Administración de dispositivos de Cisco WLC mediante TACACS+

Contenido

Introducción

Este documento describe cómo configurar TACACS+ para la administración de dispositivos de Cisco Wireless LAN Controller (WLC) con Identity Service Engine (ISE).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos de Identity Service Engine (ISE)
- Conocimiento básico de Cisco Wireless LAN Controller (WLC)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Identity Service Engine 2.4
- Controlador de LAN inalámbrica de Cisco 8.5.135

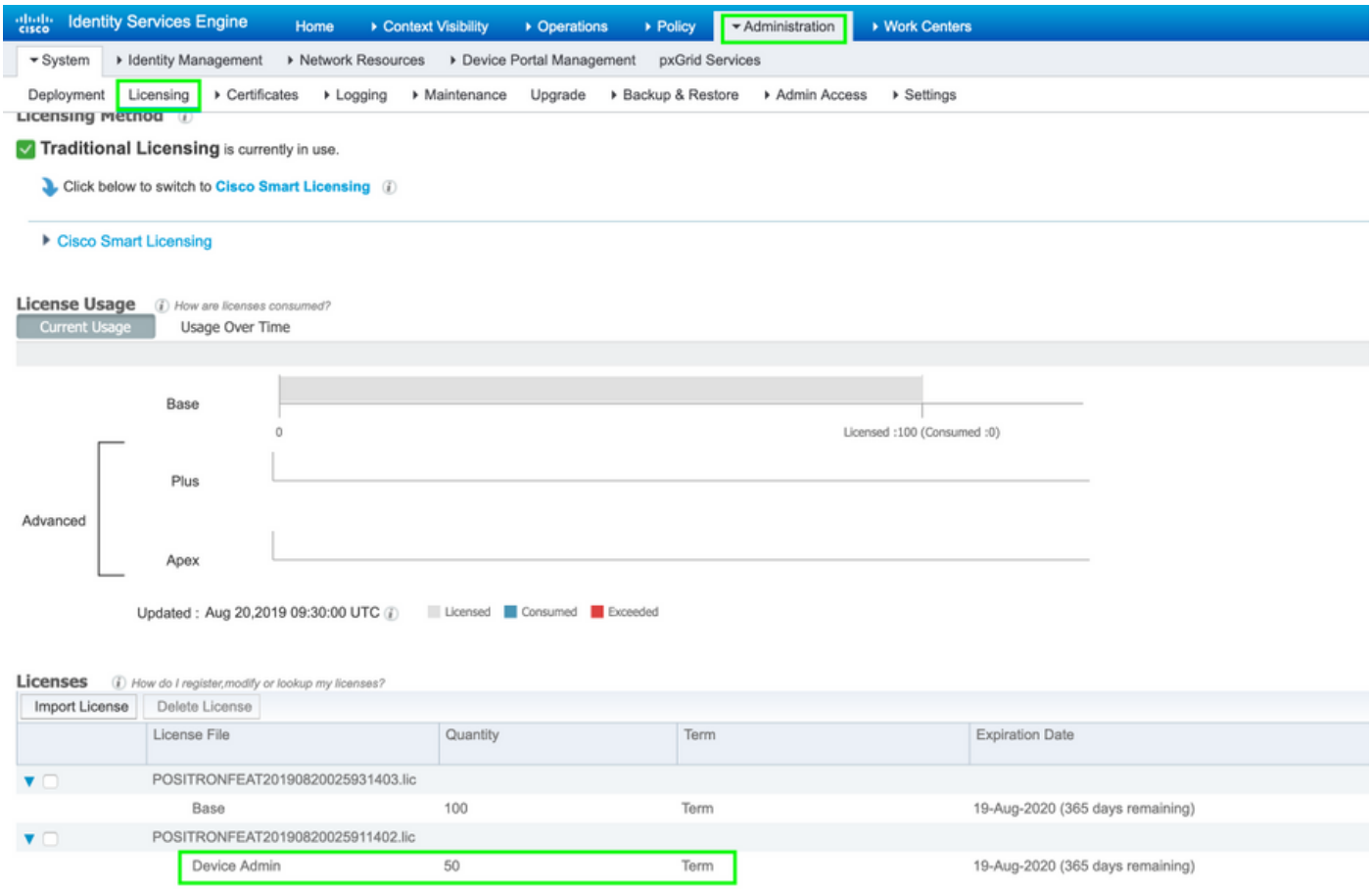
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is

live, make sure that you understand the potential impact of any command.

Configuración

Paso 1. Verifique Device Administration License.

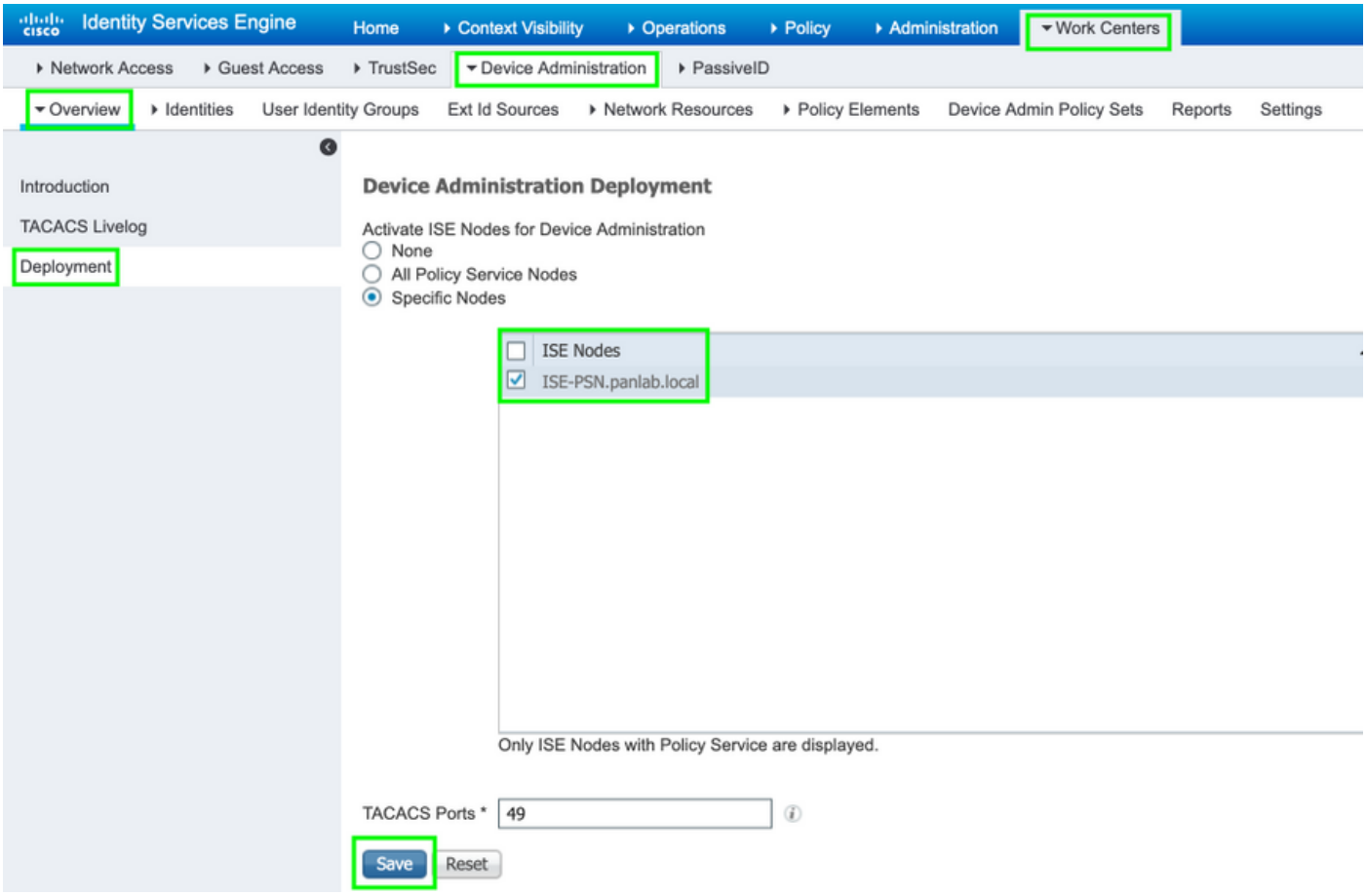
Vaya a **Administration > System > Licensing** tab y verifique que se haya instalado la licencia **Device Admin**, como se muestra en la imagen.



Nota: La licencia de administrador de dispositivos es necesaria para utilizar la función TACACS+ en ISE.

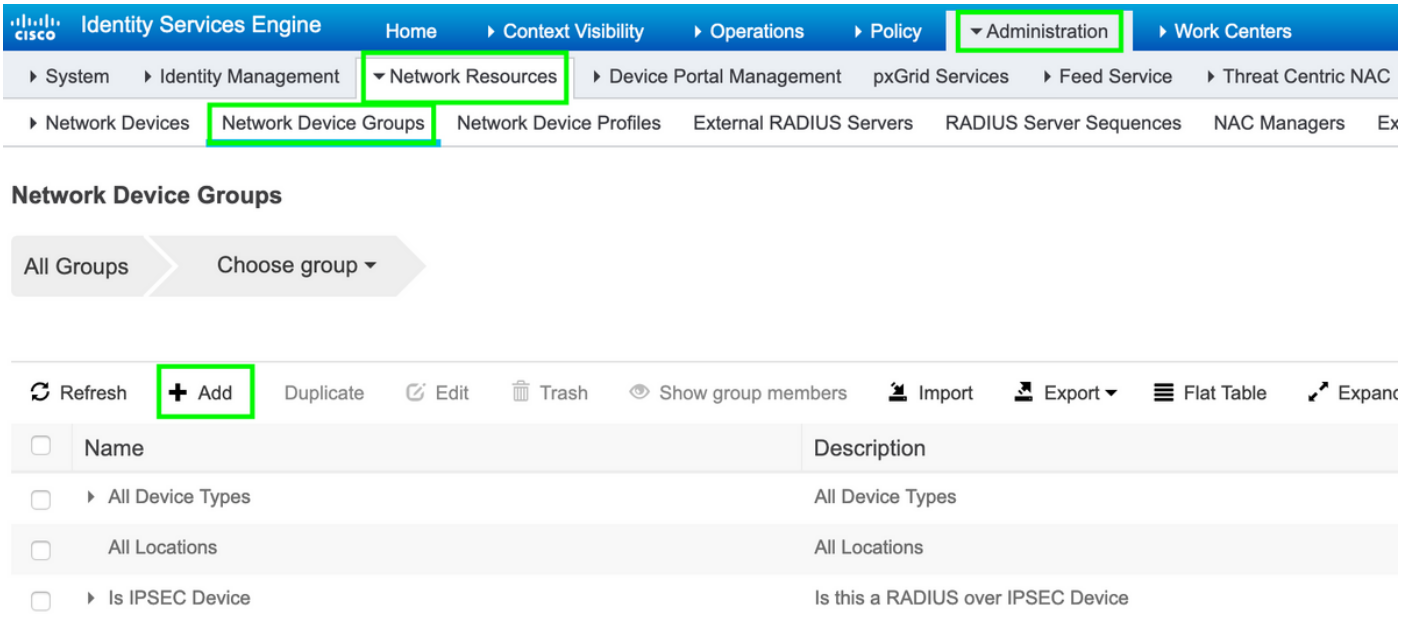
Paso 2. Habilite la administración de dispositivos en nodos PSN ISE.

Navegue hasta **Centros de Trabajo > Administración de Dispositivos > Descripción General**, haga clic en la pestaña **Implementación** , **Seleccione el botón de opción Nodo PSN específico**. **Habilite** Device Administration en el nodo ISE seleccionando la **casilla** y haga clic en **guardar**, como se muestra en la imagen:



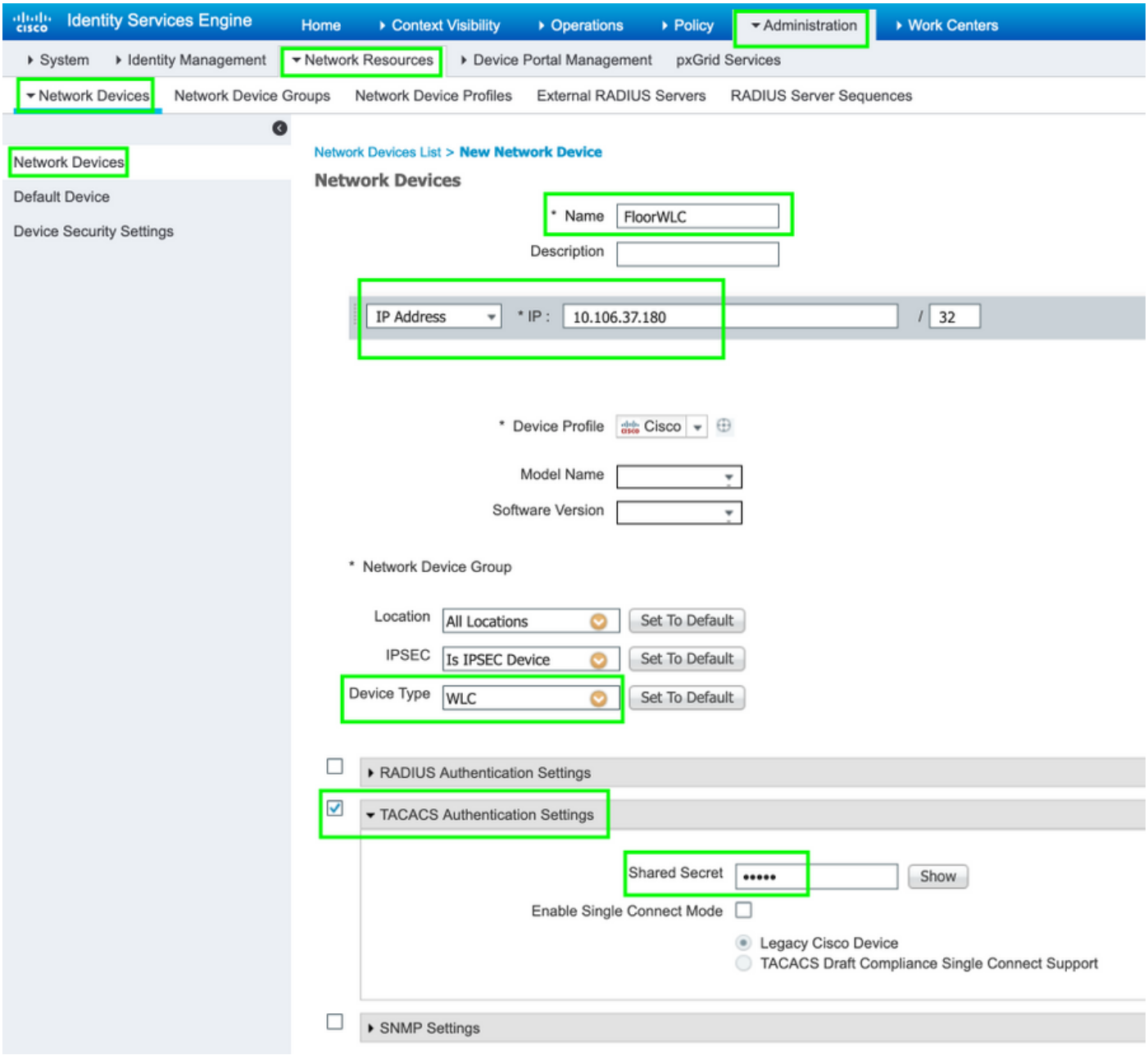
Paso 3. Cree un grupo de dispositivos de red.

Para agregar el WLC como un dispositivo de red en el ISE, navegue hasta **Administración > Recursos de Red > Grupos de Dispositivos de Red > Todos los Tipos de Dispositivo**, cree un **nuevo grupo** para el WLC, como se muestra en la imagen:



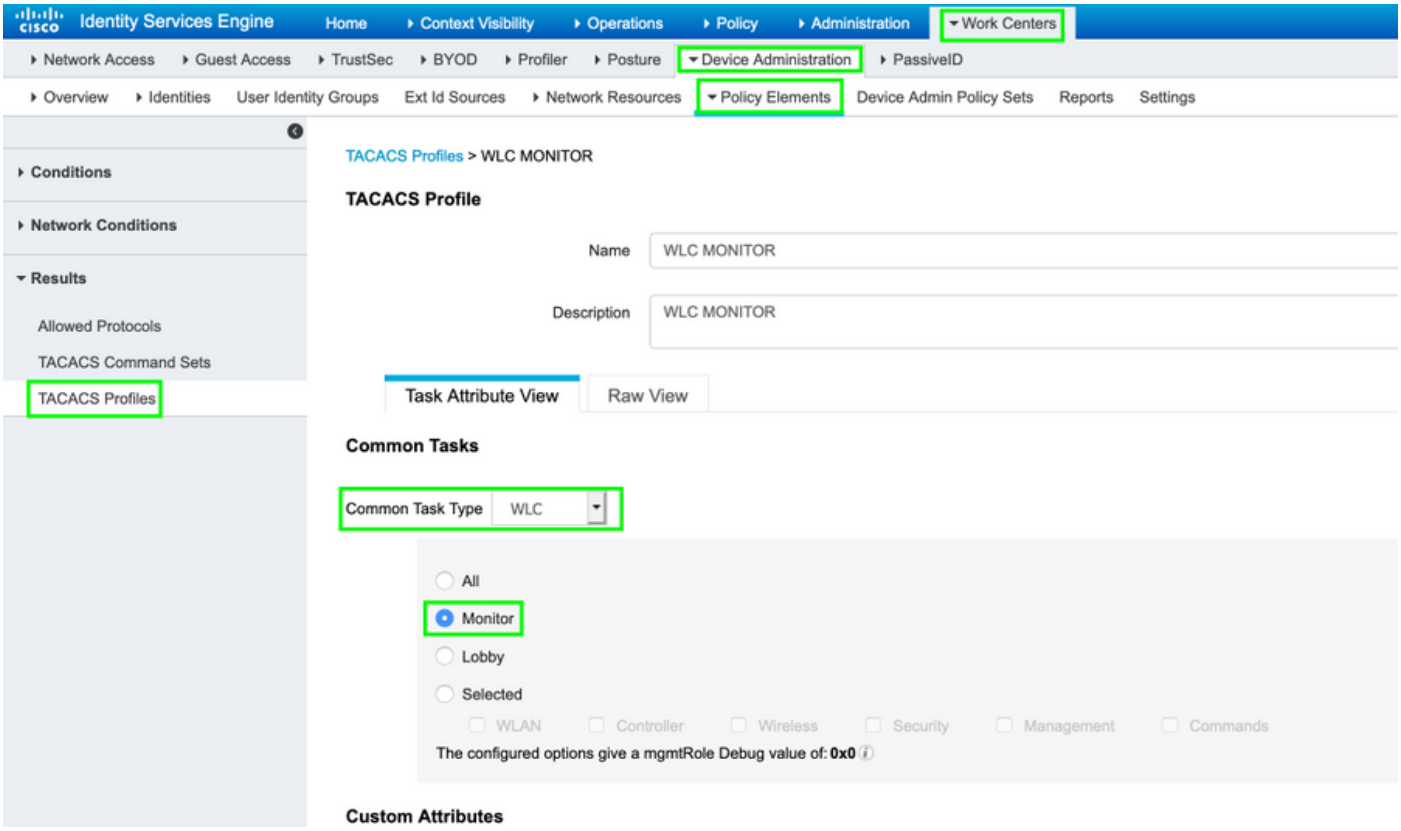
Paso 4. Agregue el WLC como dispositivo de red.

Vaya a **Centros de trabajo > Administración de dispositivos > Recursos de red > Dispositivos de red**. Haga clic en Agregar, proporcione el nombre, la dirección IP y seleccione el tipo de dispositivo como **WLC**, seleccione la casilla de verificación **TACACS+ Authentication Settings** y proporcione la clave **Secreto Compartido**, como se muestra en la imagen:

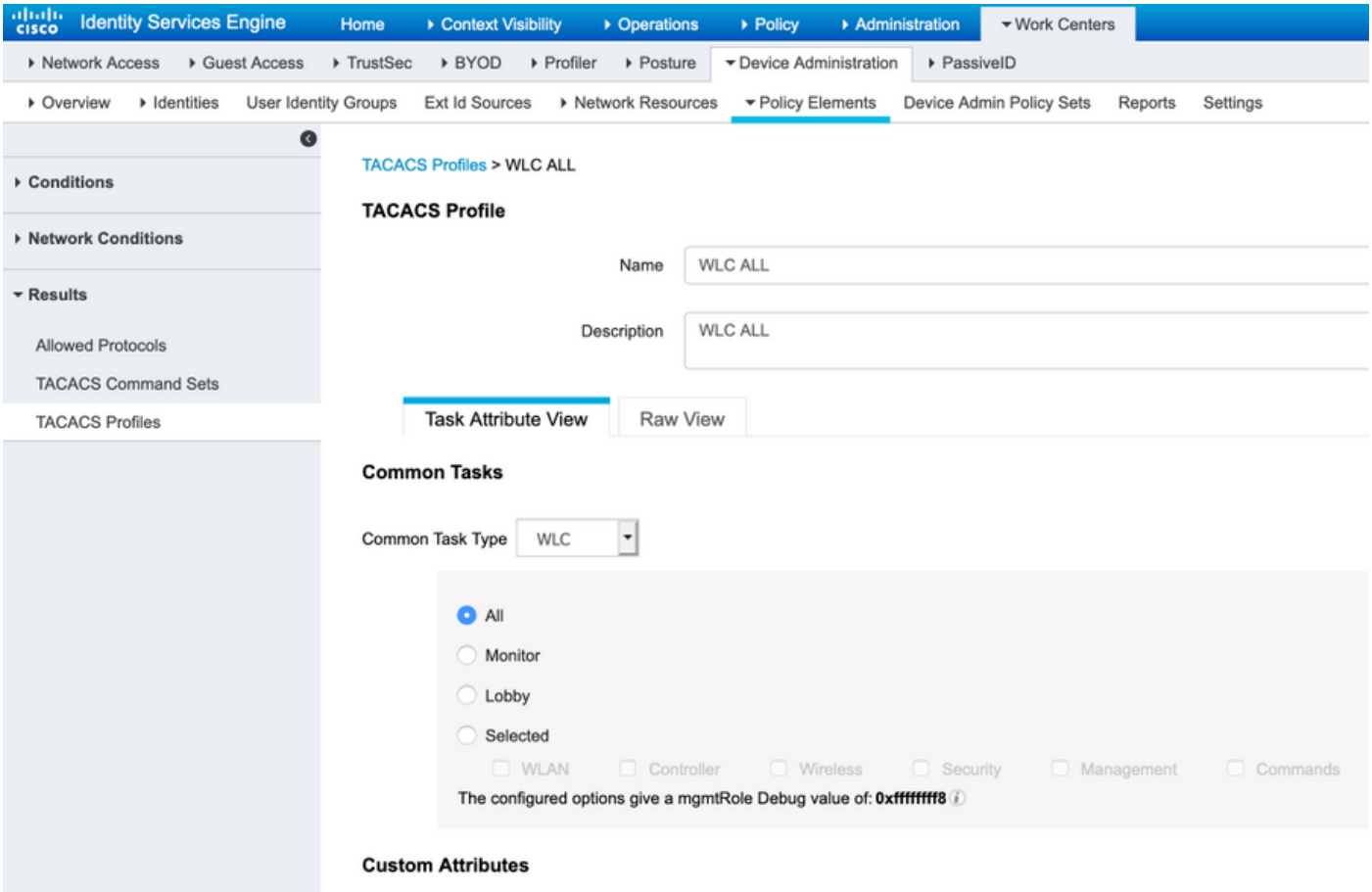


Paso 5. Cree un perfil TACACS para el WLC.

Vaya a **Centros de Trabajo > Administración de Dispositivos > Elementos de Política > Resultados > Perfiles TACACS.** Haga clic en **Agregar y** proporcione un **nombre.** En la pestaña **Vista de atributo de tarea**, seleccione **WLC** para **Tipo de tarea común.** Existen perfiles predeterminados entre los que se selecciona **Monitor** para permitir el acceso limitado a los usuarios, como se muestra en la imagen.

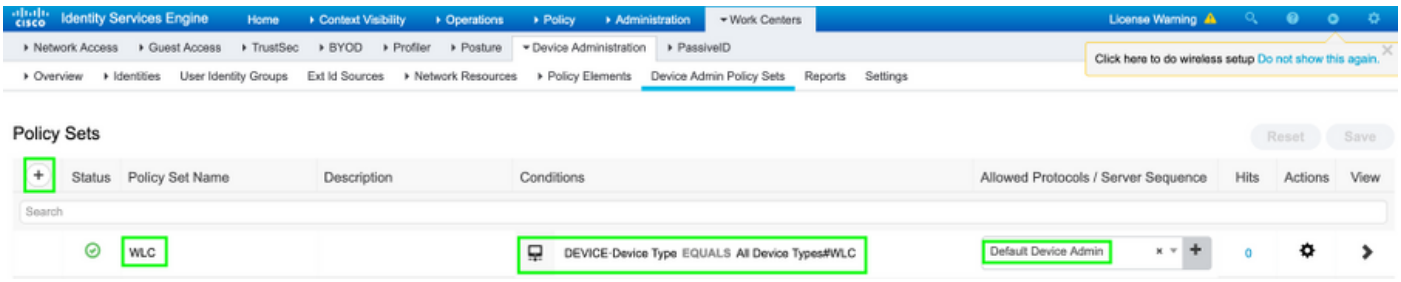


Hay otro perfil predeterminado **All** que permite el acceso completo al usuario como se muestra en la imagen.



Paso 6. Cree un conjunto de políticas.

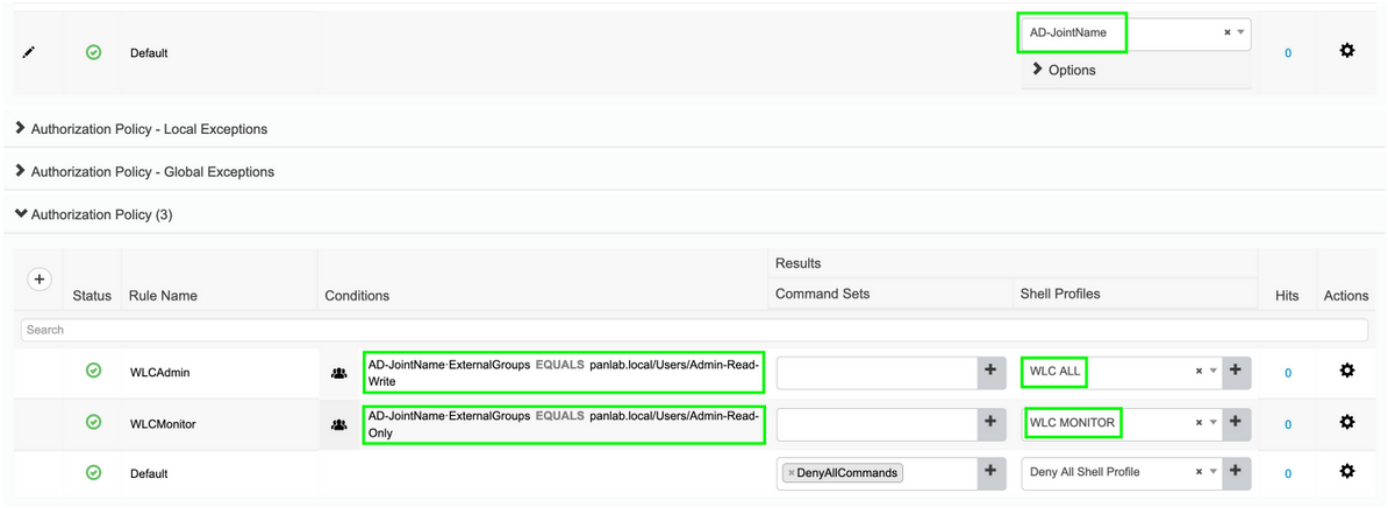
Vaya a **Centros de trabajo > Administración de dispositivos > Conjuntos de políticas de administración de dispositivos.** Haga clic **(+)** y asigne un nombre al conjunto de políticas. En la condición de política seleccione **Device Type** as WLC, Allowed Protocols puede ser **Default Device Admin**, como se muestra en la imagen.



Paso 7. Cree políticas de autenticación y autorización.

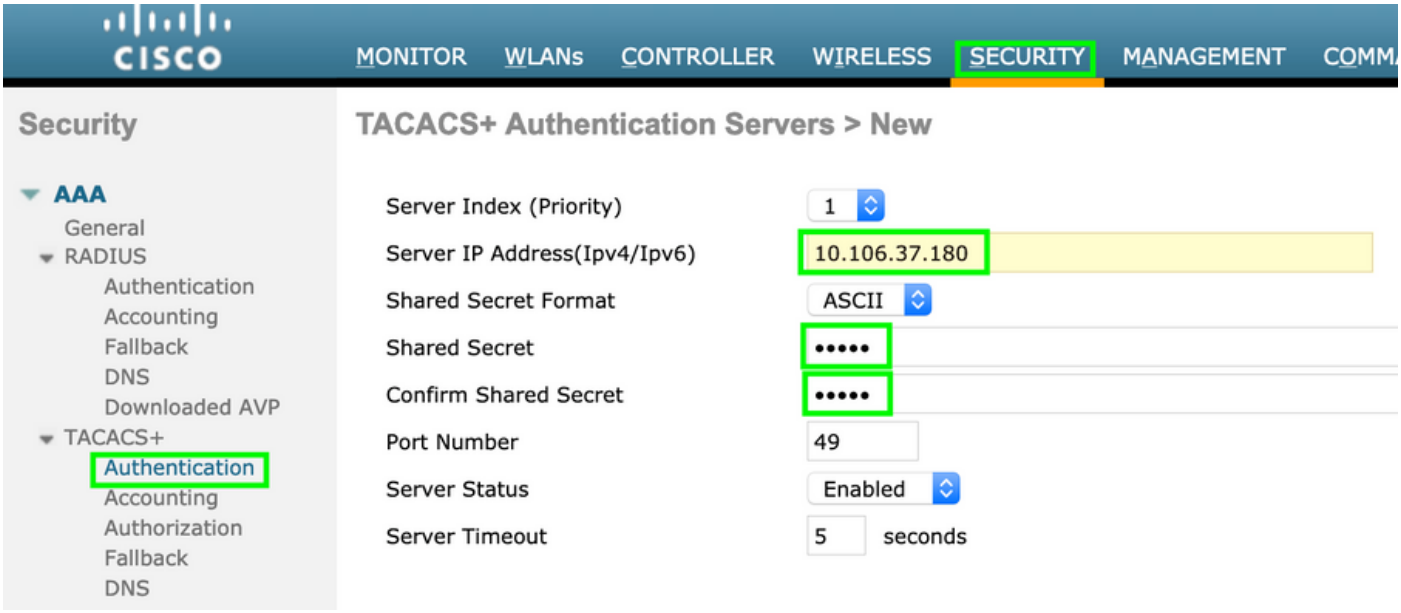
En este documento, se configuran dos grupos de ejemplo **Admin-Read-Write** y **Admin-Read-Only** en el directorio activo y un usuario dentro de cada grupo **admin1** , **admin2** respectivamente. Active Directory se integra con ISE a través de un punto de unión denominado **AD-JointName.**

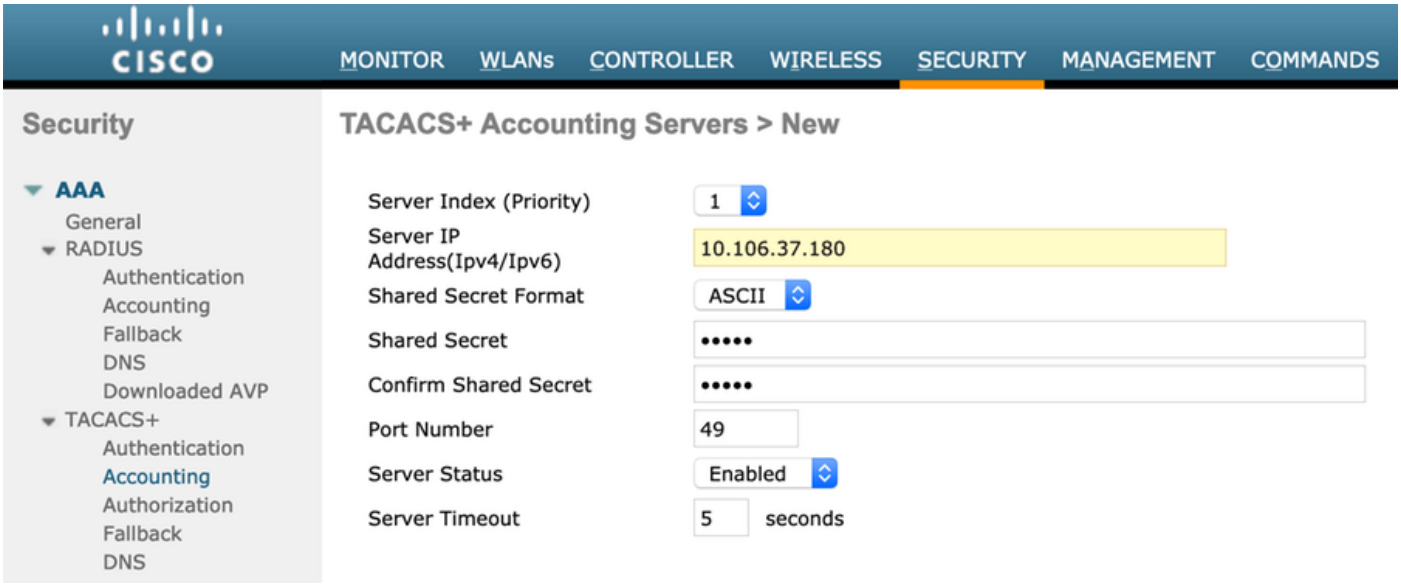
Cree dos políticas de autorización, como se muestra en la imagen:



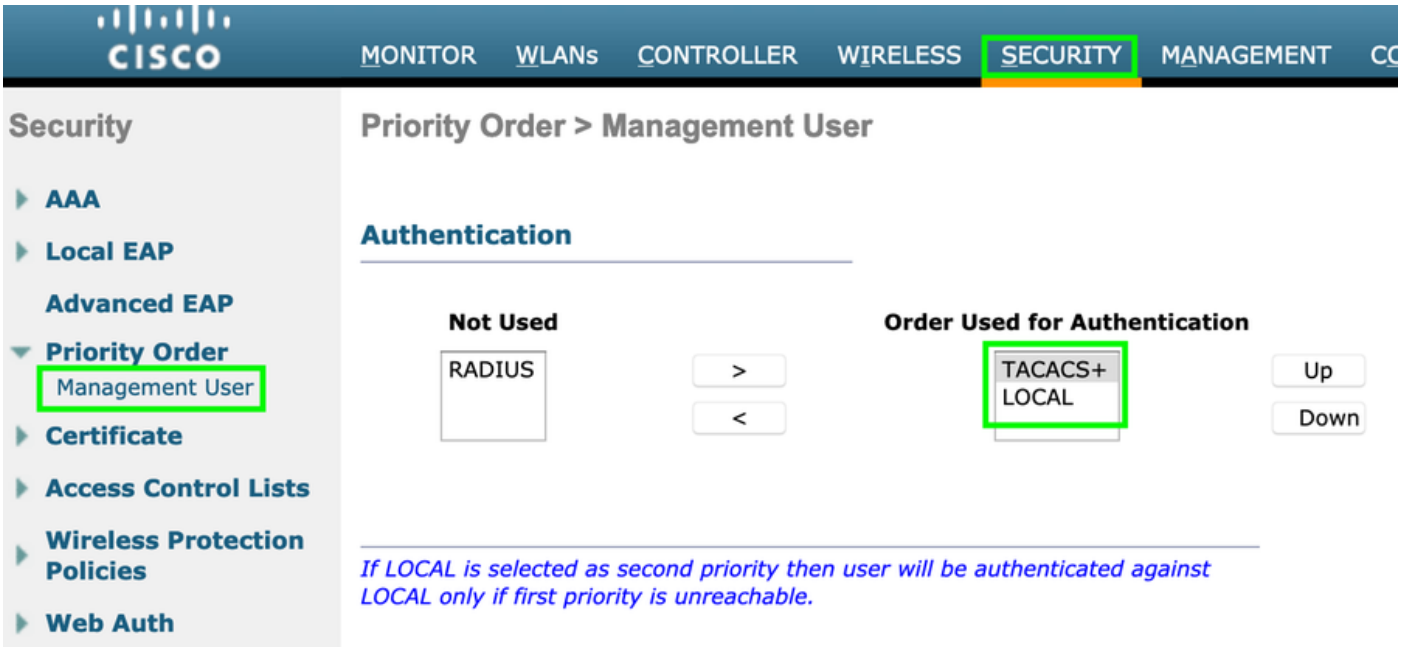
Paso 8. Configure el WLC para la Administración del Dispositivo.

Navegue hasta **Seguridad > AAA > TACACS+** haga clic en **Nuevo** y agregue Authentication, Accounting server, como se muestra en la imagen.





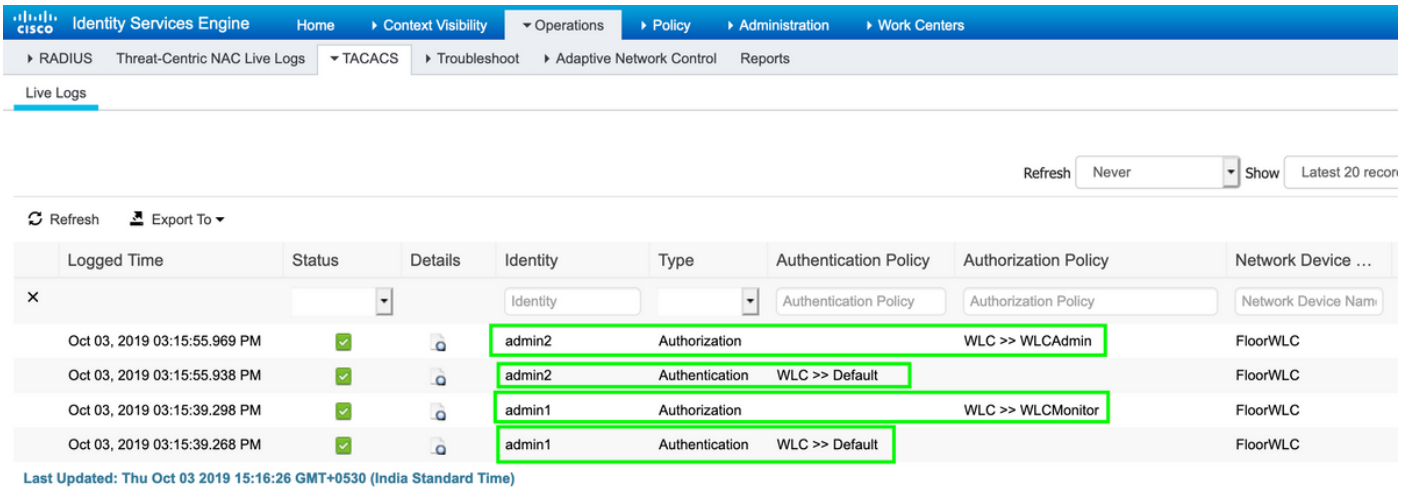
Cambie el orden de prioridad y haga TACACS+ arriba y Local abajo, como se muestra en la imagen:



Precaución: No cierre la sesión actual de WLC GUI. Se recomienda abrir la GUI del WLC en diferentes navegadores web y verificar si el login con las credenciales TACACS+ funciona o no. Si no es así, verifique la configuración y conectividad con el nodo ISE en el puerto TCP 49.

Verificación

Navegue hasta **Operaciones > TACACS > Registros en directo** y monitoree los **Registros en directo**. Abra la GUI del WLC e inicie sesión con las credenciales del usuario de Active Directory, como se muestra en la imagen



Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.