

Configure RADIUS and TACACS+ for GUI and CLI Authentication on 9800 Wireless LAN Controllers

Contents

[Introduction](#)

[Background Information](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configurations](#)

[RADIUS WLC configuration](#)

[RADIUS ISE configuration](#)

[Tacacs+ WLC configuration](#)

[Tacacs+ ISE configuration](#)

[Troubleshooting](#)

Introduction

This document describes how to configure a 9800 Wireless LAN Controllers (WLC) for RADIUS or TACACS+ external authentication when accessing its Graphic User Interface (GUI) or Command Line Interface (CLI).

Background Information

When an user is trying to access the CLI or the GUI of the WLC, it will be prompted to input a username and password.

By default these credentials are compared against the local database of users, which is present on device itself.

Alternatively the WLC can be instructed to compare the input credentials against a remote AAA server: the WLC can either talk to the server using RADIUS or TACACS+.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Catalyst Wireless 9800 configuration model
- AAA, RADIUS and TACACS+ concepts

Components Used

The information in this document is based on these software and hardware versions:

- C9800-CL v16.10
- ISE 2.2.0

Configurations

In this example we will configure two types of users on the AAA server (ISE), respectively 'adminuser' and 'helpdeskuser'.

The user 'adminuser' is expected to be granted full access to the WLC, whereas the 'helpdeskuser' is meant to only be granted monitor privileges to the WLC, hence no configuration access.

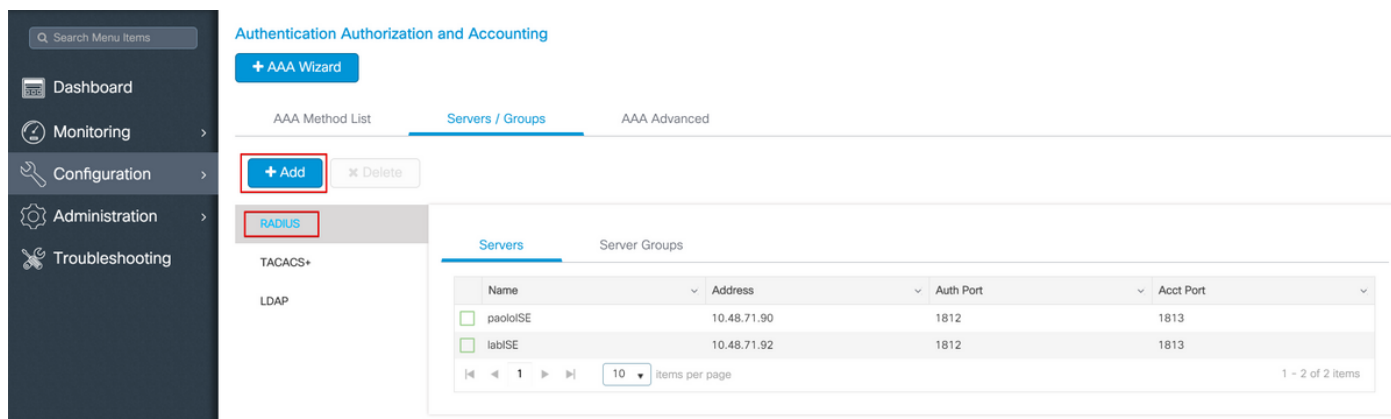
First we will do the configurations on the WLC and on ISE for a RADIUS authentication, and later we will do the same for TACACS+.

RADIUS WLC configuration

Step 1. Declare the RADIUS server

First of all we need to create the RADIUS server ISE on the WLC.

This can be done from the GUI WLC page <https://<WLC-IP>/webui/#/aaa> :



A popup window will open, where you can type the server name (it does not have to match the ISE system name), its IP address, the shared secret, and the port being used for authentication and accounting, along with other parameters.

From CLI:

```
paolo-9800(config)#radius server labISE
paolo-9800(config-radius-server)# address ipv4 10.48.71.92 auth-port 1812 acct-port 1813
paolo-9800(config-radius-server)# key Cisco123
```

Step 2. Map the RADIUS server to a Server Group

In case you have multiple RADIUS servers that can be used for authentication, it is recommended to map all these servers to the same Server Group: the WLC will then take care of load balancing

different authentications among the servers in the server group.

From the same GUI tab:

Authentication Authorization and Accounting

+ AAA Wizard

AAA Method List **Servers / Groups** AAA Advanced

+ Add ✕ Delete

RADIUS

TACACS+

LDAP

Servers **Server Groups**

Name	Server 1
AAAServers	paoloISE
radGroup	labISE

1 10 items per page

In the popup, give a name to the group, and move the desired servers to the Assigned list.

From CLI:

```
paolo-9800(config)#aaa group server radius radGroup  
paolo-9800(config-sg-radius)# server name labISE
```

Step 3. Create a AAA authentication login method pointing to the RADIUS server group

Always in the GUI page <https://<WLC-IP>/webui/#/aaa> , move to the AAA Method list tab, and create the Authentication method:

Authentication Authorization and Accounting

+ AAA Wizard

AAA Method List Servers / Groups AAA Advanced

General

Authentication

Authorization

Accounting

+ Add ✕ Delete

Name	Type	Group Type	Group1
tacAuthMethod	login	local	tacGroup
radAuthMethod	login	local	radGroup
default	dot1x	local	N/A

1 10 items per page

In the popup, give a name to the method, choose type as 'login', and assign the group server created in the previous step.

Note:

- if you select Group Type as 'local' the WLC will first check the if the user exists locally, and will

then fallback to the server group

CLI:

```
paolo-9800(config)#aaa authentication login radAuthMethod local group radGroup
```

- If you select Group Type as 'group', and no fallback to local option checked, the WLC will just check the user against the server group

CLI:

```
paolo-9800(config)#aaa authentication login radAuthMethod group radGroup
```

- If you select Group Type as 'group', and the fallback to local option is checked, the WLC will check the user against the server group, and will query the local database only if the server is not responding: if the server sends a reject, the user won't be authenticated, even though it may exists on the local database

CLI:

```
paolo-9800(config)#aaa authentication login radAuthMethod group radGroup local
```

In this example setup, we have some users which are only created locally, and some users only on the ISE server, hence we use the first option.

Step 4. Create a AAA authorization exec method pointing to the RADIUS server group

The user has to be also authorized in order to be granted access. From the same tab:

The screenshot shows the Cisco ISE GUI for 'Authentication Authorization and Accounting'. The 'AAA Method List' tab is active. On the left, the 'Configuration' menu is expanded, and 'Authorization' is selected. In the main area, the 'General' tab is selected. A '+ Add' button is highlighted with a red box. Below it, a table lists the configured methods:

	Name	Type	Group Type	Group1
☐	tacAuthzMethod	exec	local	tacGroup
☐	radAuthzMethod	exec	local	radGroup
☐	default	credential-download	local	N/A

At the bottom, there are pagination controls showing '1' of 1 items per page.

Use the same order of local/group being used for the authentication method in the previous step, and choose type as 'exec'.

From CLI:

```
paolo-9800(config)#aaa authorization exec radAuthzMethod local group radGroup
```

Step 5. Assign the methods to the HTTP configurations and to the VTY lines used for Telnet/SSH

These steps cannot be done from GUI, hence they need to be done from CLI.

- For the GUI authentication:

```
paolo-9800(config)#aaa authorization exec radAuthzMethod local group radGroup
```

- For Telnet/SSH authentication:

```
paolo-9800(config)#aaa authorization exec radAuthzMethod local group radGroup
```

Note: when doing changes to the the HTTP configurations, it is best to restart the HTTP and HTTPS services:

```
paolo-9800(config)#aaa authorization exec radAuthzMethod local group radGroup
```

RADIUS ISE configuration

Step 1. Configure the WLC as network device for RADIUS:

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration' (highlighted), and 'Work Centers'. The left sidebar shows 'Network Devices' under 'Network Resources'. The main content area is titled 'Network Devices' and contains a table with the following data:

Name	IP/Mask	Profile Name	Location	Type	Description
paolo-9800-71	10.48.71.91/32	Cisco	All Locations	All Device Types	

In the new window, add the IP address, select RADIUS, and type the same shared secret used on the WLC.

Step 2. Create an authorization result, to return the privilege

In order to do do configurations, 'adminuser' needs to have a privilege level of 15, which will allow to access the exec prompt shell.

The other user instead, 'helpdeskuser' will not need exec prompt shell access, and it can be assigned a privilege level lower than 15.

To do so, create an authorization profile result for 'adminuser':

The screenshot shows the Cisco ISE Policy configuration page. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy' (highlighted), 'Administration', and 'Work Centers'. The left sidebar shows 'Authorization' under 'Policy Elements'. The main content area is titled 'Standard Authorization Profiles' and contains a table with the following data:

Name	Profile
9800_admin_priv	Cisco
9800_helpdesk_priv	Cisco

Especially, the profile for 'adminuser' has to look like:

Authorization Profile

* Name

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco +

Service Template ☐

Track Movement ☐ i

Passive Identity Tracking ☐ i

Common Tasks

Advanced Attributes Settings

Cisco:cisco-av-pair = shell:priv-lvl=15

+

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = shell:priv-lvl=15

Create then a similar one for the 'helpdeskuser', changing only the string 'shell:priv-lvl=15' to 'shell:priv-lvl=X', and replace X with the desired privilege level.

In this example, we use 1.

Step 3. Create the users on ISE:

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

Identities
Groups
External Identity Sources
Identity Source Sequences
Settings

Users

Network Access Users

Edit
+ Add
Change Status
Import
Export
Delete
Duplicate

Status	Name	Description	First Name	Last Name
☐ ✔ Enabled	adminuser			
☐ ✔ Enabled	helpdeskuser			

The credentials given to the users will be the ones that you will type in the WLC later when authenticating.

Step 4. Authenticate the users:

In this scenario the default authentication policy rule of ISE preconfigured is already allowing default network access, hence there is no need to change it:

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication. For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Policy Type ☐ Simple ☒ Rule-Based

Status	Protocol	Condition	Action
✓	MAB	: If Wired_MAB OR	
	Wireless_MAB	Allow Protocols : Default Network Access and	
✓	Default	:use Internal Endpoints	
✓	Dot1X	: If Wired_802.1X OR	
	Wireless_802.1X	Allow Protocols : Default Network Access and	
✓	Default	:use All_User_ID_Stores	
✓	Default Rule (If no match)	: Allow Protocols : Default Network Access and use : All_User_ID_Stores	

Step 5. Authorize the users:

After the login attempt passes the authentication policy, it needs to be authorized, and ISE needs to return the authorization profile created earlier (permit accept, along with the privilege level).

In this example, we filter the login attempt based on the device IP address (which is the WLC IP address), and distinguish the privilege level to be granted based on the username.

Another valid approach would be to assign all the admin users to a certain group, and to grant privilege level 15 only to the users belonging to such group.

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order. For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

First Matched Rule Applies

► Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	9800_adminuser	if (Network Access:Device IP Address EQUALS 10.48.71.91 AND Radius:Service-Type EQUALS Outbound AND Network Access:UserName EQUALS adminuser)	then 9800_admin_priv
✓	9800_helpdeskuser	if (Network Access:Device IP Address EQUALS 10.48.71.91 AND Radius:Service-Type EQUALS Outbound AND Network Access:UserName EQUALS helpdeskuser)	then 9800_helpdesk_priv

Tacacs+ WLC configuration

Step 1. Declare the Tacacs+ server

First of all we need to create the Tacacs+ server ISE on the WLC.

This can be done from the GUI WLC page <https://<WLC-IP>/webui/#/aaa> :

Name	Server Address	Port
labISE	10.48.71.92	49

10 items per page

1 - 1 of 1 items

A popup window will open, where you can type the server name (it does not have to match the ISE system name), its IP address, the shared key, and the port being used and the timeout.

From CLI:

```
paolo-9800(config)#aaa authorization exec radAuthzMethod local group radGroup
```

Step 2.Map the Tacacs+ server to a Server Group

In case you have multiple Tacacs+ servers that can be used for authentication, it is recommended to map all these servers to the same Server Group: the WLC will then takes care of load balancing different authentications among the servers in the server group.

From the same GUI tab:

Name	Server 1	Server 2	Server 3
tacGroup	labISE	N/A	N/A

10 items per page

In the popup, give a name to the group, and move the desired servers to the Assigned list.

From CLI:

```
paolo-9800(config)#aaa authorization exec radAuthzMethod local group radGroup
```

Step 3.Create a AAA authentication login method pointing to the Tacacs+ server group

Always in the GUI page <https://<WLC-IP>/webui/#/aaa> , move to the AAA Method list tab, and create the Authentication method:

Name	Type	Group Type	Group1	Group2	Group3	Group4
default	login	local	N/A	N/A	N/A	N/A
localwebauth	login	local	N/A	N/A	N/A	N/A
tacAuthMethod	login	local	tacGroup	N/A	N/A	N/A
radAuthMethod	login	local	radGroup	N/A	N/A	N/A
default	dot1x	local	radGroup	N/A	N/A	N/A

10 items per page

1 - 5 of 5 items

In the popup, give a name to the method, choose type as 'login', and assign the group server created in the previous step.

Note:

- if you select Group Type as 'local' the WLC will first check the if the user exists locally, and will then fallback to the server group

CLI:

```
paolo-9800(config)#aaa authorization exec radAuthzMethod local group radGroup
```

- If you select Group Type as 'group', and no fallback to local option checked, the WLC will just check the user against the server group

CLI:

```
paolo-9800(config)#aaa authorization exec radAuthzMethod local group radGroup
```

- If you select Group Type as 'group', and the fallback to local option is checked, the WLC will check the user against the server group, and will query the local database only if the server is not responding: if the server sends a reject, the user won't be authenticated, even though it may exist on the local database

CLI:

```
paolo-9800(config)#aaa authorization exec radAuthzMethod local group radGroup
```

In this setup, some users are only created locally and some users only on the ISE server, hence we use the first option.

Step 4. Create a AAA authorization exec method pointing to the Tacacs+ server group

The user has to be also authorized in order to be granted access. From the same tab:

[Authentication Authorization and Accounting](#)

[+ AAA Wizard](#)

AAA Method List							
Servers / Groups AAA Advanced							
General							
Authentication							
Authorization							
Accounting							
+ Add x Delete							
Name	Type	Group Type	Group1	Group2	Group3	Group4	
☒ tacAuthzMethod	exec	local	tacGroup	N/A	N/A	N/A	
☐ radAuthzMethod	exec	local	radGroup	N/A	N/A	N/A	
☐ default	network	local	N/A	N/A	N/A	N/A	
☐ radAuthzNetworkMethod	network	group	radGroup	N/A	N/A	N/A	
☐ default	credential-download	local	N/A	N/A	N/A	N/A	
1 10 items per page							

Use the same order of local/group being used for the authentication method in the previous step, and choose type as 'exec'.

From CLI:

```
paolo-9800(config)#aaa authorization exec radAuthzMethod local group radGroup
```

Step 5. Assign the methods to the HTTP configurations and to the VTY lines used for Telnet/SSH

These steps cannot be done from GUI, hence they need to be done from CLI.

- For the GUI authentication:

```
paolo-9800(config)#aaa authorization exec radAuthzMethod local group radGroup
```

- For Telnet/SSH authentication:

```
paolo-9800(config)#aaa authorization exec radAuthzMethod local group radGroup
```

Note: when doing changes to the HTTP configurations, it is best to restart the HTTP and HTTPS services:

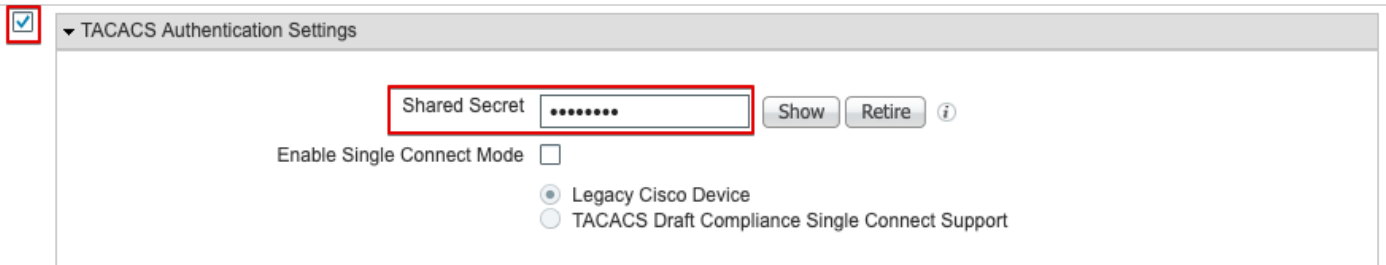
```
paolo-9800(config)#aaa authorization exec radAuthzMethod local group radGroup
```

Tacacs+ ISE configuration

Step 1. Configure the WLC as network device for Tacacs+:

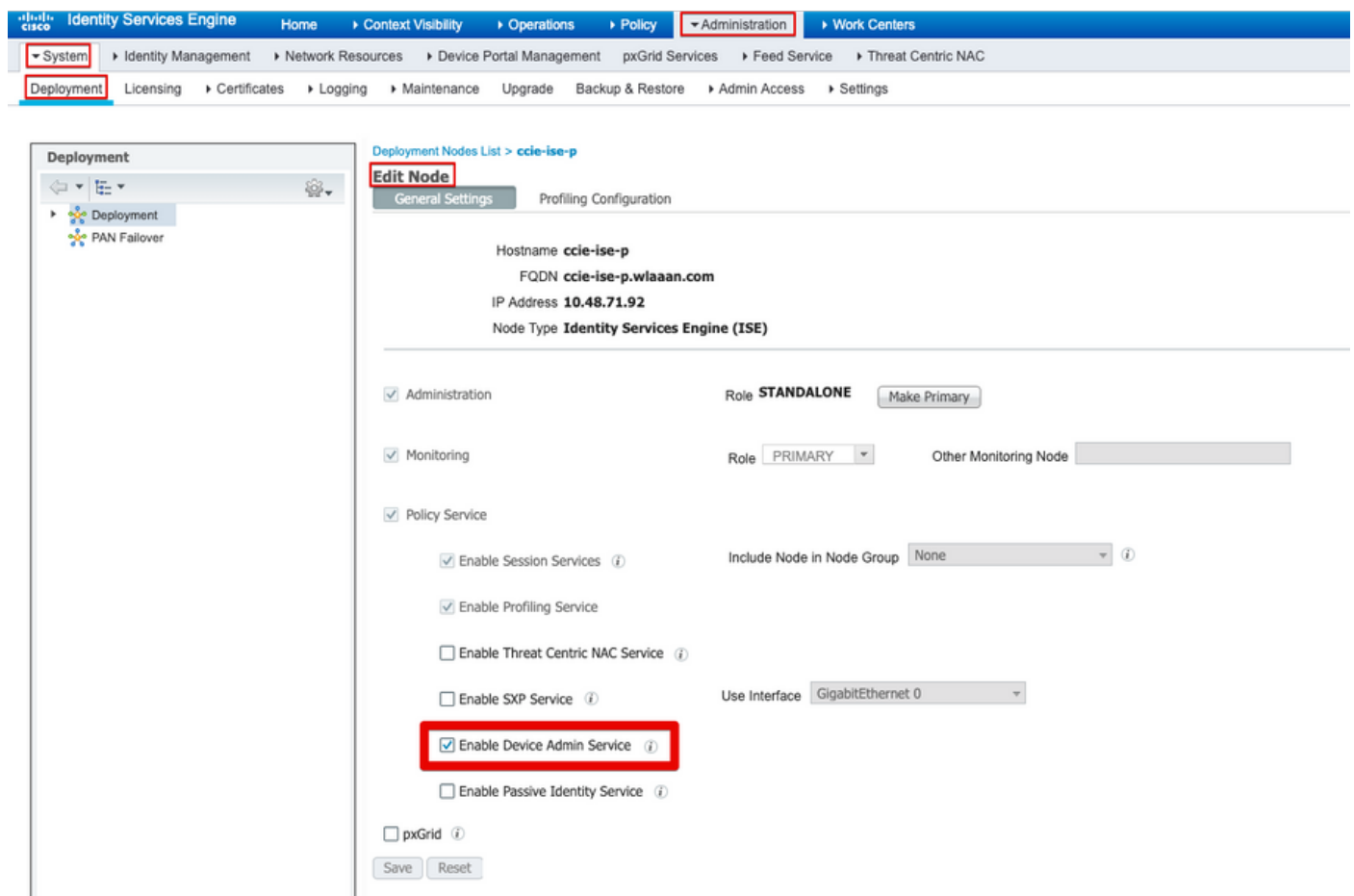
Identity Services Engine						
Home Context Visibility Operations Policy Administration Work Centers						
System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC						
Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services						
Network devices						
Default Device						
Device Security Settings						
Network Devices						
Edit Add Duplicate Import Export Generate PAC Delete						
Name	IP/Mask	Profile Name	Location	Type	Description	
☒ paolo-9800-71	10.48.71.91/32	Cisco	All Locations	All Device Types		

Note that in this example, the WLC is already added for RADIUS, hence click on edit, and scroll down to TACACS Authentication Settings, and add the needed secret:



Note: in order to use ISE as TACACS+ server, you must have a Device Administration license package, and either a Base or a Mobility license.

Also, once the licenses are installed, you must enable the Device Admin feature for the node. To do so, edit the node deployment node under Administrator > Deployment, and check the box:



Step 2. Create TACACS Profiles, to return the privilege

In order to do configurations, 'adminuser' needs to have a privilege level of 15, which will allow to access the exec prompt shell.

The other user instead, 'helpdeskuser' will not need exec prompt shell access, and it can be assigned a privilege level lower than 15.

To do so, create TACACS Profiles:

Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers

Network Access > Guest Access > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID

Overview > Identities > User Identity Groups > Ext Id Sources > Network Resources > Policy Elements > Device Admin Policy Sets > Reports > Settings

Conditions

Network Conditions

Results

Allowed Protocols

TACACS Command Sets

TACACS Profiles

TACACS Profiles

0 Selected Rows/Page 6 1 / 1 Go 6 Total Rows

Refresh Add Duplicate Trash Edit Filter

☐	Name	Type	Description
☐	Default Shell Profile		Default Shell Profile
☐	WLC ALL	WLC	WLC ALL
☐	WLC MONITOR	WLC	WLC MONITOR
☐	Deny All Shell Profile	Shell	Deny All Shell Profile
☐	IOS_Helpdesk	Shell	
☐	IOS_Admin	Shell	

Configure an admin profile with privilege 15 as follows :

[TACACS Profiles](#) > [IOS_Admin](#)

TACACS Profile

Name

Description

Task Attribute View

Raw View

Common Tasks

Common Task Type

☒	Default Privilege	15	(Select 0 to 15)
☐	Maximum Privilege		(Select 0 to 15)
☐	Access Control List		
☐	Auto Command		
☐	No Escape		(Select true or false)
☐	Timeout		Minutes (0-9999)
☐	Idle Time		Minutes (0-9999)

Custom Attributes

+ Add Trash Edit

☐	Type	Name	Value
No data found.			

Cancel

Save

In the Helpdesk profile instead, the Default Privilege is set as 1.

Step 3. Create the users on ISE:

This is the same as on step 3 of the RADIUS ISE configuration

Step 4. Create a Device Admin Policy Set:

Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Device Admin Policy Sets

Policy Sets

Search policy names & descriptions.

Summary of Policies

A list of all your policies

Global Exceptions

Rules across entire deployment

IOS-9800

Default

Tacacs_Default

Save Order

Reset Order

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Status	Name	Description	Conditions
☒	IOS-9800		Network Access:Device IP Address EQUALS 10.48.71.91

Regular ☐ Proxy Sequence ☐

Proxy Server Sequence

Proxy server sequence:

Authentication Policy

Default Rule (If no match) : Allow Protocols : Default Device Admin and use : All_User_ID_Stores

Authorization Policy

Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles
☒	Admin-access	if InternalUser.Name EQUALS adminuser	then Permit_all AND IOS_Admin	
☒	Helpdesk-access	if InternalUser.Name EQUALS helpdeskuser	then Permit_all AND IOS_Helpdesk	
☒	Tacacs_Default	if no matches, then	DenyAllCommands	

The specific Policy Set "IOS-9800", in this example, filters requests with IP Address equal to the example 9800 IP.

As authentication policy, we leave the Default Rule, and have set up two Authorization rules:

- the first one is triggered when the username is 'adminuser', it permits all commands (via the default 'Permit_all') rule, and it assigns privilege 15 (via 'IOS_Admin')
- the second one is triggered when the username is 'helpdeskuser', it permits all commands (via the default 'Permit_all') rule, and it assigns privilege 15 (via 'IOS_Helpdesk')

Troubleshooting

In order to troubleshoot TACACS+ access to the WLC's GUI or CLI, issue the 'debug tacacs' command, along with 'term mon' and see the live output when a login attempt is made.

A successful login attempt of the 'adminuser' user is shown below:

```
paolo-9800(config)#aaa authorization exec radAuthzMethod local group radGroup
```

It can be seen that the Tacacs+ server returns the correct privilege 'AV priv-lvl=15'

When doing RADIUS authentication, instead, we will have a similar debug output, concerning the RADIUS traffic.

'debug aaa authentication' and 'debug aaa authorization' will instead show which method list is being selected by the WLC when the user tries to login.