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

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

Components Used

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

- 9800 WLC IOS-XE Gibraltar v16.12
- Identity Service Engine (ISE) v2.4

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.

Configure

Network Diagram
AAA Configuration on 9800 WLC

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

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.
Step 2. Create an authorization method list

Navigate to **Configuration > Security > AAA > AAA Method List > Authorization > + Add**
Quick Setup: AAA Authorization

Method List Name*  
CWAauthz

Type*  
network

Group Type  
group

Fallback to local

Authenticated

Available Server Groups

Idao
tacacs+

Assigned Server Groups

radius

Step 4 (optional). Create an accounting method list
Note: CWA will not work if you decide to load-balance (from the IOS-XE CLI configuration) your radius servers due to CSCvh03827. Using external load-balancers is fine.

Step 5 (optional)

You can define the AAA policy to send the SSID name as Called-station-id attribute, which can be useful if you want to leverage this condition on ISE later in the process.

Go to **Configuration > Security > Wireless AAA Policy** and either edit the default aaa policy or create a new one.
You can choose SSID as option 1. Be mindful that even when choosing SSID only, the called station id will still append the AP MAC address to the SSID name.

**WLAN Configuration**

**Step 1. Create the WLAN**

**GUI:**

Navigate to **Configuration > Tags & Profiles > WLANs > + Add** and configure the network as needed.
Step 2. Enter the WLAN information

### Add WLAN

<table>
<thead>
<tr>
<th>General</th>
<th>Security</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name*</td>
<td>cwa-ssid</td>
<td>Radio Policy</td>
</tr>
<tr>
<td>SSID*</td>
<td>cwa-ssid</td>
<td>Broadcast SSID</td>
</tr>
<tr>
<td>WLAN ID*</td>
<td>2</td>
<td>Status</td>
</tr>
</tbody>
</table>

**CLI:**

```
# config t
(config)#wlan cwa-ssid 2 cwa-ssid
(config-wlan)#mac-filtering CWAauthz
```

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.

### Edit WLAN

<table>
<thead>
<tr>
<th>Layer2</th>
<th>Layer3</th>
<th>AAA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2 Security Mode</td>
<td>None</td>
<td>Lobby Admin Access</td>
</tr>
<tr>
<td>MAC Filtering</td>
<td>✓</td>
<td>Fast Transition</td>
</tr>
<tr>
<td>Transition Mode WLAN ID</td>
<td>0</td>
<td>Over the DS</td>
</tr>
<tr>
<td>Authorization List*</td>
<td>CWAauthz</td>
<td>Reassociation Timeout</td>
</tr>
</tbody>
</table>

**CLI:**

```
# config t
(config)#wlan cwa-ssid 2 cwa-ssid
(config-wlan)#mac-filtering CWAauthz
```
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.

Ensure the profile is enabled.
Step 2. Select the VLAN

Navigate to **Access Policies** tab and select the vlan name from the drop down or manually type the VLAN-ID. DO NOT configure an ACL in the policy profile.
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.

CLI:

```
# config
# wireless profile policy <policy-profile-name>
# aaa-override
# nac
# vlan <vlan-id_or_vlan-name>
# accounting-list <acct-list>
# no shutdown
```

**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 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**, 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
You need to deny traffic to your ISE PSNs nodes as well as deny DNS and permit all the rest. This redirect ACL is not a security ACL but a punt ACL that will define what traffic goes to the CPU (on permits) for further treatment (like redirection) and what traffic stays on the dataplane (on deny) and will avoid redirection.

The ACL must look like this (Replace 10.48.39.28 with you 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. The WLC will only look into traffic that it can redirect (port 80 and 443 by default).

**CLI:**

```
ip access-list extended REDIRECT
deny ip any host 10.48.39.28
deny ip host 10.48.39.28 any
deny udp any any eq domain
deny udp any eq domain any
permit tcp any eq domain
deny tcp any any eq 80
```

**Note**: If you end the ACL with a "permit ip any any" instead of a permit focused on port 80, the WLC will also redirect HTTPS, which is often undesirable as it will have to provide its...
own certificate and will always create a certificate violation.

You can improve the ACL by only denying the guest port 8443 towards the ISE server.

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.
<table>
<thead>
<tr>
<th><strong>Network Devices</strong></th>
<th><strong>New Network Device</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Devices</strong></td>
<td><strong>Network Devices</strong></td>
</tr>
<tr>
<td>Default Device</td>
<td>* Name: 9800WLC</td>
</tr>
<tr>
<td>Device Security Settings</td>
<td>Description:</td>
</tr>
<tr>
<td></td>
<td><strong>IP Address</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Device Profile</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Model Name</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Software Version</strong></td>
</tr>
<tr>
<td>* Network Device Group</td>
<td>Location: All Locations</td>
</tr>
<tr>
<td></td>
<td><strong>IPSEC</strong> Is IPSEC Device</td>
</tr>
<tr>
<td></td>
<td><strong>Device Type</strong> All Device Types</td>
</tr>
</tbody>
</table>

**RADIUS Authentication Settings**

**RADIUS UDP Settings**

- **Protocol** RADIUS
- * Shared Secret: Password
- Use Second Shared Secret
- CoA Port: 1700

**RADIUS DTLS Settings**

- DTLS Required
- Shared Secret: radius/dtls
- CoA Port: 2083
- Issuer CA of ISE Certificates for CoA
- DNS Name

**General Settings**

- Enable KeyWrap
- * Key Encryption Key
- * Message Authenticator Code Key
- Key Input Format: ASCII | HEXADECIMAL

**Submit** | **Cancel**
For more information about **Network Device Groups** review the ISE admin guide:

ISE - Network Device Groups

Create New User on ISE

Step 1. Navigate to **Administration > Identity Management > Identities > Users > Add**

![Image of ISE interface with highlighted steps]

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. Note that in recent versions of ISE, a Cisco_Webauth authorization result already exists. Here we will edit it to modify the redirection ACL name to match what we configured on the WLC.

Step 1. Navigate to Policy > Policy Elements > Results > Authorization > Authorization Profiles. Click add to create your own or edit the Cisco_Webauth default result.
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 > Policy Sets. Click on the appropriate policy sets (if you already have
several configured) or the default's View arrow on the right of the screen.

Step 2. Expand Authentication policy. For the MAB rule (matching on wired or wireless MAB), expand Options and chose the CONTINUE option in case "If User not found".

Step 3. Click 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. On the same Policy set page, close down the Authentication Policy and expand Authorization policy.

Step 2. Recent ISE versions will start with a pre-created rule called Wifi_Redirect_to_Guest_Login which matches mostly our need. Turn the grey sign on the left to enable.
Step 3. That rule matches on Wireless_MAB only and returns the CWA redirection attributes. We will now optionally add a little twist and make it match only on our specific SSID. Click on the condition (Wireless_MAB as of now) to make the Conditions Studio appear. Add a condition on the right and choose the Radius dictionary with the Called-Station-ID attribute. Make it match your SSID name. Validate by clicking Use at the bottom of the screen.

Step 4. You now need a second rule, defined with a higher priority, that will match on the Guest Flow condition in order to return network access details once the user has authenticated on the portal. You can use the Wifi Guest Access rule which is also pre-created by default on recent ISE versions. You then only have to enable the rule with a green mark on the left. You can return the default PermitAccess or configure more precise access lists restrictions.

Step 5. Save the rules

Click Save at the bottom of the rules.

In case of Flexconnect local switching access points ONLY

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

Chose 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**.
Make sure that you have "ip http server" configured.

Certificates

To have the client trust the web authentication certificate, it is not required to install any certificate on the WLC as the only certificate presented will be the ISE certificate (which has to be trusted by the client).

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>
```

Here is the relevant part of the configuration of the WLC corresponding to this example:

```
aaa new-model
!
aaa authentication dot1x CWA group radius
aaa authorization network default group radius
aaa authorization credential-download wcm_loc_serv_cert local
aaa accounting identity CWAacct start-stop group radius
!
aaa server radius dynamic-author
    client 10.48.39.28 server-key cisco123
!
aaa session-id common
!
!
radius server nicoISE
    address ipv4 10.48.39.28 auth-port 1812 acct-port 1813
    key cisco123
!
wireless aaa policy default-aaa-policy
wireless cts-sxp profile default-sxp-profile

wireless profile policy central-switching-NAC
    aaa-override
    no central association
    no central switching
    nac
    vlan 1468
    no shutdown
wireless tag policy flexpolicy
    wlan Nico9800flexx policy central-switching-NAC
    wlan cwa-ssid 2 cwa-ssid
    mac-filtering default
```
no security wpa
no security wpa wpa2 ciphers aes
no security wpa akm dot1x
no shutdown
ap a46c.2a75.fb80
  policy-tag flexpolicy
  site-tag FlexSite
ap f80b.cbe4.7f40
  policy-tag flexpolicy
  site-tag FlexSite
ip http server
ip http secure-server

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 ONLY
Certificates
Verify
Troubleshoot
Examples

Troubleshoot

If you are only redirected when typing an HTTPS ip address and not on HTTP packets, make sure that you have "ip http server" configured on the WLC configuration. As of now, the web admin portal configuration is tied with the web authentication portal configuration and it needs to be listening on port 80 in order to redirect. This will change in 17.3 and later.

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.

# 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.

# show logging

Step 3. Verify if any debug conditions are enabled.

# 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_aaaaabbbbcccc_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_aaaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.d/ra-FILENAME.txt

Display the content:

# more bootflash:ra_trace_MAC_aaaaabbbbcccc_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.

```bash
# 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:

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

Display the content:

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

Step 11. Remove the debug conditions.

```bash
# clear platform condition all
```

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

**Examples**

If the authentication result is not what you expect, it is important to go to the ISE Operations > Live logs page and get the details of the authentication result.

You will be presented with the reason of the failure (if there is a failure) and all the Radius attributes received by ISE.

In the below example, ISE rejected authentication because no authorization rule matched. This is because we see the Called-station-ID attribute sent as SSID name appended to the AP mac address, while the authorization was an exact match to the SSID name. It will be fixed by changing that rule to "contains" instead of "equal"

<table>
<thead>
<tr>
<th>Event</th>
<th>5400 Authentication Failed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure Reason</td>
<td>15031 Rejected per authorization profile</td>
</tr>
<tr>
<td>Resolution</td>
<td>Authorization Profile with ACCESS_REJECT attribute was selected as a result of the matching authorization rule. Check the appropriate Authorization policy rule results.</td>
</tr>
<tr>
<td>Root cause</td>
<td>Selected Authorization Profile contains ACCESS_REJECT attribute</td>
</tr>
<tr>
<td>Username</td>
<td>E8:36:17:1F:A1:62</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event</th>
<th>10049 Queried PAP - Radius.NAS-Port-Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>15048</td>
<td>Queried PAP - Network Access.Username</td>
</tr>
<tr>
<td>15048</td>
<td>Queried PIP - IdentityGroup.Name (2 times)</td>
</tr>
<tr>
<td>15049</td>
<td>Queried PIP - EndPoints.LogicalProfile</td>
</tr>
<tr>
<td>15049</td>
<td>Queried PIP - Radius.ScheduledStation.Cc</td>
</tr>
<tr>
<td>15049</td>
<td>Queried PAP - Network Access.AuthenticationStatus</td>
</tr>
<tr>
<td>15016</td>
<td>Selected Authorization Profile - DenyAccess</td>
</tr>
<tr>
<td>15033</td>
<td>Rejected per authorization profile</td>
</tr>
<tr>
<td>11003</td>
<td>Returned RADIUS Access-Reject</td>
</tr>
</tbody>
</table>