

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

目次

[はじめに](#)

[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](#)

[ネットワーク デバイスの追加](#)

[ユーザ ID グループの設定](#)

[ユーザの設定](#)

[デバイス管理サービスの有効化](#)

[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 ASA ファイアウォールの設定](#)

[確認](#)

[Cisco ASA ファイアウォールの確認](#)

[ISE 2.0 の検証](#)

[トラブルシューティング](#)

[関連情報](#)

[Cisco サポート コミュニティ - 特集対話](#)

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。

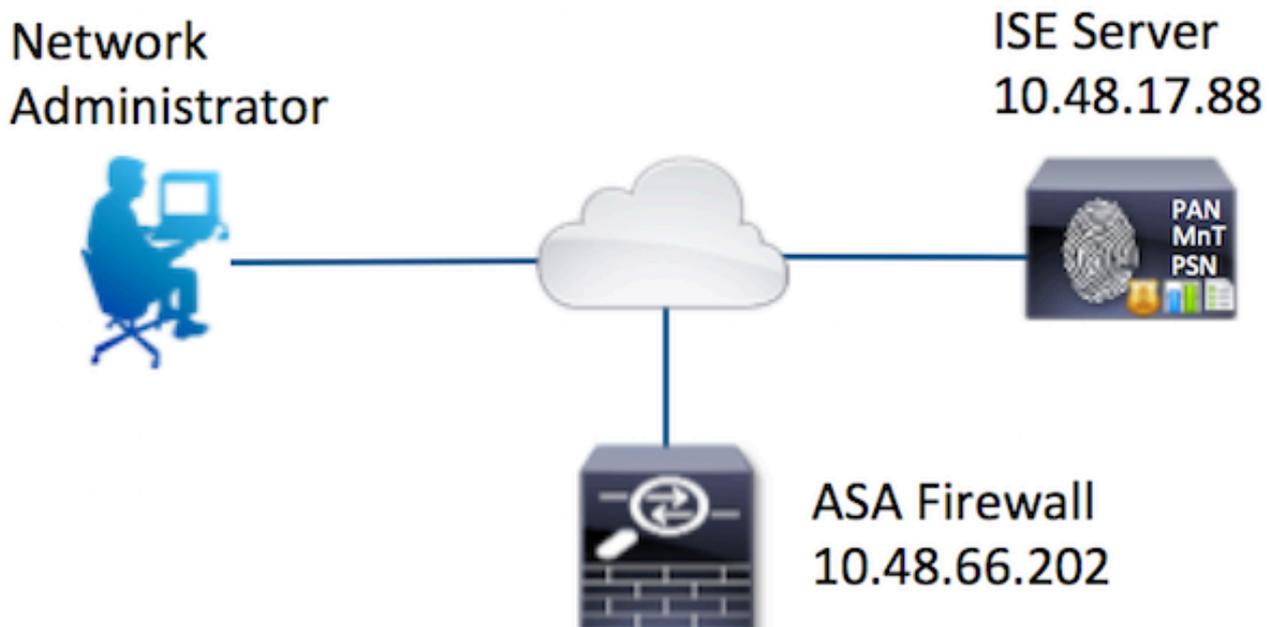
ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

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

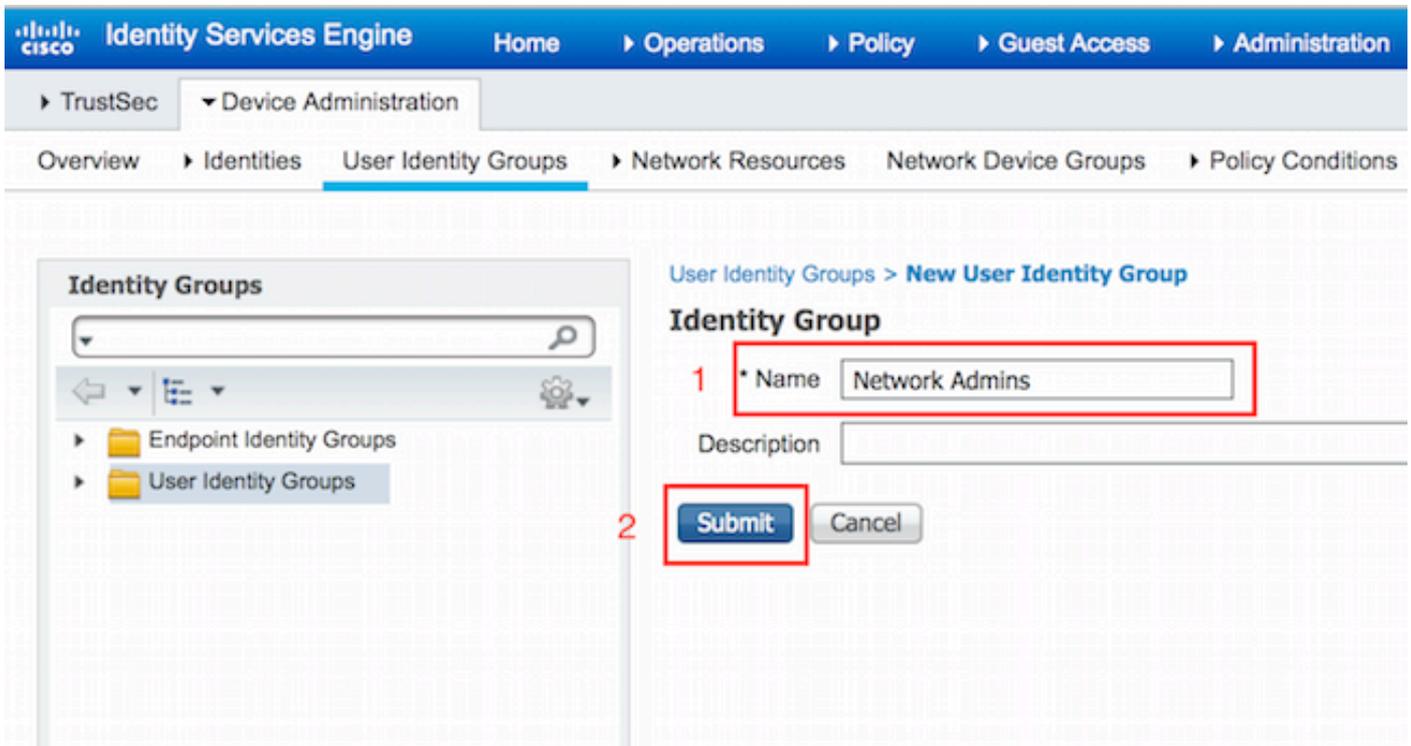
[Work Centers] > [Device Administration] > [Network Resources] > [Network Devices] を選択します。 [Add] をクリックします。 [Name] と [IP Address] を入力し、[TACACS+ Authentication Settings] チェックボックスをオンにして、[Shared Secret] に共有秘密キーを入力します。（任意）デバイスのタイプ/ロケーションを指定できます。

The screenshot shows the 'New Network Device' configuration page in the Cisco Identity Services Engine (ISE) interface. The page is titled 'Network Devices List > New Network Device'. The left sidebar contains 'Network Devices', 'Default Devices', 'TACACS External Servers', and 'TACACS Server Sequence'. The main content area is titled 'Network Devices' and contains the following fields and sections:

- Name:** A text input field containing 'ASA', highlighted with a red box and labeled '1'.
- Description:** An empty text input field.
- IP Address:** A text input field containing '10.48.66.202' and a dropdown menu set to '32', highlighted with a red box and labeled '2'.
- Device Profile:** A dropdown menu set to 'Cisco'.
- Model Name:** An empty dropdown menu.
- Software Version:** An empty dropdown menu.
- Network Device Group:** A section containing:
 - Location:** A dropdown menu set to 'All Locations' and a 'Set To Default' button.
 - Device Type:** A dropdown menu set to 'Firewall' and a 'Set To Default' button.
- RADIUS Authentication Settings:** A section with a checkbox that is unchecked.
- TACACS+ Authentication Settings:** A section with a checkbox that is checked, highlighted with a red box and labeled '3'. It contains a 'Shared Secret' field with masked characters and a 'Show' button.
- Enable Single Connect Mode:** A checkbox that is unchecked.

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 Maintenance 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。

▼ Network Access User

* Name 1

Status Enabled ▼

Email

▼ Passwords 2

	Password	Re-Enter Password	
* Login Password	<input type="password" value="....."/>	<input type="password" value="....."/>	<input type="button" value="i"/>
Enable Password	<input type="password"/>	<input type="password"/>	<input type="button" value="i"/>

▼ User Information

First Name

Last Name

▼ Account Options

Description

Change password on next login

3

▼ User Groups

手順を繰り返して、user ユーザを設定し、Network Maintenance 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

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

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。

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] 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。

Command Set

1

Name * PermitPingShowCommands

Description

Permit any command that is not listed below

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

2

Cancel Save

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。

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

TACACS Command Sets

TACACS Profiles

TACACS Profiles > New

TACACS Profile

1 Name * ShellProfile

Description

Task Attribute View Raw View

Common Tasks

2 Default Privilege 15 (Select 0 to 15)

Maximum Privilege (Select 0 to 15)

Access Control List

Auto Command

No Escape (Select true or false)

Timeout

Idle Time

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。

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

Regular Proxy Sequence

▶ Authentication Policy

▼ Authorization Policy

▶ Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles
<input checked="" type="checkbox"/>	Tacacs_Default	if no matches, then	DenyAllCommands	Edit

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。

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

Regular Proxy Sequence

▼ Proxy Server Sequence

Proxy server sequence:

▶ Authentication Policy

▼ Authorization Policy

▶ Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles
<input checked="" type="checkbox"/>	ASAPermitAllCommands	if Network Admins	then PermitAllCommands AND ShellProfile	Edit
<input checked="" type="checkbox"/>	ASAPermitShowPingCommands	if Network Maintenance Team	then PermitPingShowCommands AND ShellProfile	Edit

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 ssh 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
```

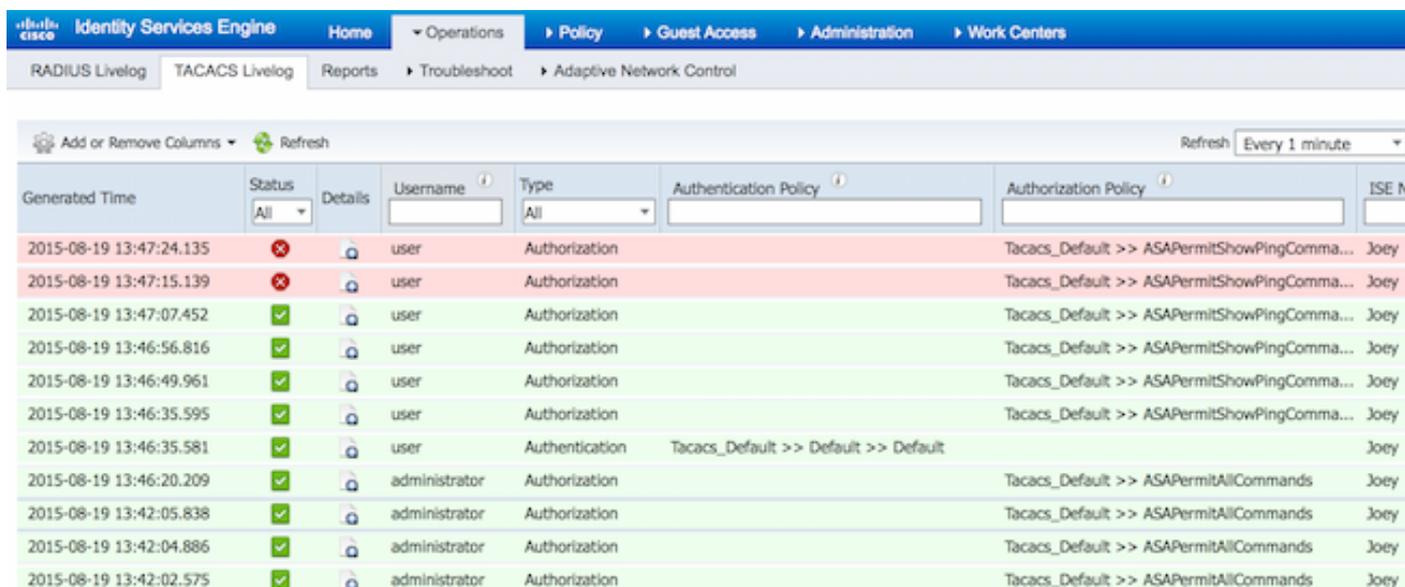
```
ciscoasa(config)# exit
ciscoasa#
```

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。



Generated Time	Status	Details	Username	Type	Authentication Policy	Authorization Policy	ISE N
2015-08-19 13:47:24.135	✖		user	Authorization		Tacacs_Default >> ASAPermitShowPingComma...	Joey
2015-08-19 13:47:15.139	✖		user	Authorization		Tacacs_Default >> ASAPermitShowPingComma...	Joey
2015-08-19 13:47:07.452	✔		user	Authorization		Tacacs_Default >> ASAPermitShowPingComma...	Joey
2015-08-19 13:46:56.816	✔		user	Authorization		Tacacs_Default >> ASAPermitShowPingComma...	Joey
2015-08-19 13:46:49.961	✔		user	Authorization		Tacacs_Default >> ASAPermitShowPingComma...	Joey
2015-08-19 13:46:35.595	✔		user	Authorization		Tacacs_Default >> ASAPermitShowPingComma...	Joey
2015-08-19 13:46:35.581	✔		user	Authentication	Tacacs_Default >> Default >> Default		Joey
2015-08-19 13:46:20.209	✔		administrator	Authorization		Tacacs_Default >> ASAPermitAllCommands	Joey
2015-08-19 13:42:05.838	✔		administrator	Authorization		Tacacs_Default >> ASAPermitAllCommands	Joey
2015-08-19 13:42:04.886	✔		administrator	Authorization		Tacacs_Default >> ASAPermitAllCommands	Joey
2015-08-19 13:42:02.575	✔		administrator	Authorization		Tacacs_Default >> ASAPermitAllCommands	Joey

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。

Overview

Request Type	Authorization
Status	Fail
Session Key	Joey/229297775/274
Message Text	Failed-Attempt: Command Authorization failed
Username	user
Authorization Policy	Tacacs_Default >> ASAPermitShowPingCommands
Shell Profile	
Matched Command Set	
Command From Device	traceroute 8.8.8.8

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](#)