

使用TACACS+管理Cisco WLC的裝置

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[組態](#)

[步驟1.檢查裝置管理許可證。](#)

[步驟2.在ISE PSN節點上啟用裝置管理。](#)

[步驟3.建立網路裝置組。](#)

[步驟4.將WLC新增為網路裝置。](#)

[步驟5.為WLC建立TACACS設定檔。](#)

[步驟6.建立策略集。](#)

[步驟7.建立身份驗證和授權策略。](#)

[步驟8.配置WLC進行裝置管理。](#)

[驗證](#)

[疑難排解](#)

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。

The screenshot displays the Cisco ISE Administration interface. The top navigation bar includes 'Administration' and 'Work Centers'. The 'Licensing' sub-menu is active, showing 'Traditional Licensing' is currently in use. Below this, there is a 'License Usage' section with a chart showing 'Base' license usage (Licensed: 100, Consumed: 0). The 'Licenses' table below lists two licenses, with the 'Device Admin' license highlighted.

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)

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：

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 *

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：

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

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釹取方塊並提供Shared Secret，如下圖所示：

The screenshot displays the 'New Network Device' configuration page in the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation path is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Network Devices. The left sidebar shows 'Network Devices' selected. The main content area is titled 'Network Devices List > New Network Device' and 'Network Devices'. The configuration fields are as follows:

- 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 (Set To Default)
 - IPSEC:** Is IPSEC Device (Set To Default)
 - Device Type:** WLC (Set To Default)
- RADIUS Authentication Settings:** (unchecked)
- TACACS Authentication Settings:** (checked)
 - Shared Secret:** (masked with dots, Show button)
 - Enable Single Connect Mode:** (unchecked)
 - Legacy Cisco Device:** (selected)
 - TACACS Draft Compliance Single Connect Support:** (unchecked)
- SNMP Settings:** (unchecked)

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。

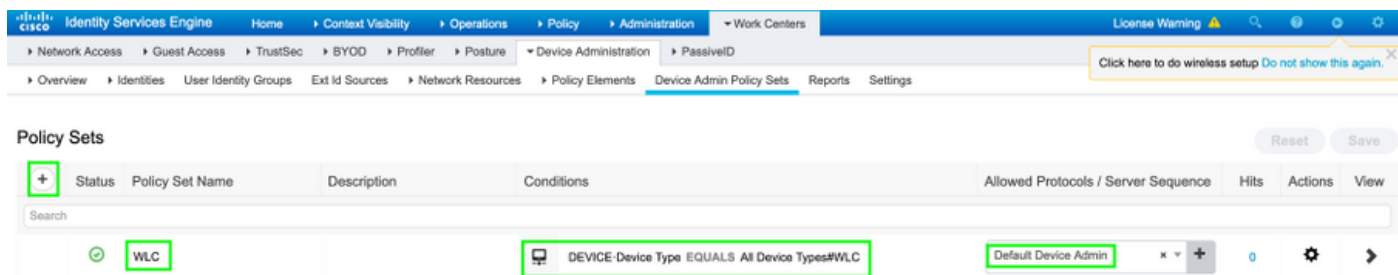
The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation path is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Policy Elements. The left sidebar shows a tree view with 'TACACS Profiles' selected. The main content area displays the configuration for the 'WLC MONITOR' TACACS Profile. The 'Name' and 'Description' fields are both set to 'WLC MONITOR'. Below this, there are tabs for 'Task Attribute View' (selected) and 'Raw View'. Under the 'Common Tasks' section, the 'Common Task Type' is set to 'WLC'. A list of radio buttons includes 'All', 'Monitor' (selected), 'Lobby', and 'Selected'. Below these are several checkboxes for 'WLAN', 'Controller', 'Wireless', 'Security', 'Management', and 'Commands'. A note at the bottom of this section states: 'The configured options give a mgmtRole Debug value of: 0x0'. The 'Custom Attributes' section is visible at the bottom but is empty.

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。

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface for the 'WLC ALL' TACACS Profile. The breadcrumb navigation path is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Policy Elements. The left sidebar shows 'TACACS Profiles' selected. The main content area displays the configuration for the 'WLC ALL' TACACS Profile. The 'Name' and 'Description' fields are both set to 'WLC ALL'. Below this, there are tabs for 'Task Attribute View' (selected) and 'Raw View'. Under the 'Common Tasks' section, the 'Common Task Type' is set to 'WLC'. A list of radio buttons includes 'All' (selected), 'Monitor', 'Lobby', and 'Selected'. Below these are several checkboxes for 'WLAN', 'Controller', 'Wireless', 'Security', 'Management', and 'Commands'. A note at the bottom of this section states: 'The configured options give a mgmtRole Debug value of: 0xffffffff8'. The 'Custom Attributes' section is visible at the bottom but is empty.

步驟6.建立策略集。

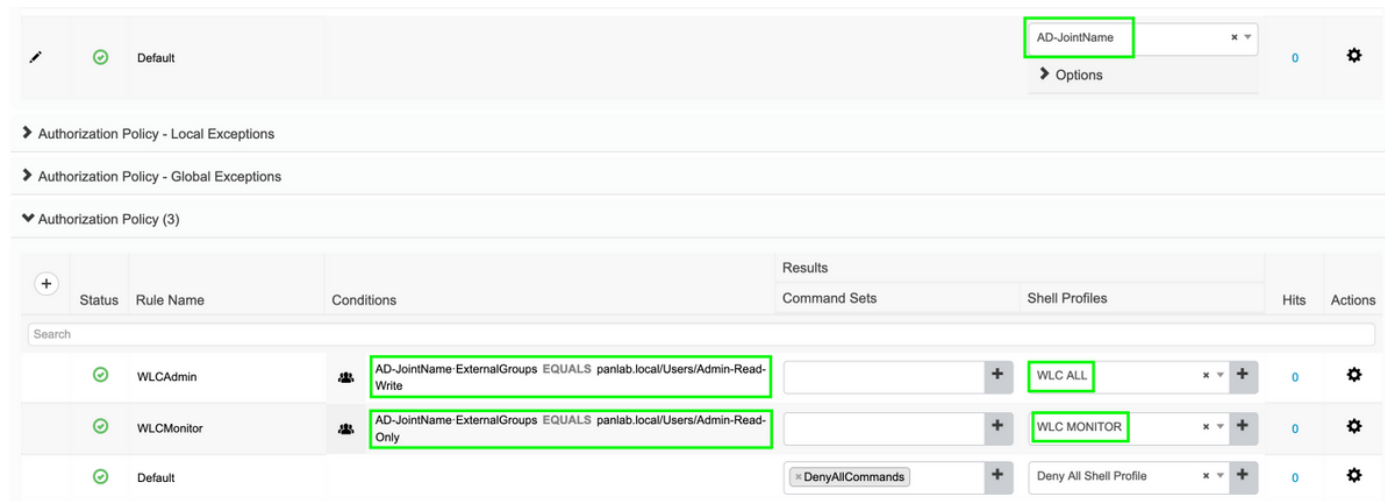
導航到工作中心>裝置管理>裝置管理策略集。按一下(+), 然後為策略集指定一個名稱。在策略條件中選擇Device Type as WLC, Allowed protocols可以是Default Device Admin, 如下圖所示。



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。

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)

Server IP Address(Ipv4/Ipv6)

Shared Secret Format

Shared Secret

Confirm Shared Secret

Port Number

Server Status

Server Timeout 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)

Server IP Address(Ipv4/Ipv6)

Shared Secret Format

Shared Secret

Confirm Shared Secret

Port Number

Server Status

Server Timeout seconds

變更優先順序並使TACACS+位於頂端、本地到底，如下圖所示：

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		Order Used for Authentication	
<input type="text" value="RADIUS"/>	> <	<input type="text" value="TACACS+
LOCAL"/>	Up Down

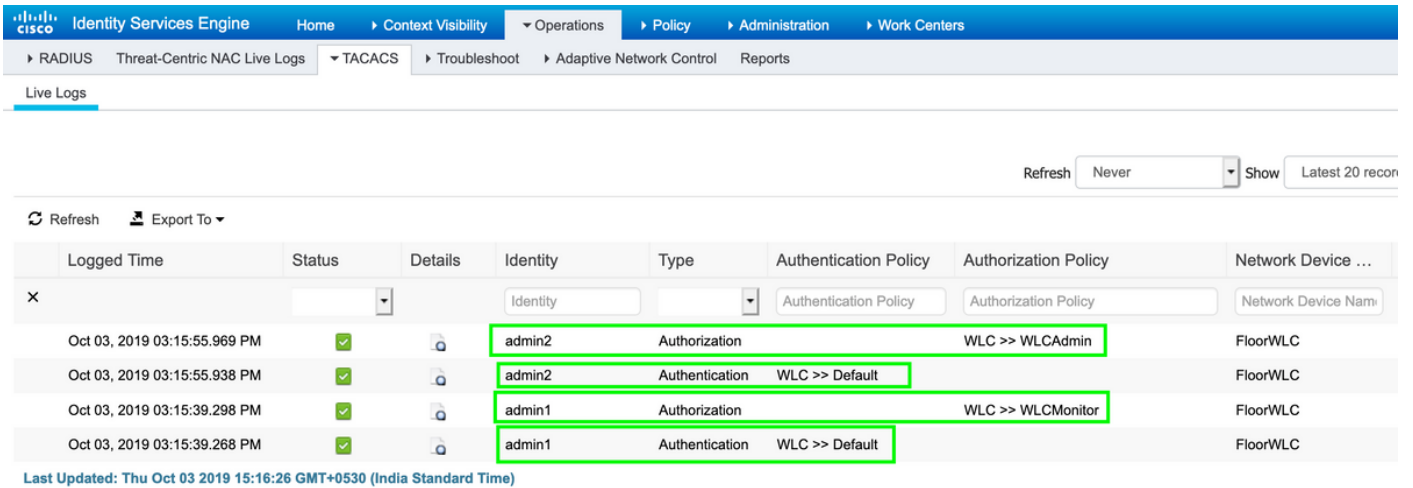
If LOCAL is selected as second priority then user will be authenticated against LOCAL only if first priority is unreachable.

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



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)

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。