ワイヤレス LAN コントローラ向け

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：Aruna Yerragudi（Hsing-Tsu Lai 編集）

日付：2015 年 12 月

目次

このガイドについて

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、ルータまたはネットワーク アクセス デバイスへの管理アクセスを提供するため、ユーザに一元化されたセキュリティ制御を実装します。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 Wireless LAN Controller（WLC）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

このガイドは、WLC の管理者アクセスを ISE が管理できるようにする各アクティビティに応じて、2 部に分かれています。

- パート 1：ISE のデバイス管理の設定
- パート 2：WLC 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 リリース 2.0
- AireOS ソフトウェア バージョン 7.6 および 8.0 の WLC

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。

デバイス管理の ISE 設定

ISE でのデバイス管理のライセンス

デバイス管理は展開ごとにライセンスされますが、存在する有効な 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。

ステップ 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。

ステップ 2 [管理（Administration）] > [システム（System）] > [展開（Deployment）] に移動します。ISE ノードの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。

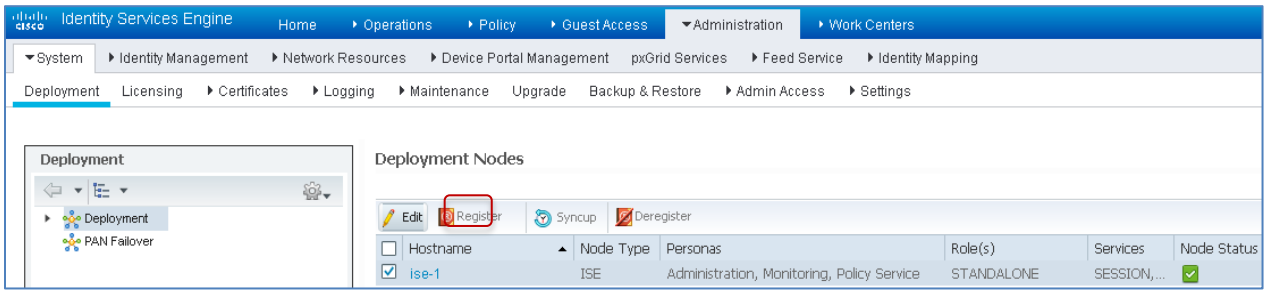

図 1. ISE 展開ページ

ステップ 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。

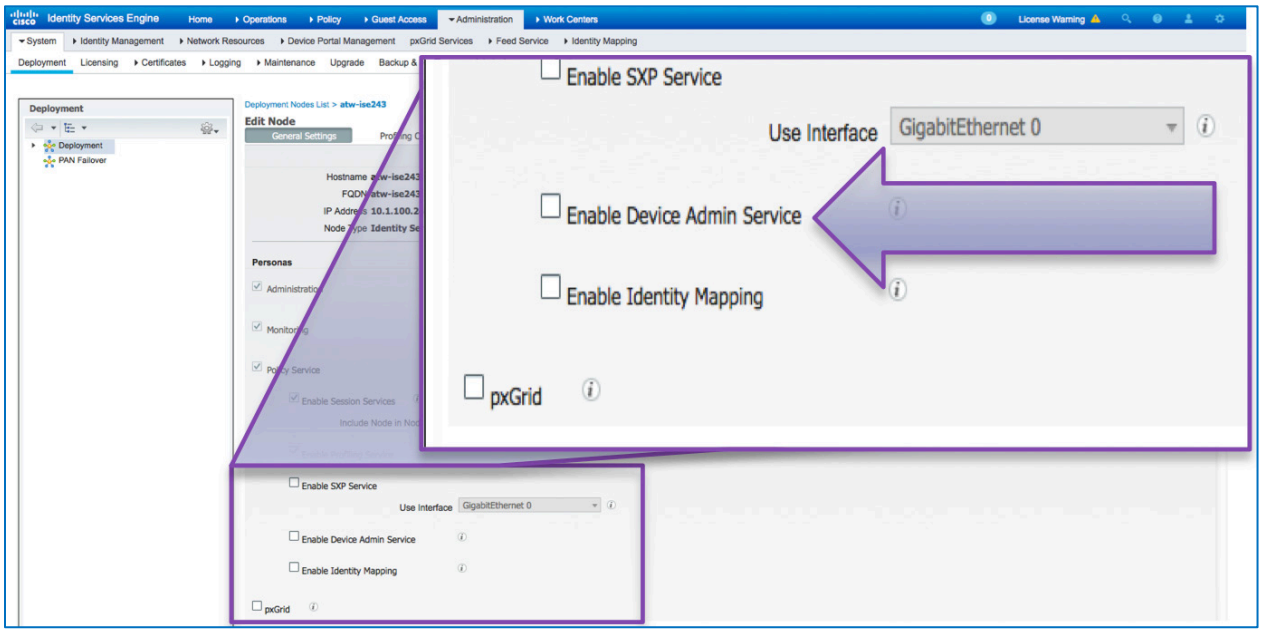

図 2. ISE 展開の全般設定

ステップ 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。

デバイス管理のワーク センター

ISE 2.0 では TrutSec およびデバイス管理にワーク センターを導入しています。ワーク センターには特定の機能のすべての要素が含まれています。

ステップ 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。

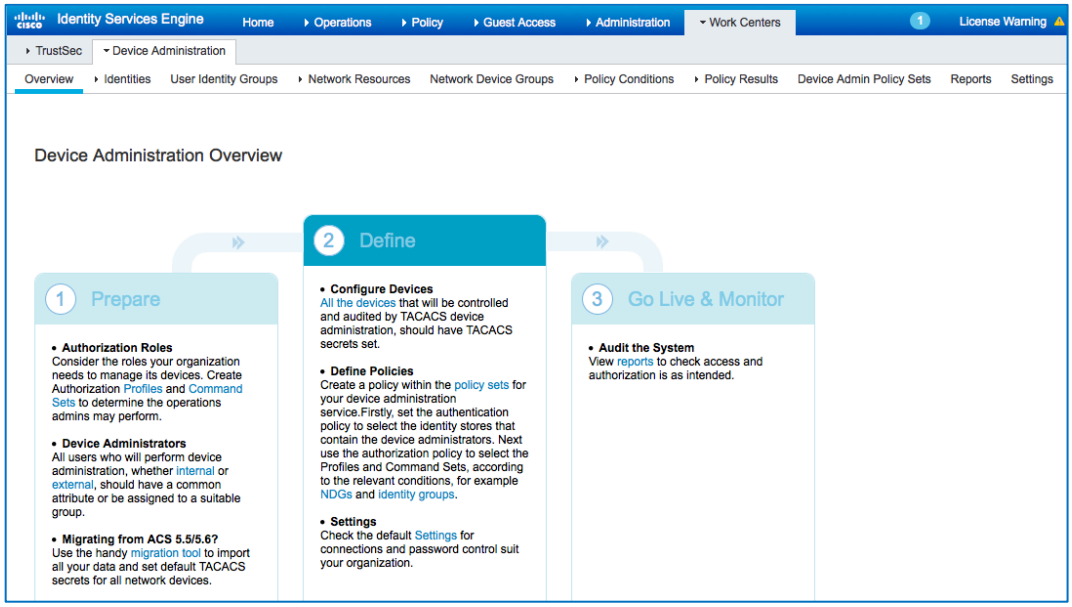

図 3. デバイス管理の概要

[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 グループの設定

ネットワーク デバイスとネットワーク デバイスのグループ化を調査してみましょう。

ISE では、複数のデバイス グループ階層の形で強力なデバイス 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。

ステップ 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。

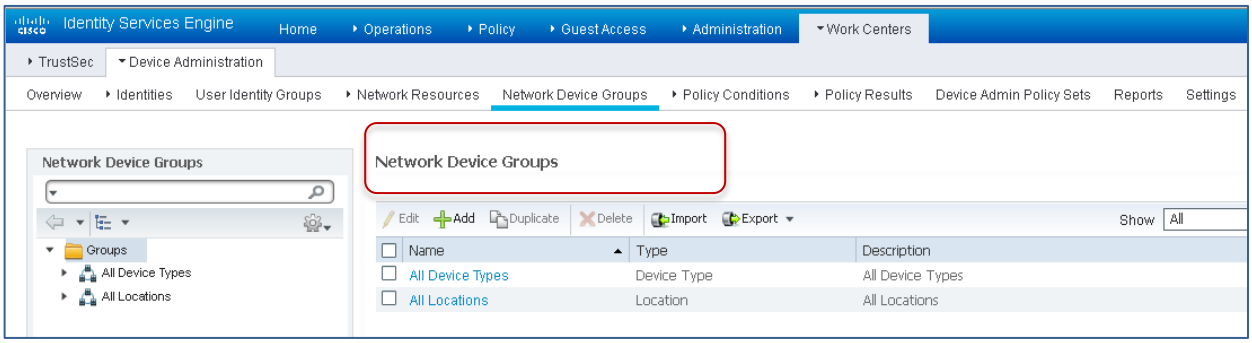

図 4. ネットワーク デバイス グループ

[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。独自の階層を追加することも、後でポリシー条件に使用するネットワーク 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することもできます。

ステップ 2 さまざまな階層を定義すると、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。

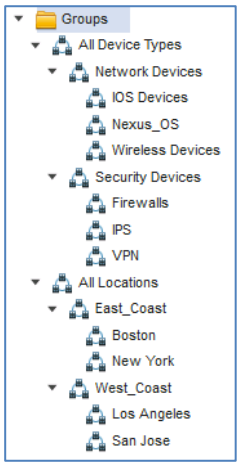

図 5. ネットワーク デバイス グループのツリー ビュー

ここでは、さまざまなデバイス タイプとロケーションを追加しています。

ステップ 3 ここでは、ネットワーク デバイスとして WLC 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_vWLC** を追加します。

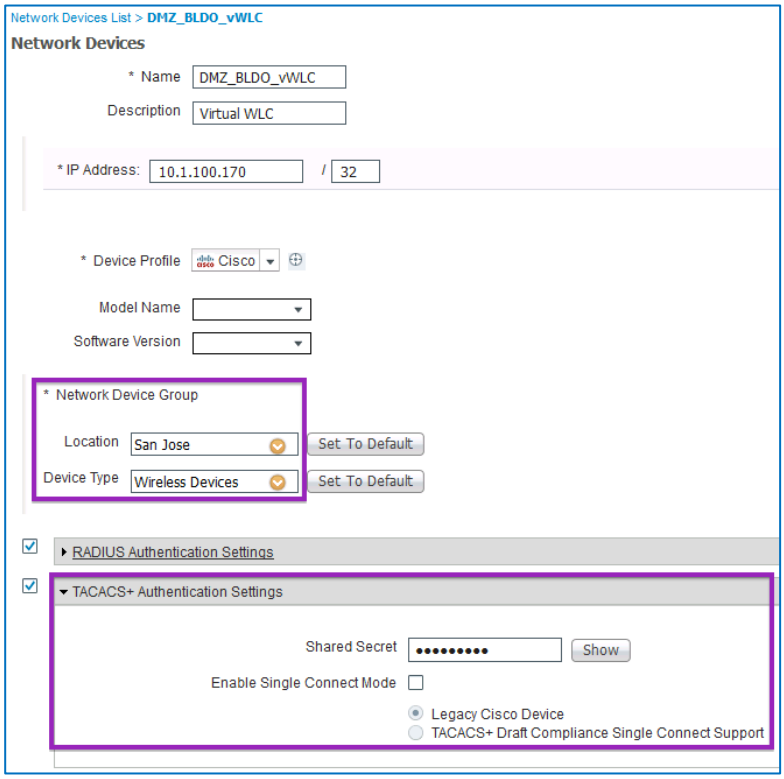

図 6. ネットワーク デバイスの追加

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 ストアの定義

ここでは、デバイス管理者の ID ストアを定義します。ID ストアは、ISE 内部ユーザやサポートされている外部 ID ソースにすることができます。この設定では、外部 ID ソースの Active Directory（AD）を使用します。

ステップ 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 Active Directory 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。

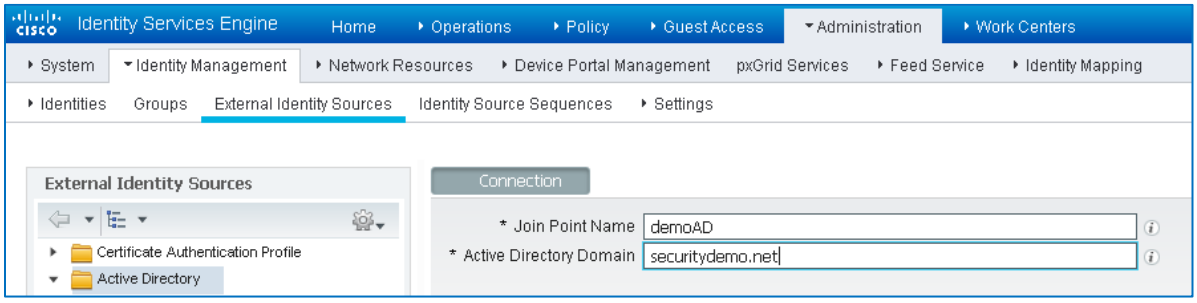

図 6. AD 参加ポイントの追加

ステップ 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。

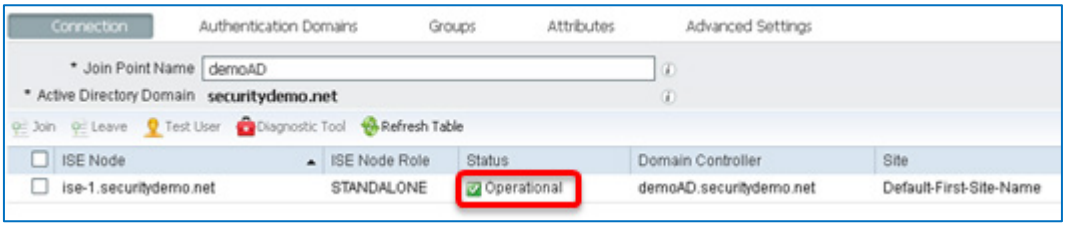

図 8. ISE の AD への参加

ステップ 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に示します。

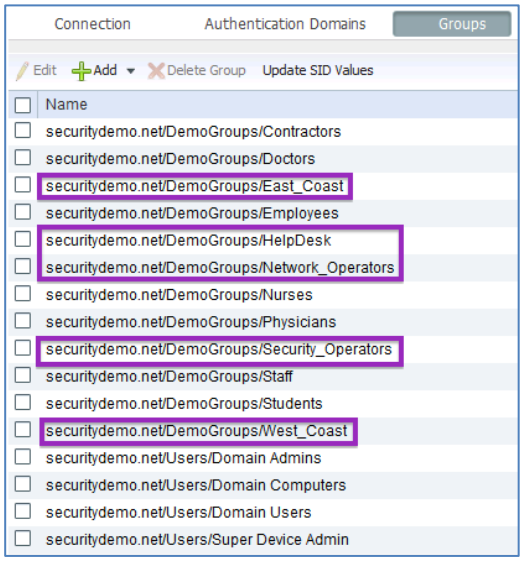

図 9. AD グループ

TACACS プロファイルの設定

承認ポリシーで使用する 3 つの TACACS プロファイルを定義します。

- WLC_Monitor_Only：[モニタ（Monitor）] タブへのアクセス権を持つヘルプデスク
- WLC_Security_Access：[セキュリティ（Security）] タブと [コマンド（Commands）] タブへのアクセス権を持つセキュリティ オペレータ
- WLC_Admin：フル アクセス権を持つ管理者

WLC は role1、role2 などとして定義する必要がある TACACS+ カスタム属性を使用します。使用可能なロールは、MONITOR、WLAN、CONTROLLER、WIRELESS、SECURITY、MANAGEMENT、COMMAND、ALL、および LOBBY です。最初の 7 つは、WLC 管理 Web UI のメニュー オプションに対応します。1 つ以上のロールを入力し、特定の機能への読み取り/書き込みアクセスを許可し、残りの機能には読み取り専用のアクセスを許可することができます。

WLAN、SECURITY、CONTROLLER への読み取り/書き込みアクセスを付与するには、次のテキストを入力します。

```
role1=WLAN
role2=SECURITY
role3=CONTROLLER
```

ステップ 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。**WLC_Monitor_Only** という新しい TACACS プロファイルを追加します。[カスタム属性（Custom Attributes）] セクションまで下にスクロールし、MONITOR のみへのアクセスを定義します。

図 10. WLC_Monitor_Only 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。

ステップ 2 **WLC_Security_Access** という別のプロファイルを追加し、SECURITY と COMMANDS へのアクセスを提供します。

図 11. WLC_Security_Access 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。

ステップ 3 属性として role1=ALL を持つ、すべてのタブにアクセスできる **WLC_Admin** という 3 番目のプロファイルを追加します。

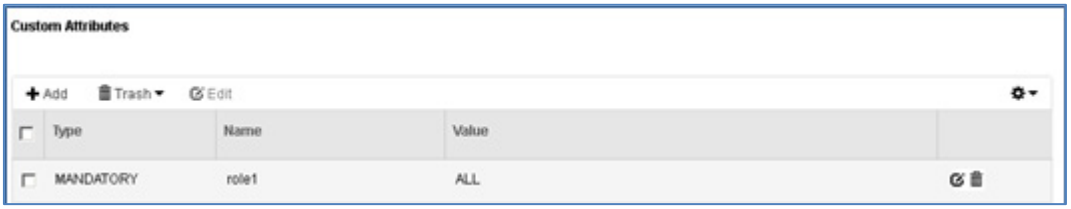

図 12. WLC_Admin の TACACS プロファイル

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。

ステップ 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。**WirelessLanControllers** という条件付きの新しいポリシー セットを追加します。

DEVICE:Device Type EQUALS Device Type#All Device Types#Network Device#Wireless Devices

図 13. ポリシー セットの条件

ステップ 2 承認ポリシーを作成します。認証では、ID ストアとして Active Directory を使用します。

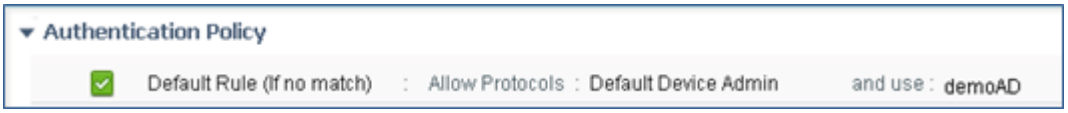

図 14. 認証ポリシー（Authentication policy）

ステップ 3 承認ポリシーを定義します。ここでは、Active Directory 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、Active Directory グループ West Coast のユーザは West Coast にあるデバイスだけにアクセスでき、Active Directory グループ East Coast のユーザは East Coast にあるデバイスだけにアクセスできます。

S	ルール名	条件	シェル プロファイル
✓	WLC HelpDesk West	demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/HelpDesk AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast AND DEVICE:Location CONTAINS All Locations#West_Coast	WLC_Monitor_Only
✓	WLC HelpDesk East	demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/HelpDesk AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/East_Coast AND DEVICE:Location CONTAINS All Locations#East_Coast	WLC_Monitor_Only

S	ルール名	条件	シェル プロファイル
✓	WLC Security West	demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Security_Operators AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast AND DEVICE:Location CONTAINS All Locations#West_Coast	WLC_Security_Access
✓	WLC Security East	demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Security_Operators AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/East_Coast AND DEVICE:Location CONTAINS All Locations#East_Coast	WLC_Security_Access
✓	WLC Admin E and W	demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Network_Operators AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast	WLC_Admin
✓	WLC Admin West	demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Network_Operators AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast AND DEVICE:Location CONTAINS All Locations#West_Coast	WLC_Admin
✓	WLC Admin East	demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Network_Operators AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/East_Coast AND DEVICE:Location CONTAINS All Locations#East_Coast	WLC_Admin
✓	デフォルト	DenyAllCommands	

図 15. 許可ポリシー

これで、WLC のデバイス管理の ISE 設定が完了しました。

WLC の TACACS+ の設定

WLC コントローラで TACACS+ を設定するには、次の手順を実行する必要があります。

1. TACACS+ 認証サーバの追加
2. TACACS+ 許可サーバの追加
3. TACACS+ アカウンティング サーバの追加
4. 管理ユーザ認証の優先順位の設定

TACACS+ 認証サーバの追加

TACACS+ 認証サーバを追加するには、次の手順を実行します。

ステップ 1 WLC GUI から、[セキュリティ(Security)] > [AAA] > [TACACS+] > [認証(Authentication)] に移動し、[新規(New…)] をクリックします。

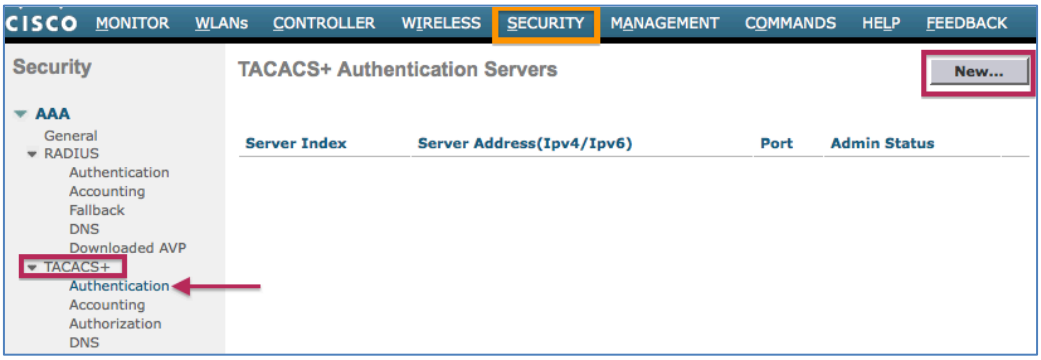

図 16. TACACS+ 認証サーバ

ステップ 2 TACACS+ サーバとして ISE サーバの IP アドレスと、共有秘密キーを入力します。

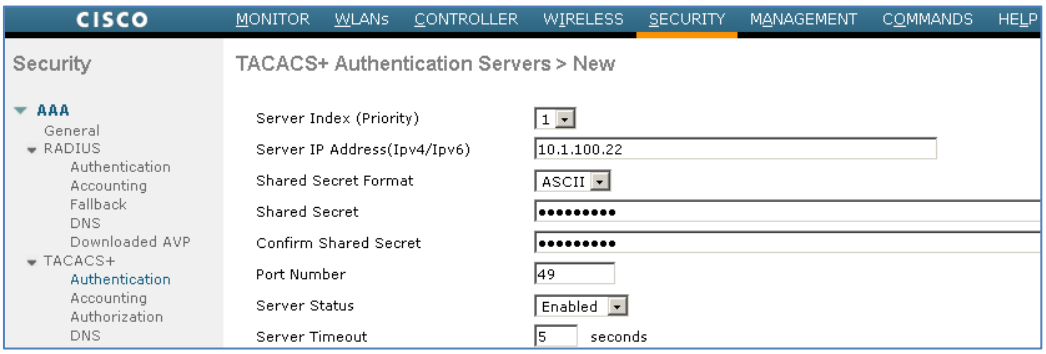

図 17. TACACS+ 認証サーバの追加

ステップ 3 [適用(Apply)] をクリックします。

TACACS+ 許可サーバの追加

TACACS+ 許可サーバを追加するには、次の手順を実行します。

ステップ 1 WLC GUI から、[セキュリティ(Security)] > [AAA] > [TACACS+] > [認証(Authorization)] に移動し、[新規(New…)] をクリックします。

ステップ 2 サーバ IP アドレスとして ISE サーバの IP アドレスと、共有秘密キーを追加します。

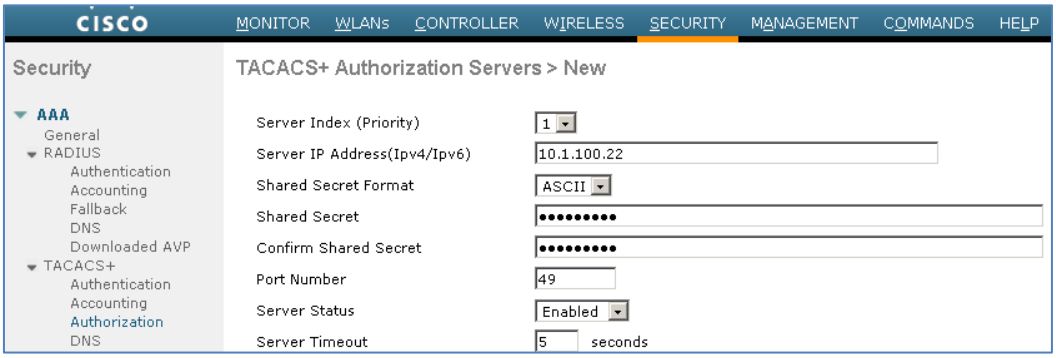

図 18. TACACS+ 許可サーバの追加

ステップ 3 [適用(Apply)] をクリックします。

TACACS+ アカウンティング サーバの追加

TACACS+ アカウンティング サーバを追加するには、次の手順を実行します。

ステップ 1 WLC GUI から、[セキュリティ(Security)] > [AAA] > [TACACS+] > [アカウンティング(Accounting)] に移動し、[新規(New…)] をクリックします。

ステップ 2 サーバ IP アドレスとして ISE サーバの IP アドレスと、共有秘密キーを入力します。

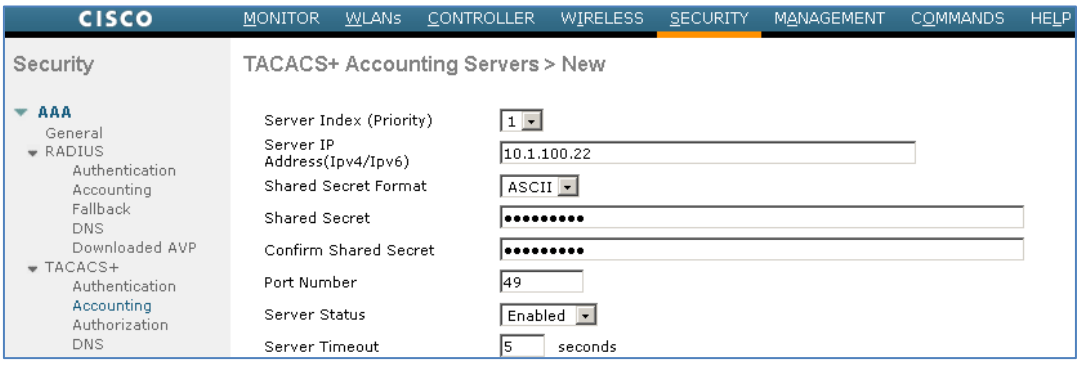

図 19. TACACS+ アカウンティング サーバの追加

ステップ 3 [適用(Apply)] をクリックします。

管理ユーザ認証の優先順位の設定

この手順では、管理ユーザ認証の優先順位を設定する方法を説明します。デフォルトのコントローラ設定は、*ローカルおよびRADIUS* です。TACACS+ では、認証の順序は **TACACS+ およびローカル**、または**ローカルおよび TACACS+** にすることができます。

ステップ 1　GUI から、[セキュリティ（Security）] > [優先順位（Priority Order）] > [管理ユーザ（Management User）] に移動します。矢印、[上（Up）]、および [下（Down）] ボタンを使用して、認証を TACACS+ に LOCAL が続くように選択して並べ替えます。

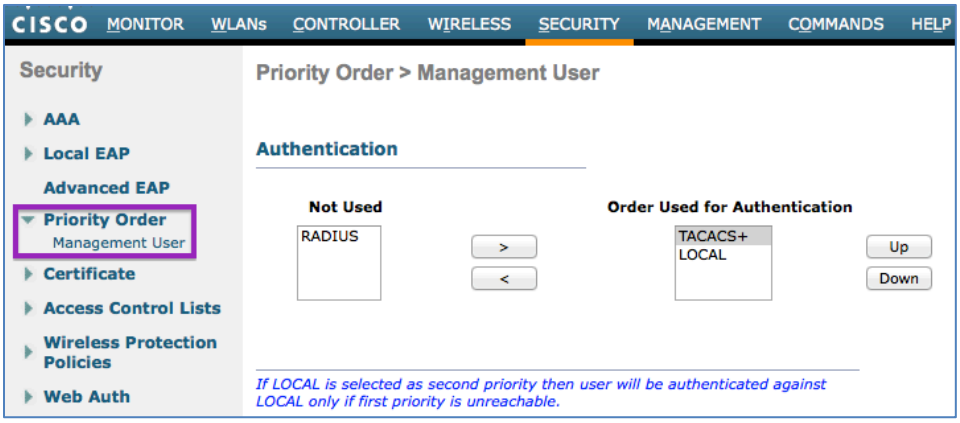

図 20. 認証の順序の設定

ステップ 2　[適用（Apply）] をクリックします。

WLC の TACACS+ の設定が完了しました。

次のステップ

この時点で、WLC のデバイス管理に必要なすべての設定は完了です。設定を確認する必要があります。

ステップ 1 異なるグループに属し、異なるデバイスにアクセスするさまざまなユーザとして WLC にログインします。

ステップ 2 ログインしたら、ユーザが適切なタブにアクセスできることを確認します。

ステップ 3 ヘルプデスク ユーザであるユーザの場合、さまざまなタブに移動し、追加/変更/削除を試します。たとえば、[WLAN(WLANs)] に移動し、WLAN の 1 つの削除を試みます。このユーザには MONITOR アクセスしかないため、次のエラーにより操作は拒否されます。

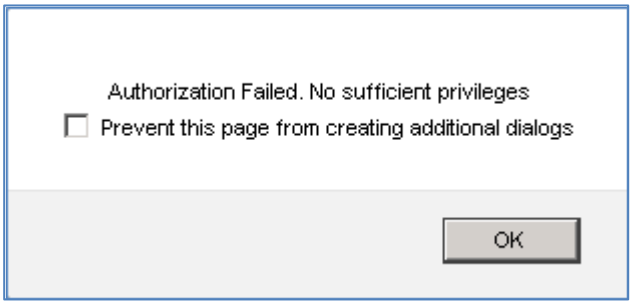

図 21. WLC の認証失敗によるエラー メッセージ

ステップ 4 ISE GUI から、[運用(Operations)] > [TACACS Livelog] 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。

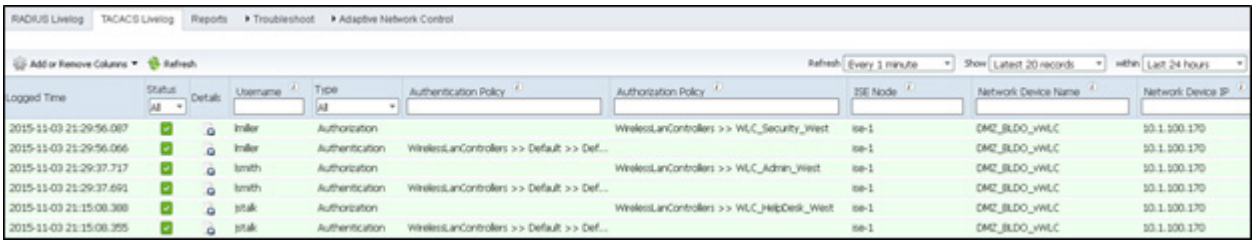

図 22. TACACS Livelog

ステップ 5 履歴レポートを確認する場合は、ISE で、[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)] 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。