Configure 802.1x Authentication on Catalyst 9800 Wireless Controller Series

Contents

Introduction
Prerequisites
Requirements
Components Used
Configure
Network Diagram
Configuration
AAA Configuration on 9800 WLCs
WLAN Profile Configuration
Policy Profile Configuration
Policy Tag Configuration
Policy Tag Assignation
ISE Configuration
Verify
Troubleshoot

Introduction

This document describes how to set up a Wireless Local Area Network (WLAN) with 802.1x security on an Cisco Catalyst 9800 Series Wireless Controllers by Graphic User Interface (GUI) or Command Line Interface (CLI).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- 802.1x

Components Used

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

- Catalyst 9800 Wireless Controller Series (Catalyst 9800-CL)
- Cisco IOS-XE Gibraltar 16.10

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, ensure that you understand the potential impact of any command.
Configuration

AAA Configuration on 9800 WLCs

GUI:

Step 1. Declare RADIUS server. Navigate to Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add and enter the RADIUS server's information.
Ensure **Support for CoA** is enabled if you plan to use Central Web Authentication (or any kind of security that requires CoA) in the future.

![Create AAA Radius Server](image)

Step 2. Add the RADIUS server to a RADIUS group. Navigate to **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add.**

Enter the information:
CLI:

```
# config t
# aaa new-model
# dot1x system-auth-control

# radius server <radius-server-name>
# address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813
# timeout 300
# retransmit 3
# key <shared-key>
# exit

# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>
# aaa authentication dot1x <dot1x-list-name> group <radius-grp-name>
```

**WLAN Profile Configuration**

**GUI:**

Step 1. Create the WLAN. Navigate to **Configuration > Wireless > WLANs > + Add** and configure the network as needed.
Step 2. Enter the WLAN information

Step 3. Navigate to **Security** tab and select the needed security method. In this case WPA2 + 802.1x.
Step 4. From Security > AAA tab, select the authentication method created on step 3 from AAA Configuration on 9800 WLC section.
CLI:

```
# config t
# wlan <profile-name> <wlan-id> <ssid-name>
# security dot1x authentication-list <dot1x-list-name>
# no shutdown
```

**Policy Profile Configuration**

Inside a Policy Profile you can decide to which VLAN assign the clients, among other settings (like Access Controls List [ACLs], Quality of Service [QoS], Mobility Anchor, Timers and so on).

You can either use your default policy profile or you can create a new.

GUI:

Navigate to **Configuration > Tags & Profiles > Policy Profile** and either configure your **default-policy-profile** or create a new one.
Ensure the profile is enabled.

Also, if your Access Point (AP) is in local mode, ensure the policy profile have **Central Switching** and **Central Authentication** enabled.

Select the VLAN where the clients need to be assigned in the **Access Policies** tab.
If you plan to have ISE return attributes in the Access-Accept like VLAN Assignment, please enable AAA override in the **Advanced** tab:
CLI:

```
# config
# wireless profile policy <policy-profile-name>
# aaa-override # central switching # description "<description>" # vlan <vlanID-or-VLAN_name> #
no shutdown
```

**Policy Tag Configuration**

Policy Tag is used to link the SSID with the Policy Profile. You can either create a new Policy Tag or use the default-policy tag.

**Note:** The default-policy-tag automatically maps any SSID with a WLAN ID between 1 to 16 to the default-policy-profile. It cannot be modified nor deleted. If you have a WLAN with ID 17 or higher, the default-policy-tag cannot be used.

GUI:

Navigate to **Configuration > Tags & Profiles > Tags > Policy** and add a new one if needed.
Link your WLAN Profile to the desired Policy Profile.
CLI:

```
# config t
# wireless tag policy <policy-tag-name>
# wlan <profile-name> policy <policy-profile-name>
```

**Policy Tag Assignment**

Assign the Policy Tag to the needed APs.

GUI:
To assign the tag to one AP, navigate to Configuration > Wireless > Access Points > AP Name > General Tags, assign the relevant policy tag and then click Update & Apply to Device.

**Note:** Be aware that when the policy tag on an AP is changed, it drops its association to the 9800 WLC and will join back.

To assign the same Policy Tag to several APs navigate to Configuration > Wireless Setup > Advanced > Start Now > Apply.
Select the APs to which you want to assign the tag and click + Tag APs
Select the applicable Tags for Policy, Site and RF and click **Save & Apply to Device**

**ISE Configuration**

**Declare WLC on ISE**

Step 1. Open ISE console and navigate to **Administration > Network Resources > Network Devices > Add** as shown in the image.
Step 2. Enter the values.

Optionally, it can be a specified Model name, software version, description and assign Network Device groups based on device types, location or WLCs.

a.b.c.d correspond to the WLC’s interface that sends the authentication requested. By default it is the management interface as shown in the image.
For more information about **Network Device Groups** review this link:

ISE - Network Device Groups

Create New User on ISE
Step 1. Navigate to **Administration > Identity Management > Identities > Users > Add** as shown in the image.

Step 2. Enter the information. In this example, this user belongs to a group called **ALL_ACCOUNTS** but it can be adjusted as needed as shown in the image.
Create Authentication Rule

Authentication rules are used to verify if the credentials of the users are right (verify if the user really is who it says it is) and limit the authentication methods that are allowed to be used by it.
Step 1. Navigate to **Policy > Authentication** as shown in the image.

Step 2. Insert a new authentication rule as shown in the image.

Step 3. Enter the values. This authentication rule allows all the protocols listed under the **Default Network Access** list, this applies to the authentication request for Wireless 802.1x clients and with Called-Station-ID and ends with `ise-ssid` as shown in the image.

Also, choose the **Identity Source** for the clients that matches this authentication rule. This example uses **Internal Users** identity source list as shown in the image.
Once finished, click **Done** and **Save** as shown in the image.

For more information about Allow Protocols Policies consult this link:

[Allowed Protocols Service](#)

For more information about Identity sources consult this link:

[Create a User Identity Group](#)

### Create Authorization Profile

The authorization profile determines if the client has access or not to the network, push Access Control Lists (ACLs), VLAN override or any other parameter. The authorization profile shown in this example sends an access accept for the client and assigns the client to VLAN 2404.

**Step 1.** Navigate to **Policy > Policy Elements > Results** as shown in the image.

Step 3. Enter the values as shown in the image. Here we can return AAA override attributes like VLAN as example. WLC 9800 accepts tunnel attributes 64,65,81 using VLAN id or Name, and accepts also the usage of the AirSpace-Interface-Name Attribute.