

Administration des périphériques de Cisco WLC à l'aide de TACACS+

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Étape 1. Vérifiez la licence d'administration de périphériques.](#)

[Étape 2. Activez l'administration des périphériques sur les noeuds PSN ISE.](#)

[Étape 3. Créez un groupe de périphériques réseau.](#)

[Étape 4. Ajoutez le WLC en tant que périphérique réseau.](#)

[Étape 5. Créez un profil TACACS pour WLC.](#)

[Étape 6. Créer un jeu de stratégies.](#)

[Étape 7. Créez des stratégies d'authentification et d'autorisation.](#)

[Étape 8. Configurez le WLC pour l'administration des périphériques.](#)

[Vérification](#)

[Dépannage](#)

Introduction

Ce document décrit comment configurer TACACS+ pour l'administration des périphériques du contrôleur LAN sans fil Cisco (WLC) avec Identity Service Engine (ISE).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base de Identity Service Engine (ISE)
- Connaissances de base du contrôleur LAN sans fil Cisco (WLC)

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Identity Service Engine 2.4
- Contrôleur LAN sans fil 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.

Configuration

Étape 1. Vérifiez la licence d'administration de périphériques.

Accédez à **Administration > System > Licensing** et vérifiez que la licence **Device Admin** est installée, comme le montre l'image.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The navigation menu at the top includes 'Administration', which is highlighted with a green box. Below the navigation, the 'Licensing Method' section indicates that 'Traditional Licensing' is currently in use. The 'License Usage' section shows a bar chart for 'Base' licenses with 100 licensed and 0 consumed. The 'Licenses' table below shows two license files, with the 'Device Admin' license highlighted in green.

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

Note: Une licence d'administration de périphérique est requise pour utiliser la fonctionnalité TACACS+ sur ISE.

Étape 2. Activez l'administration des périphériques sur les noeuds PSN ISE.

Accédez à **Work Centers > Device Administration > Overview**, cliquez sur l'onglet **Deployment**, sélectionnez la case d'option **Specific PSN Node**. Activez l'administration des périphériques sur le noeud ISE en cochant la case et en cliquant sur **enregistrer**, comme illustré dans l'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

Introduction
TACACS Livelog
Deployment

Device Administration Deployment

Activate ISE Nodes for Device Administration

None
 All Policy Service Nodes
 Specific Nodes

ISE Nodes
 ISE-PSN.panlab.local

Only ISE Nodes with Policy Service are displayed.

TACACS Ports * 49 ⓘ

Save Reset

Étape 3. Créez un groupe de périphériques réseau.

Afin d'ajouter le WLC en tant que périphérique réseau sur l'ISE, accédez à **Administration > Network Resources > Network Device Groups > All Device Types**, créez un **nouveau groupe** pour le WLC, comme illustré dans l'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 **+ Add** Duplicate Edit Trash Show group members Import Export ▾ Flat Table Expand

<input type="checkbox"/>	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

Étape 4. Ajoutez le WLC en tant que périphérique réseau.

Accédez à **Centres de travail > Administration des périphériques > Ressources réseau > Périphériques réseau**. Cliquez sur Add, indiquez Name, IP Address et sélectionnez le type de périphérique en tant que **WLC**, activez la case à cocher **TACACS+ Authentication Settings** et fournissez la clé **Shared Secret**, comme illustré dans l'image :

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences

Network Devices

Default Device

Device Security Settings

Network Devices List > New Network Device

Network Devices

* Name FloorWLC

Description

IP Address * IP : 10.106.37.180 / 32

* Device Profile Cisco

Model Name

Software Version

* Network Device Group

Location All Locations Set To Default

IPSEC Is IPSEC Device Set To Default

Device Type WLC Set To Default

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret Show

Enable Single Connect Mode

Legacy Cisco Device
 TACACS Draft Compliance Single Connect Support

SNMP Settings

Étape 5. Créez un profil TACACS pour WLC.

Accédez à **Centres de travail > Administration des périphériques > Éléments de stratégie > Résultats > Profils TACACS**. Cliquez sur **Ajouter** et indiquez un **nom**. Dans l'onglet **Affichage des attributs de tâche**, sélectionnez **WLC** pour **Common Task Type**. Il existe des profils par défaut à partir desquels sélectionner **Monitor** pour autoriser un accès limité aux utilisateurs, comme l'illustre l'image.

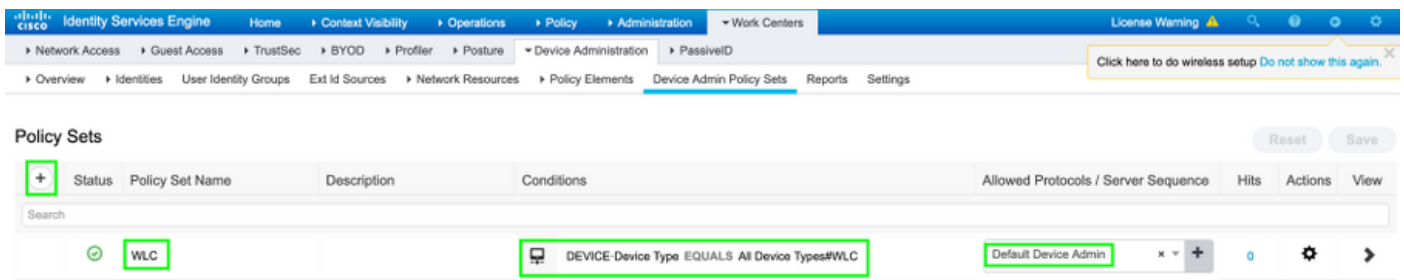
The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Policy Elements. The page title is "TACACS Profiles > WLC MONITOR". The "TACACS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

Il existe un autre profil par défaut **All** qui permet un accès complet à l'utilisateur comme illustré dans l'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". 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" and "Raw View". The "Common Tasks" section has a "Common Task Type" dropdown set to "WLC". Underneath, there are radio buttons for "All", "Monitor", "Lobby", and "Selected". The "All" option is selected. Below the radio buttons are checkboxes for "WLAN", "Controller", "Wireless", "Security", "Management", and "Commands". A note states: "The configured options give a mgmtRole Debug value of: 0xffffffff".

Étape 6. Créer un jeu de stratégies.

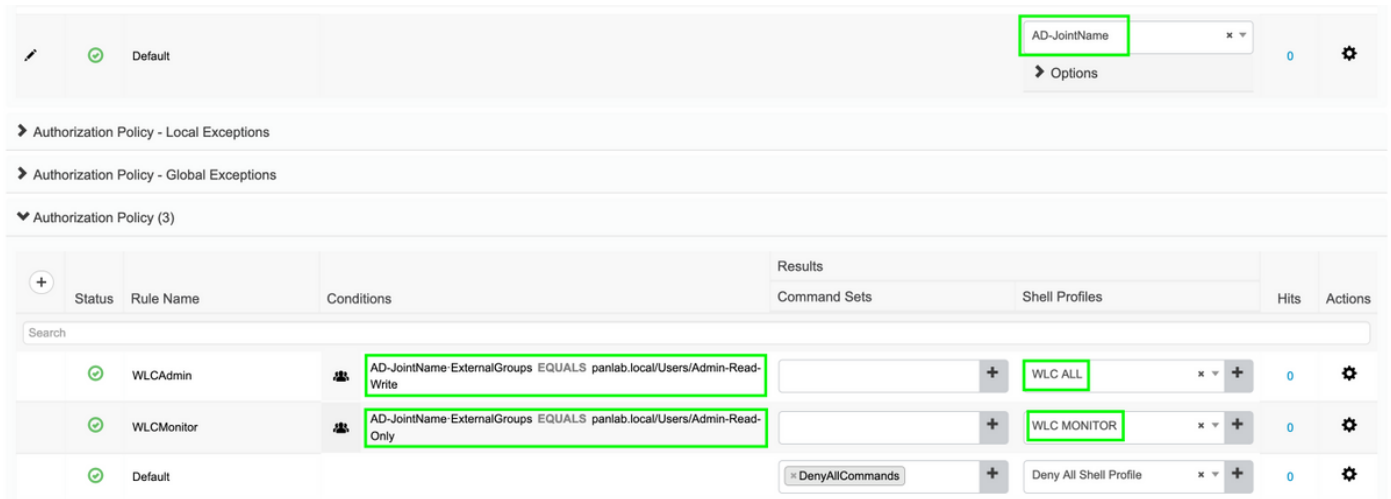
Accédez à **Centres de travail > Administration de périphériques > Jeux de stratégies d'administration de périphériques**. Cliquez sur (+) et donnez un nom au jeu de stratégies. Dans la condition de stratégie, sélectionnez **Type de périphérique** en tant que WLC, les protocoles autorisés peuvent être **Default Device Admin**, comme l'illustre l'image.



Étape 7. Créez des stratégies d'authentification et d'autorisation.

Dans ce document, deux groupes d'exemples **Admin-Read-Write** et **Admin-Read-Only** sont configurés sur le répertoire Active et un utilisateur dans chaque groupe **admin1**, **admin2** respectivement. Active Directory est intégré à l'ISE via un point d'accès appelé **AD-JointName**.

Créez deux stratégies d'autorisation, comme l'illustre l'image :



Étape 8. Configurez le WLC pour l'administration des périphériques.

Naviguez jusqu'à **Security > AAA > TACACS+** cliquez sur **New** et ajoutez Authentication, Accounting server, comme illustré dans l'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

Modifiez l'ordre de priorité et placez TACACS+ en haut et Local en bas, comme illustré dans l'image :

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.

Attention : Ne fermez pas la session GUI actuelle du WLC. Il est recommandé d'ouvrir l'interface graphique du WLC dans un navigateur Web différent et de vérifier si la connexion avec les informations d'identification TACACS+ fonctionne ou non. Dans le cas contraire, vérifiez la configuration et la connectivité au noeud ISE sur le port TCP 49.

Vérification

Accédez à **Opérations > TACACS > Journaux en direct** et surveillez les **Journaux en direct**. Ouvrez l'interface utilisateur graphique du WLC et connectez-vous avec les informations d'identification de l'utilisateur Active Directory, comme illustré dans l'image

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)

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.