使用TACACS+管理Cisco WLC的裝置

目錄

簡介

本檔案介紹如何使用身分識別服務引擎(ISE)為思科無線LAN控制器(WLC)的裝置管理設定TACACS+。

必要條件

需求

思科建議您瞭解以下主題：

- 身份服務引擎(ISE)基礎知識
- 思科無線LAN控制器(WLC)的基本知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

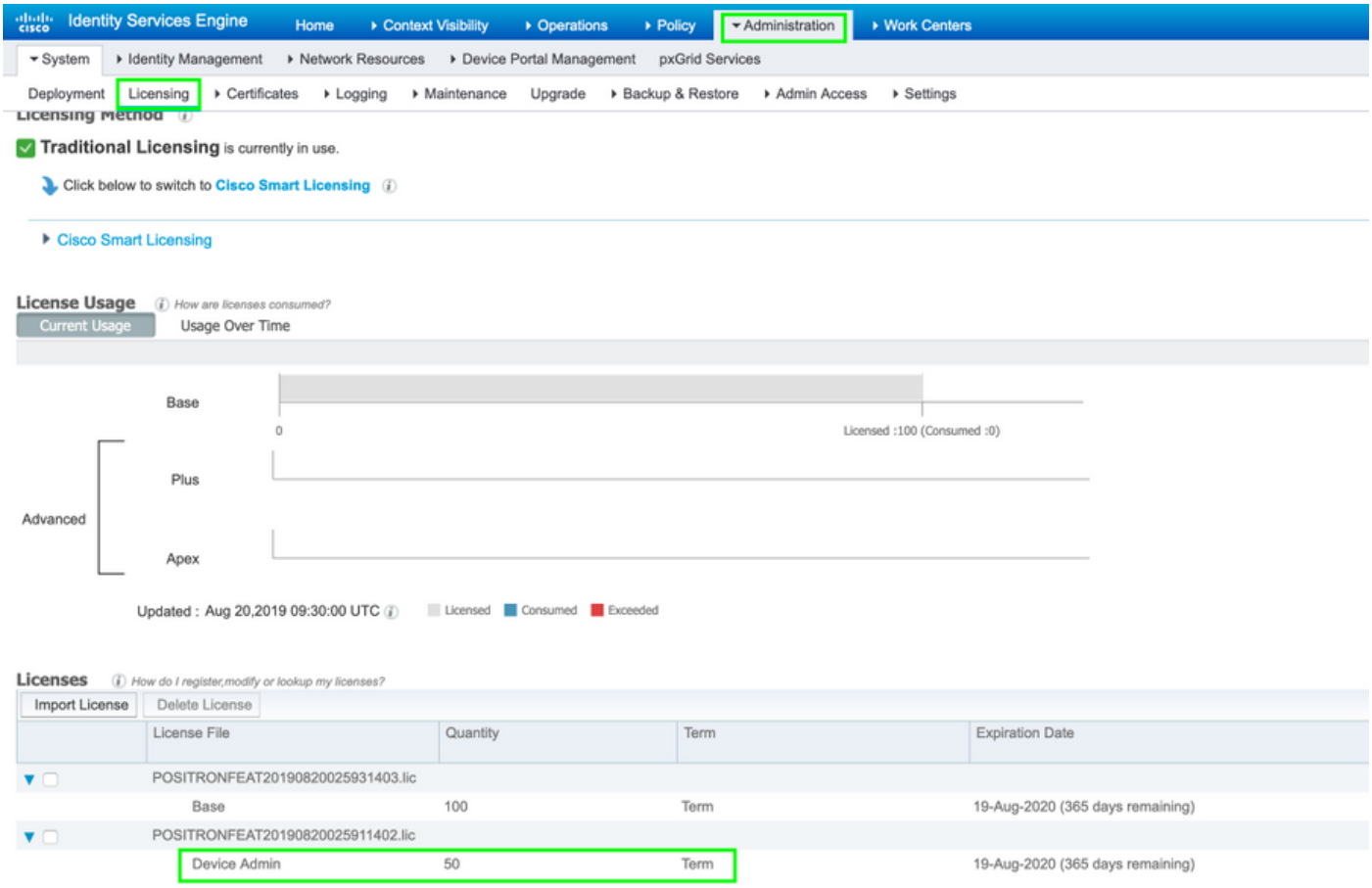
- 思科身分識別服務引擎2.4
- 思科無線LAN控制器8.5.135

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

組態

步驟1.檢查裝置管理許可證。

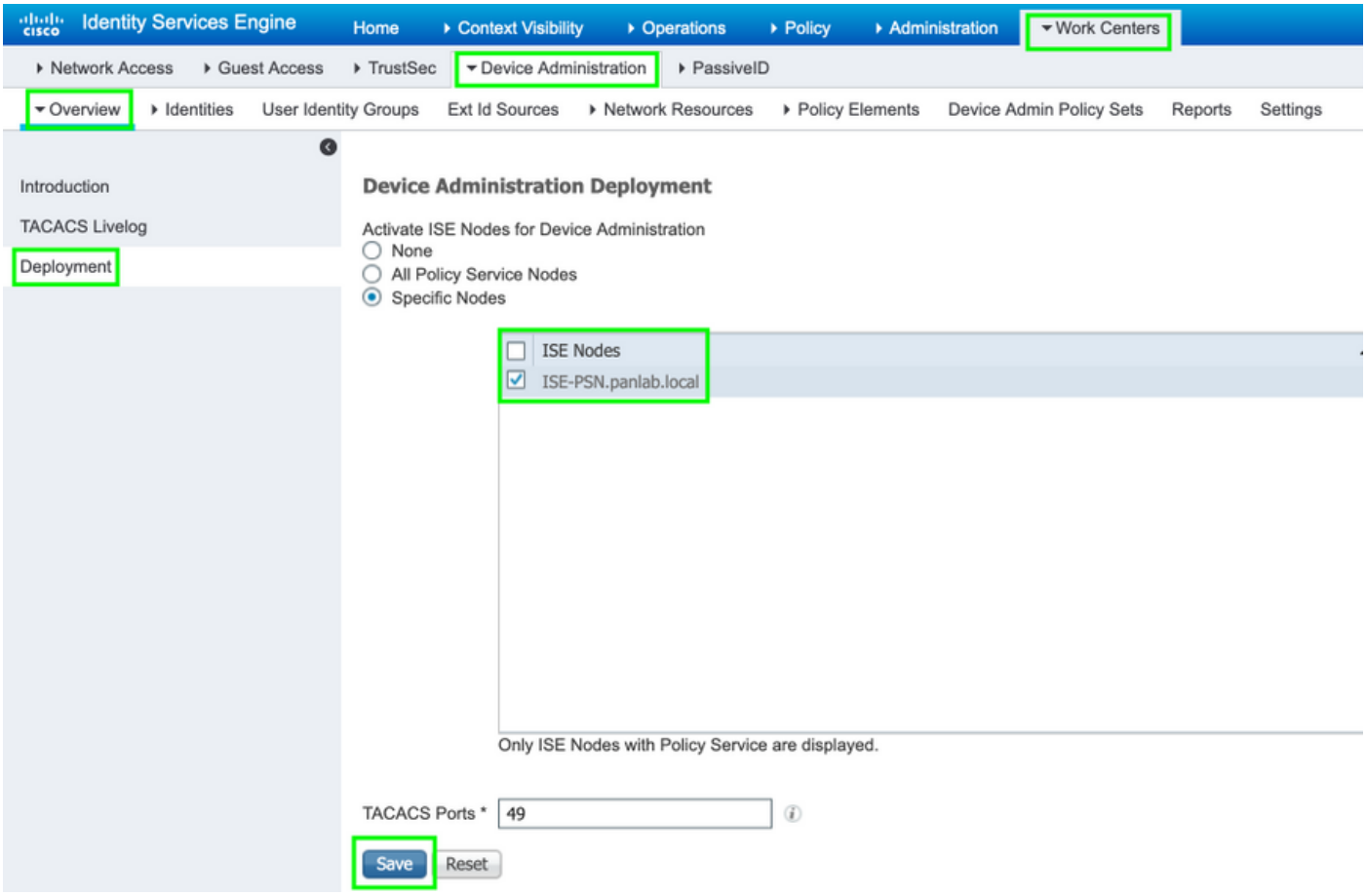
導覽至**Administration > System > Licensing**索引標籤，並驗證**Device Admin**許可證是否已安裝，如下圖所示。



附註：在ISE上使用TACACS+功能需要裝置管理員許可證。

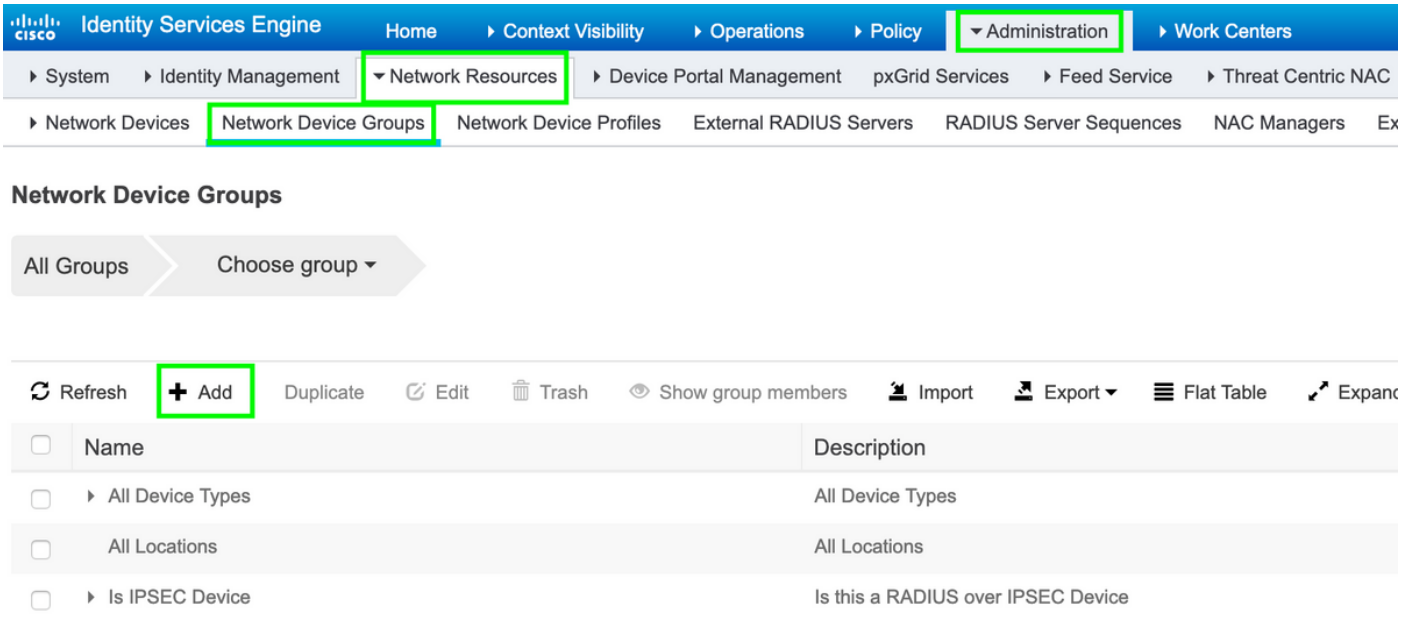
步驟2.在ISE PSN節點上啟用裝置管理。

導航到**工作中心>裝置管理>概述**，按一下**部署**頁籤，選擇**特定PSN節點。選中**覈取方塊並按一下**save，在ISE節點上啟用裝置**管理，如下圖所示：



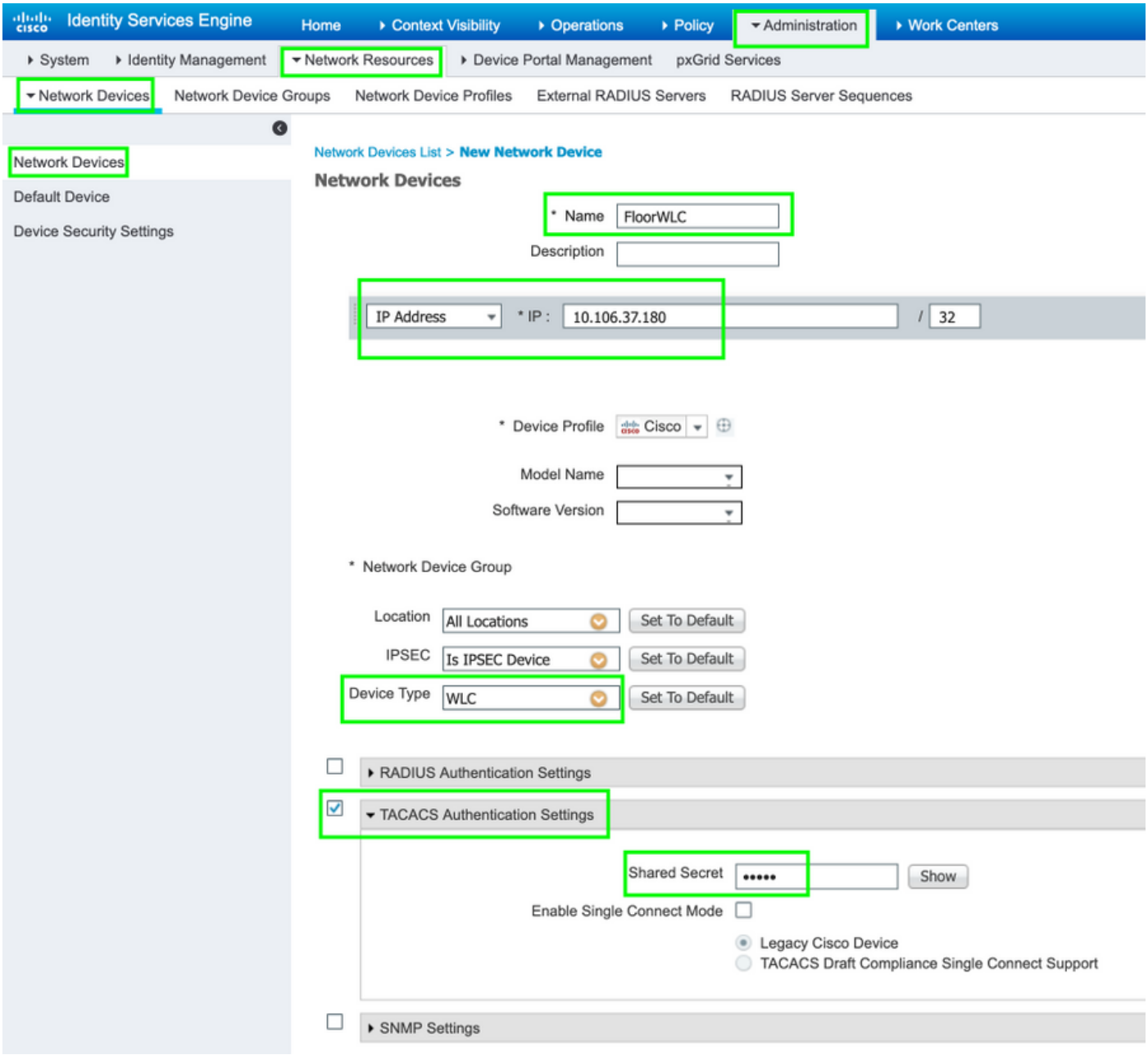
步驟3.建立網路裝置組。

若要將WLC新增為ISE上的網路裝置，請導覽至**Administration > Network Resources > Network Device Groups > All Device Types**，為WLC建立一個新**群組**，如下圖所示：



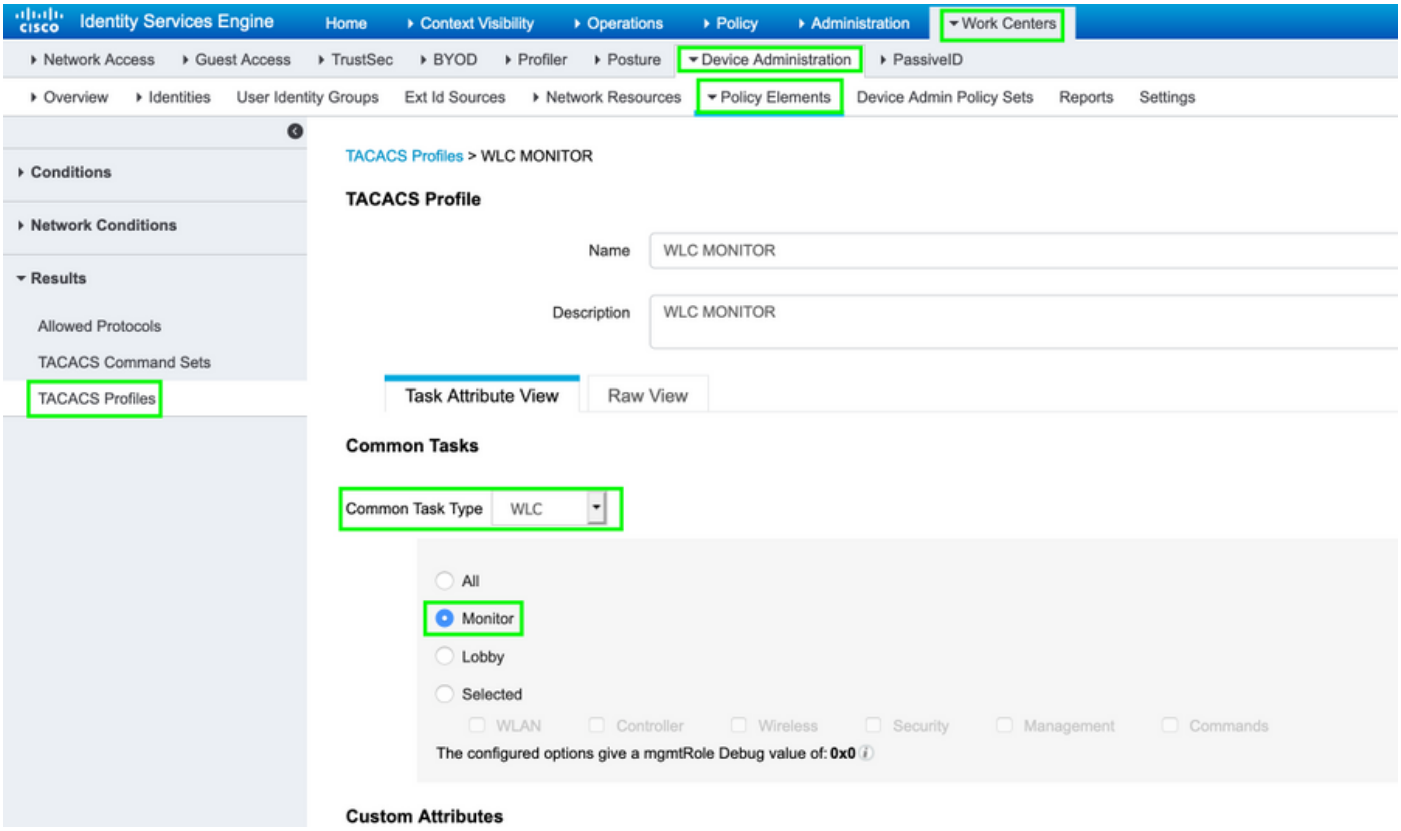
步驟4.將WLC新增為網路裝置。

導航至**工作中心>裝置管理>網路資源>網路裝置**。按一下Add，提供Name、IP Address，然後選擇Device type as **WLC**，選中**TACACS+ Authentication Settings**覈取方塊並提供Shared Secret，如下圖所示：

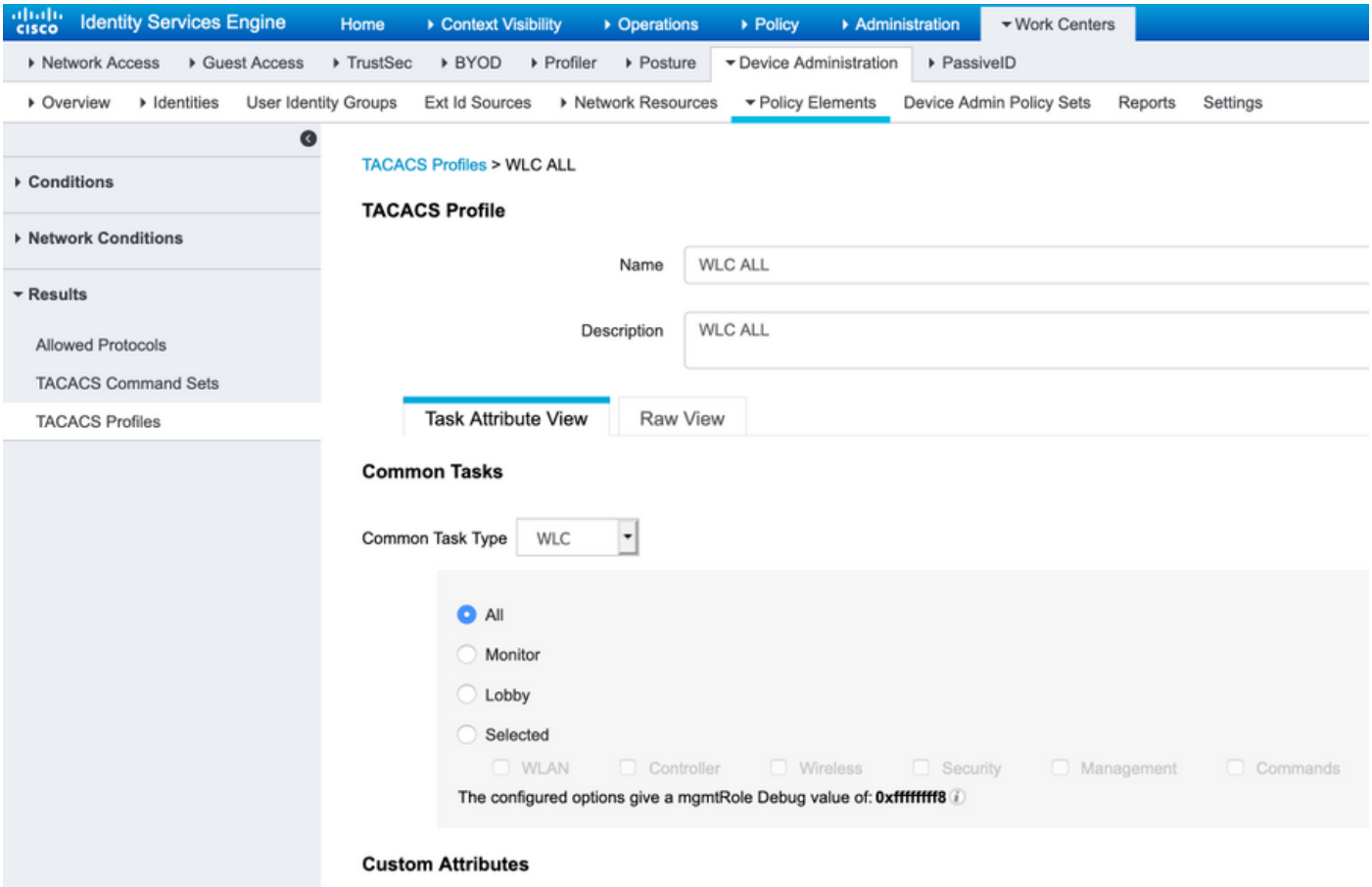


步驟5.為WLC建立TACACS設定檔。

導航到**工作中心(Work Centers)>裝置管理(Device Administration)>策略元素(Policy Elements)>結果(Results)> TACACS配置檔案(TACACS Profiles)。按一下Add並提供名稱。在任務屬性檢視**頁籤中，選擇WLC作為**通用任務型別**。存在預設配置檔案，可從中選擇Monitor以允許使用者有限訪問，如下圖所示。

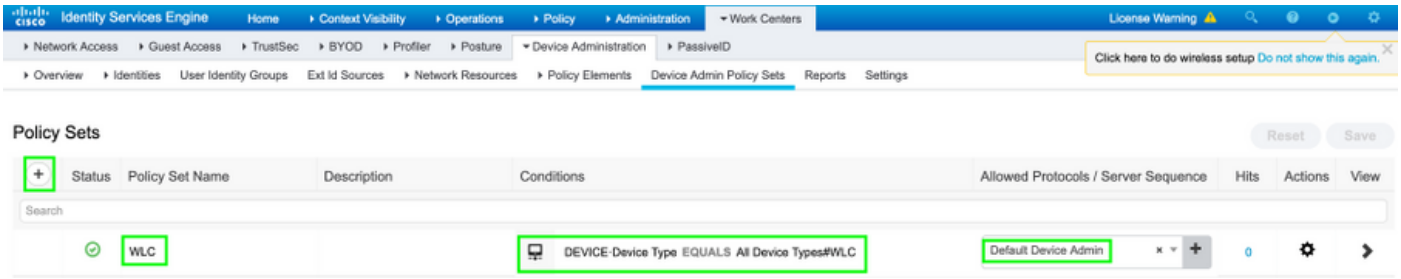


還有另一個預設配置檔案All，它允許對使用者進行完全訪問，如下圖所示。



步驟6.建立策略集。

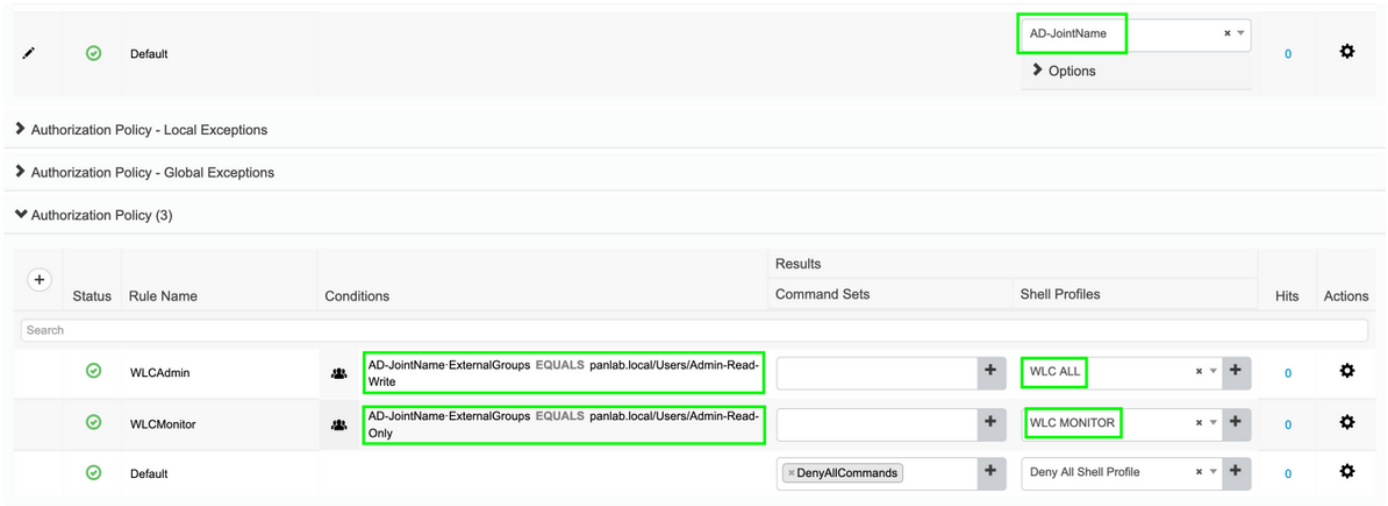
導航到**工作中心>裝置管理>裝置管理策略集。**按一下**(+)**，然後為策略集指定一個名稱。在策略條件中選擇**Device Type** as WLC，Allowed protocols可以是**Default Device Admin**，如下圖所示。



步驟7.建立身份驗證和授權策略。

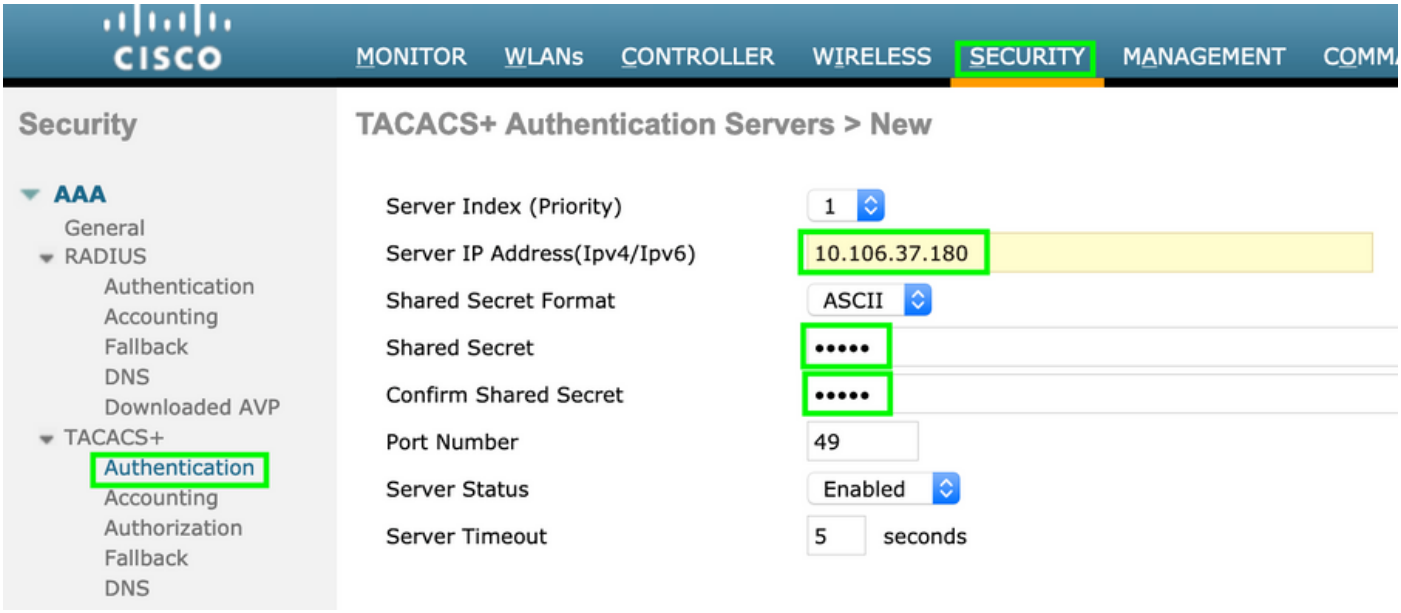
本文檔中，在Active Directory上分別配置兩個示例組**Admin-Read-Write**和**Admin-Read-Only**，並在每個組**admin1**和**admin-Read-Only**中分別配置一個使用者。Active Directory通過名為**AD-JointName**的連線點與ISE整合。

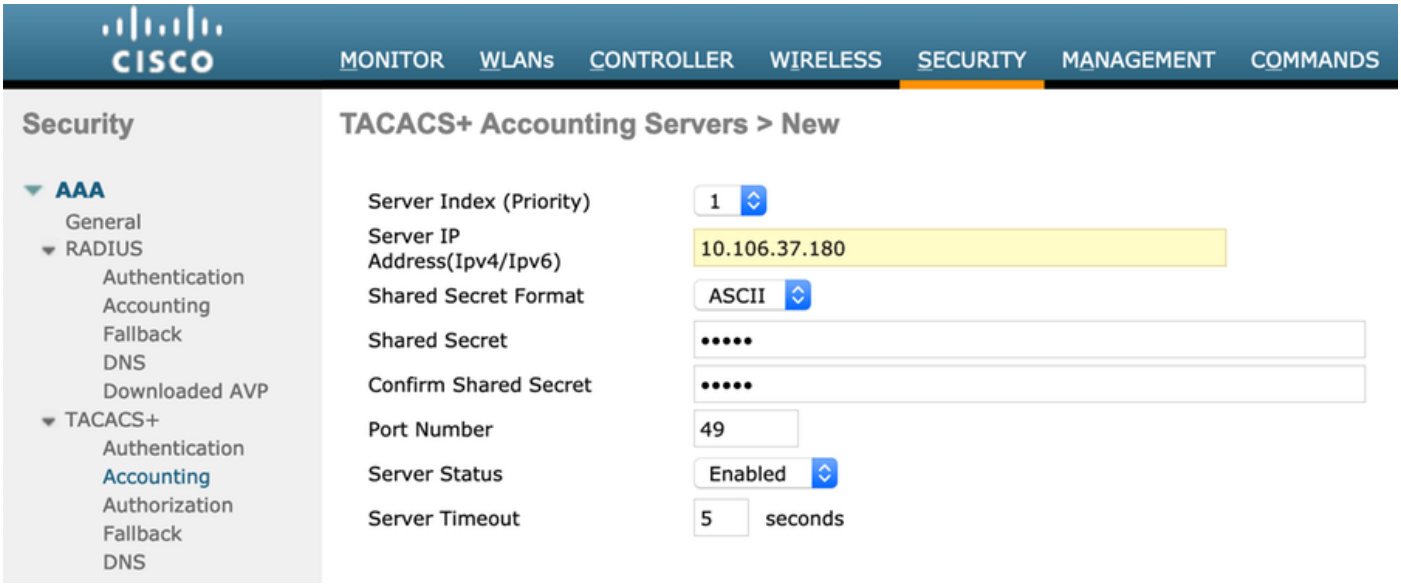
建立兩個授權策略，如下圖所示：



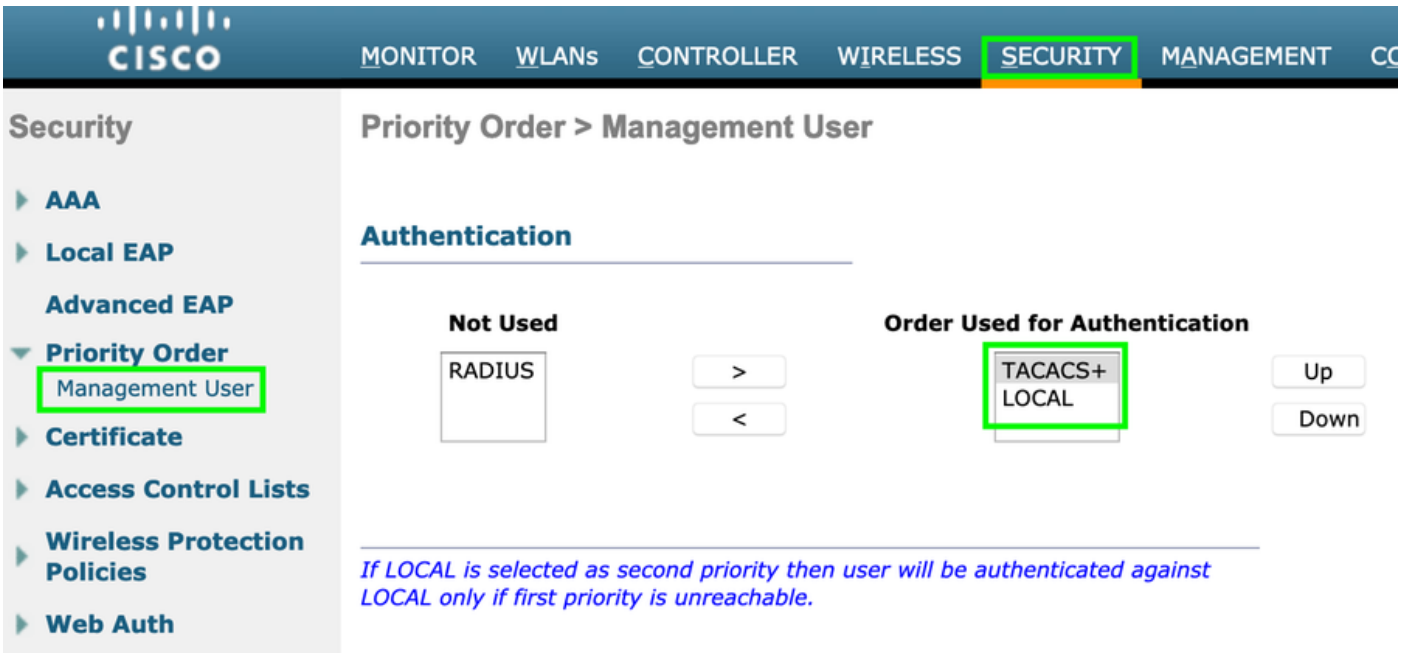
步驟8.配置WLC進行裝置管理。

導覽至**Security > AAA > TACACS+**按一下**New**，然後新增驗證記帳伺服器，如下圖所示。





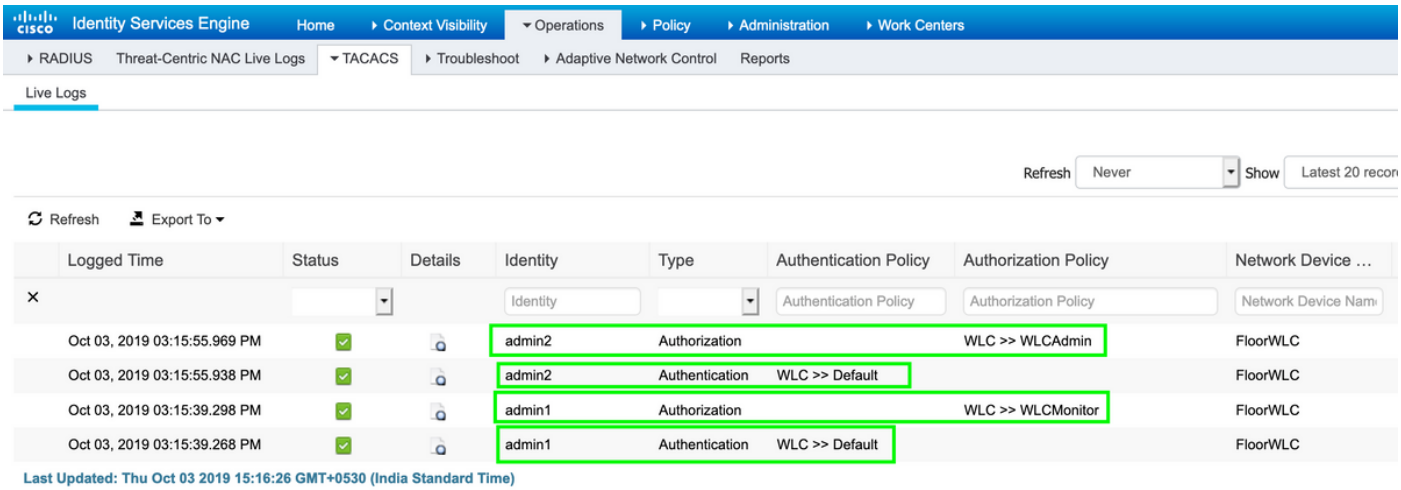
變更優先順序並使TACACS+位於頂端、本地到底，如下圖所示：



注意：請勿關閉目前的WLC GUI作業階段。建議在不同的Web瀏覽器中開啟WLC GUI，並檢查使用TACACS+憑證登入是否有效。如果不是，請驗證TCP埠49上的ISE節點的配置和連線。

驗證

導覽至**Operations > TACACS > Live logs**，並監控**Live Logs**。開啟WLC GUI並使用Active Directory使用者憑據登入，如下圖所示



疑難排解

目前尚無適用於此組態的具體疑難排解資訊。