

# Geräteadministration von Cisco WLC mit TACACS+

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfiguration](#)

[Schritt 1: Aktivieren Sie Device Administration License \(Gerätelizenz\).](#)

[Schritt 2: Aktivieren Sie die Geräteadministration auf ISE-PSN-Knoten.](#)

[Schritt 3: Erstellen einer Netzwerkgerätegruppe.](#)

[Schritt 4: Fügen Sie WLC als Netzwerkgerät hinzu.](#)

[Schritt 5: Erstellen Sie ein TACACS-Profil für WLC.](#)

[Schritt 6: Erstellen eines Policy Set](#)

[Schritt 7: Erstellen von Authentifizierungs- und Autorisierungsrichtlinien.](#)

[Schritt 8: WLC für die Geräteadministration konfigurieren.](#)

[Überprüfen](#)

[Fehlerbehebung](#)

## Einführung

In diesem Dokument wird beschrieben, wie TACACS+ für die Geräteadministration von Cisco Wireless LAN Controller (WLC) mit der Identity Service Engine (ISE) konfiguriert wird.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundkenntnisse der Identity Service Engine (ISE)
- Grundkenntnisse des Cisco Wireless LAN Controller (WLC)

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

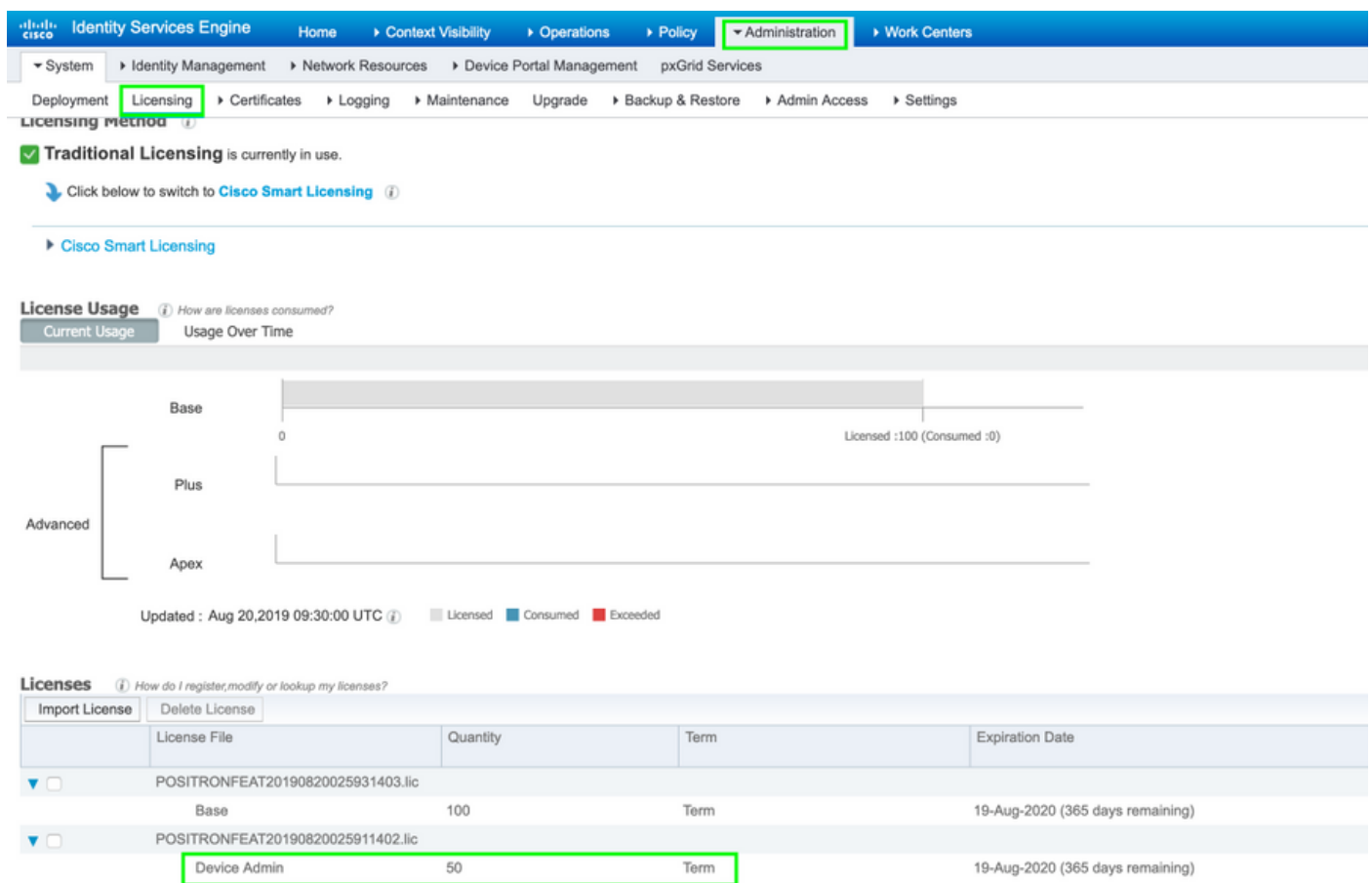
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren

(Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Konfiguration

### Schritt 1: Aktivieren Sie Device Administration License (Gerätelizenz).

Navigieren Sie zur Registerkarte **Administration > System > Licensing** (Administration > System > Lizenzierung), und überprüfen Sie, ob die **Device Admin**-Lizenz installiert ist, wie im Bild gezeigt.



**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 Legend: Licensed (grey), Consumed (blue), Exceeded (red)

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

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)

**Hinweis:** Für die Verwendung der TACACS+-Funktion auf der ISE ist eine Device Admin-Lizenz erforderlich.

### Schritt 2: Aktivieren Sie die Geräteadministration auf ISE-PSN-Knoten.

Navigieren Sie zu **Work Centers > Device Administration > Overview**, klicken Sie auf die Registerkarte **Deployment**, wählen Sie das Optionsfeld **Specific PSN Node** (Spezifischer PSN-Knoten). **Aktivieren Sie** die Geräteadministration auf dem ISE-Knoten, indem Sie das **Kontrollkästchen aktivieren** und auf **Speichern** klicken, wie im Bild gezeigt:

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 \*  ⓘ

### Schritt 3: Erstellen einer Netzwerkgerätegruppe.

Um WLC als Netzwerkgerät zur ISE hinzuzufügen, wählen Sie **Administration > Network Resources > Network Device Groups > All Device Types (Verwaltung > Netzwerkressourcen > Netzwerkgerätegruppen > Alle Gerätetypen)**, erstellen Sie eine neue Gruppe für WLC, wie im Bild gezeigt:

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

### Schritt 4: Fügen Sie WLC als Netzwerkgerät hinzu.

Navigieren Sie zu **Work Centers > Device Administration > Network Resources > Network Devices**. Klicken Sie auf **Hinzufügen**, geben Sie **Name**, **IP-Adresse** an, wählen Sie den Gerätetyp als **WLC** aus, aktivieren Sie das **Kontrollkästchen TACACS+ Authentication Settings (TACACS+-Authentifizierungseinstellungen)**, und stellen Sie den Schlüssel für den gemeinsamen geheimen Schlüssel bereit, wie im Bild gezeigt:

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

## Schritt 5: Erstellen Sie ein TACACS-Profil für WLC.

Navigieren Sie zu **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles**. Klicken Sie auf **Hinzufügen**, und geben Sie einen **Namen** an. Wählen Sie auf der Registerkarte **Aufgabenattribut-Ansicht WLC** für **allgemeinen Aufgabentyp** aus. Es sind Standardprofile vorhanden, aus denen **Monitor** ausgewählt wird, um den Benutzern eingeschränkten Zugriff zu ermöglichen, wie im Bild gezeigt.

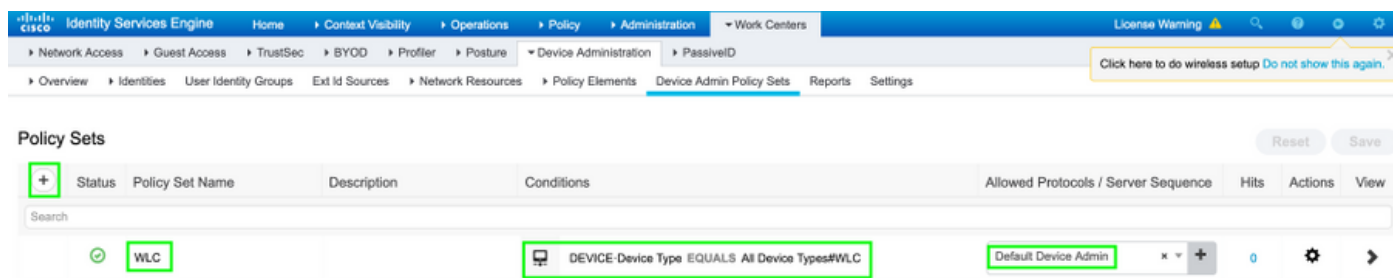
The screenshot shows the Cisco Identity Services Engine (ISE) interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Policy Elements. The left sidebar shows a tree view with 'TACACS Profiles' selected. The main content area displays the configuration for a TACACS Profile named 'WLC MONITOR'. The 'Name' and 'Description' fields both contain '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 radio button selection is shown with 'Monitor' selected. Below the radio buttons are several checkboxes: 'WLAN', 'Controller', 'Wireless', 'Security', 'Management', and 'Commands', all of which are currently unchecked. 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 empty.

Es gibt ein anderes Standardprofil **All**, das den vollen Zugriff auf den Benutzer ermöglicht, wie im Bild gezeigt.

The screenshot shows the Cisco Identity Services Engine (ISE) interface for a different TACACS Profile. The breadcrumb navigation 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 a TACACS Profile named 'WLC ALL'. The 'Name' and 'Description' fields both contain '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 radio button selection is shown with 'All' selected. Below the radio buttons are several checkboxes: 'WLAN', 'Controller', 'Wireless', 'Security', 'Management', and 'Commands', all of which are currently unchecked. A note at the bottom of this section states: 'The configured options give a mgmtRole Debug value of: 0xffffffff'. The 'Custom Attributes' section is visible at the bottom but empty.

## Schritt 6: Erstellen eines Policy Set

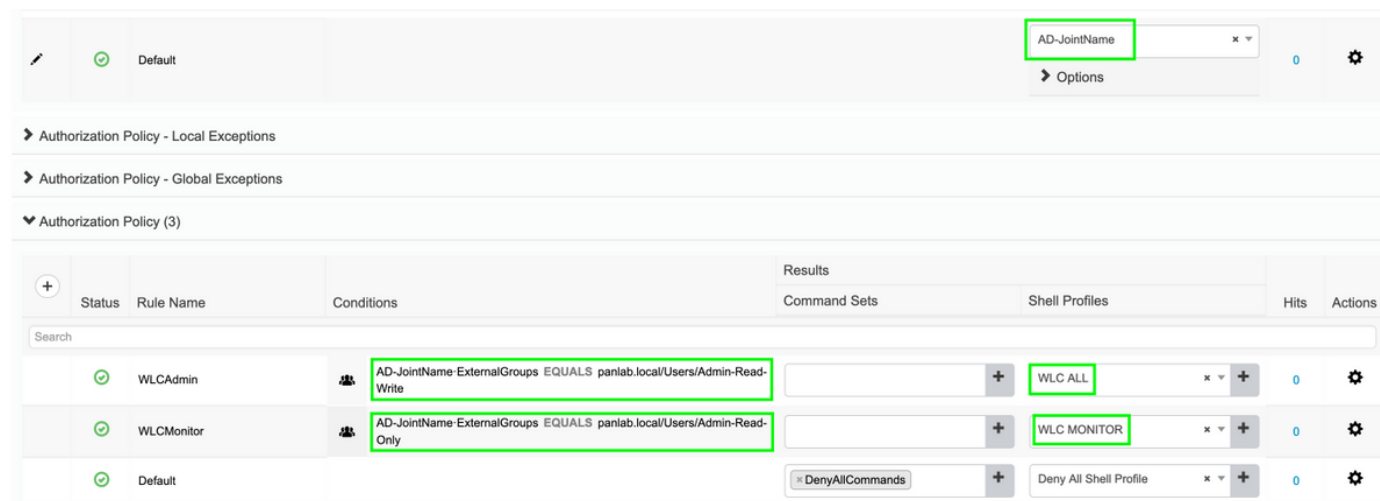
Navigieren Sie zu **Work Center > Device Administration > Device Admin Policy Sets (Geräteverwaltung > Geräte-Admin-Richtliniensätze)**. Klicken Sie auf (+), und geben Sie dem Policy Set einen Namen. Wählen Sie in der Richtlinienbedingung **Gerätetyp** als WLC aus. Zulässige Protokolle können **Standardgerätadministrator** sein, wie im Bild gezeigt.



## Schritt 7: Erstellen von Authentifizierungs- und Autorisierungsrichtlinien.

In diesem Dokument werden zwei Beispielgruppen **Admin-Read-Write** und **Admin-Read-Only** im Active Directory und ein Benutzer in jeder Gruppe **admin1**, **admin2** konfiguriert. Active Directory ist über einen Joinpoint namens **AD-JointName** in die ISE integriert.

Erstellen Sie zwei Autorisierungsrichtlinien, wie im Bild gezeigt:



## Schritt 8: WLC für die Geräteadministration konfigurieren.

Navigieren Sie zu **Security > AAA > TACACS+** klicken Sie auf **New**, und fügen Sie, wie im Bild gezeigt, den Authentication, Accounting Server hinzu.

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

Ändern Sie die Prioritätsreihenfolge, und machen Sie TACACS+ oben und lokal nach unten, wie im Bild gezeigt:

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.*



**Vorsicht:** Schließen Sie die aktuelle GUI-Sitzung des WLC nicht. Es wird empfohlen, die WLC-GUI in einem anderen Webbrowser zu öffnen und zu überprüfen, ob die Anmeldung mit TACACS+-Anmeldeinformationen funktioniert. Falls nicht, überprüfen Sie die Konfiguration und die Verbindung zum ISE-Knoten am TCP-Port 49.

## Überprüfen

Navigieren Sie zu **Operations > TACACS > Live logs (Vorgänge > TACACS > Live-Protokolle)**, und überwachen Sie die **Live Logs (Live-Protokolle)**. Öffnen Sie die WLC-GUI, und melden Sie sich mit den Anmeldeinformationen des Active Directory-Benutzers an, wie im Bild gezeigt.

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)

## Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.