

ISE 2.0 TACACS+認証コマンド許可の設定

内容

[概要](#)

[背景説明](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[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](#)

[ネットワーク デバイスの追加](#)

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

[TACACSコマンドセットの設定](#)

[TACACSプロファイルの設定](#)

[TACACS認可ポリシーの設定](#)

[認証および認可のための Cisco IOS ルータの設定](#)

[確認](#)

[Cisco IOS ルータ の検証](#)

[ISE 2.0 の検証](#)

[トラブルシュート](#)

[関連情報](#)

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。

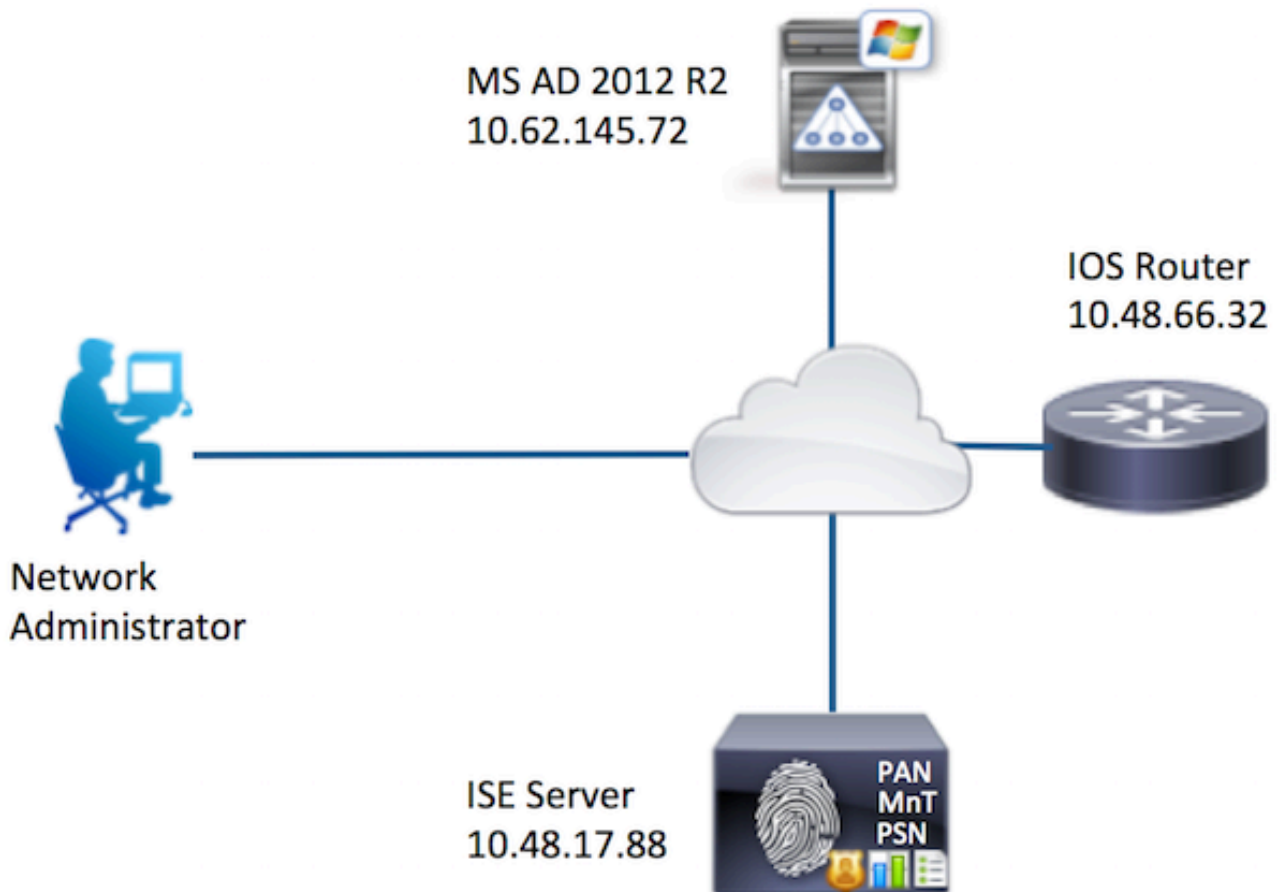
ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

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

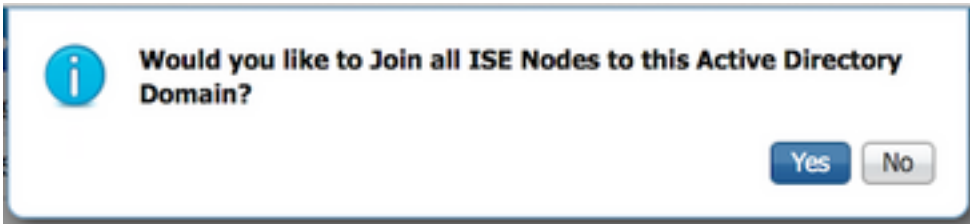
認証および認可のための ISE の設定

ISE 2.0 の Active Directory への参加

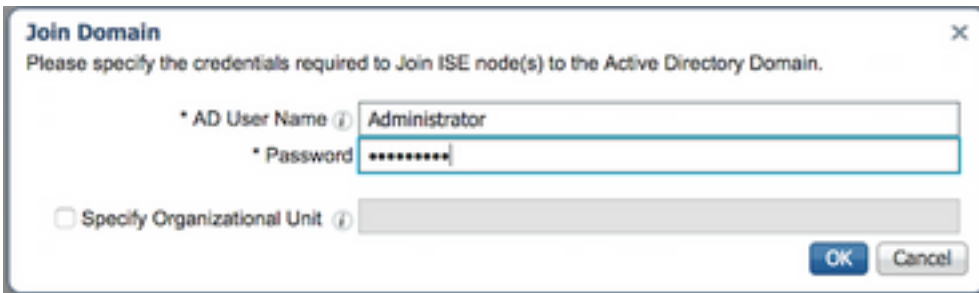
1. [Administration] > [Identity Management] > [External Identity Stores] > [Active Directory] > [Add] に移動します。[Join Point Name] と [Active Directory Domain] に入力し、[Submit] をクリックします。

The screenshot shows the ISE 2.0 Administration console. The navigation menu includes: Operations, Policy, Guest Access, Administration (selected), and Work Centers. Under Administration, there are links for sources, Device Portal Management, pxGrid Services, Feed Service, and pxGrid Identity Mapping. The main content area shows 'Identity Source Sequences' > 'Settings'. A 'Connection' tab is active, displaying two input fields: 'Join Point Name' with the value 'AD' and 'Active Directory Domain' with the value 'example.com'. Both fields are highlighted with a red border. Below the fields are 'Submit' and 'Cancel' buttons.

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。

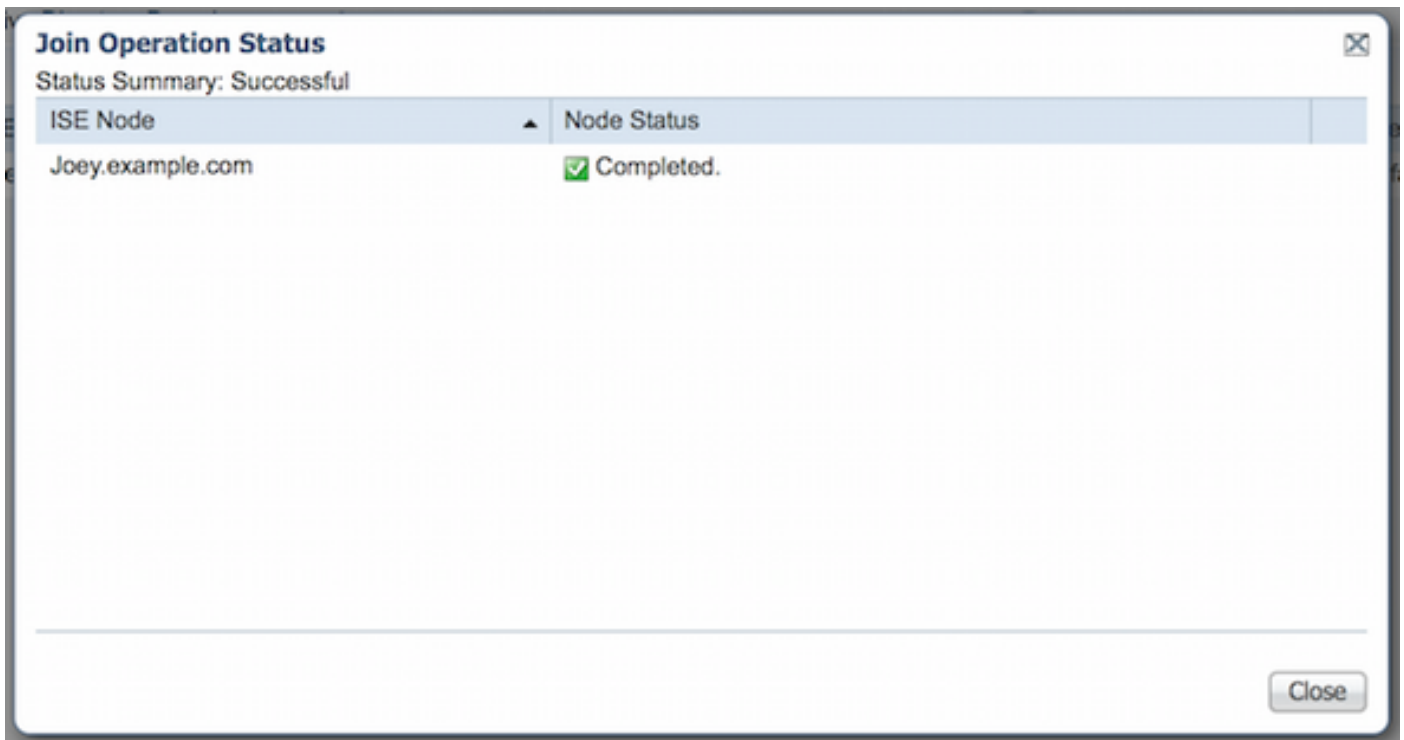


ISEのドメインアクセスに必要なADアカウントは、次のいずれかを持つことができます。

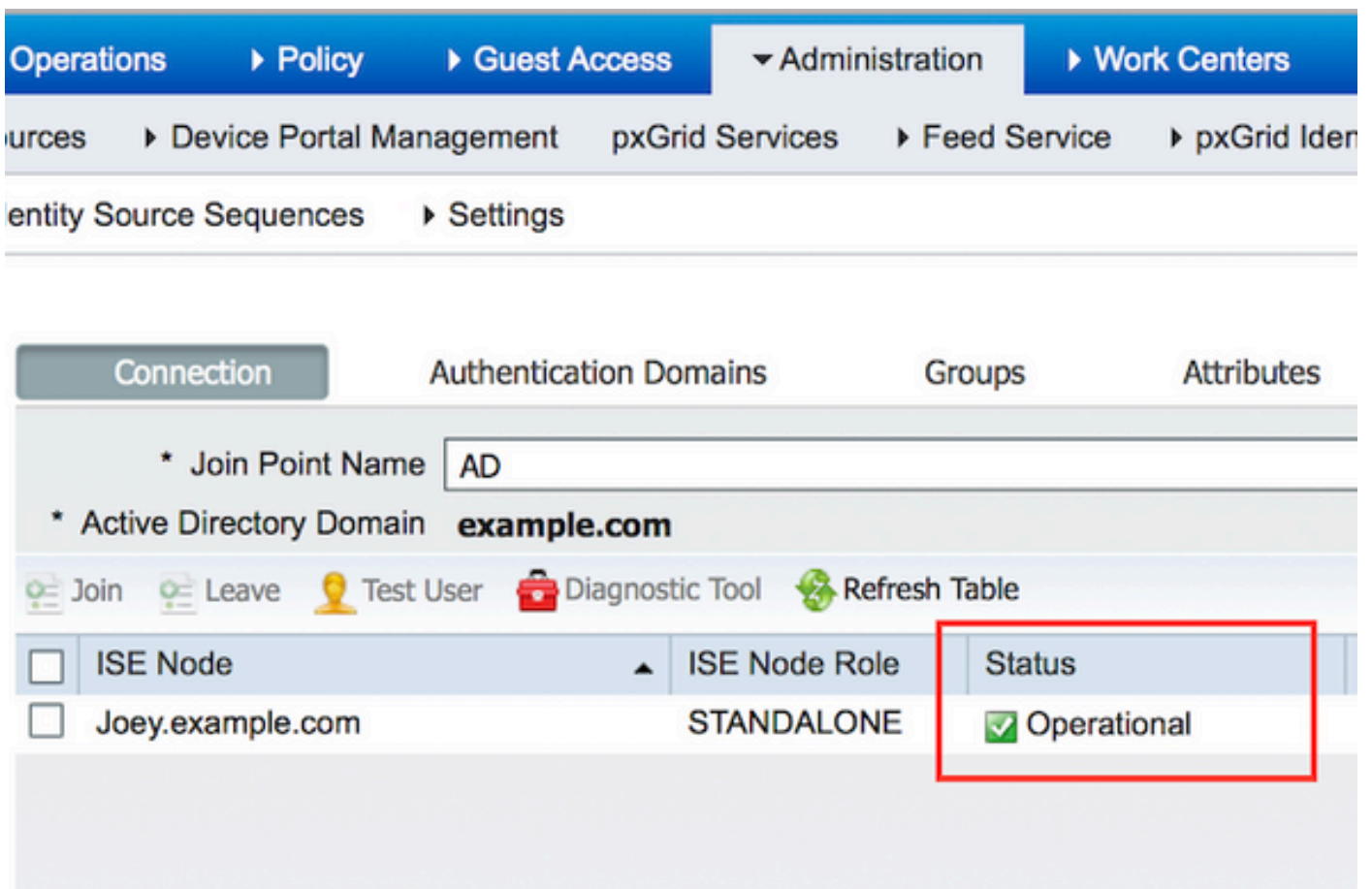
- 各ドメインのドメインユーザ権限にワークステーションを追加する
- ISEマシンをドメインに結合する前にISEマシンのアカウントが作成される各コンピュータコンテナに対するコンピュータオブジェクトの作成またはコンピュータオブジェクトの削除の権限

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。



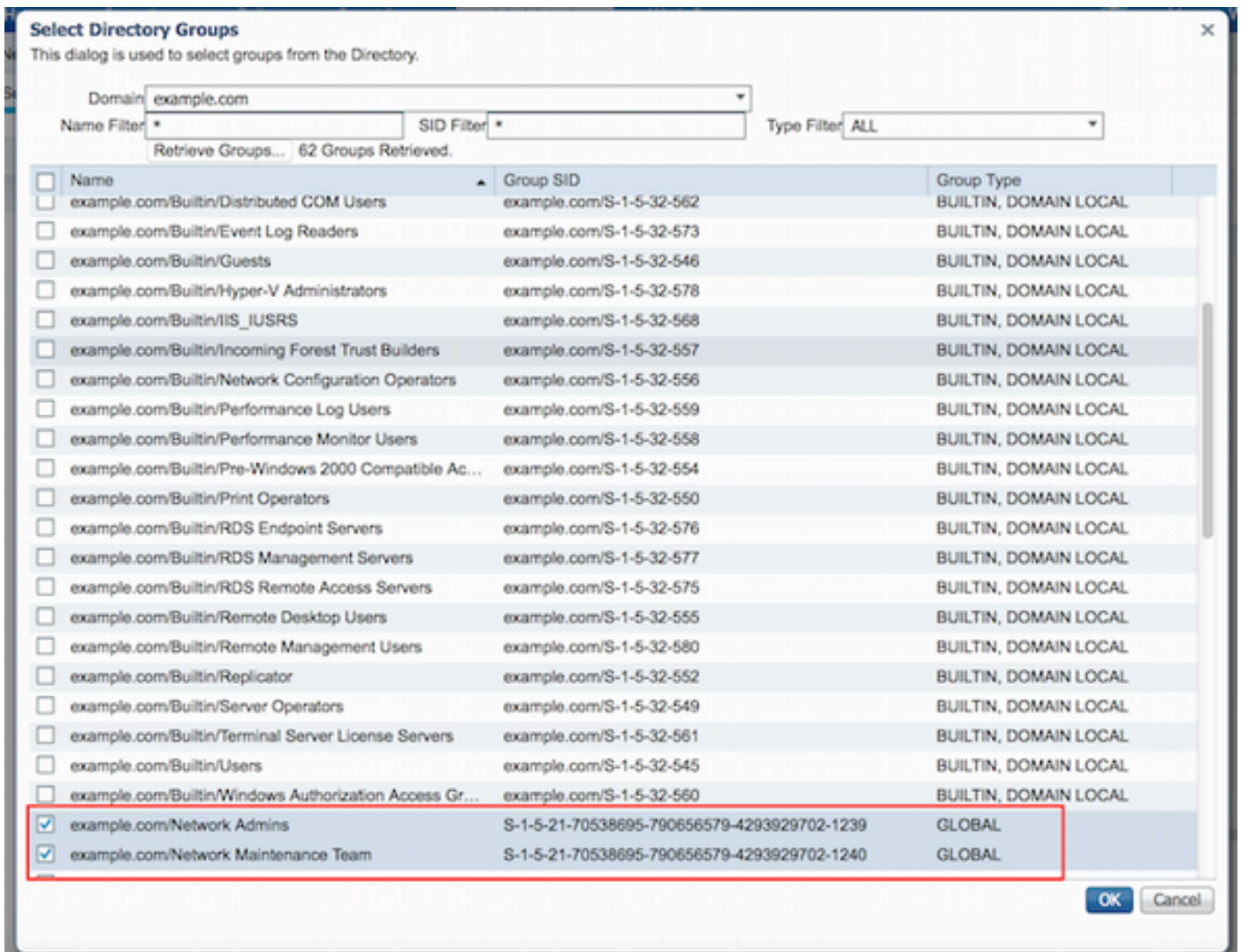
5. ADのステータスは[Operational]です。



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。

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu at the top includes: Home, Operations, Policy, Guest Access, Administration, and Work Centers. The breadcrumb trail is: System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > pxGrid Identity Mapping. The main menu includes: Identities, Groups, External Identity Sources (selected), Identity Source Sequences, and Settings.

The 'External Identity Sources' section is active, showing a tree view on the left with categories: Certificate Authentication Profile, Active Directory (selected), AD, LDAP, RADIUS Token, RSA SecurID, and SAML Id Providers.

The 'Groups' tab is selected, displaying a table of groups. The table has columns for Name and SID. The groups listed are:

Name	SID
example.com/Network Admins	S-1-5-21-70538695-790656579-4293929702-1239
example.com/Network Maintenance Team	S-1-5-21-70538695-790656579-4293929702-1240

At the bottom of the page, the 'Save' button is highlighted with a red box, and the 'Reset' button is visible next to it.

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。

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

TrustSec Device Administration

Overview Identities User Identity Groups Network Resources Network Device Groups Policy Conditions Policy Results Policy Sets Reports Settings

Network Devices List > New Network Device

Network Devices

Default Devices
TACACS External Servers
TACACS Server Sequence

1 * Name Router
Description

2 * IP Address: 10.48.66.32 / 32

* Device Profile Cisco
Model Name
Software Version

* Network Device Group
Location All Locations Set To Default
Device Type All Device Types Set To Default

RADIUS Authentication Settings
 TACACS+ Authentication Settings
Shared Secret ***** Show
Enable Single Connect Mode

[デバイス管理服务を有効にする (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。

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', 'Administration', and 'Work Centers'. The main content area shows the configuration for a node named 'Joey.example.com' with IP address 10.48.17.88. Under the 'Personas' section, the 'Enable Device Admin Service' checkbox is checked and highlighted with a red box, with a red '1' next to it. At the bottom, the 'Save' button is highlighted with a red box, with a red '2' next to it. Other visible options include 'Administration' (Role: STANDALONE), 'Monitoring' (Role: PRIMARY), 'Policy Service' (with sub-options for Session, Profiling, SXP, and Identity Mapping), and 'pxGrid'.

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。

TACACS Command Sets > New

Command Set

1

Name * PermitAllCommands

Description

2

Permit any command that is not listed below

<input type="checkbox"/>	Grant	Command	Arguments
No data found.			

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 Command Sets > New

Command Set

1 **Name ***

Description

Permit any command that is not listed below

0 Selected

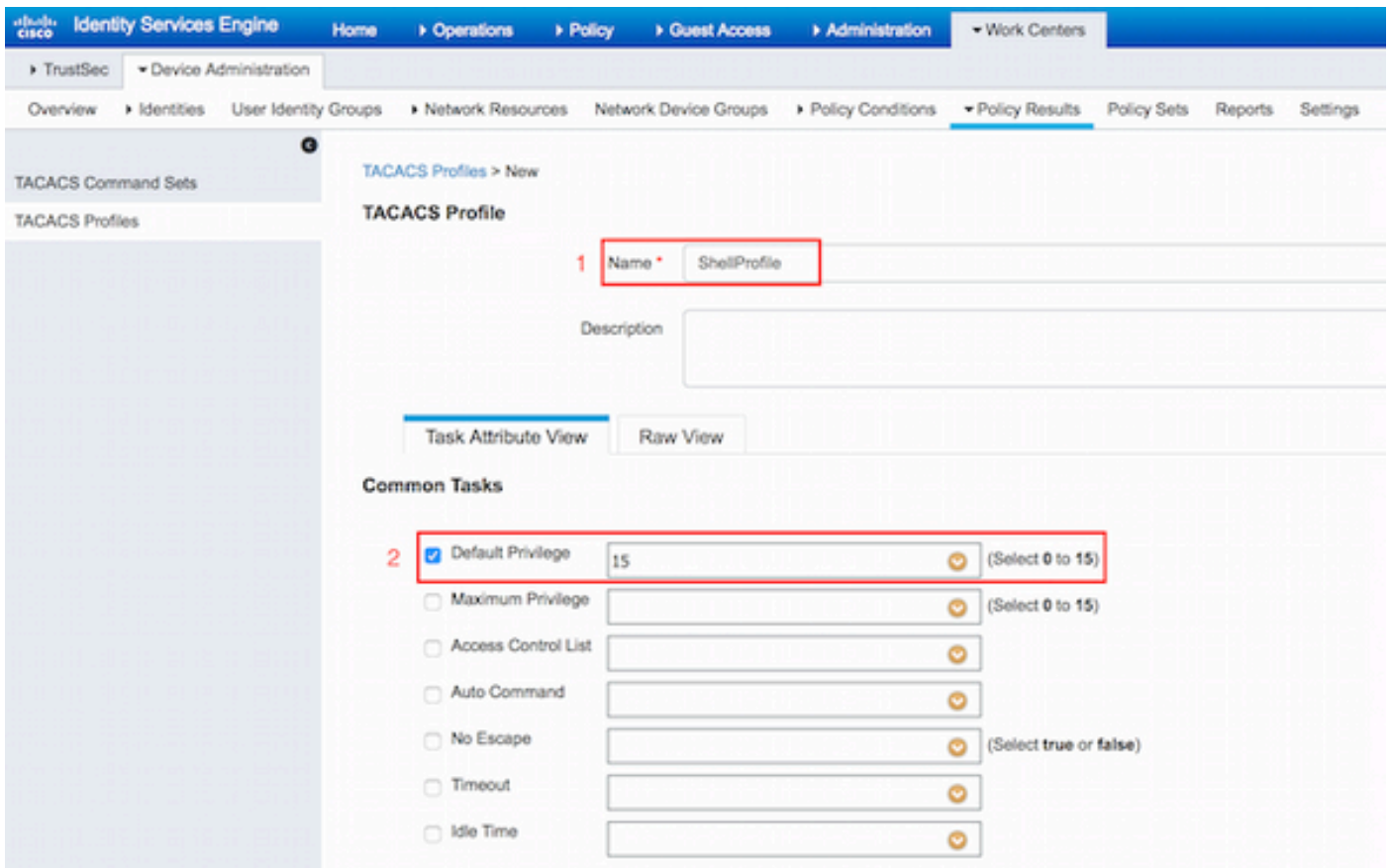
2 **+ Add**

<input type="checkbox"/>	Grant	Command	Arguments
<input type="checkbox"/>	PERMIT	show	
<input type="checkbox"/>	PERMIT	exit	

3

TACACSプロファイルの設定

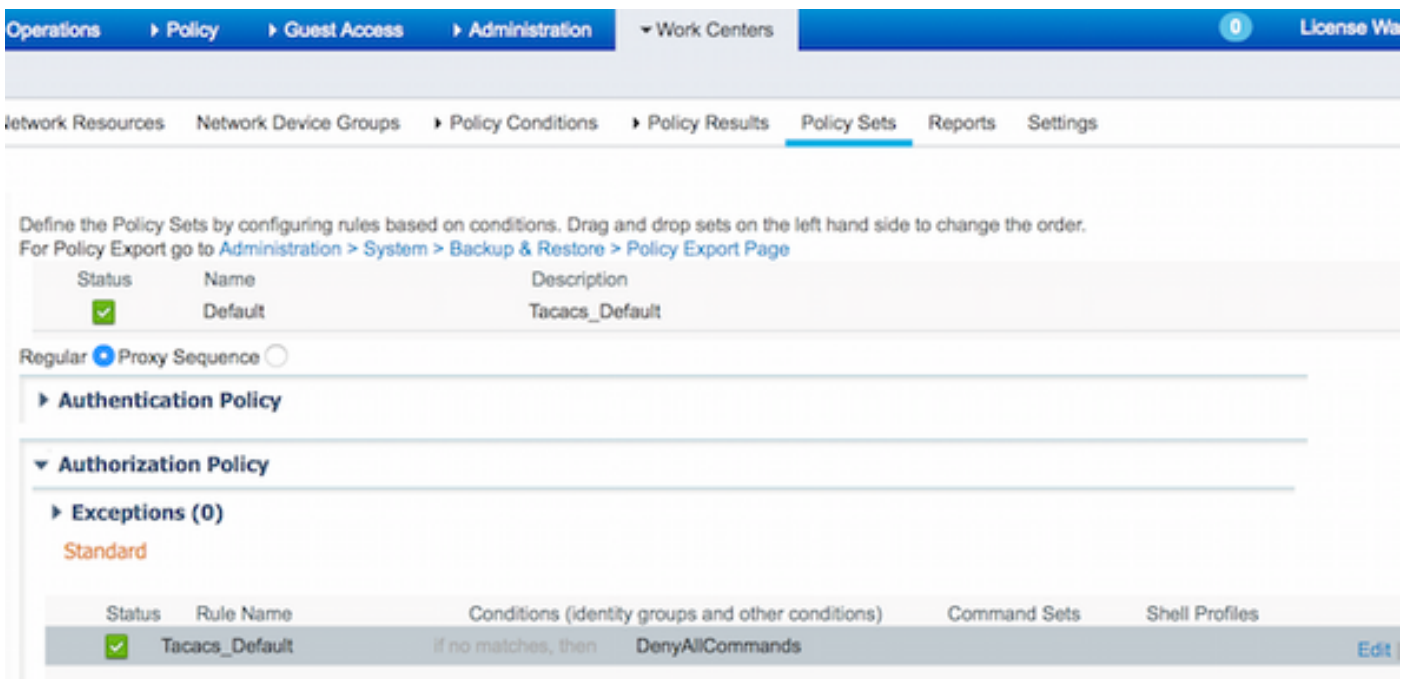
1つのTACACSプロファイルを設定します。TACACSプロファイルは、ACSのシェルプロファイルと同じ概念です。実際のコマンドの適用は、コマンドセットを通じて行います。[Work Centers] > [Device Administration] > [Policy Results] > [TACACS Profiles] を選択します。[Add] をクリックします。[Name]に[ShellProfile]と入力し、[Default Privilege] チェックボックスをオンにして値15を入力します。[Submit]をクリックします。



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

まず、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。

The screenshot shows the Cisco ISE Policy Administration console. The breadcrumb navigation is: Operations > Policy > Guest Access > Administration > Work Centers. The main navigation bar includes: Network Resources, Network Device Groups, Policy Conditions, Policy Results, Policy Sets (selected), Reports, and Settings. Below the navigation, there is a breadcrumb for Policy Export: Administration > System > Backup & Restore > Policy Export Page. A table shows the Policy Set configuration:

Status	Name	Description
<input checked="" type="checkbox"/>	Default	Tacacs_Default

Below the table, there are radio buttons for Regular (selected) and Proxy Sequence. The main configuration area is titled "Authorization Policy" and contains an "Exceptions (0)" section. A table lists the exceptions:

Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles	
<input checked="" type="checkbox"/>	PermitAllCommands	if AD:ExternalGroups EQUALS example.com/Network Admins	then PermitAllCommands AND ShellProfile		Edit ▾
<input checked="" type="checkbox"/>	PermitShowCommands	if AD:ExternalGroups EQUALS example.com/Network Maintenance Team	then PermitShowCommands AND ShellProfile		Edit ▾
<input checked="" type="checkbox"/>	Tacacs_Default	if no matches, then	DenyAllCommands		Edit ▾

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
```



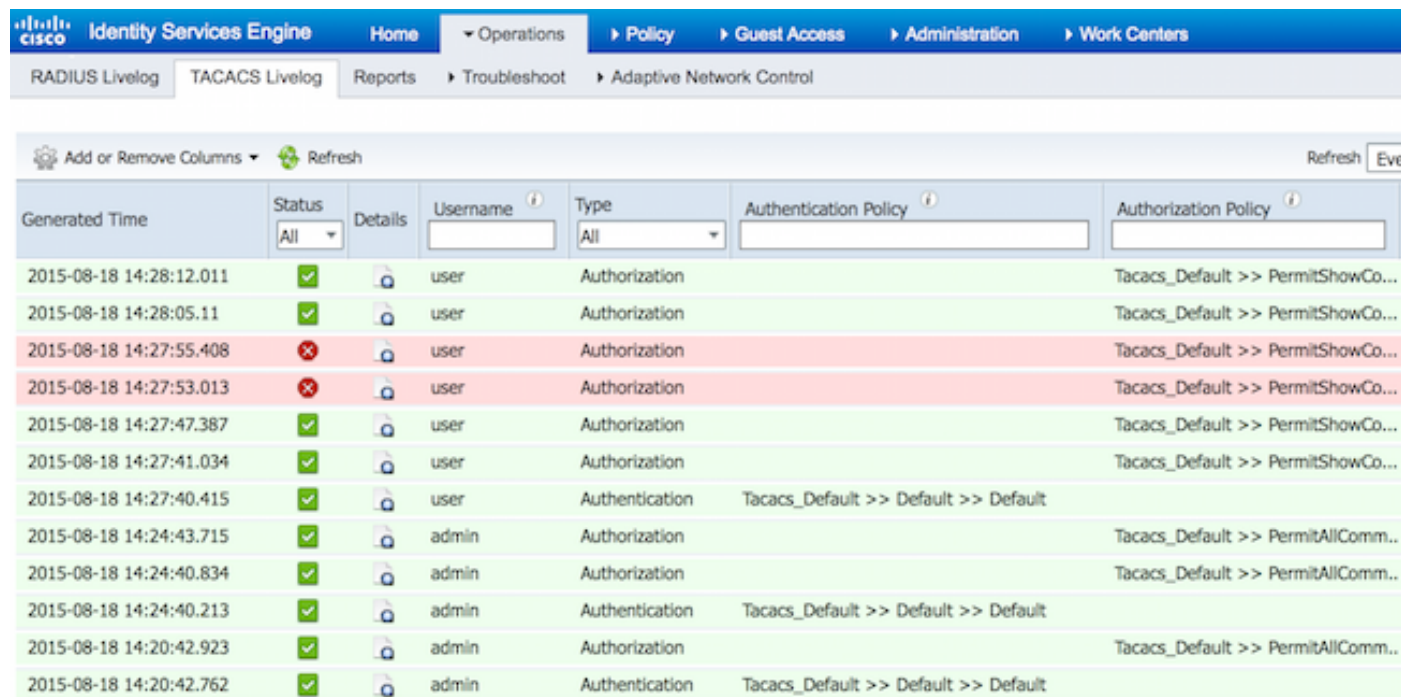
```
Router#ping 8.8.8.8
Command authorization failed.
```

```
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。



Generated Time	Status	Details	Username	Type	Authentication Policy	Authorization Policy
2015-08-18 14:28:12.011	✓		user	Authorization		Tacacs_Default >> PermitShowCo...
2015-08-18 14:28:05.11	✓		user	Authorization		Tacacs_Default >> PermitShowCo...
2015-08-18 14:27:55.408	✗		user	Authorization		Tacacs_Default >> PermitShowCo...
2015-08-18 14:27:53.013	✗		user	Authorization		Tacacs_Default >> PermitShowCo...
2015-08-18 14:27:47.387	✓		user	Authorization		Tacacs_Default >> PermitShowCo...
2015-08-18 14:27:41.034	✓		user	Authorization		Tacacs_Default >> PermitShowCo...
2015-08-18 14:27:40.415	✓		user	Authentication	Tacacs_Default >> Default >> Default	
2015-08-18 14:24:43.715	✓		admin	Authorization		Tacacs_Default >> PermitAllComm..
2015-08-18 14:24:40.834	✓		admin	Authorization		Tacacs_Default >> PermitAllComm..
2015-08-18 14:24:40.213	✓		admin	Authentication	Tacacs_Default >> Default >> Default	
2015-08-18 14:20:42.923	✓		admin	Authorization		Tacacs_Default >> PermitAllComm..
2015-08-18 14:20:42.762	✓		admin	Authentication	Tacacs_Default >> Default >> Default	

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

トラブルシューティング

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。