Central Web Authentication (CWA) on Catalyst 9800 Wireless Controllers and ISE v2.2 Configuration Example

Contents

Introduction
Prerequisites
Requirements
Components Used
Configure
Network Diagram
Configuration
AAA Configuration on 9800 WLC

WLAN Configuration
Policy Profile Configuration
Policy Tag Configuration
Policy Tag Assignment
Redirect ACL configuration
ISE Configuration
In case of Flexconnect local switching access points
Verify
Troubleshoot

Introduction

This document describes how to configure a Central Web Authentication Wireless Local Area Network (WLAN) on an Catalyst 9800 Series Wireless Controllers (9800 WLC) through the Graphic User Interface (GUI) or Command Line Interface (CLI).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- 9800 WLC configuration mode

Components Used

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

Network Diagram

RADIUS  

9800 WLC  

Client

Configuration

AAA Configuration on 9800 WLC

Step 1. Add ISE server to 9800 WLC configuration and create an authentication method list

You can follow the instructions from this link:

AAA Configuration on 9800 WLC

Step 2. Create an authorization method list

Navigate to Configuration > Security > AAA > AAA Method List > Authorization > + Add
WLAN Configuration

Step 1. Create the WLAN

GUI:

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 only MAC filtering and the list that you created at step 2 on AAA Configuration section.
Step 3. Navigate to the **AAA** tab and also select the authentication method (created in step 1 of the previous section) and the accounting method list.

CLI:

```
# config t
# wlan <ssid-name> <wlan-id> <profile-name>
# mac-filtering <AuthZ-network-list>
# no security wpa
# no security wpa akm dot1x
# no security wpa wpa2
# no security wpa wpa2 ciphers aes
# security dot1x authentication-list <dot1x-AuthC-list>
# 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:**

**Step 1. Create a new Policy Profile**

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

![Policy Profile Configuration](image)

Ensure the profile is enabled.

![Add Policy Profile](image)

**Step 2. Select the VLAN**

Navigate to **Access Policies** tab and select the vlan name from the drop down or manually type
Step 3. Configure the policy profile to accept ISE overrides (Allow AAA Override) and Change of Authorization (CoA) (NAC State). You can optionally specify an account method too.
Policy Tag Configuration

Inside the Policy Tag is where you link your SSID with your 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 or 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 Assignation**

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**, make the needed assignment and then click **Update & Apply to Device**.

**Note**: Be aware that after change the policy tag on an AP, it loses its association to the 9800 WLC and join back within about 1 minute.

To assign the same Policy Tag to several APs navigate to **Configuration > Wireless > Wireless Setup > Start Now > Apply**.
Select the APs to which you want to assign the tag and click + Tag APs
Select the wished Tag and click **Save & Apply to Device**

**CLI:**

```
# config t
# ap <ethernet-mac-addr>
# policy-tag <policy-tag-name>
# end
```

**Redirect ACL configuration**

**Step 1.** Navigate to **Configuration > Security > ACL > + Add** to create a new ACL.

Select a name for the ACL, make it **IPv4 Extended** type and add every rule as a sequence
The ACL must look like this (Replace 172.16.0.12 with your ISE’s IP address):

**Note:** For the redirection ACL, think for **deny** action as a deny redirection (not deny traffic), and **permit** action as permit redirection.

**CLI:**

```plaintext
ip access-list extended REDIRECT
deny udp any any eq domain
deny udp any eq bootps any
deny udp any any eq bootpc
deny tcp any host 172.16.0.12 eq 8443
permit tcp any any eq www
permit tcp any any eq 443 >>> This redirects all HTTPS requests towards ISE. This has traditionally caused issues in scale deployment. So, use this config with caution.
```

**ISE Configuration**
Add 9800 WLC to ISE

Step 1. Navigate to Administration > Network Resources > Network Devices.

Step 2. Click +Add and enter the 9800 WLC settings.

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.
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**
Step 2. Enter the information.

In this example, this user belongs to a group called ALL_ACCOUNTS but it can be adjusted as needed.
Create Authorization Profile

The policy profile is the result assigned to a client based on its parameters (as mac address, credentials, WLAN used and so on). It can assign specific settings like Virtual Local Area Network (VLAN), Access Control Lists (ACLs), Uniform Resource Locator (URL) redirects and so on.

These steps show how to create the authorization profile needed to redirect the client to the authentication portal.

Step 1. Navigate to Policy > Policy Elements > Results > Authorization > Authorization Profiles > Add
Step 2. Enter the redirection information. Ensure that the ACL name is the same that was configured on the 9800 WLC.
Configure Authentication Rule

Step 1. Navigate to Policy > Authentication.
Step 2. Click **Edit** from the MAB rule.

Step 3. Modify the MAB default network to continue to the authorization phase even when client is not internally found.

Step 4. Click **Done** and **Save** to save the changes.

**Configure Authorization Rules**

The authorization rule is the one in charge to determine which permissions (which authorization profile) result is applied to the client.

Step 1. Navigate to **Policy > Authorization** as shown in the image. Once there, go to the first rule, click on the arrow next to **Edit** and select **Insert New Rule Above**.

Step 2. Select the conditions for the authorization process to fall into this rule. In this example, the authorization process hits this rule if its called station ID contains **cwa-ssid**.
Step 3. Select the Authorization profile that is assigned to the clients that hit that rule, click **Done** and **Save** to save the changes.

Step 3. Duplicate the redirect rule above itself.

Step 4. Add **Network Access:UseCase EQUALS GuestFlow** as another condition of the duplicated rule and change the **Permission** to **PermitAccess**.

This rule detects if the client has been previously authenticated (using the Network Access use case) and if so, it applies a permit access. Optionally, instead of a PermitAccess permission you could build a new authorization profile and assign new parameters (Like an ACL)

Step 5. Save the rules

Click **Save** at the bottom of the rules.

**In case of Flexconnect local switching access points**

What if you have Flexconnect local switching access points and WLANs? The previous sections are still valid. However, we need an extra step in order to push the redirect ACL to the APs in advance.

Navigate to **Configuration > Tags & Profiles > Flex** and click on your Flex profile. Go to the **Policy ACL** tab.

Click **Add**
Choose your redirect ACL name and enable "Central web authentication". This checkbox automatically inverts the ACL on the AP itself (this is because a "deny" statement means "do not redirect to this IP" on the WLC in IOS-XE however on the AP the "deny" statement means the opposite, so this checkbox automatically swaps all permits and deny when pushing to the AP. You can verify this with a "show ip access list" form the AP CLI).

**Note**: In FlexConnect local switching scenario, the ACL **MUST** specifically mentions return statements (which is not necessarily required in local mode) so make sure that all your ACL rules are covering both ways traffic (to and from the ISE for example)

Don't forget to hit **Save** and then **Update and apply to device**.

**Verify**

You can use these commands to verify current configuration
# show run wlan
# show run aaa
# show aaa servers
# show ap config general
# show ap name <ap-name> config general
# show ap tag summary
# show ap name <AP-name> tag detail
# show wlan { summary | id | nme | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>

**Troubleshoot**

WLC 9800 provides ALWAYS-ON tracing capabilities. This ensures all client connectivity related errors, warning and notice level messages are constantly logged and you can view logs for an incident or failure condition after it has occurred.

**Note:** Depending on volume of logs being generated, you can go back few hours to several days.

In order to view the traces that 9800 WLC collected by default, you can connect via SSH/Telnet to the 9800 WLC and follow these steps (Ensure you are logging the session to a text file).

**Step 1.** Check controller's current time so you can track the logs in the time back to when the issue happened.

```sh
# show clock
```

**Step 2.** Collect syslogs from the controller's buffer or the external syslog as dictated by the system configuration. This provides a quick view into the system health and errors, if any.

```sh
# show logging
```

**Step 3.** Verify if any debug conditions are enabled.

```sh
# show debugging
```

**IOSXE Conditional Debug Configs:**

Conditional Debug Global State: Stop

**IOSXE Packet Tracing Configs:**

Packet Infra debugs:

<table>
<thead>
<tr>
<th>Ip Address</th>
<th>Port</th>
</tr>
</thead>
</table>

**Note:** If you see any condition listed, it means the traces are being logged up to debug level for all the processes that encounter the enabled conditions (mac address, ip address etc). This would increase the volume of logs. Therefore, it is recommended to clear all conditions when not actively debugging.
Step 4. Assuming mac address under test was not listed as a condition in Step 3, collect the always-on notice level traces for the specific mac address.

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file always-on-<FILENAME.txt>
```

You can either display the content on the session or you can copy the file to an external TFTP server.

```
# more bootflash:always-on-<FILENAME.txt>
or
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

**Conditional Debugging and Radio Active Tracing**

If the always-on traces do not give you enough information to determine the trigger for the problem under investigation, you can enable conditional debugging and capture Radio Active (RA) trace, which will provide debug level traces for all processes that interact with the specified condition (client mac address in this case). In order to enable conditional debugging, follow these steps.

Step 5. Ensure there are no debug conditions are enabled.

```
# clear platform condition all
```

Step 6. Enable the debug condition for the wireless client mac address that you want to monitor.

This commands start to monitor the provided mac address for 30 minutes (1800 seconds). You can optionally increase this time to up to 2085978494 seconds.

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

**Note:** In order to monitor more than one client at a time, run debug wireless mac <aaaa.bbbb.cccc> command per mac address.

**Note:** You do not see the output of the client activity on terminal session, as everything is buffered internally to be viewed later.

Step 7. Reproduce the issue or behavior that you want to monitor.

Step 8. Stop the debugs if the issue is reproduced before the default or configured monitor time is up.

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

Once the monitor-time has elapsed or the debug wireless has been stopped, the 9800 WLC generates a local file with the name:
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Step 9. Collect the file of the mac address activity. You can either copy the ra trace .log to an external server or display the output directly on the screen.

Check the name of the RA traces file

# dir bootflash: | inc ra_trace

Copy the file to an external server:

# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
tftp://a.b.c.d/ra-FILENAME.txt

Display the content:

# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Step 10. If the root cause is still not obvious, collect the internal logs which are a more verbose view of debug level logs. You do not need to debug the client again as we are only taking a further detailed look at debug logs that have been already collected and internally stored.

# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file ra-internal-<FILENAME>.txt

**Note:** This command output returns traces for all logging levels for all processes and is quite voluminous. Please engage Cisco TAC to help parse through these traces.

You can either copy the ra-internal-FILENAME.txt to an external server or display the output directly on the screen.

Copy the file to an external server:

# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt

Display the content:

# more bootflash:ra-internal-<FILENAME>.txt

Step 11. Remove the debug conditions.

# clear platform condition all

**Note:** Ensure that you always remove the debug conditions after a troubleshooting session.