

Administração de dispositivo do Cisco WLC usando TACACS+

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configuração](#)

[Etapa 1. Verifique a licença de administração do dispositivo.](#)

[Etapa 2. Ative a administração de dispositivos em nós PSN do ISE.](#)

[Etapa 3. Crie um grupo de dispositivos de rede.](#)

[Etapa 4. Adicione a WLC como um dispositivo de rede.](#)

[Etapa 5. Crie um perfil TACACS para WLC.](#)

[Etapa 6. Criar um Conjunto de Políticas.](#)

[Passo 7. Criar Políticas de Autenticação e Autorização.](#)

[Etapa 8. Configurar o WLC para a administração do dispositivo.](#)

[Verificar](#)

[Troubleshoot](#)

Introduction

Este documento descreve como configurar o TACACS+ para a administração de dispositivos do Cisco Wireless LAN Controller (WLC) com o Identity Service Engine (ISE).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico do Identity Service Engine (ISE)
- Conhecimento básico do Cisco Wireless LAN Controller (WLC)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Identity Service Engine 2.4
- Controladora de LAN sem fio Cisco 8.5.135

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuração

Etapa 1. Verifique a licença de administração do dispositivo.

Navegue até **Administration > System > Licensing** tab e verifique se a licença do **Device Admin** está instalada, como mostrado na imagem.

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?

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)

Note: A licença de administrador de dispositivo é necessária para usar o recurso TACACS+ no ISE.

Etapa 2. Ative a administração de dispositivos em nós PSN do ISE.

Navegue até **Centros de trabalho > Administração do dispositivo > Visão geral**, clique na guia **Implantação**, selecione o botão de opção **Nó PSN** específico. **Ative** a Administração de dispositivos no nó ISE marcando a **caixa de seleção** e clique em **salvar**, como mostrado na imagem:

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 type="checkbox"/> ISE Nodes
<input checked="" type="checkbox"/> ISE-PSN.panlab.local

Only ISE Nodes with Policy Service are displayed.

TACACS Ports * 49 ⓘ

Etapa 3. Crie um grupo de dispositivos de rede.

Para adicionar a WLC como um dispositivo de rede no ISE, navegue para **Administration > Network Resources > Network Device Groups > All Device Types**, crie um novo grupo para a WLC, como mostrado na imagem:

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

Etapa 4. Adicione a WLC como um dispositivo de rede.

Navegue até **Centros de trabalho > Administração de dispositivos > Recursos de rede > Dispositivos de rede**. Clique em Adicionar, fornecer nome, endereço IP e selecione o tipo de dispositivo como **WLC**, marque a caixa de seleção **TACACS+ Authentication Settings** e forneça a chave do **segredo compartilhado**, como mostrado na imagem:

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

Etapa 5. Crie um perfil TACACS para WLC.

Navegue até **Centros de trabalho > Administração de dispositivos > Elementos de política > Resultados > Perfis TACACS**. Clique em **Adicionar** e forneça um **Nome**. Na guia **Exibição de atributo de tarefa**, selecione **WLC** para **Tipo de tarefa comum**. Há perfis padrão presentes a partir dos quais selecione **Monitor** para permitir acesso limitado aos usuários, como mostrado na imagem.

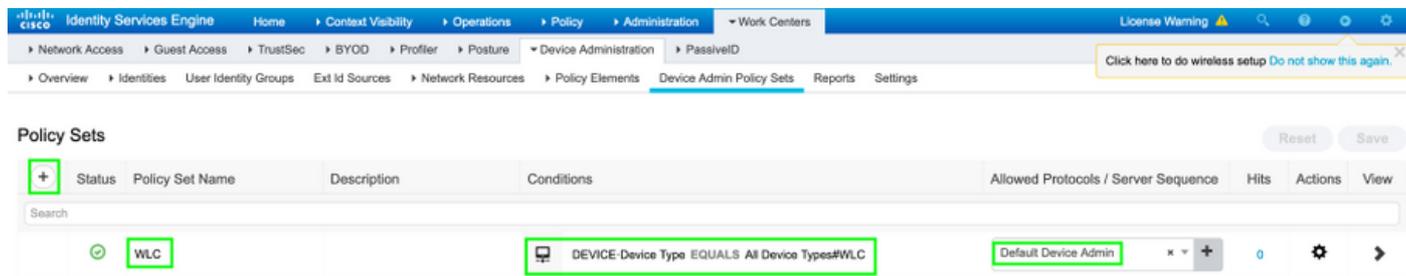
The screenshot shows the Cisco Identity Services Engine (ISE) interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Policy Elements. The left sidebar shows a tree view with 'TACACS Profiles' selected. The main content area displays the configuration for a TACACS Profile named 'WLC MONITOR'. The 'Name' and 'Description' fields are both set to 'WLC MONITOR'. Below the profile name, there are two tabs: '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 is shown, with 'Monitor' selected. Below the radio buttons, there 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 is empty.

Há outro perfil padrão **All** que permite acesso total ao usuário como mostrado na imagem.

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 ALL'. The 'Name' and 'Description' fields are both set to 'WLC ALL'. Below the profile name, there are two tabs: '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 is shown, with 'All' selected. Below the radio buttons, there 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: 0xffffffff8'. The 'Custom Attributes' section is visible at the bottom but is empty.

Etapa 6. Criar um Conjunto de Políticas.

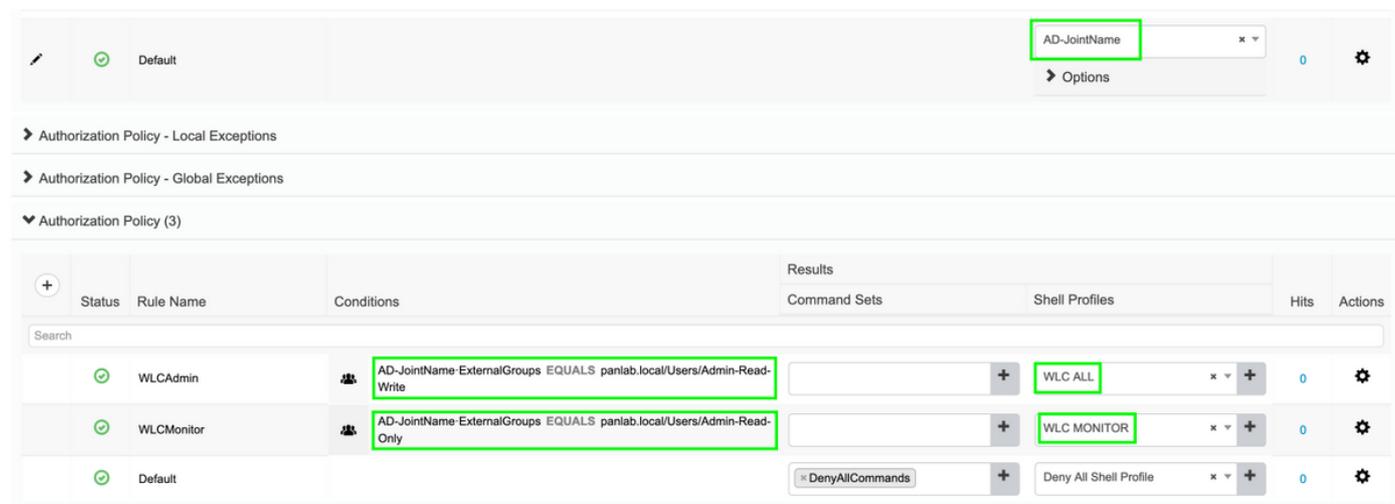
Navegue até **Centros de trabalho > Administração de dispositivos > Conjuntos de políticas de administração de dispositivos**. Clique em (+) e atribua um nome ao Conjunto de políticas. Na condição da política, selecione **Tipo de dispositivo** como WLC, os protocolos permitidos podem ser **Administrador de dispositivo padrão**, como mostrado na imagem.



Passo 7. Criar Políticas de Autenticação e Autorização.

Neste documento, dois grupos de exemplo **Admin-Read-Write** e **Admin-Read-Only** são configurados no Active Directory e um usuário dentro de cada grupo **admin1**, **admin2** respectivamente. O Active Directory está integrado ao ISE por meio de um ponto de conexão chamado **AD-JointName**.

Crie duas políticas de autorização, como mostrado na imagem:



Etapa 8. Configurar o WLC para a administração do dispositivo.

Navegue até **Security > AAA > TACACS+** clique em **New** e adicione Authentication, Accounting server, como mostrado na imagem.

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

Altere a ordem de prioridade e faça TACACS+ na parte superior e Local para baixo, como mostrado na imagem:

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

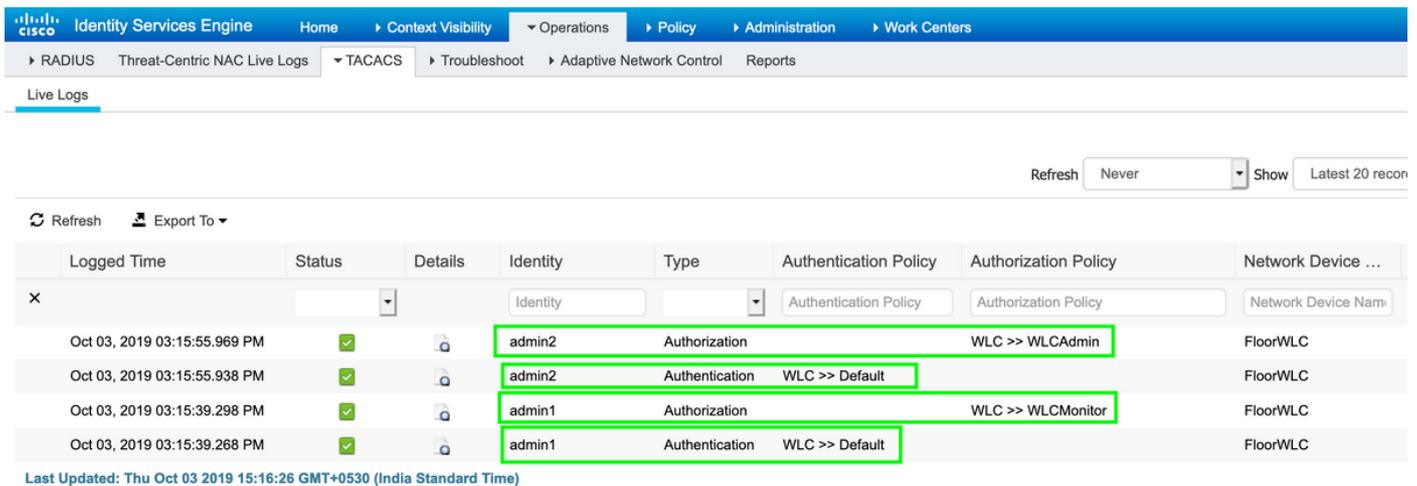
TACACS+ LOCAL Up Down

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

Caution: Não feche a sessão atual da GUI do WLC. Recomenda-se abrir a GUI do WLC em diferentes navegadores da Web e verificar se o login com credenciais TACACS+ funciona ou não. Caso contrário, verifique a configuração e a conectividade com o nó ISE na porta TCP 49.

Verificar

Navegue até **Operations > TACACS > Live logs** e monitore os **Live Logs**. Abra a GUI do WLC e faça login com as credenciais do usuário do Ative Directory, como mostrado na imagem



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)

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.