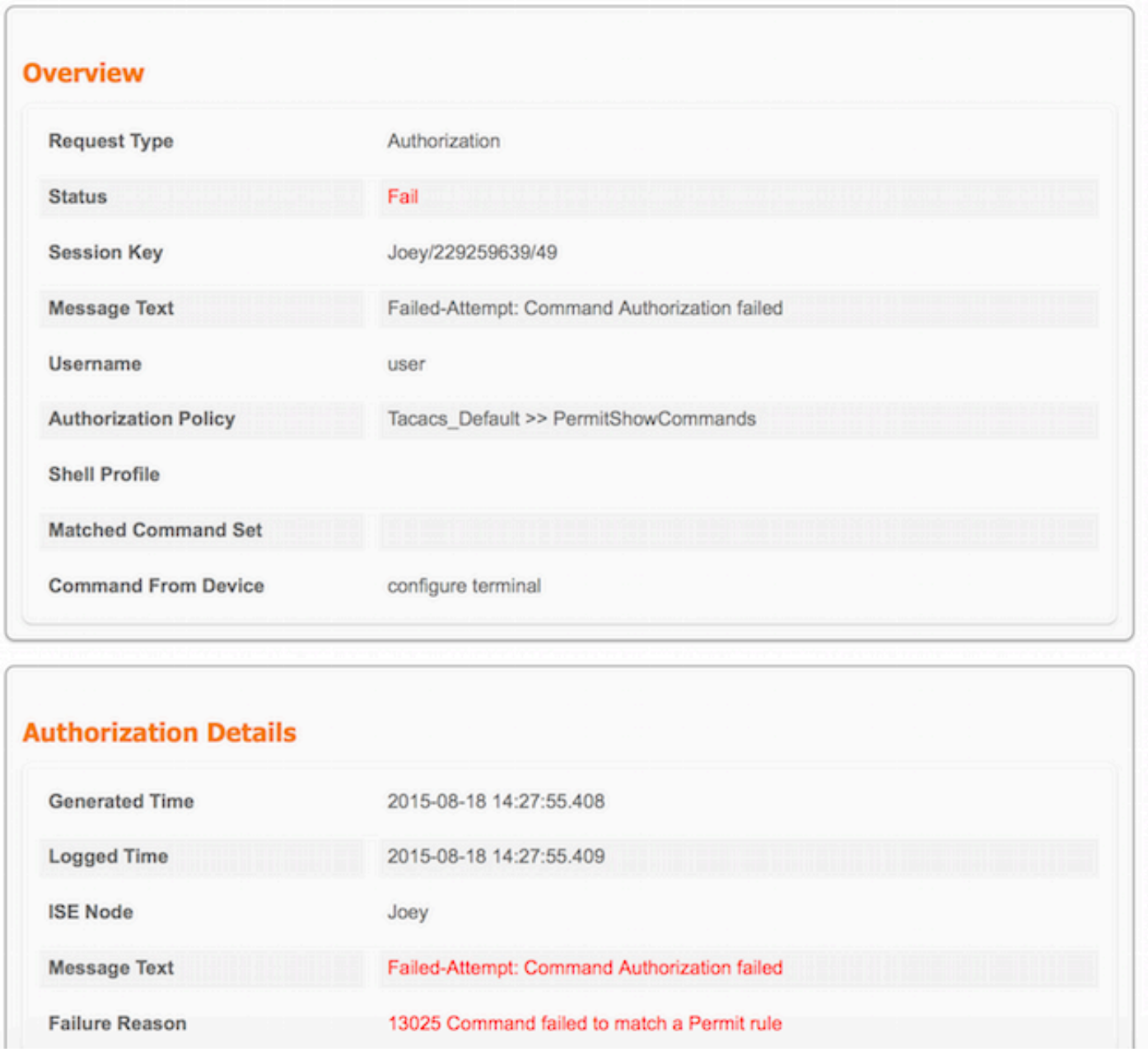
```
Router#ping 8.8.8.8
Command authorization failed.

Router#configure terminal
Command authorization failed.

Router#show running-config | include hostname
hostname Router
Router#
```

ISE 2.0 の検証

1. [Operations] > [TACACS Livelog] に移動します。実行した試行が表示されることを確認します。



2.いずれかの赤いレポートの詳細をクリックします。以前に実行された失敗したコマンドが表示されます。



Overview

Request Type	Authorization
Status	Fail
Session Key	Joey/229259639/49
Message Text	Failed-Attempt: Command Authorization failed
Username	user
Authorization Policy	Tacacs_Default >> PermitShowCommands
Shell Profile	
Matched Command Set	
Command From Device	configure terminal

Authorization Details

Generated Time	2015-08-18 14:27:55.408
Logged Time	2015-08-18 14:27:55.409
ISE Node	Joey
Message Text	Failed-Attempt: Command Authorization failed
Failure Reason	13025 Command failed to match a Permit rule

トラブルシュート

エラー:13025 Command failed to match a Permit rule

認可ポリシーで予測されるコマンド セットが選択されていることを確認するため、SelectedCommandSet 属性を確認します。

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

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。