

TACACS+を使用したCisco WLCのデバイス管理

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[コンフィギュレーション](#)

[ステップ1:\[Device Administration License\]を確認します。](#)

[ステップ2:ISE PSNノードでデバイス管理を有効にします。](#)

[ステップ3：ネットワークデバイスグループを作成します。](#)

[手順4：ネットワークデバイスとしてWLCを追加します。](#)

[手順5:WLCのTACACSプロファイルを作成します。](#)

[ステップ6：ポリシーセットを作成します。](#)

[ステップ7：認証および許可ポリシーを作成します。](#)

[手順8：デバイス管理用のWLCの設定](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、Identity Service Engine(ISE)を使用してCisco Wireless LAN Controller(WLC)のデバイス管理用にTACACS+を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Identity Service Engine(ISE)の基礎知識
- Cisco Wireless LAN Controller(WLC)に関する基礎知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

コンフィギュレーション

ステップ1:[Device Administration License]を確認します。

図に示すように、[Administration] > [System] > [Licensing]タブに移動し、[Device Admin]ライセンスがインストールされていることを確認します。

The screenshot displays the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Administration' and 'Work Centers'. The 'Licensing' tab is selected. A message indicates 'Traditional Licensing is currently in use.' Below this, the 'License Usage' section shows a bar chart for 'Base' licenses with 100 licensed and 0 consumed. The 'Licenses' table below shows a 'Device Admin' license with a quantity of 50, 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)

注：ISEでTACACS+機能を使用するには、デバイス管理ライセンスが必要です。

ステップ2:ISE PSNノードでデバイス管理を有効にします。

[Work Centers] > [Device Administration] > [Overview]に移動し、[Deployment]タブをクリックし、[Select the Specific PSN Node]オプションボタンをクリックします。図に示すように、ISEノードでDevice Administrationを有効にするには、チェックボックスを選択し、[save]をクリックします。

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

ステップ3 : ネットワークデバイスグループを作成します。

WLCをISE上のネットワークデバイスとして追加するには、次の図に示すように、**[Administration] > [Network Resources] > [Network Device Groups] > [All Device Types]**に移動して、WLCの新しいグループを作成します。

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

手順4：ネットワークデバイスとしてWLCを追加します。

[Work Centers] > [Device Administration] > [Network Resources] > [Network Devices] に移動します。[Add] をクリックし、[Name]、[IP Address]を指定し、[Device type]を[WLC]に選択し、[TACACS+ Authentication Settings]チェックボックスをオンにして、[Shared Secret]キーを指定します（図を参照）。

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

手順5:WLCのTACACSプロファイルを作成します。

[Work Centers] > [Device Administration] > [Policy Elements] > [Results] > [TACACS Profiles]に移動します。[Add]をクリックし、[Name]を指定します。[Task]属性ビュータブで、[Common Task Type]に[WLC]を選択します。図に示すように、[Monitor]を選択するデフォルトのプロファイルが存在します。

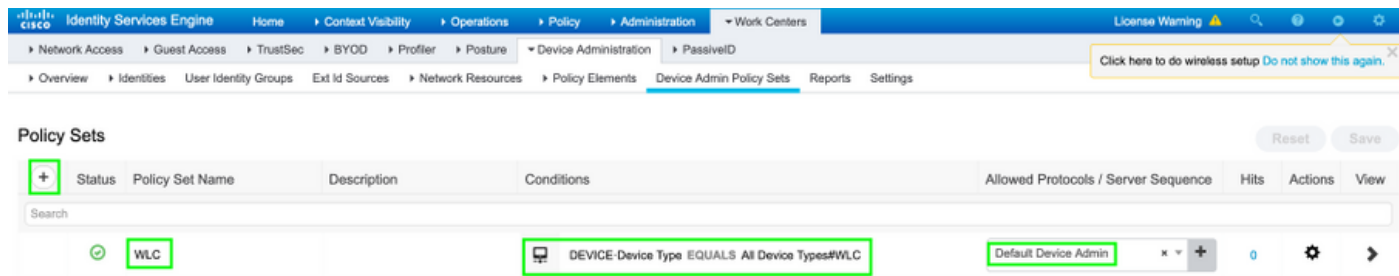
The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Policy Elements. The left sidebar shows a tree view with 'TACACS Profiles' selected. The main content area is titled 'TACACS Profiles > WLC MONITOR' and 'TACACS Profile'. The 'Name' field is 'WLC MONITOR' and the 'Description' field is 'WLC MONITOR'. Below this, there are tabs for 'Task Attribute View' (selected) and 'Raw View'. Under 'Common Tasks', the 'Common Task Type' is set to 'WLC'. The 'Monitor' radio button is selected, while 'All', 'Lobby', and 'Selected' are unselected. Below the radio buttons are several checkboxes: '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'. At the bottom, there is a section for 'Custom Attributes'.

図に示すように、ユーザへのフルアクセスを許可する別のデフォルトプロファイル[All]があります。

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 left sidebar shows 'TACACS Profiles' selected. The main content area is titled 'TACACS Profiles > WLC ALL' and 'TACACS Profile'. The 'Name' field is 'WLC ALL' and the 'Description' field is 'WLC ALL'. Below this, there are tabs for 'Task Attribute View' (selected) and 'Raw View'. Under 'Common Tasks', the 'Common Task Type' is set to 'WLC'. The 'All' radio button is selected, while 'Monitor', 'Lobby', and 'Selected' are unselected. Below the radio buttons are several checkboxes: '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'. At the bottom, there is a section for 'Custom Attributes'.

ステップ6 : ポリシーセットを作成します。

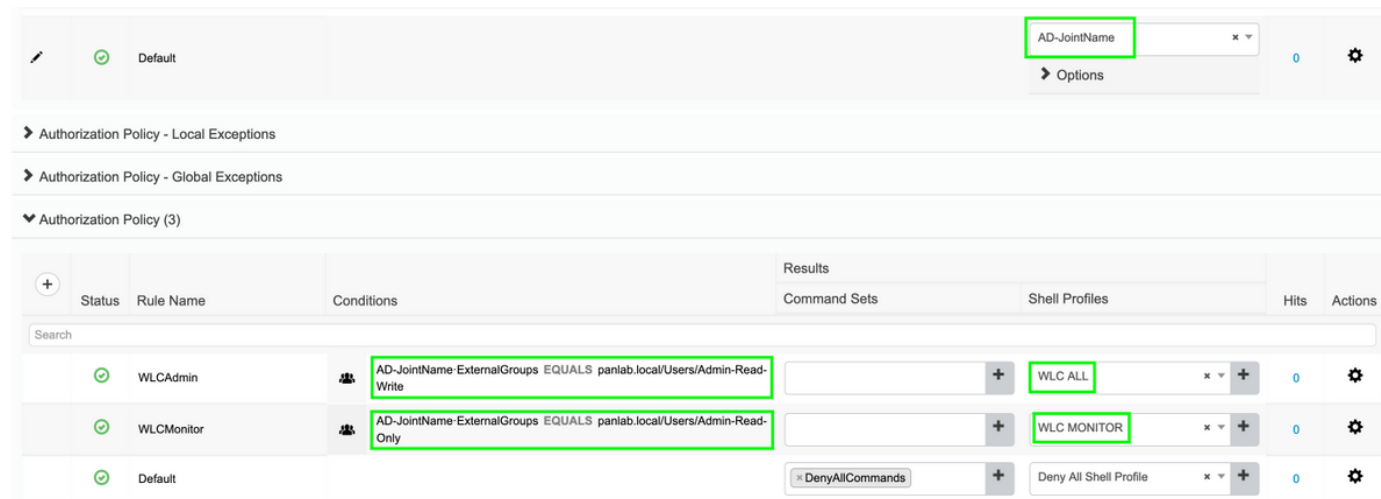
[ワークセンター] > [デバイス管理] > [デバイス管理ポリシーセット]に移動します。(+)をクリックし、ポリシーセットに名前を付けます。ポリシー条件で、[Device Type]に[WLC]を選択します。図に示すように、[Allowed protocols]は[Default Device Admin]にすることができます。



ステップ7：認証および許可ポリシーを作成します。

このドキュメントでは、2つのサンプルグループ **Admin-Read-Write** と **Admin-Read-Only** が Active Directory に設定され、各グループ **admin1**、**admin2** にそれぞれ1人のユーザが設定されています。Active Directory は、**AD-JointName** という名前のジョイントポイントを介して ISE と統合されています。

図に示すように、2つの認可ポリシーを作成します。



手順8：デバイス管理用のWLCの設定

図に示すように、[Security] > [AAA] > [TACACS+]に移動し、[New]をクリックして、認証、アカウントングサーバを追加します。

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

次の図に示すように、優先順位を変更し、TACACS+を上、ローカルを下にします。

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.

注意：現在のWLC GUIセッションを閉じないでください。異なるWebブラウザでWLC GUIを開き、TACACS+クレデンシャルを使用したログインが機能するかどうかを確認することをお勧めします。そうでない場合は、TCPポート49のISEノードの設定と接続を確認します。

確認

[Operations] > [TACACS] > [Live logs]に移動し、ライブログを監視します。図に示すように、WLC GUIを開き、Active Directoryユーザクレデンシャルでログインします

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)

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。