

Amministrazione di dispositivi di Cisco WLC con TACACS+

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Passaggio 1. Controllare la licenza di amministrazione del dispositivo.](#)

[Passaggio 2. Abilitare l'amministrazione dei dispositivi sui nodi PSN ISE.](#)

[Passaggio 3. Creare un gruppo di dispositivi di rete.](#)

[Passaggio 4. Aggiungere WLC come dispositivo di rete.](#)

[Passaggio 5. Creare un profilo TACACS per WLC.](#)

[Passaggio 6. Creare un set di criteri.](#)

[Passaggio 7. Creazione di criteri di autenticazione e autorizzazione.](#)

[Passaggio 8. Configurare WLC per Device Administration.](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

Questo documento descrive come configurare TACACS+ per l'amministrazione dei dispositivi di Cisco Wireless LAN Controller (WLC) con Identity Service Engine (ISE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di Identity Service Engine (ISE)
- Conoscenze base di Cisco Wireless LAN Controller (WLC)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Identity Service Engine 2.4
- Cisco Wireless LAN Controller 8.5.135

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Passaggio 1. Controllare la licenza di amministrazione del dispositivo.

Passare a **Amministrazione > Sistema > scheda Licenze** e verificare che la licenza di **Device Admin** sia installata, come mostrato nell'immagine.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar includes 'Administration', which is highlighted with a green box. Below the navigation bar, the 'Licensing' menu item is also highlighted with a green box. The main content area shows the 'License Usage' section, which includes a bar chart for 'Current Usage'. The chart shows 'Base' licenses at 100 and 'Consumed' licenses at 0. Below the chart, the 'Licenses' table is visible, showing a license for 'Device Admin' with a quantity of 50, highlighted with a green box.

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)

Nota: Per usare la funzionalità TACACS+ su ISE, è necessaria una licenza di amministratore del dispositivo.

Passaggio 2. Abilitare l'amministrazione dei dispositivi sui nodi PSN ISE.

Passare a **Centri di lavoro > Amministrazione dispositivi > Panoramica**, fare clic su **Distribuzione** scheda, **Selezionare** il pulsante di scelta Nodo PSN specifico. **Abilitare** Device Administration sul nodo ISE selezionando la **casella di controllo** e facendo clic su **save**, come mostrato nell'immagine:

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

Passaggio 3. Creare un gruppo di dispositivi di rete.

Per aggiungere il WLC come dispositivo di rete sull'ISE, selezionare **Amministrazione > Risorse di rete > Gruppi di dispositivi di rete > Tutti i tipi di dispositivo**, quindi creare un nuovo gruppo per il WLC, come mostrato nell'immagine:

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

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

Passaggio 4. Aggiungere WLC come dispositivo di rete.

Passare a **Centri di lavoro > Amministrazione dispositivi > Risorse di rete > Dispositivi di rete**. Fare clic su **Add**, fornire **Name**, **IP Address** e selezionare il tipo di dispositivo come **WLC**, selezionare la casella di controllo **TACACS+Authentication Settings** e fornire la **chiave Shared Secret**, come mostrato nell'immagine:

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

Description

IP Address * IP : /

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret

Enable Single Connect Mode

Legacy Cisco Device
 TACACS Draft Compliance Single Connect Support

SNMP Settings

Passaggio 5. Creare un profilo TACACS per WLC.

Passare a **Centri di lavoro > Amministrazione dispositivi > Elementi della policy > Risultati > Profili TACACS**. Fare clic su **Add (Aggiungi)** e specificare un **nome**. Nella scheda **Visualizzazione attributi task**, selezionare **WLC** per **Tipo di task comune**. Sono presenti profili predefiniti dai quali selezionare **Controlla** per consentire un accesso limitato agli utenti, come mostrato nell'immagine.

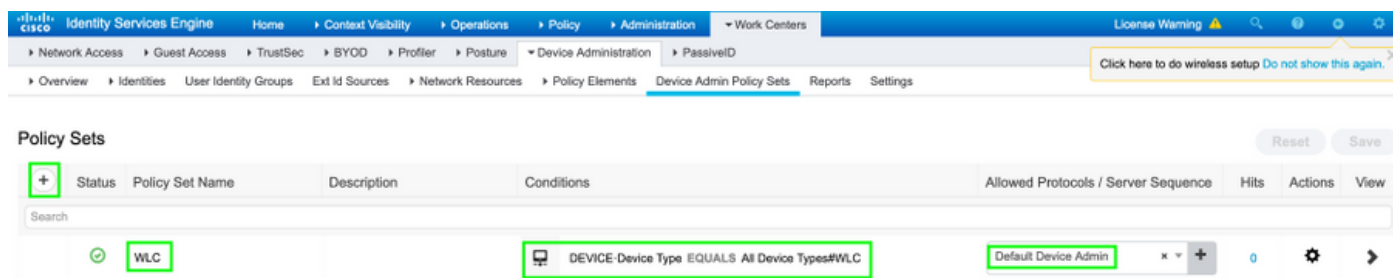
The screenshot shows the Cisco Identity Services Engine (ISE) interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > PassiveID > Policy Elements. The left sidebar shows a tree view with 'TACACS Profiles' selected. The main content area is titled 'TACACS Profiles > WLC MONITOR' and 'TACACS Profile'. The 'Name' field contains 'WLC MONITOR' and the 'Description' field contains 'WLC MONITOR'. Below these fields are 'Task Attribute View' and 'Raw View' tabs. Under the 'Common Tasks' section, the 'Common Task Type' dropdown is set to 'WLC'. The radio button for 'Monitor' is selected. Below the radio buttons are checkboxes for 'WLAN', 'Controller', 'Wireless', 'Security', 'Management', and 'Commands', all of which are unselected. A note states: 'The configured options give a mgmtRole Debug value of: 0x0'. The 'Custom Attributes' section is empty.

Esiste un altro profilo predefinito **All** che consente l'accesso completo all'utente, come mostrato nell'immagine.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > PassiveID > Policy Elements. The left sidebar shows a tree view with 'TACACS Profiles' selected. The main content area is titled 'TACACS Profiles > WLC ALL' and 'TACACS Profile'. The 'Name' field contains 'WLC ALL' and the 'Description' field contains 'WLC ALL'. Below these fields are 'Task Attribute View' and 'Raw View' tabs. Under the 'Common Tasks' section, the 'Common Task Type' dropdown is set to 'WLC'. The radio button for 'All' is selected. Below the radio buttons are checkboxes for 'WLAN', 'Controller', 'Wireless', 'Security', 'Management', and 'Commands', all of which are unselected. A note states: 'The configured options give a mgmtRole Debug value of: 0xffffffff'. The 'Custom Attributes' section is empty.

Passaggio 6. Creare un set di criteri.

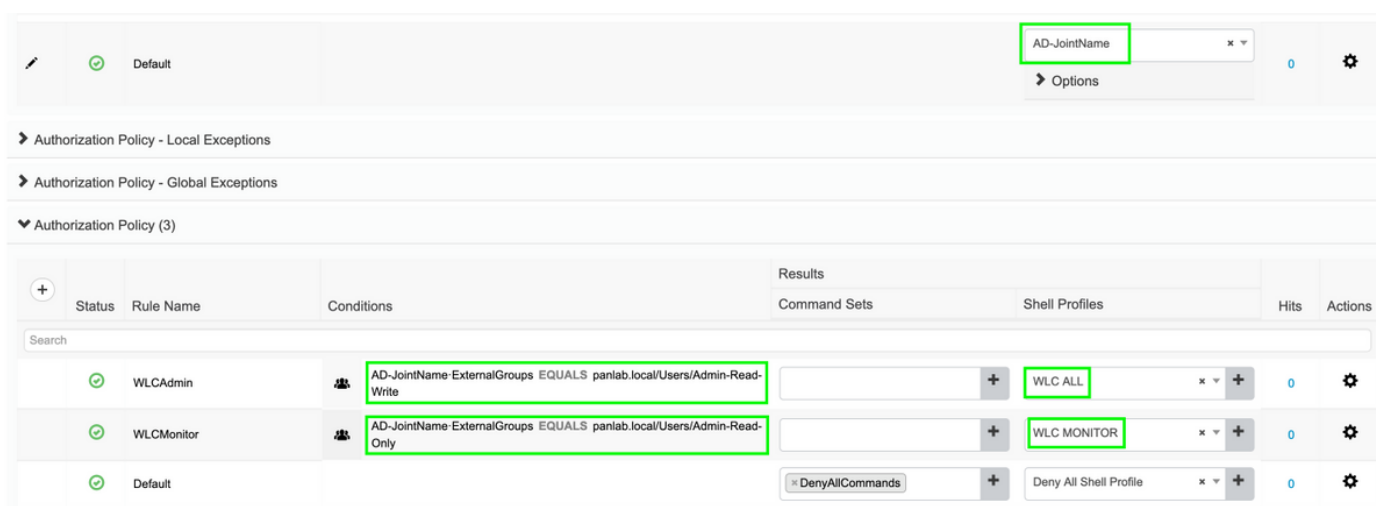
Passare a **Centri di lavoro > Amministrazione dispositivi > Set di criteri di amministrazione dispositivi**. Fare clic su (+) e assegnare un nome al set di criteri. Nella condizione del criterio selezionare **Device Type** as WLC, Allowed protocols can be **Default Device Admin**, come mostrato nell'immagine.



Passaggio 7. Creazione di criteri di autenticazione e autorizzazione.

In questo documento, due gruppi di esempio, **Admin-Read-Write** e **Admin-Read-Only** sono configurati su Active Directory e un utente all'interno di ogni gruppo **admin1**, **admin2** rispettivamente. Active Directory è integrato con ISE tramite un punto di unione denominato **AD-JointName**.

Creare due criteri di autorizzazione, come illustrato nell'immagine:



Passaggio 8. Configurare WLC per Device Administration.

Selezionare **Security > AAA > TACACS+** fare clic su **New (Nuova)** e aggiungere **Authentication (Autenticazione)**, **Accounting server**, come mostrato nell'immagine.

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

Modificare l'ordine di priorità e impostare TACACS+ in alto e Local in basso, come mostrato nell'immagine:

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.

Attenzione: Non chiudere la sessione GUI WLC corrente. Si consiglia di aprire la GUI del WLC in un browser Web diverso e verificare se l'accesso con le credenziali TACACS+ funziona o meno. In caso contrario, verificare la configurazione e la connettività al nodo ISE sulla porta TCP 49.

Verifica

Passare a **Operazioni > TACACS > Live Log** e monitorare i **Live Log**. Aprire l'interfaccia utente WLC e accedere con le credenziali utente di Active Directory, come mostrato nell'immagine

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

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

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.