

# Administración de dispositivos de Cisco WLC mediante TACACS+

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configuración](#)

[Paso 1. Verifique Device Administration License.](#)

[Paso 2. Habilite la administración de dispositivos en nodos PSN ISE.](#)

[Paso 3. Cree un grupo de dispositivos de red.](#)

[Paso 4. Agregue el WLC como dispositivo de red.](#)

[Paso 5. Cree un perfil TACACS para el WLC.](#)

[Paso 6. Cree un conjunto de políticas.](#)

[Paso 7. Cree políticas de autenticación y autorización.](#)

[Paso 8. Configure el WLC para la Administración del Dispositivo.](#)

[Verificación](#)

[Troubleshoot](#)

## 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.

**Licensing Method**

Traditional Licensing is currently in use.

Click below to switch to Cisco Smart Licensing

Cisco Smart Licensing

**License Usage** How are licenses consumed?

Current Usage Usage Over Time

Advanced

Base

Plus

Apex

Updated : Aug 20,2019 09:30:00 UTC

Licensed Consumed Exceeded

**Licenses** How do I register, modify or lookup my licenses?

Import License Delete License

License File	Quantity	Term	Expiration Date
POSITRONFEAT20190820025931403.lic			
Base	100	Term	19-Aug-2020 (365 days remaining)
POSITRONFEAT20190820025911402.lic			
Device Admin	50	Term	19-Aug-2020 (365 days remaining)

**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.

Navigate 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:

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Overview

### Device Administration Deployment

Activate ISE Nodes for Device Administration

None  
 All Policy Service Nodes  
 Specific Nodes

ISE Nodes
<input checked="" type="checkbox"/> ISE-PSN.panlab.local

Only ISE Nodes with Policy Service are displayed.

TACACS Ports \*

### 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:

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Network Resources > Network Device Groups

### Network Device Groups

All Groups > Choose group

Name	Description
<input type="checkbox"/> All Device Types	All Device Types
<input type="checkbox"/> All Locations	All Locations
<input type="checkbox"/> Is IPSEC Device	Is this a RADIUS over IPSEC Device

## Add Group



Name \*

WLC

Description

Parent Group \*

All Device Types



Cancel

Save

### 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:

The screenshot displays the 'New Network Device' configuration page in the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Network Resources > Network Devices > New Network Device. The left sidebar shows 'Network Devices' selected. The main form contains the following fields and settings:

- Name:** FloorWLC
- Description:** (empty)
- IP Address:** 10.106.37.180 / 32
- Device Profile:** Cisco
- Model Name:** (empty)
- Software Version:** (empty)
- Network Device Group:**
  - Location:** All Locations
  - IPSEC:** Is IPSEC Device
  - Device Type:** WLC
- Authentication Settings:**
  - RADIUS Authentication Settings:** (unchecked)
  - TACACS Authentication Settings:** (checked)
  - Shared Secret:** (masked with dots)
  - Enable Single Connect Mode:** (unchecked)
  - Legacy Cisco Device:** (selected)
  - TACACS Draft Compliance Single Connect Support:** (unselected)
- SNMP Settings:** (unchecked)

## 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.

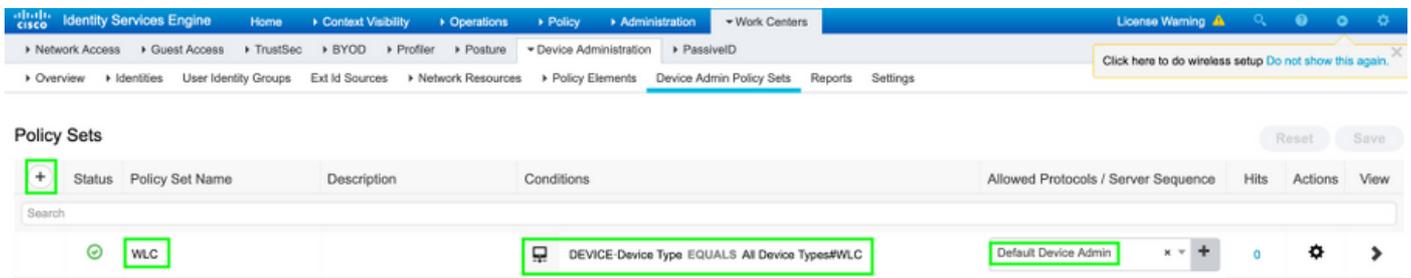
The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > PassiveID > Policy Elements. The page title is "TACACS Profiles > WLC MONITOR". The "TACACS Profile" section shows the Name as "WLC MONITOR" and the Description as "WLC MONITOR". Below this, there are tabs for "Task Attribute View" (selected) and "Raw View". Under "Common Tasks", the "Common Task Type" is set to "WLC". The "Monitor" radio button is selected, and the "mgmtRole Debug" value is 0x0. Other options like "All", "Lobby", "Selected", "WLAN", "Controller", "Wireless", "Security", "Management", and "Commands" are unselected.

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

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface for a different TACACS profile. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > PassiveID > Policy Elements. The page title is "TACACS Profiles > WLC ALL". The "TACACS Profile" section shows the Name as "WLC ALL" and the Description as "WLC ALL". Below this, there are tabs for "Task Attribute View" (selected) and "Raw View". Under "Common Tasks", the "Common Task Type" is set to "WLC". The "All" radio button is selected, and the "mgmtRole Debug" value is 0xffffffff. Other options like "Monitor", "Lobby", "Selected", "WLAN", "Controller", "Wireless", "Security", "Management", and "Commands" are unselected.

**Paso 6. Cree un conjunto de políticas.**

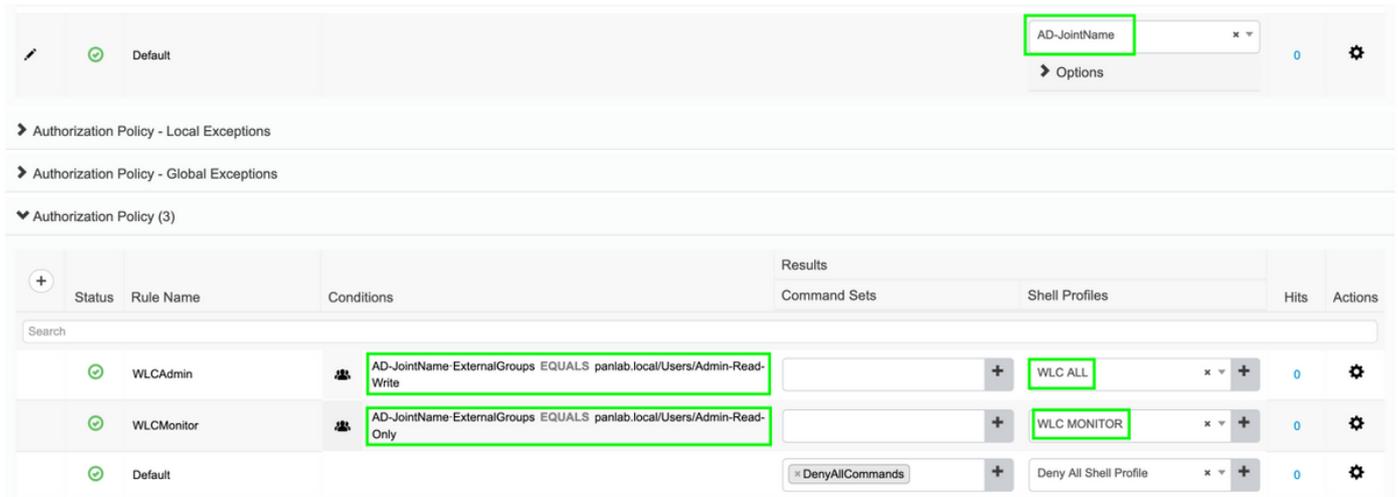
Vaya a **Centros de trabajo > Administración de dispositivos > Conjuntos de políticas de administración de dispositivos**. Haga clic (+) y asigne un nombre al conjunto de políticas. En la condición de política seleccione **Device Type** as **WLC**, Allowed Protocols puede ser **Default Device Admin**,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

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

CISCO MONITOR WLANs CONTROLLER WIRELESS **SECURITY** MANAGEMENT COMM

**Security**

- AAA
  - General
  - RADIUS
    - Authentication
    - Accounting
    - Fallback
    - DNS
    - Downloaded AVP
  - TACACS+
    - Authentication**
    - Accounting
    - Authorization
    - Fallback
    - DNS

**TACACS+ Authentication Servers > New**

Server Index (Priority) 1

Server IP Address(Ipv4/Ipv6) 10.106.37.180

Shared Secret Format ASCII

Shared Secret .....

Confirm Shared Secret .....

Port Number 49

Server Status Enabled

Server Timeout 5 seconds

CISCO MONITOR WLANs CONTROLLER WIRELESS **SECURITY** MANAGEMENT COMMANDS

**Security**

- AAA
  - General
  - RADIUS
    - Authentication
    - Accounting
    - Fallback
    - DNS
    - Downloaded AVP
  - TACACS+
    - Authentication
    - Accounting**
    - Authorization
    - Fallback
    - DNS

**TACACS+ Accounting Servers > New**

Server Index (Priority) 1

Server IP Address(Ipv4/Ipv6) 10.106.37.180

Shared Secret Format ASCII

Shared Secret .....

Confirm Shared Secret .....

Port Number 49

Server Status Enabled

Server Timeout 5 seconds

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

CISCO MONITOR WLANs CONTROLLER WIRELESS **SECURITY** MANAGEMENT CO

**Security**

- AAA
- Local EAP
- Advanced EAP
- Priority Order**
  - Management User**
- Certificate
- Access Control Lists
- Wireless Protection Policies
- Web Auth

**Priority Order > Management User**

**Authentication**

**Not Used**

RADIUS > <

**Order Used for Authentication**

TACACS+ LOCAL Up Down

*If LOCAL is selected as second priority then user will be authenticated against LOCAL only if first priority is unreachable.*

**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

Navigue 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

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Network Device ...
Oct 03, 2019 03:15:55.969 PM	Success		admin2	Authorization	WLC >> WLCAdmin	WLC >> WLCAdmin	FloorWLC
Oct 03, 2019 03:15:55.938 PM	Success		admin2	Authentication	WLC >> Default	WLC >> Default	FloorWLC
Oct 03, 2019 03:15:39.298 PM	Success		admin1	Authorization	WLC >> WLCMonitor	WLC >> WLCMonitor	FloorWLC
Oct 03, 2019 03:15:39.268 PM	Success		admin1	Authentication	WLC >> Default	WLC >> Default	FloorWLC

Last Updated: Thu Oct 03 2019 15:16:26 GMT+0530 (India Standard Time)

## Troubleshoot

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