

Apparaatbeheer van Cisco WLC met TACACS+

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configuratie](#)

[Stap 1. Controleer de licentie voor apparaatbeheer.](#)

[Stap 2. Schakel apparaatbeheer in op ISE PSN-knooppunten.](#)

[Stap 3. Maak een netwerkkapparaatgroep.](#)

[Stap 4. Voeg WLC als netwerkkapparaat toe.](#)

[Stap 5. Maak een TACACS-profiel voor WLC.](#)

[Stap 6. Maak een beleidsset.](#)

[Stap 7. Maak verificatie- en autorisatiebeleid.](#)

[Stap 8. Configureer de WLC voor apparaatbeheer.](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft hoe u TACACS+ kunt configureren voor apparaatbeheer van Cisco draadloze LAN-controller (WLC) met de Identity Services Engine (ISE).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van Identity Services Engine (ISE)
- Basiskennis van Cisco draadloze LAN-controller (WLC)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Identity Services Engine 2.4
- Cisco draadloze LAN-controller 8.5.135

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configuratie

Stap 1. Controleer de licentie voor apparaatbeheer.

Navigeer naar **Beheer > Systeem > Licentie** tabblad en controleer of de licentie voor **apparaatbeheer** is geïnstalleerd, zoals in de afbeelding wordt weergegeven.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes Home, Context Visibility, Operations, Policy, Administration (highlighted), and Work Centers. The main menu includes System, Identity Management, Network Resources, Device Portal Management, and pxGrid Services. The sub-menu includes Deployment, Licensing (highlighted), Certificates, Logging, Maintenance, Upgrade, Backup & Restore, Admin Access, and Settings.

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: Licensed :100 (Consumed :0)

Plus

Apex

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

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)

Opmerking: De licentie voor apparaatbeheer is vereist om de functie TACACS+ op ISE te kunnen gebruiken.

Stap 2. Schakel apparaatbeheer in op ISE PSN-knooppunten.

navigeren naar **werkcentra > Apparaatbeheer > Overzicht**, klik op tabblad **Plaatsing**, selecteer de radioknop **Specifieke PSN Node**. Apparaatbeheer op het ISE-knooppunt **inschakelen** door het **selectieteken** te selecteren en op **opslaan** te klikken, zoals in de afbeelding wordt weergegeven:

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 * ⓘ

Stap 3. Maak een netwerkapparaatgroep.

Als u WLC als netwerkapparaat in ISE wilt toevoegen, navigeer dan naar **Beheer > Netwerkbronnen > Netwerkgroepen > Alle apparaten**, maakt u een **nieuwe groep** voor WLC, zoals in de afbeelding wordt getoond:

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

<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

Stap 4. Voeg WLC als netwerkapparaat toe.

Blader naar **werkcentra > Apparaatbeheer > Netwerkbronnen > Netwerkapparaten**. Klik op **Add**, specificeer **Name**, **IP Address** en selecteer het Type APPARAAT als **WLC**, selecteer **TACACS+ Verificatie Instellingen** en specificeer de **Shared Secret-toets**, zoals getoond in de afbeelding:

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

Stap 5. Maak een TACACS-profiel voor WLC.

Navigeer naar **werkcentra > Apparaatbeheer > Beleids-elementen > Resultaten > TACACS profielen**. Klik op **Toevoegen** en geef een naam op. In het tabblad **Weergave** van de taakbalk selecteert u **WLC** voor **Type taak**. Er zijn standaardprofielen aanwezig waaruit **monitor** wordt geselecteerd om beperkte toegang tot gebruikers mogelijk te maken, zoals in de afbeelding wordt weergegeven.

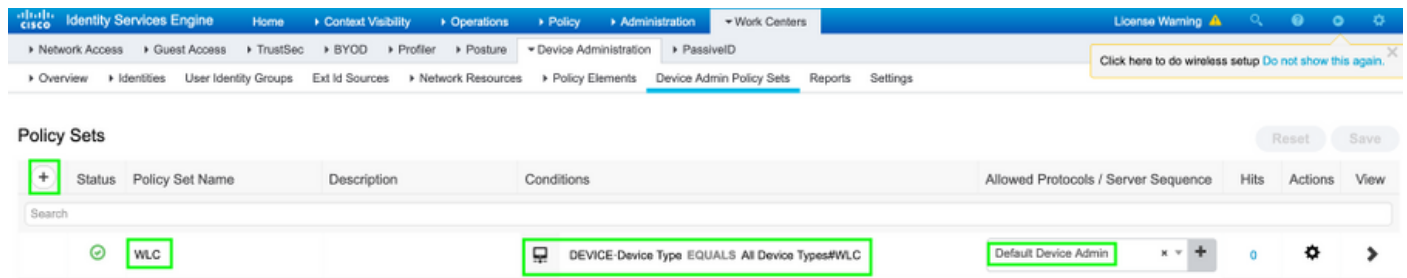
The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation path is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Policy Elements. The left sidebar shows a tree view with 'TACACS Profiles' 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 these fields are tabs for 'Task Attribute View' (selected) and 'Raw View'. Under the 'Common Tasks' section, 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.

Er is een ander standaardprofiel **All** dat volledige toegang tot de gebruiker mogelijk maakt zoals in de afbeelding wordt weergegeven.

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 these fields are tabs for 'Task Attribute View' (selected) and 'Raw View'. Under the 'Common Tasks' section, 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.

Stap 6. Maak een beleidsset.

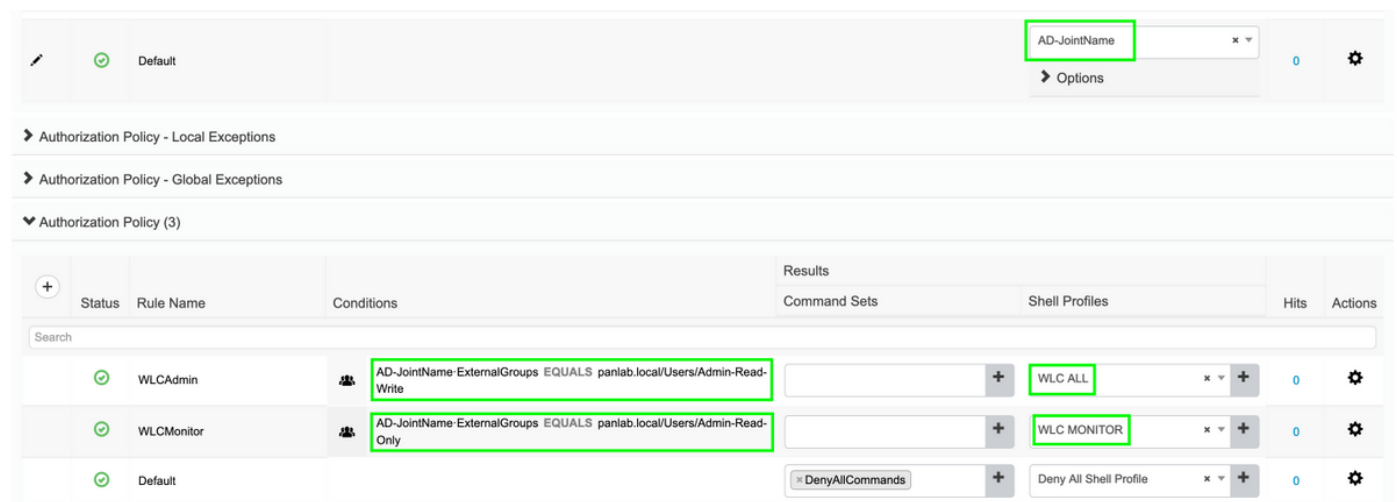
Blader naar **werkcentra > Apparaatbeheer > ApparaatAdmin Beleidssets**. Klik op (+) en geef een naam aan de Beleidsset. Selecteer in de beleidsconditie het **type apparaat** als WLC en de toegestane protocollen kunnen **standaard apparaatbeheer** zijn, zoals in de afbeelding.



Stap 7. Maak verificatie- en autorisatiebeleid.

In dit document worden twee voorbeeldgroepen **Admin-Read-Write** en **Admin-Read-Only** geconfigureerd op het actieve directoraat en één gebruiker in elke groep **admin1**, **admin2**. Actieve Map wordt met ISE geïntegreerd via een punt met de naam **AD-JointName**.

Maak twee autorisatiebeleid, zoals in de afbeelding:



Stap 8. Configureer de WLC voor apparaatbeheer.

Navigeren in op **Beveiliging > AAA > TACACS+** klik op **Nieuw** en voeg verificatie, accounting server toe zoals in de afbeelding weergegeven.

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

Wijzig prioriteitsvolgorde en maak TACACS+ op boven en lokaal tot onder, zoals in de afbeelding:

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.

Voorzichtig: Sluit de huidige WLC GUI-sessie niet. Aanbevolen wordt om WLC GUI in verschillende web-browser te openen en controleer of de inlognaam met TACACS+ referenties werkt of niet. Als dit niet het geval is, controleer de configuratie en connectiviteit met het ISE-knooppunt op TCP poort 49.

Verifiëren

Navigeer naar **bewerkingen > TACACS > Live loggen** en controleer de **Live Logs**. Open WLC GUI en log in met actieve gebruikersreferenties van de map, zoals in de afbeelding

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)

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.