# TACACS+を使用したCisco WLCのデバイス管理

## 内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[コンフィギュレーション](#)
[ステップ1:[Device Administration License]を確認します。](#)
[ステップ2:ISE PSNノードでデバイス管理を有効にします。](#)
[ステップ3：ネットワークデバイスグループを作成します。](#)
[手順4：ネットワークデバイスとしてWLCを追加します。](#)
[手順5:WLCのTACACSプロファイルを作成します。](#)
[ステップ6：ポリシーセットを作成します。](#)
[ステップ7：認証および許可ポリシーを作成します。](#)
[手順8：デバイス管理用のWLCの設定](#)
[確認](#)
[トラブルシュート](#)

## 概要

このドキュメントでは、Identity Service Engine(ISE)を使用してCisco Wireless LAN Controller(WLC)のデバイス管理用にTACACS+を設定する方法について説明します。

## 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。

- Identity Service Engine(ISE)の基礎知識
- Cisco Wireless LAN Controller(WLC)に関する基礎知識

### 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。

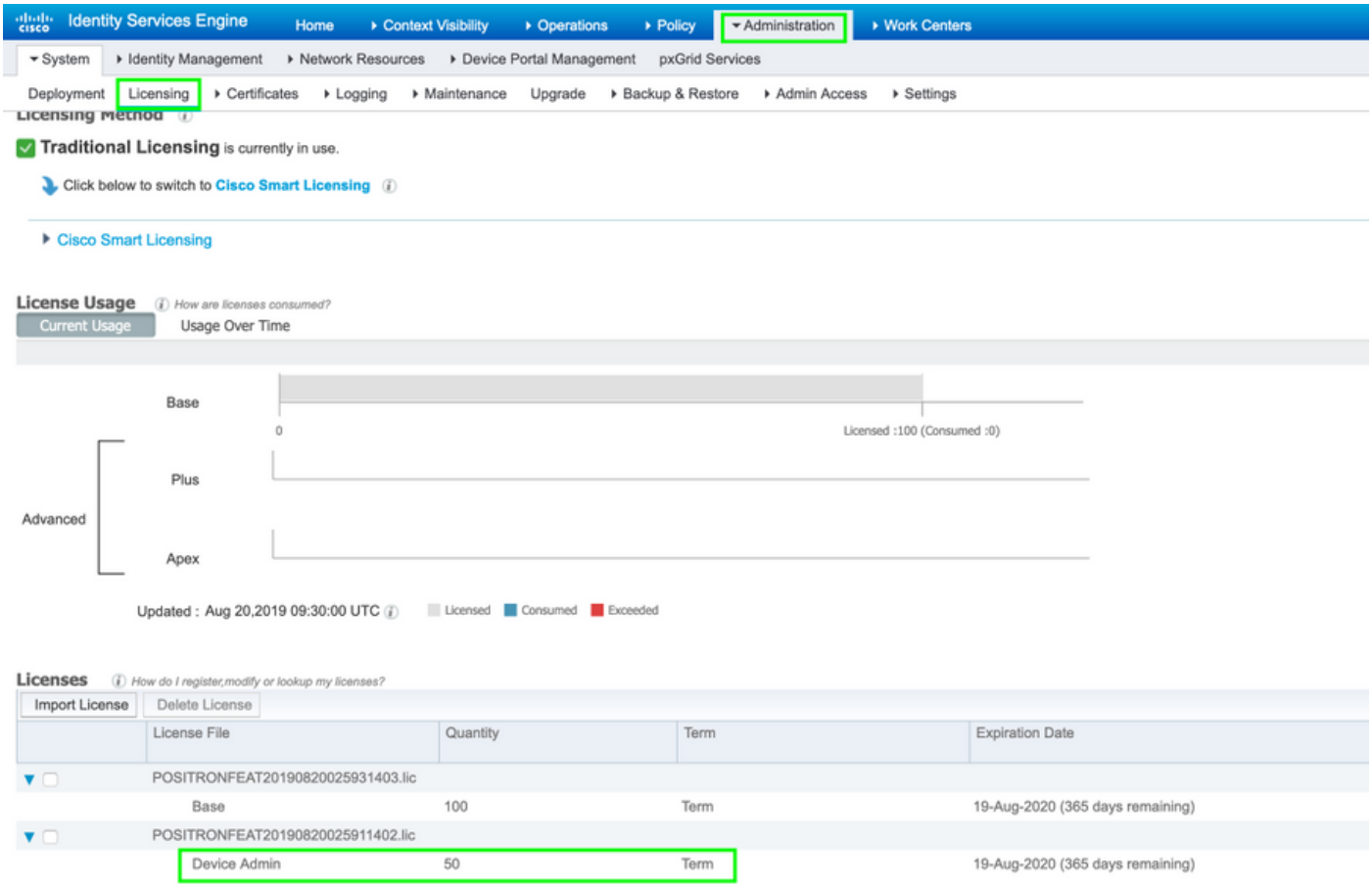
- Cisco Identity Service Engine 2.4
- Cisco Wireless LAN Controller 8.5.135

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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

# コンフィギュレーション

## ステップ1:[Device Administration License]を確認します。

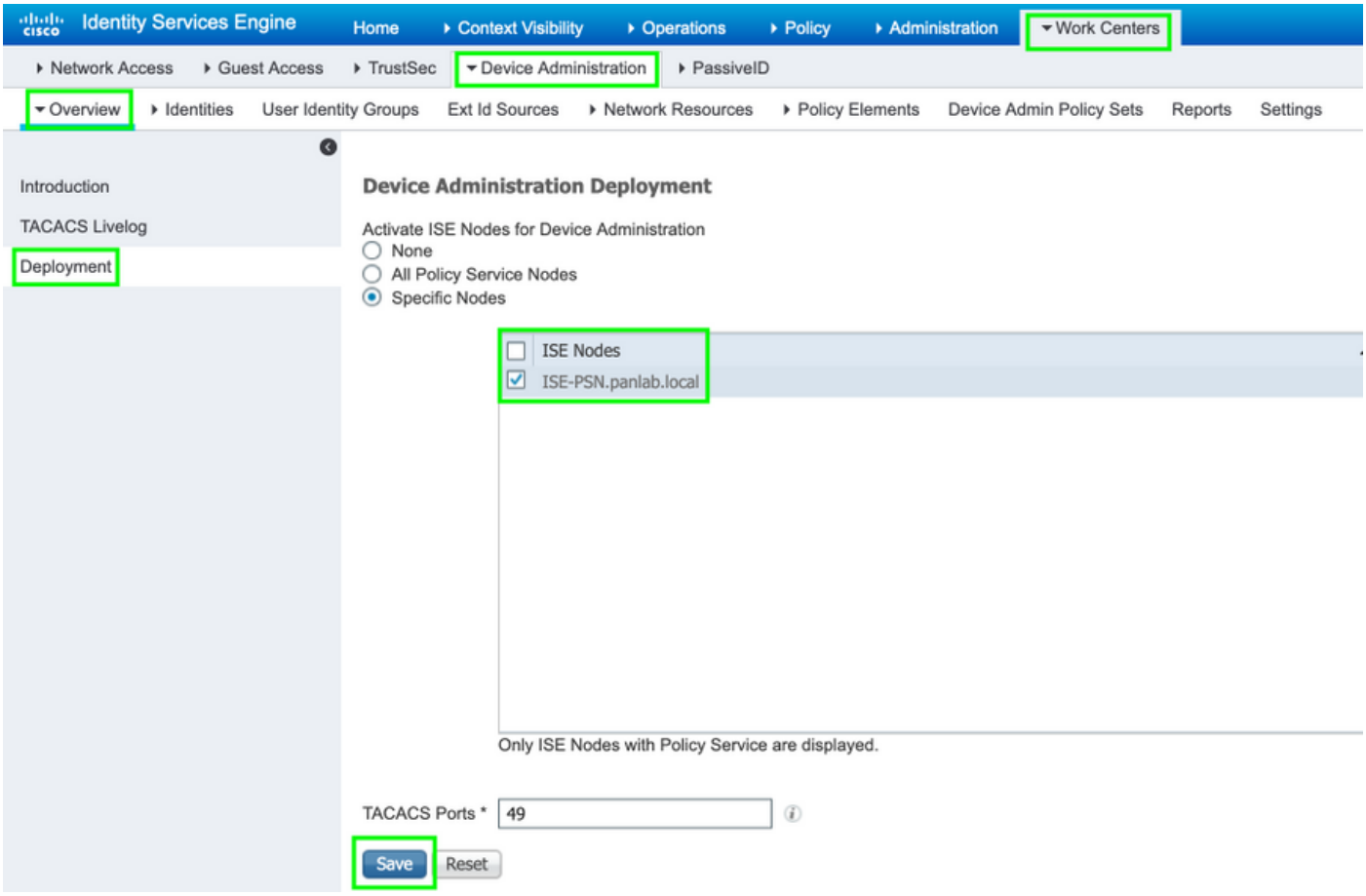
図に示すように、[Administration] > [System] > [Licensing]タブに移動し、[Device Admin]ライセンスがインストールされていることを確認します。




**注**：ISEでTACACS+機能を使用するには、デバイス管理ライセンスが必要です。

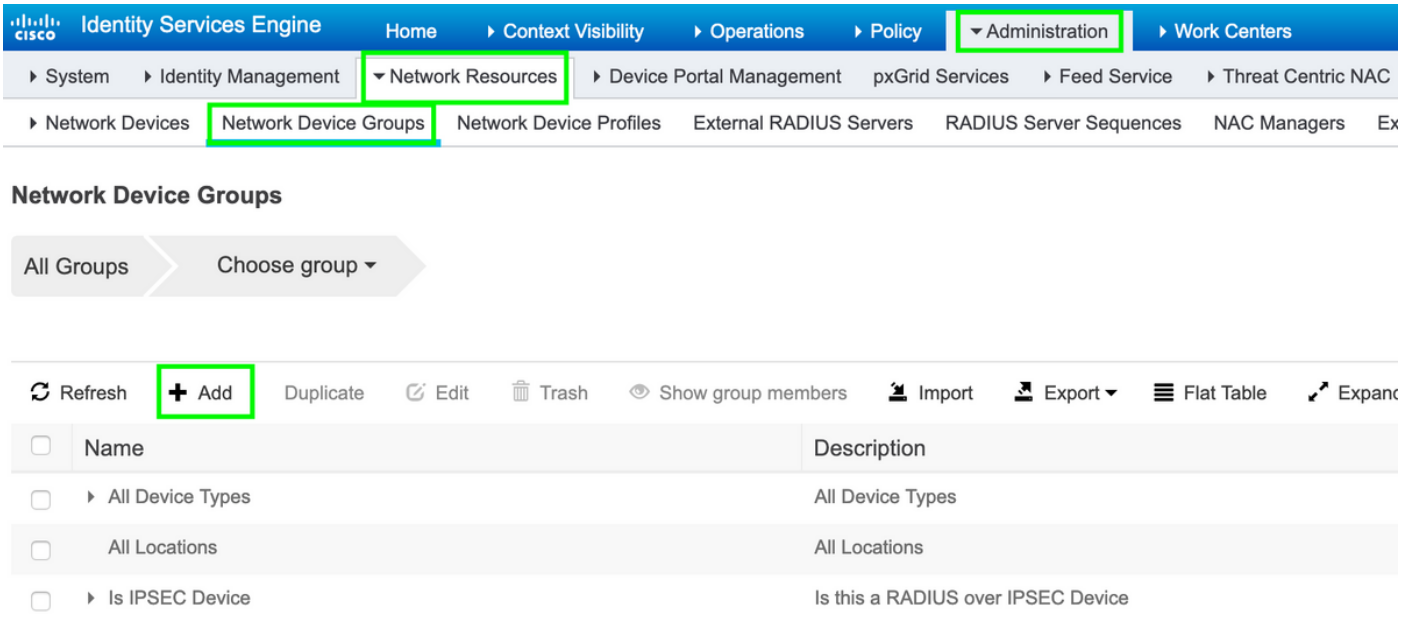
## ステップ2:ISE PSNノードでデバイス管理を有効にします。

[Work Centers] > [Device Administration] > [Overview]に移動し、[Deployment]タブをクリックし、[Select the Specific PSN Node]オプションボタンをクリックします。図に示すように、ISEノードでDevice Administrationを有効にするには、チェックボックスを選択し、[save]をクリックします。



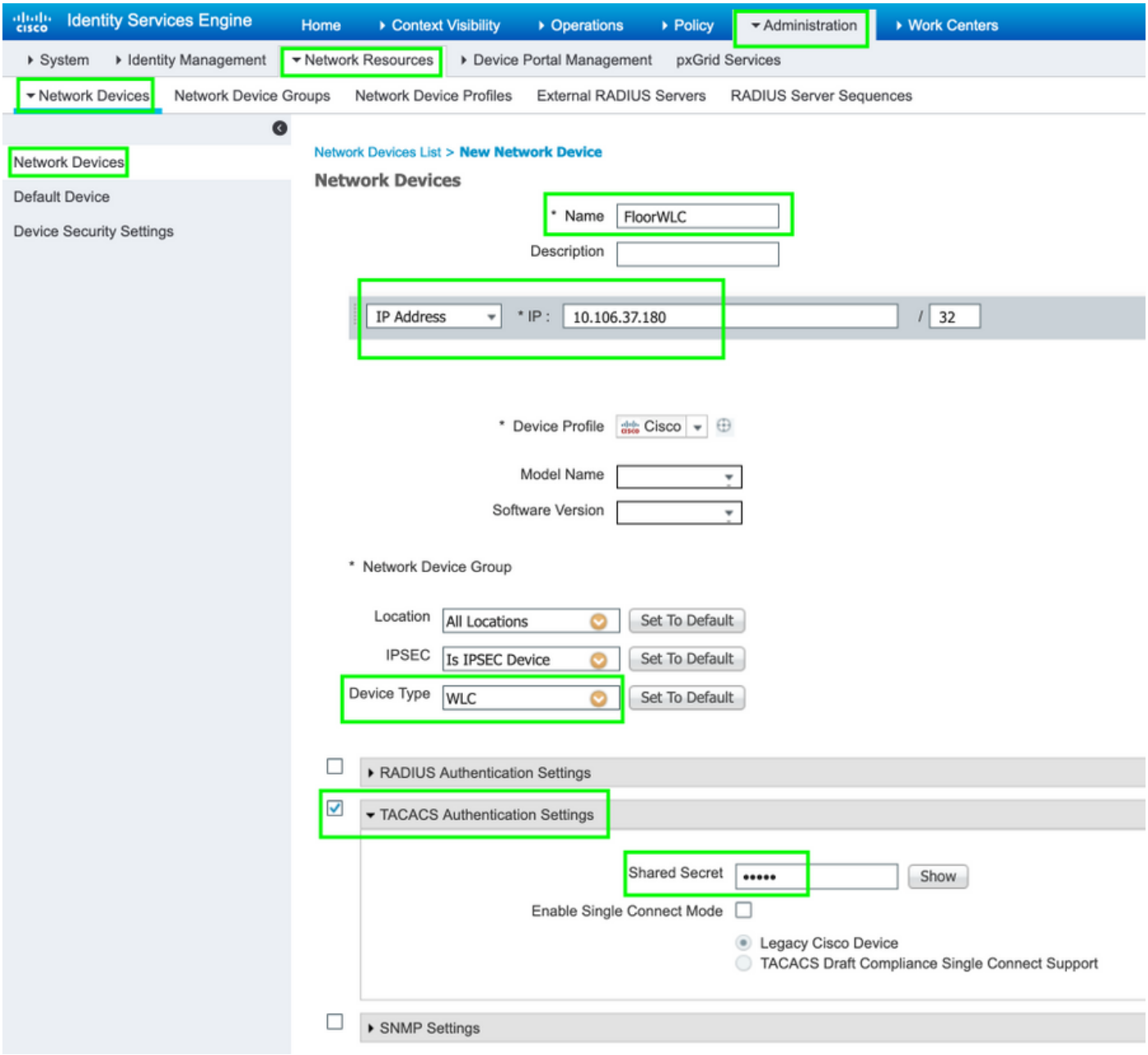

## ステップ3：ネットワークデバイスグループを作成します。

WLCをISE上のネットワークデバイスとして追加するには、次の図に示すように、**[Administration] > [Network Resources] > [Network Device Groups] > [All Device Types]に移動して、WLCの新しいグループを作成します。**



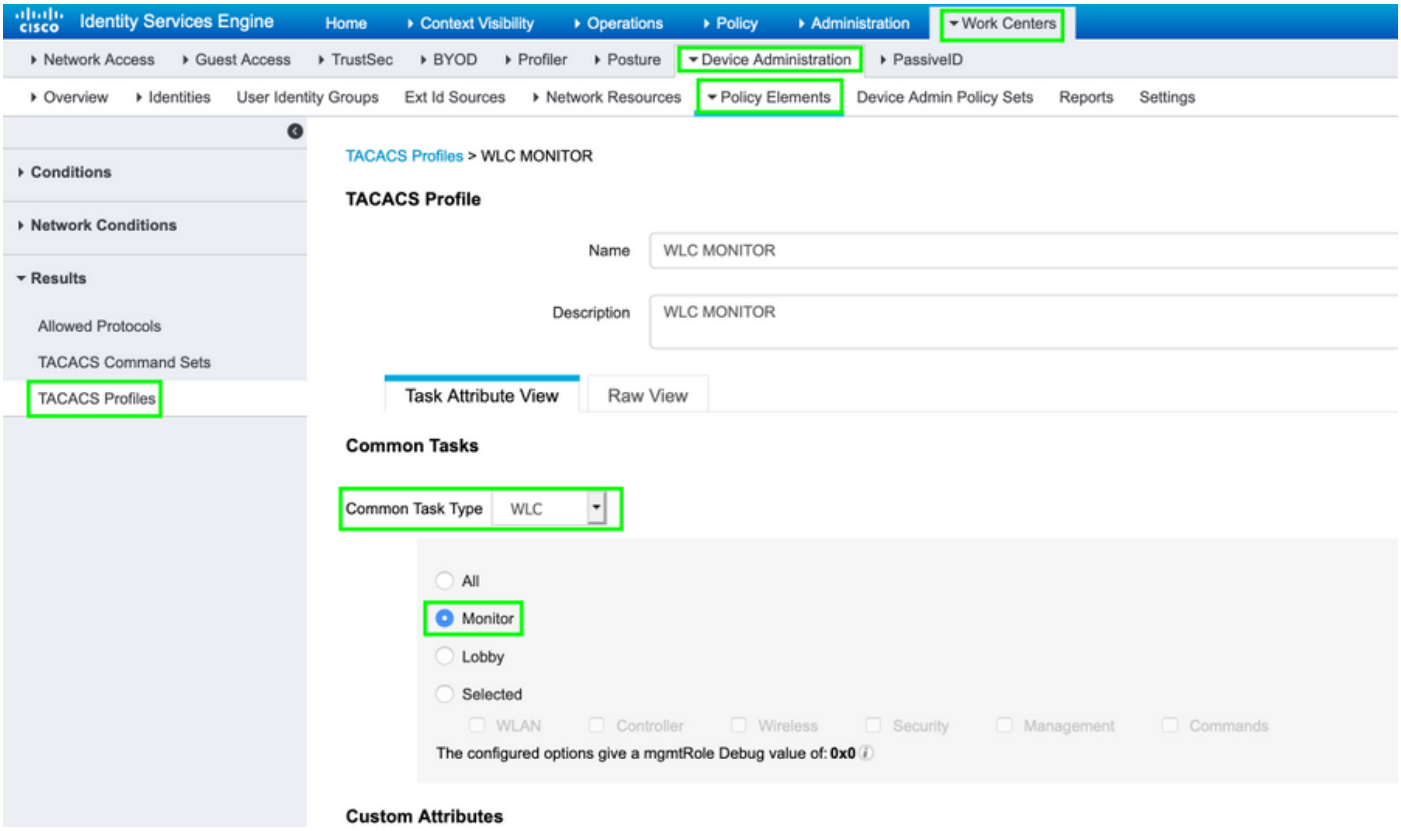

### 手順4：ネットワークデバイスとしてWLCを追加します。

[Work Centers] > [Device Administration] > [Network Resources] > [Network Devices] **に移動します。**[Add] をクリックし、[Name]、[IP Address]を指定し、[Device type]を**[WLC]**に選択し、**[TACACS+ Authentication Settings]**チェックボックスをオンにして、[Shared Secret]キーを指定します（図を参照）。

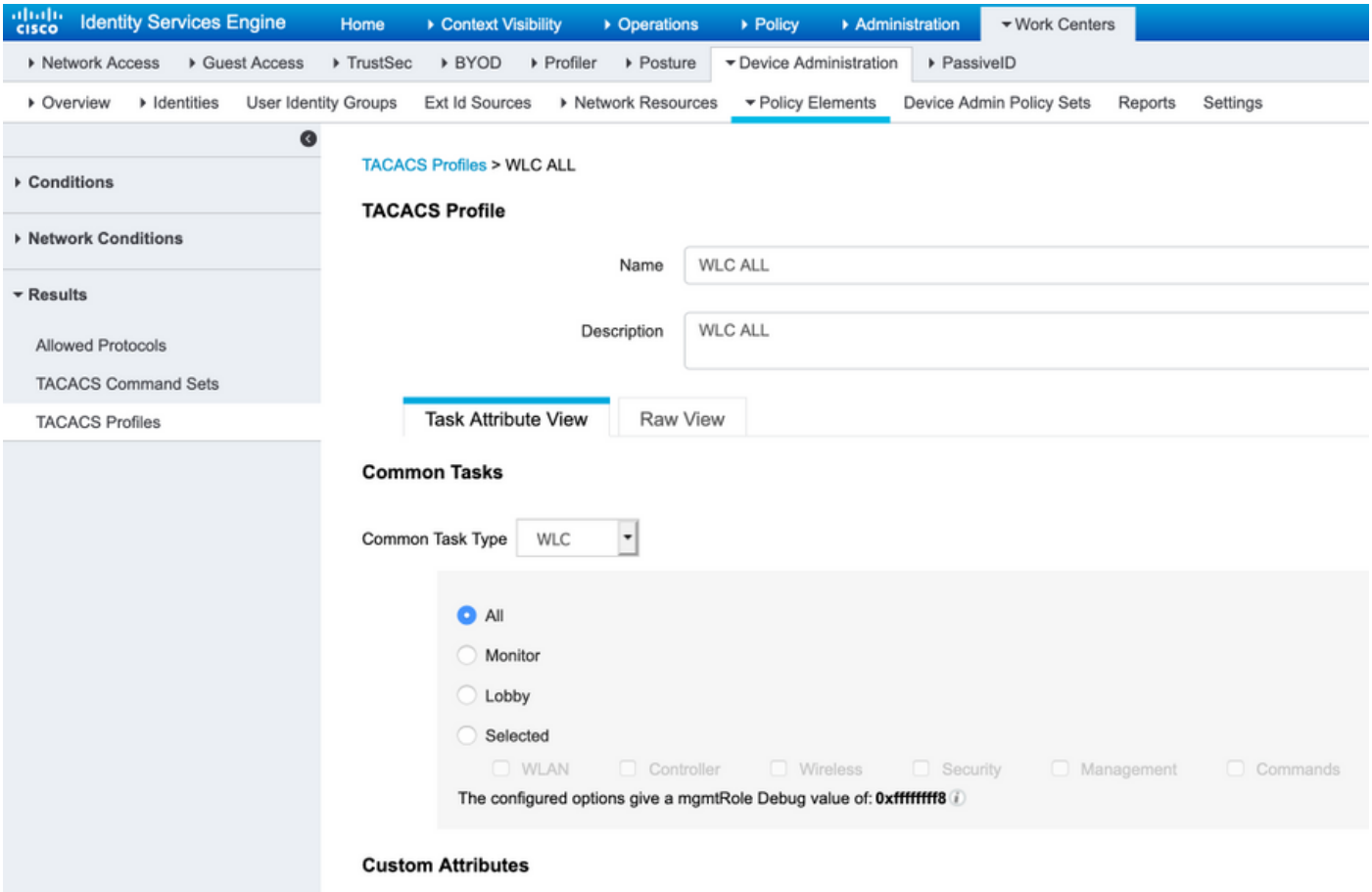



## 手順5:WLCのTACACSプロファイルを作成します。

[Work Centers] > [Device Administration] > [Policy Elements] > [Results] > [TACACS Profiles]に移動します。[Add]をクリックし、[Name]を指定します。[Task]属性ビューで、[Common Task Type]に[WLC]を選択します。図に示すように、[Monitor]を選択するデフォルトのプロファイルが存在します。

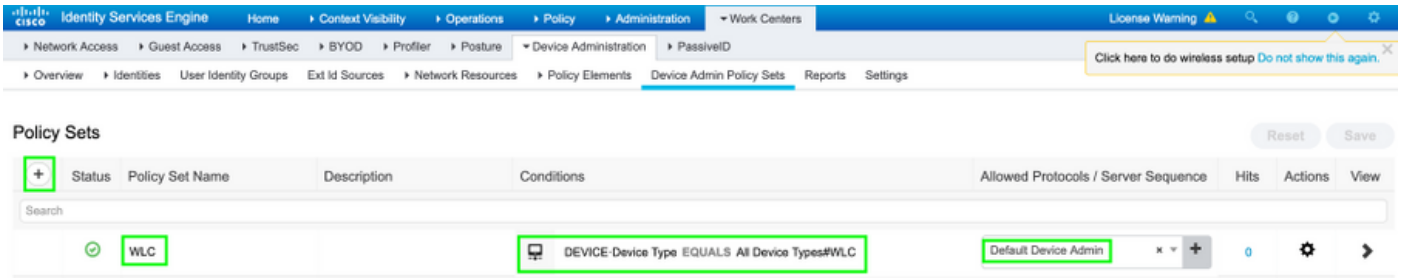



図に示すように、ユーザへのフルアクセスを**許可する**別のデフォルトプロファイル[All]があります。




## ステップ6：ポリシーセットを作成します。

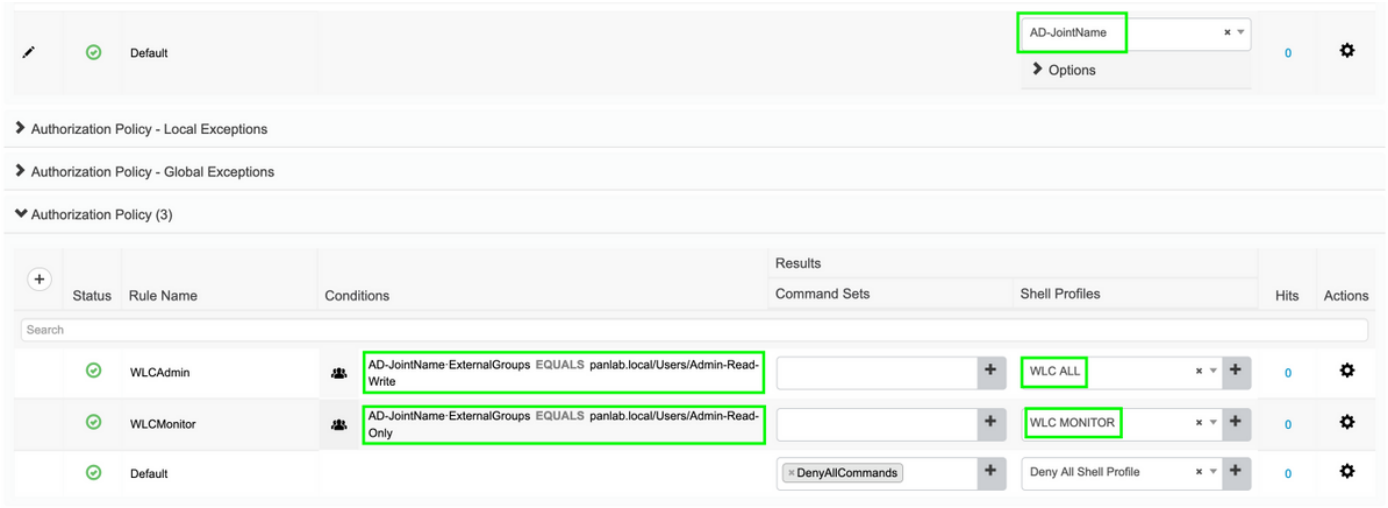
[ワークセンター] > [デバイス管理] > [デバイス管理ポリシーセット]に移動します。(+)をクリックし、ポリシーセットに名前を付けます。ポリシー条件で、[Device Type]に[WLC]を選択します。図に示すように、[Allowed protocols]は[Default Device Admin]にすることができます。




## ステップ7：認証および許可ポリシーを作成します。

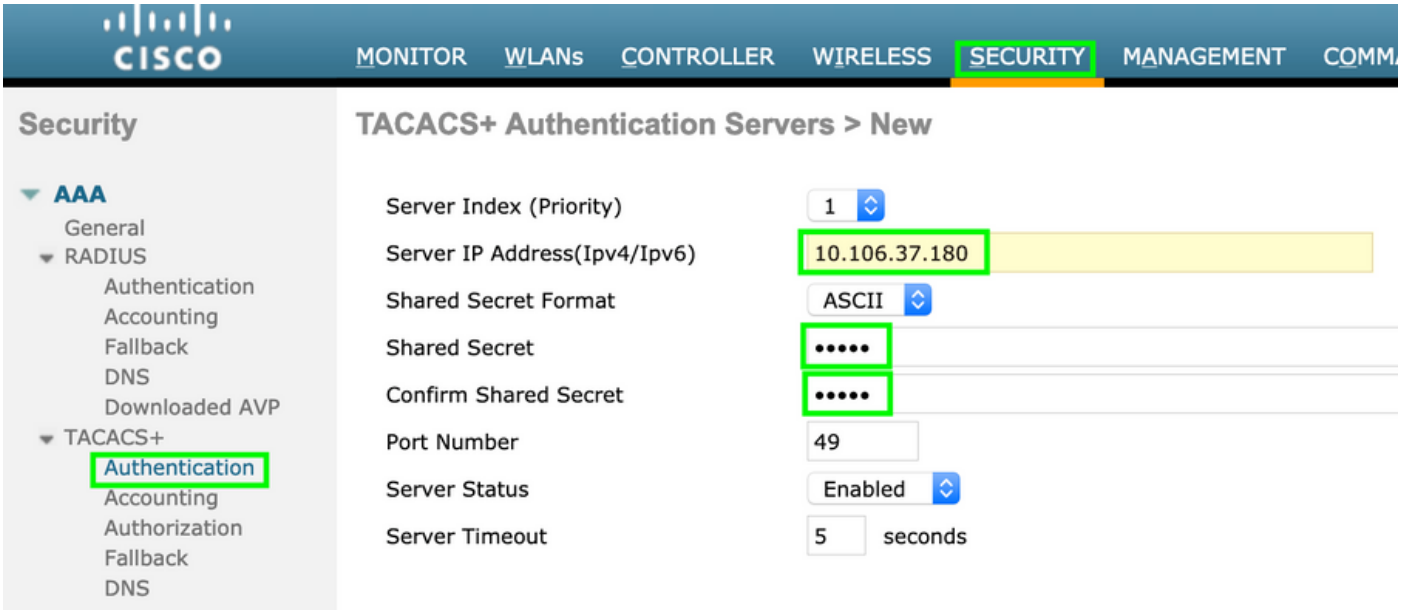
このドキュメントでは、2つのサンプルグループAdmin-Read-WriteとAdmin-Read-OnlyがActive Directoryに設定され、各グループadmin1、admin2にそれぞれ1人のユーザが設定されています。Active Directoryは、AD-JointNameという名前のジョイントポイントを介してISEと統合されています。

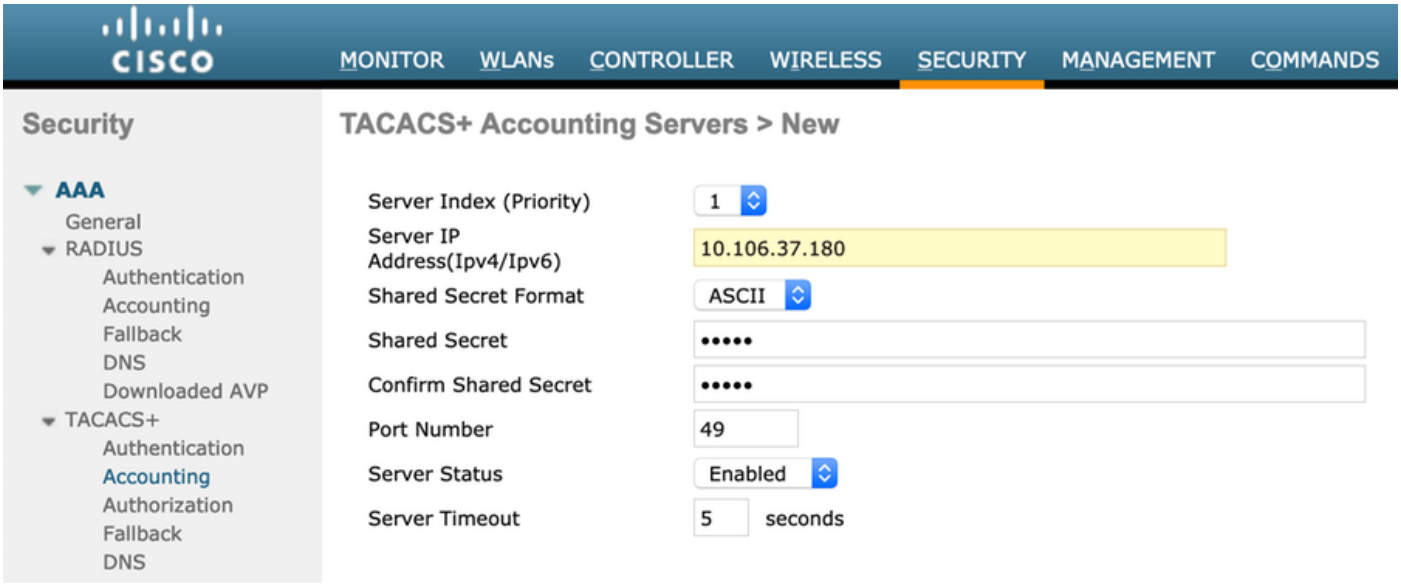
図に示すように、2つの認可ポリシーを作成します。



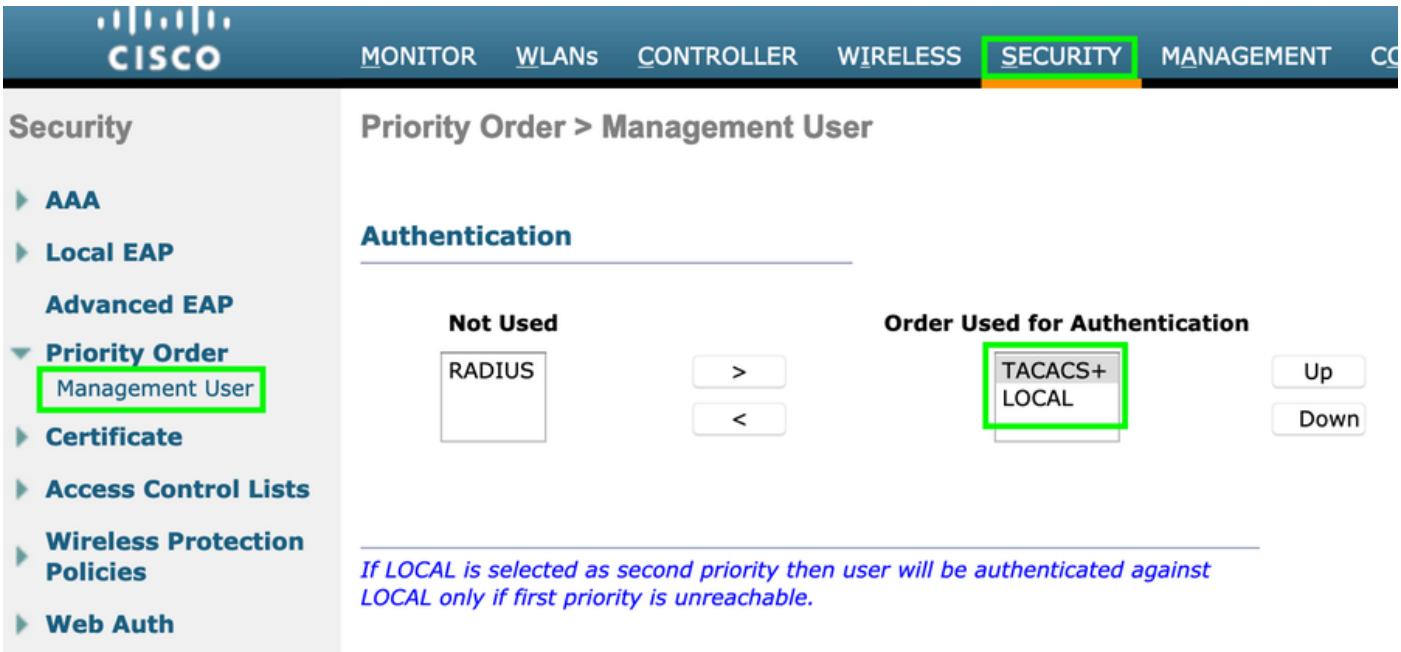

## 手順8：デバイス管理用のWLCの設定

図に示すように、[Security] > [AAA] > [TACACS+]に移動し、[New]をクリックして、認証、アカウンティングサーバを追加します。



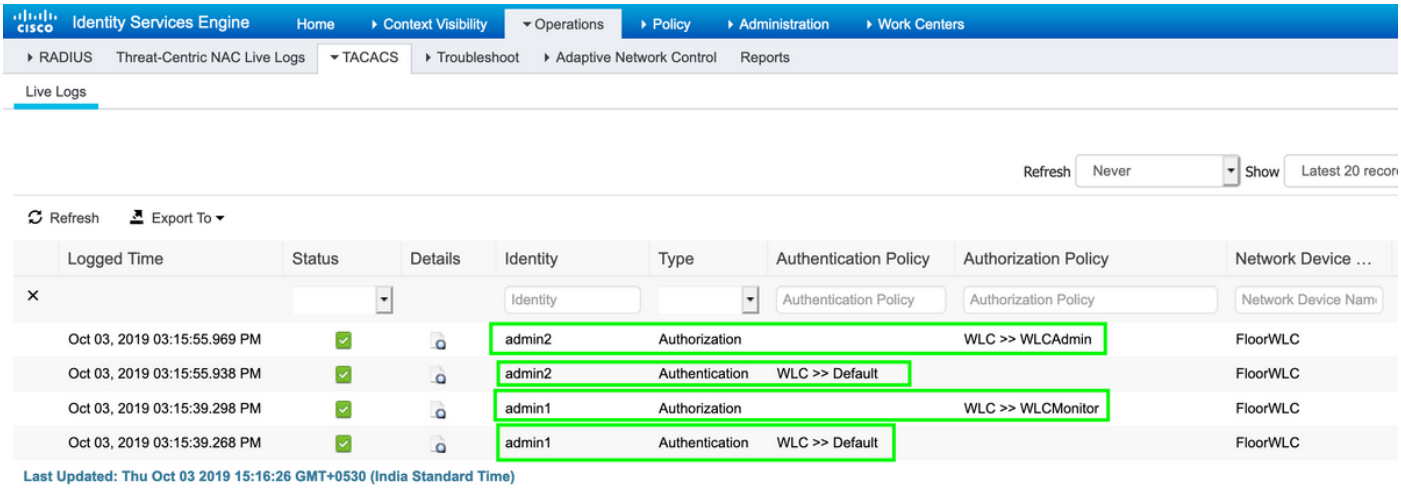

次の図に示すように、優先順位を変更し、TACACS+を上、ローカルを下にします。



**注意**：現在のWLC GUIセッションを閉じないでください。異なるWebブラウザでWLC GUIを開き、TACACS+クレデンシャルを使用したログインが機能するかどうかを確認することをお勧めします。そうでない場合は、TCPポート49のISEノードの設定と接続を確認します。

# 確認

[Operations] > [TACACS] > [Live logs]に移動し、ライブログを監視します。図に示すように、WLC GUIを開き、Active Directoryユーザクレデンシャルでログインします




# トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。