

# Configure TACACS+ for Device Administration of Cisco WLC

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Configuration](#)

[Step 1. Check Device Administration License.](#)

[Step 2. Enable Device Administration on ISE PSN Nodes.](#)

[Step 3. Create a Network Device Group.](#)

[Step 4. Add WLC as a Network Device.](#)

[Step 5. Create a TACACS Profile for WLC.](#)

[Step 6. Create a Policy Set.](#)

[Step 7. Create Authentication and Authorization Policies.](#)

[Step 8. Configure WLC for Device Administration.](#)

### [Verify](#)

### [Troubleshoot](#)

---

## Introduction

This document describes how to configure TACACS+ for device administration of Cisco Wireless LAN Controller (WLC) with Identity Service Engine (ISE).

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of Identity Service Engine (ISE)
- Basic knowledge of Cisco Wireless LAN Controller (WLC)

### Components Used

The information in this document is based on these software and hardware versions:

- Cisco Identity Service Engine 2.4
- Cisco Wireless LAN Controller 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, ensure that you understand the potential impact of any command.

# Configuration

## Step 1. Check Device Administration License.

Navigate to **Administration > System > Licensing** tab and verify **Device Admin** license is installed, as shown in the image.

**Administration** > System > Licensing

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

Base 0 Licensed :100 (Consumed :0)

Plus

Apex

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

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

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)

**Note:** Device admin license is required to use the TACACS+ feature on ISE.

## Step 2. Enable Device Administration on ISE PSN Nodes.

Navigate to **Work Centers > Device Administration > Overview**, click **Deployment** tab, select the **Specific PSN Node** radio button. Enable Device Administration on the ISE node by selecting the **checkbox** and click **Save**, as shown in the image:

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

Network Access > Guest Access > TrustSec > Device Administration > PassiveID

Overview > Identities > User Identity Groups > Ext Id Sources > Network Resources > Policy Elements > Device Admin Policy Sets > Reports > Settings

### 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 \*

### Step 3. Create a Network Device Group.

In order to add WLC as a network device on the ISE, navigate to **Administration > Network Resources > Network Device Groups > All Device Types**, create a new group for WLC, as shown in the image:

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

System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC

Network Devices > Network Device Groups > Network Device Profiles > External RADIUS Servers > RADIUS Server Sequences > NAC Managers > Ex

### Network Device Groups

All Groups > Choose group

Refresh  Duplicate Edit Trash Show group members Import Export Flat Table Expand

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

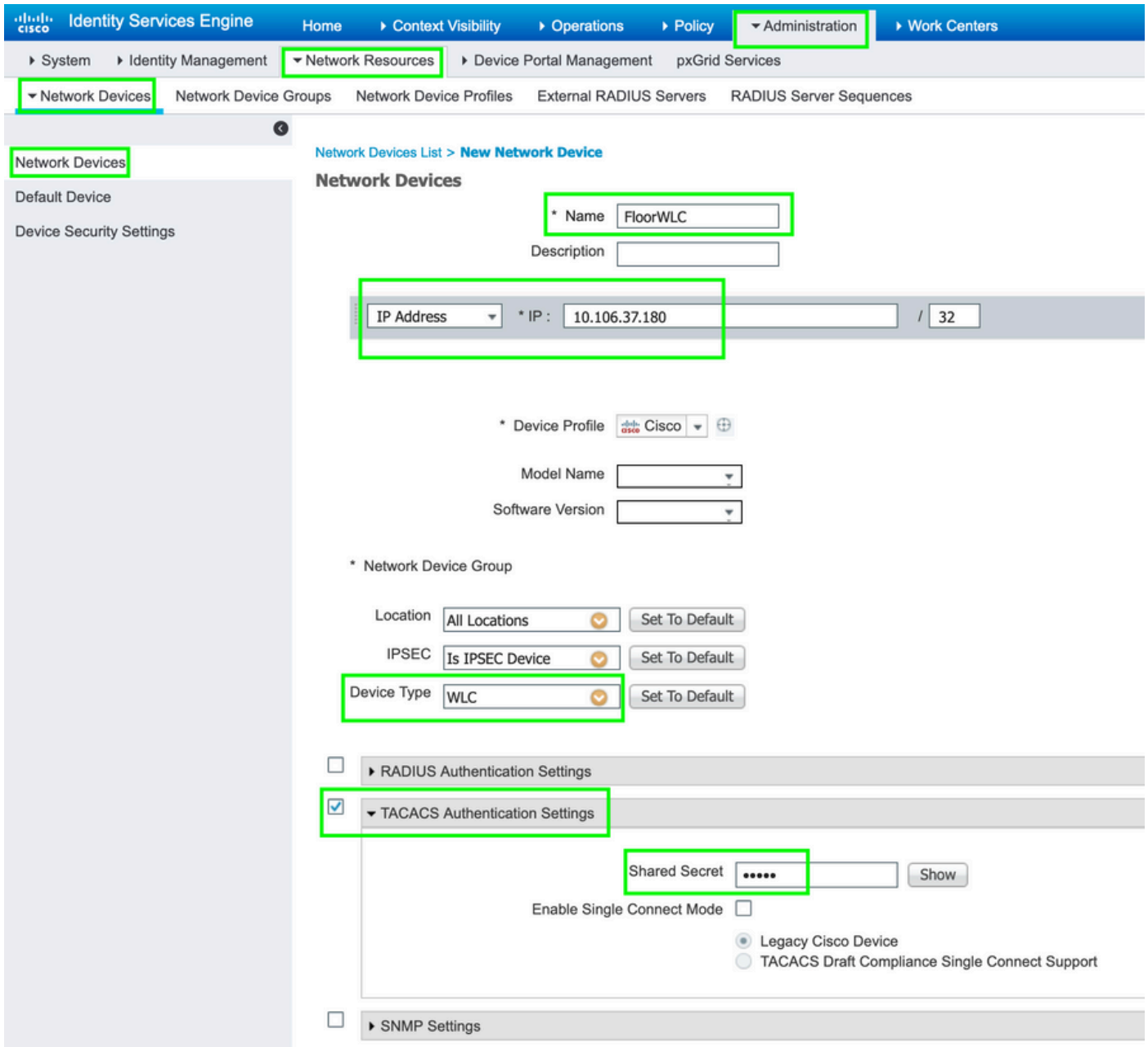


Cancel

Save

### Step 4. Add WLC as a Network Device.

Navigate to **Work Centers > Device Administration > Network Resources > Network Devices**. Click **Add**, provide **Name**, **IP Address** and select the Device type as **WLC**, select **TACACS+ Authentication Settings** checkbox and provide the **Shared Secret** key, as shown in the image:



## Step 5. Create a TACACS Profile for WLC.

Navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles**. Click **Add** and provide a **Name**. In the **Task attribute view** tab, select **WLC** for **Common Task Type**. There are default profiles present from which select **Monitor** to allow limited access to users, as shown in the image.

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 > Policy Elements. The page title is "TACACS Profiles > WLC MONITOR".

**TACACS Profile**

Name: WLC MONITOR  
Description: WLC MONITOR

Task Attribute View | Raw View

**Common Tasks**

Common Task Type: WLC

All  
 Monitor  
 Lobby  
 Selected

WLAN    Controller    Wireless    Security    Management    Commands

The configured options give a mgmtRole Debug value of: 0x0

**Custom Attributes**

There is another default profile **All** which allows full access to the user as shown in the image.

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 > Policy Elements. The page title is "TACACS Profiles > WLC ALL".

**TACACS Profile**

Name: WLC ALL  
Description: WLC ALL

Task Attribute View | Raw View

**Common Tasks**

Common Task Type: WLC

All  
 Monitor  
 Lobby  
 Selected

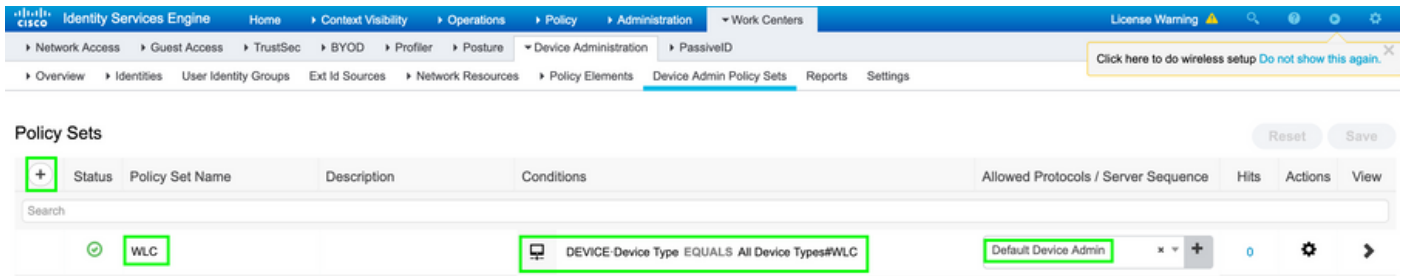
WLAN    Controller    Wireless    Security    Management    Commands

The configured options give a mgmtRole Debug value of: 0xffffffff

**Custom Attributes**

**Step 6. Create a Policy Set.**

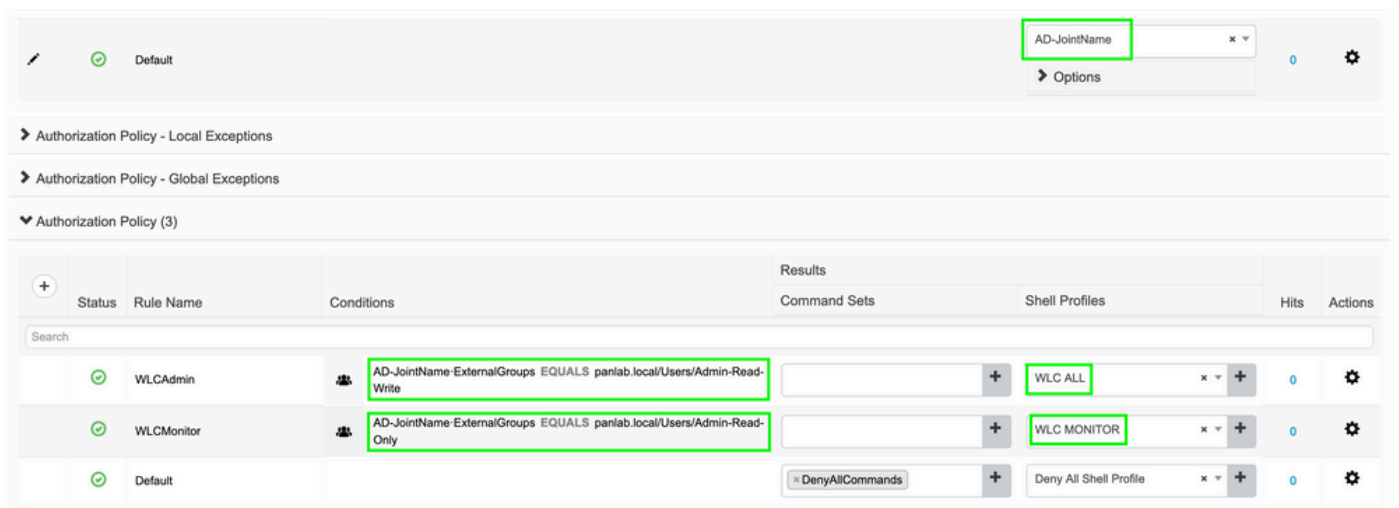
Navigate to **Work centers > Device administration > Device Admin Policy Sets**. Click (+) and give a name to the Policy Set. In the policy condition select **Device Type** as WLC, Allowed protocols can be **Default Device Admin**, as shown in the image.



## Step 7. Create Authentication and Authorization Policies.

In this document, two sample groups **Admin-Read-Write** and **Admin-Read-Only** are configured on the Active directory and one user inside each group **admin1**, **admin2** respectively. Active Directory is integrated with the ISE via a joinpoint named **AD-JointName**.

Create two authorization policies, as shown in the image:



## Step 8. Configure WLC for Device Administration.

Navigate to **Security > AAA > TACACS+** click **New** and add Authentication, Accounting server, as shown in the image.

**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

Change priority order and make TACACS+ on top and Local to bottom, as shown in the image:



CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT

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.*

**Caution:** Do not close the current WLC GUI session. Its recommended to open WLC GUI in different web-browser and check whether login with TACACS+ credentials works or not. If not, verify the configuration and connectivity to the ISE node on TCP port 49.

## Verify

Navigate to **Operations > TACACS > Live logs** and monitor the **Live Logs**. Open WLC GUI and log in with Active Directory user credentials, as shown in the image

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

RADIUS Threat-Centric NAC Live Logs TACACS Troubleshoot Adaptive Network Control Reports

Live Logs

Refresh Never Show Latest 20 recon

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

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

## Troubleshoot

There is currently no specific troubleshooting information available for this configuration.