Cisco IOS ベースのネットワーク デバイスの ISE TACACS+ 構成ガイド

セキュア アクセスを実現するハウツー ユーザ シリーズ

作成者：シスコ、セキュリティ ビジネス グループ、ポリシーとアクセス、テクニカル マーケティング

日付：2016 年 1 月

目次

目次 2
このマニュアルについて 3
概要 3
このガイドの使用方法 3
使用するコンポーネント 3
ISE のデバイス管理の設定 4
ISE でのデバイス管理のライセンス 4
ISE でのデバイス管理の有効化 4
デバイス管理ワーク センター 5
ネットワーク デバイスとネットワーク デバイス グループ 6
ID ストア 7
TACACS プロファイル 8
IOS HelpDesk Privilege 9
IOS Admin Privilege 9
TACACS コマンド セット 10
HelpDesk コマンド 10
IOS セキュリティ コマンド 11
Permit All コマンド 11
デバイス管理ポリシー セット 11
IOS の TACACS+ の設定 14
TACACS+ 認証とフォールバック 14
TACACS+ コマンド認証 15
TACACS+ コマンド アカウンティング 16
次のステップ 17

このマニュアルについて

概要

クライアント/サーバ プロトコルである Terminal Access Controller Access Control System Plus（TACACS+）は、ルータなどの多くのタイプのネットワーク アクセス デバイスに管理アクセスするための、一元化されたセキュリティ制御を提供します。TACACS+ では、次の AAA サービスを提供します。

- Authentication（認証）：ユーザは誰か
- Authorization（許可）：ユーザは何を実行できるか
- Accounting（アカウンティング）：誰が何を、いつ実行したか

このドキュメントでは、TACACS+ サーバとして Cisco Identity Services Engine（ISE）、TACACS+ クライアントとして Cisco IOS ネットワーク デバイスを使用する TACACS+ の設定例を示します。

このガイドの使用方法

このガイドでは、次の 2 部構成で、Cisco IOS ベースのネットワーク デバイスへの管理アクセスを ISE で管理できるようにします。

- パート 1：ISE のデバイス管理の設定
- パート 2：Cisco IOS の TACACS+ の設定

使用するコンポーネント

このドキュメントの情報は、以下のソフトウェア バージョンおよびハードウェア バージョンに基づいています。

- ISE VMware 仮想アプライアンス リリース 2.0
- シスコ クラウド サービス ルータ 1000V（CSRv）、Cisco IOS XE バージョン 03.16.00.S

Cisco IOS-XR を除き、ほとんどの Cisco IOS デバイスでも動作します（権限レベルではなくユーザのタスク グループを使用する ASR9000 など）。

このドキュメントの資料はラボ環境のデバイスから作成されています。すべてのデバイスはクリア済み（デフォルト）の設定で開始しています。

ISE のデバイス管理の設定

ISE でのデバイス管理のライセンス

デバイス管理（TACACS+）は展開ごとにライセンスされ、有効な ISE BASE ライセンスまたはモビリティ ライセンスが必要です。

ISE でのデバイス管理の有効化

デバイス管理サービス（TACACS+）は ISE ノードでデフォルトで有効になっていません。最初の手順は、有効にすることです。

手順 1 サポートされているブラウザの 1 つを使用して ISE 管理 Web ポータルにログインします。

手順 2 [管理（Administration）] > [システム（System）] > [展開（Deployment）] に移動します。ISE ノードの隣にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。

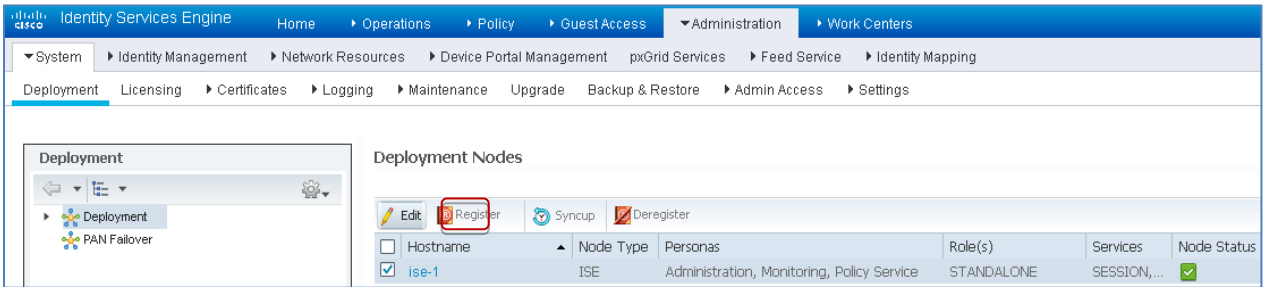

図 1. ISE 展開ページ

手順 3 [全般設定（General Settings）] で下にスクロールし、[デバイス管理サービスを有効にする（Enable Device Admin Service）] の隣にあるチェックボックスをオンにします。

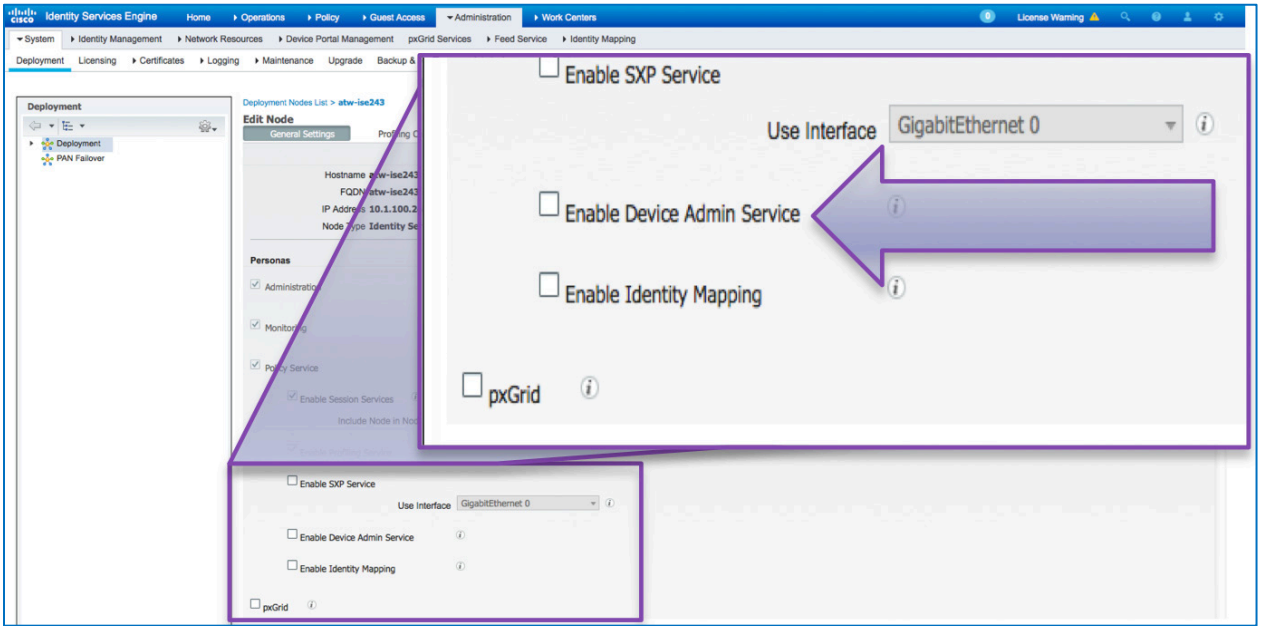

図 2. ISE 展開の全般設定

手順 4 [保存(Save)] で設定を保存します。これでデバイス管理サービスが ISE で有効になります。

デバイス管理ワーク センター

ISE 2.0 はワーク センターを導入しています。ワーク センターは、それぞれが特定のフィーチャのすべての要素を包含しています。

手順 1 [ワーク センター(Work Centers)] > [デバイス管理(Device Administration)] > [概要(Overview)] に移動します。

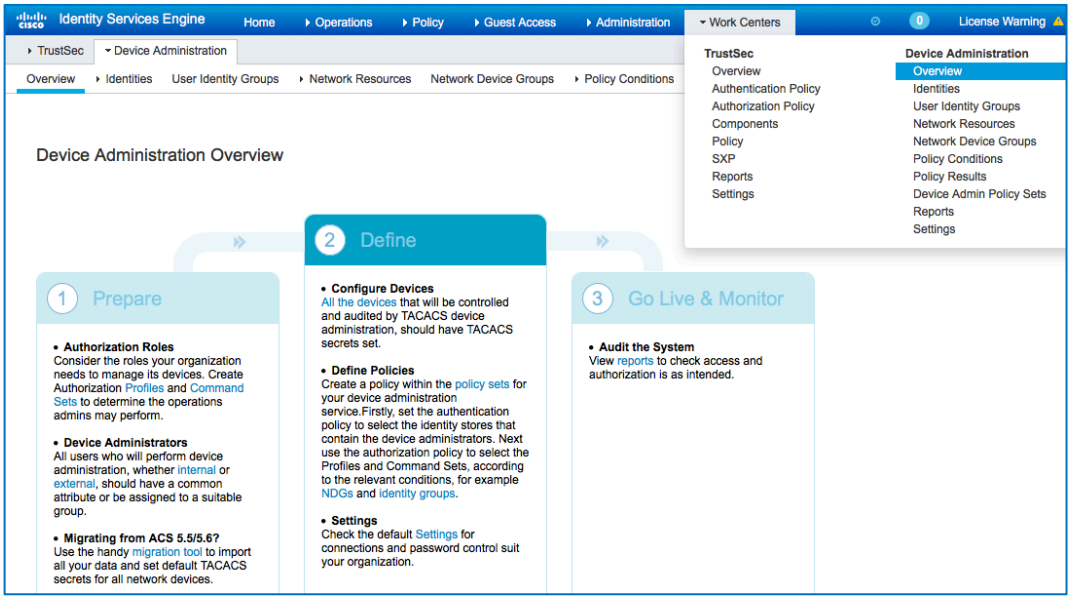

図 3. デバイス管理の概要

[デバイス管理の概要(Device Administration Overview)] では、デバイス管理の使用例に必要な手順の概要を提供します。

ネットワーク デバイスとネットワーク デバイス グループ

ISE では、複数のデバイス グループ階層を使用する強力なデバイス グループ化機能を提供しています。各階層はネットワーク デバイスの別個の独立した分類を表します。

手順 1 [ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワーク デバイス グループ（Network Device Groups）] に移動します。

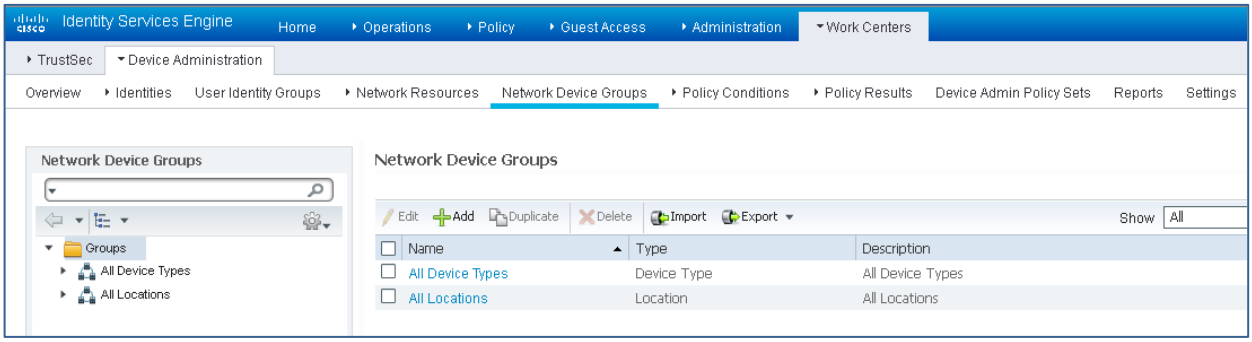

図 4. ネットワーク デバイス グループ

[すべてのデバイス タイプ（All Device Types）] と [すべてのロケーション（All Locations）] は、ISE により提供されるデフォルトの階層です。独自の階層を追加したり、後でポリシー条件に使用できるネットワーク デバイスを識別するためにさまざまなコンポーネントを定義したりできます。

手順 2 階層を定義すると、ネットワーク デバイス グループは、次のように表示されます。

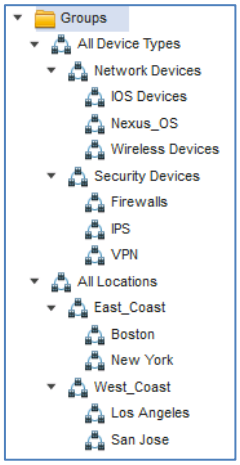

図 5. ネットワーク デバイス グループのツリー ビュー

手順 3 ここでは、ネットワーク デバイスとして CSRv を追加します。[ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワーク リソース（Network Resources）] に移動します。[追加（Add）] をクリックし、新しいネットワーク デバイス **DMZ_BLDO_CSRv** を追加します。

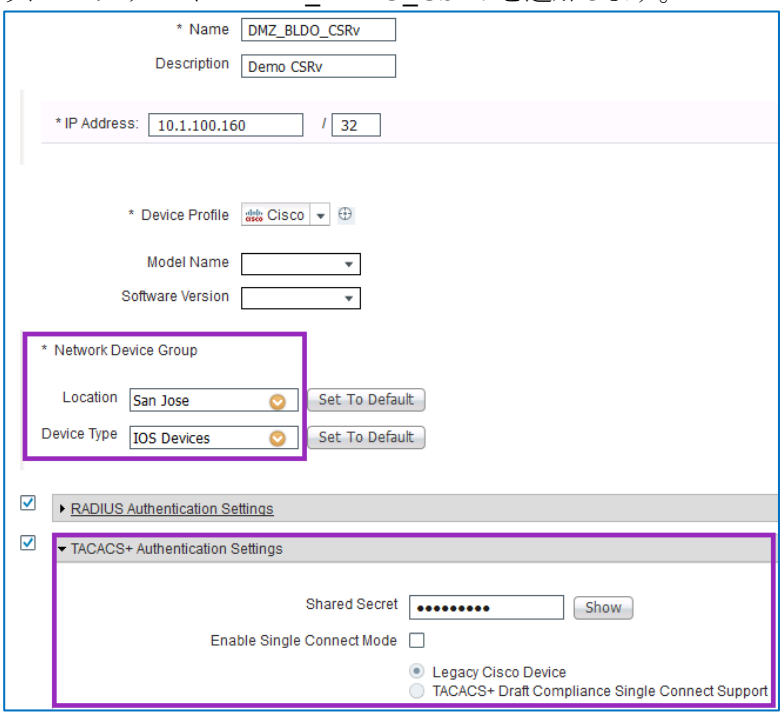

図 6. ネットワーク デバイスの追加

デバイスの IP アドレスを入力し、デバイスの [ロケーション（Location）] と [デバイス タイプ（Device Type）] がマッピングされることを確認します。最後に、[TACACS+ 認証設定（TACACS+ Authentication Settings）] を有効にし、[共有秘密（Shared Secret）] を指定します。

ID ストア

このセクションでは、デバイス管理者の ID ストアを定義します。ID ストアは ISE 内部ユーザおよびサポートされる外部 ID ソースにすることができます。ここでは、Active Directory（AD）、外部 ID ソースを使用します。

手順 1 [管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory] に移動します。[追加（Add）] をクリックし、新しい AD の参加ポイントを定義します。参加ポイント名と AD ドメイン名を指定し、[送信（Submit）] をクリックします。

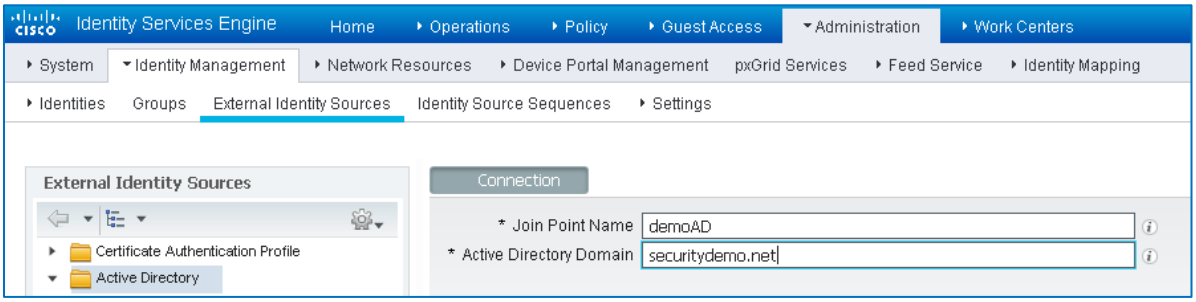

図 3. AD 参加ポイントの追加

手順 2 「この Active Directory ドメインにすべての ISE ノードを参加させますか?(Would you like to Join all ISE Nodes to this Active Directory Domain?)」というプロンプトが表示されたら、[はい(Yes)] をクリックします。AD への参加特権があるクレデンシャルを入力し、[参加(Join)] で ISE を AD に参加させます。[ステータス(Status)] をチェックし、稼働中であることを確認します。

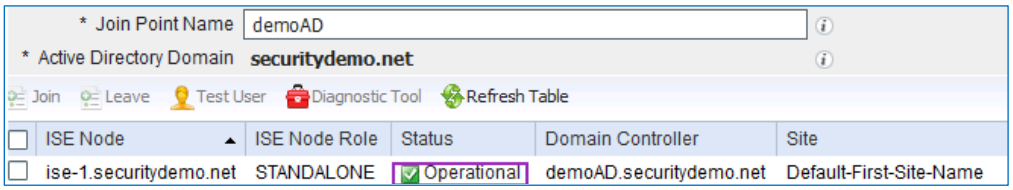

図 4. ISE の AD への参加

手順 3 [グループ(Groups)] タブに移動し、[追加(Add)] をクリックして、デバイス アクセスが許可されるユーザに基づいて必要なグループをすべて取得します。このガイドの承認ポリシーに使用するグループを以下の例に示します。

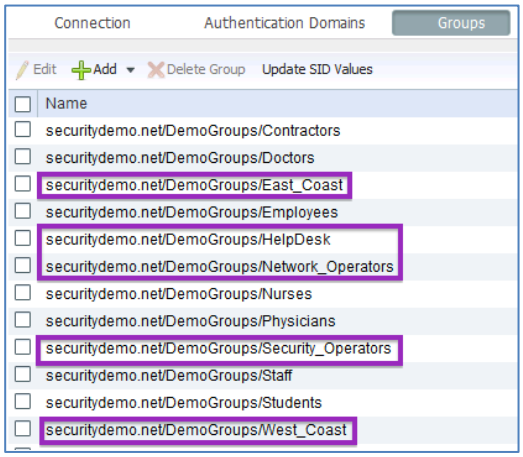

図 5. AD グループ

TACACS プロファイル

Cisco IOS は 16 のレベルのアクセス権を提供します。次の 3 つはデフォルトで定義されています。

権限レベル 0:*disable*、*enable*、*exit*、*help*、および *logout* コマンドを許可します。ログイン後、1 が最低限のアクセス可能レベルなので、このレベル 0 のすべてのコマンドはすべてのユーザが実行できます。

権限レベル 1:非特権またはユーザ EXEC モードは、ログインしたユーザのデフォルトの権限レベルです。シェル プロンプトは、「Router>」など、デバイス名の後に山カッコが続きます。

権限レベル 15:特権 EXEC モードは、enable コマンド後のレベルです。シェル プロンプトは、「Router#」など、デバイスのホスト名の後にシャープ記号が続きます。

EXEC 認証では、ユーザにシェル（EXEC）セッションの開始が許可されているかどうかを確認するために、IOS デバイスは認証直後に AAA サーバに TACACS+ 認証要求を送信します。ここでは、ISE を構成して 2 つの属性を設定し、ユーザごとにカスタマイズします。

デフォルトの権限（Default Privilege）：シェル セッションに対する初期（デフォルト）の権限レベルを指定します。承認済みユーザはレベル 1 ではなく、このレベルに初期化されます。このレベルのアクセスで十分な場合は、ユーザが enable コマンドを使用する必要はありません。

最大権限（Maximum Privilege）：シェル セッションで許可される最大レベルを指定します。承認済みユーザは、より低いデフォルト レベルにログインし、enable コマンドを使用して、この属性で割り当てられた値に達するまで、より高いレベルに移行できます。

2 つの TACACS プロファイル、IOS_HelpDesk_Privilege と IOS_Admin_Privilege を定義します。

IOS HelpDesk Privilege

ヘルプ デスクのトラブルシューティングを行うには、通常はレベル 1 のコマンドで十分なので、ヘルプデスク アナリストにデフォルトの特権としてこのレベルを割り当てます。まれに、より多くの権限を必要とするので、最大特権レベルとして 15 を許可します。

手順 1 ISE GUI で、[ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー結果（Policy Results）] > [TACACS プロファイル（TACACS Profiles）] に移動します。新しい TACACS プロファイルを追加し、**IOS_HelpDesk_Privilege** という名前を付けます。

手順 2 [共通タスク（Common Tasks）] セクションまでスクロールします。ドロップダウン セレクタから値が 1 のデフォルトの権限、ドロップダウンから値が 15 の最大権限を有効にします。

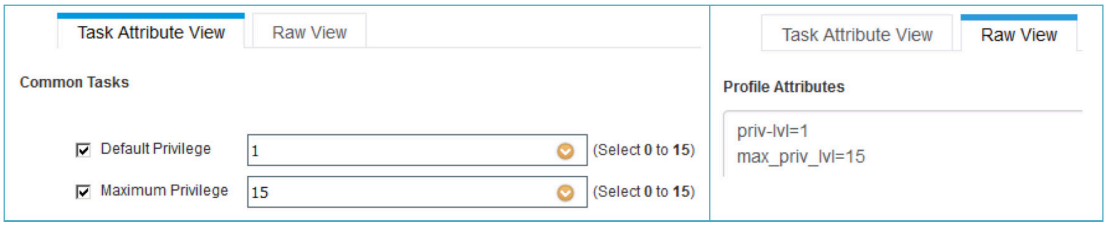

図 6. IOS_HelpDesk_Privilege の TACACS プロファイル

[保存（Save）] をクリックしてプロファイルを保存します。

IOS Admin Privilege

一般的に、ネットワーク管理者にはより多くの権限が必要なので、レベル 15 がデフォルトで直接設定されます。

手順 3 別のプロファイルを追加し、**IOS_Admin_Privilege** という名前を付けます。

手順 4 [共通タスク（Common Tasks）] セクションまでスクロールします。ドロップダウン セレクタから値が 15 のデフォルトの権限、ドロップダウンから値が 15 の最大権限を有効にします。

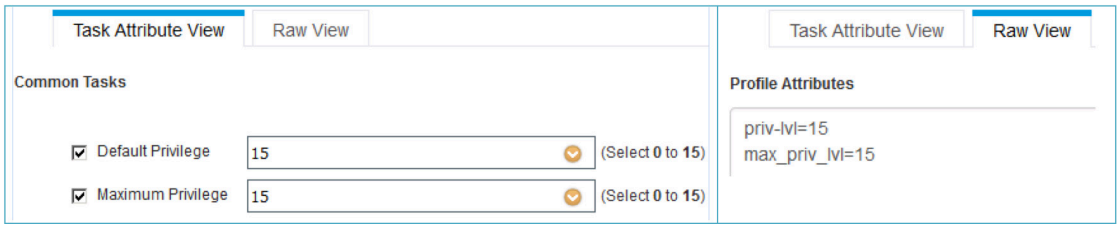

図 7. IOS_Admin_Privilege の TACACS プロファイル

[保存(Save)] をクリックしてプロファイルを保存します。

TACACS コマンド セット

IOS コマンド認証は、デバイスの管理者がコマンドの発行を承認されているかどうか確認するために、設定された TACACS+ サーバを照会します。ISE は、さまざまな権限レベルで使用できるコマンドを最適化するために、ユーザに付与されたコマンドの一覧を提供できます。

3 つのコマンドセット、HelpDesk_Commands、IOS_Security_Commands、および Permit_All_Commands を定義します。

HelpDesk コマンド

手順 1 ISE GUI で、[ワーク センター(Work Centers)] > [デバイス管理(Device Administration)] > [ポリシー結果(Policy Results)] > [TACACS コマンド セット(TACACS Command Sets)] の順に移動します。新しいセットを追加し、**HelpDesk_Commands** という名前を付けます。

手順 2 [+追加(+Add)] をクリックして、セットにエントリを設定します。

付与	コマンド	引数
許可	debug	
許可	undebug	
許可	traceroute	
拒否	ping	^([0-9]{1,3})\.([0-9]{1,3})\.([0-9]{1,3})\.255$
許可	ping	
許可	show	

ヘルプデスクのアナリストに、debug、undebug、traceroute、および show の実行を許可します。ping については、引数列の正規表現に示すように、ネットワーク サブネットはブロードキャスト アドレスを 255 までと想定しているため、ブロードキャスト ping は制限されています。

手順 3 行を保持するには、各エントリの末尾にある ✓ チェックマークをクリックします。

手順 4 [保存(Save)] をクリックして、コマンド セットを保存します。

IOS セキュリティ コマンド

手順 5 新しいセットを追加し、**IOS_Security_Commands** という名前を付けます。

手順 6 [+追加(+Add)] をクリックして、セットにエントリを設定します。

付与	コマンド	引数
許可	config*	
DENY_ALWAYS	interface	GigabitEthernet 1
DENY_ALWAYS	interface	GigabitEthernet ([0-9]{1,3}) 0
許可	interface	
許可	shut	
許可	No	shut

このサンプル コマンド セットでは、セキュリティ管理者が、DENY_ALWAYS エントリで指定された 2 種類のインターフェイスを除くすべてのインターフェイスで shut と no shut アクションを実行できます。この 2 つ目のタイプでは、インターフェイス パターン `GigabitEthernet <0-999>/0` を指定します。

手順 7 行を保持するには、各エントリの末尾にある ✓ チェックマークをクリックします。

手順 8 [保存(Save)] をクリックして、コマンド セットを保存します。

Permit All コマンド

手順 9 新しいセットを追加し、**Permit_All_Commands** という名前を付けます。

手順 10 [下にリストされていないコマンドを許可(Permit any command that is not listed below) ☑] の隣にあるチェックボックスをオンにして、コマンド リストを空のままにします。

付与	コマンド	引数

手順 11 [保存(Save)] をクリックして、コマンド セットを保存します。

デバイス管理ポリシー セット

ポリシー セットはデバイス管理でデフォルトで有効になっています。ポリシー セットはデバイス タイプに基づいてポリシーを分割できるため、TACACS プロファイルの適用が容易になります。たとえば、Cisco IOS デバイスでは特権レベルとコマンド セットを使用し、WLC デバイスではカスタム属性を使用します。

手順 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)] に移動します。次の新しいポリシーセット **IOS Devices** を追加します。

S	名前	説明	条件
✓	IOS Devices		DEVICE:Device Type EQUALS Device Type#All Device Types#Network Devices#IOS Devices

図 8. ポリシー セットの条件

手順 2 承認ポリシーを作成します。認証では、ID ストアとして AD を使用します。

認証ポリシー
✓ Default Rule(なにも一致しない場合): : Allow Protocols : Default Device Admin and use: demoAD

図 9. 認証ポリシー

手順 3 承認ポリシーを定義します。ここでは、AD のユーザ グループとデバイスのロケーションに基づいて承認ポリシーを定義します。たとえば、AD グループ West Coast のユーザは、West Coast のデバイスのみにアクセスできます。

S	ルール名	条件	コマンド セット	シェル プロファイル
✓	HelpDesk West	DEVICE:Location CONTAINS All Locations#West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/HelpDesk	HelpDesk_Commands	IOS_HelpDesk_Privilege
✓	HelpDesk East	DEVICE:Location CONTAINS All Locations#East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/HelpDesk	HelpDesk_Commands	IOS_HelpDesk_Privilege
✓	Security West	DEVICE:Location CONTAINS All Locations#West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Security_Operators	IOS_Security_Commands AND HelpDesk_Commands	IOS_Admin_Privilege
✓	Security East	DEVICE:Location CONTAINS All Locations#East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Security_Operators	IOS_Security_Commands AND HelpDesk_Commands	IOS_Admin_Privilege
✓	Admin West	DEVICE:Location CONTAINS All Locations#West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Network_Operators	Permit_All_Commands	IOS_Admin_Privilege

S	ルール名	条件	コマンド セット	シェル プロファイル
✓	Admin East	DEVICE:Location CONTAINS All Locations#East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Network_Operators	Permit_All_Commands	IOS_Admin_Privilege
✓	Default	なにも一致しない場合	DenyAllCommands	

図 10.　許可ポリシー

これで、IOS のデバイス管理の ISE 設定が完了しました。

IOS の TACACS+ の設定

Cisco IOS デバイスの TACACS+ AAA は次の順序で設定可能です。

1. TACACS+ 認証とフォールバックを有効化する
2. TACACS+ コマンド認証を有効化する
3. TACACS+ コマンド アカウンティングを有効化する

TACACS+ 認証とフォールバック

TACACS+ を設定する前に、SSH または適切なリモート接続プロトコルを最初に設定する必要があります。次に、SSH を有効化する設定例を示します。

```
hostname CSRv
no ip domain-lookup
ip domain-name securitydemo.net
crypto key generate rsa modulus 2048

ip ssh version 2

enable secret ISEisC00L
username local-admin privilege 15 secret ISEisC00L

aaa new-model
aaa authentication login CON none
aaa authentication login default local

interface GigabitEthernet1
 ip address 10.1.100.160 255.255.255.0

ip access-list extended vtyAccess
 permit tcp 10.1.100.0 0.0.0.255 any eq 22

line con 0
 exec-timeout 0 0
 login authentication CON
 logging synchronous

!! Below assumes only 5 VTY lines (from 0 to 4)
line vty 0 4
 access-class vtyAccess in
 transport input ssh
 logging synchronous
```

この段階で上述のサンプル ネットワーク デバイスに有効な IP アドレスがあるため、コンソール ログインは認証されていなくても、10.1.100.0/24 のクライアントからこの IOS デバイスに SSH 通信できます。AAA 設定時に発生する可能性のあるアクセス問題を避けるために、CONSOLE の EXEC タイムアウトは無効にされていることに注意してください。

TACACS+ 認証は、次のような設定で有効化できます。

```
tacacs server ise-1
 address ipv4 10.1.100.21
 key ISEisC00L

aaa group server tacacs+ demoTG
 server name ise-1

aaa authentication login VTY group demoTG local
aaa authentication enable default group demoTG enable

line vty 0 4
 login authentication VTY
```

ここでは、VTY の行を認証するために TACACS+ に切り替えました。「イネーブル」認証には、デフォルトの一覧しかないため、VTY と CONSOLE の両方が TACACS+ を使用して「イネーブル」アクセスを認証することに注意してください。

設定された TACACS+ サーバが利用できなくなるイベントでは、ログイン認証は「ローカル」のユーザ データベースにフォールバックし、イネーブル認証は「イネーブル」シークレットにフォールバックします。

TACACS+ コマンド認証

EXEC 認証は、コマンド認証の特別な形式です。ユーザのログイン直後に行われ、以下を追加することで有効化できます。

```
aaa authorization exec CON none
aaa authorization console
aaa authorization exec VTY group demoTG local if-authenticated

line con 0
 authorization exec CON

line vty 0 4
 authorization exec VTY
```

この時点で、デフォルトの権限属性を持つシェル プロファイルは、新しい SSH セッションに適用されます。

コンフィギュレーション モードと、さまざまな権限レベルの TACACS+ コマンド認証の拡張は、以下を追加することで有効化できます。

```
aaa authorization config-commands
aaa authorization commands 1 VTY group demoTG local if-authenticated
aaa authorization commands 15 VTY group demoTG local if-authenticated

line vty 0 4
 authorization commands 1 VTY
 authorization commands 15 VTY
```

TACACS+ コマンド アカウンティング

コマンド アカウンティングによって、実行された各コマンドの情報（コマンド、日付、ユーザ名など）が送信されます。以下は、前述の設定例に、このアカウンティング機能の有効化を追加します。

```
aaa accounting exec default start-stop group demoTG
aaa accounting commands 1 default start-stop group demoTG
aaa accounting commands 15 default start-stop group demoTG
```

ここでは、接続の種類に基づいた個別のアカウンティングは必要ではないため、デフォルトのメソッド一覧を使用します。

IOS の TACACS+ の設定が完了しました。

次のステップ

Cisco IOS のデバイス管理者の設定が完了しました。設定を確認する必要があります。

手順 1 SSH 通信で、さまざまなロールとして IOS デバイスにログインします。

手順 2 デバイスのコマンドライン インターフェイス(CLI)で、ユーザが適切なコマンドにアクセスできることを確認します。たとえば、ヘルプデスクのユーザは通常の IP アドレス(10.1.10.1 など)を ping できますが、ブロードキャスト アドレス(10.1.10.255 など)の ping は拒否されなければなりません。

手順 3 ユーザ接続を表示するには、以下を発行します。

```
show users
```

出力例は次のとおりです。

```
CSRv#show users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 01:54:52
*  1 vty 0     neo        idle                 00:00:00 10.1.100.6
...
```

手順 4 次のデバッグは、TACACS+ のトラブルシューティングに役に立ちます。

```
debug aaa authorization
debug tacacs
debug tacacs packet
```

次にデバック出力例を示します。

```
CSRv#debug tacacs
TACACS access control debugging is on
...
*Jan  4 06:24:43.001: tty2 AAA/AUTHOR/CMD (2087247696): Port='tty2' list='VTY' service=CMD
*Jan  4 06:24:43.001: AAA/AUTHOR/CMD: tty2 (2087247696) user='admin'
*Jan  4 06:24:43.001: tty2 AAA/AUTHOR/CMD (2087247696): send AV service=shell
*Jan  4 06:24:43.001: tty2 AAA/AUTHOR/CMD (2087247696): send AV cmd=debug
*Jan  4 06:24:43.001: tty2 AAA/AUTHOR/CMD (2087247696): send AV cmd-arg=tacacs
*Jan  4 06:24:43.001: tty2 AAA/AUTHOR/CMD (2087247696): send AV cmd-arg=<cr>
*Jan  4 06:24:43.001: tty2 AAA/AUTHOR/CMD(2087247696): found list "VTY"
*Jan  4 06:24:43.001: tty2 AAA/AUTHOR/CMD (2087247696): Method=demoTG (tacacs+)
*Jan  4 06:24:43.001: AAA/AUTHOR/TAC+: (2087247696): user=admin
*Jan  4 06:24:43.001: AAA/AUTHOR/TAC+: (2087247696): send AV service=shell
*Jan  4 06:24:43.001: AAA/AUTHOR/TAC+: (2087247696): send AV cmd=debug
*Jan  4 06:24:43.001: AAA/AUTHOR/TAC+: (2087247696): send AV cmd-arg=tacacs
*Jan  4 06:24:43.001: AAA/AUTHOR/TAC+: (2087247696): send AV cmd-arg=<cr>
*Jan  4 06:24:43.203: AAA/AUTHOR (2087247696): Post authorization status = PASS_ADD
*Jan  4 06:24:43.203: AAA/MEMORY: free_user (0x7FF239502490) user='admin' ruser='CSRv'
port='tty2' rem_addr='10.1.100.203' authen_type=ASCII service=NONE priv=15 vrf= (id=0)
...
```

手順 5 ISE GUI から、[運用（Operations）] > [TACACS ライブログ（TACACS Livelog）] の順に移動します。すべての TACACS 認証要求と許可要求がここでキャプチャされており、詳細ボタンにより、特定のトランザクションが成功または失敗した理由の詳細情報を確認できます。

Username	Type	Authorization Policy	Network Device Name	Remote Address	Matched Comman...	Shell Profile
	All					
lsmith	Authorization	IOS_Devices >> Admin West	DMZ_BLDO_CSRv	10.1.100.203	Permit_All_Command	
lsmith	Authorization	IOS_Devices >> Admin West	DMZ_BLDO_CSRv	10.1.100.203		IOS_Admin_Privilege
lsmith	Authentication		DMZ_BLDO_CSRv	10.1.100.203		
lmiller	Authorization	IOS_Devices >> Security West	DMZ_BLDO_CSRv	10.1.100.203		
lmiller	Authorization	IOS_Devices >> Security West	DMZ_BLDO_CSRv	10.1.100.203	IOS_Security_Com...	
lmiller	Authorization	IOS_Devices >> Security West	DMZ_BLDO_CSRv	10.1.100.203		IOS_Admin_Privilege
lmiller	Authentication		DMZ_BLDO_CSRv	10.1.100.203		
jstalk	Authorization	IOS_Devices >> HelpDesk West	DMZ_BLDO_CSRv	10.1.100.203	HelpDesk_Commands	
jstalk	Authorization	IOS_Devices >> HelpDesk West	DMZ_BLDO_CSRv	10.1.100.203		IOS_HelpDesk_Privilege
jstalk	Authentication		DMZ_BLDO_CSRv	10.1.100.203		

図 11. TACACS Livelog

手順 6 履歴レポートを確認する場合は、[ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [レポート（Reports）] > [デバイス管理（Device Administration）] の順に移動し、認証、許可、アカウンティングのレポートを取得します。