

Configure Central Web Authentication (CWA) on Catalyst 9800 WLC and ISE

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Network Diagram](#)

[AAA Configuration on 9800 WLC](#)

[WLAN Configuration](#)

[Policy Profile Configuration](#)

[Policy Tag Configuration](#)

[Policy Tag Assignment](#)

[Redirect ACL Configuration](#)

[Enable Redirection for HTTP or HTTPS](#)

[ISE Configuration](#)

[Add 9800 WLC to ISE](#)

[Create New User on ISE](#)

[Create Authorization Profile](#)

[Configure Authentication Rule](#)

[Configure Authorization Rules](#)

[Flexconnect Local Switching Access Points Only](#)

[Certificates](#)

[Verify](#)

[Troubleshoot](#)

[Checklist](#)

[Service Port Support for RADIUS](#)

[Collect Debugs](#)

[Examples](#)

Introduction

This document describes how to configure a CWA Wireless LAN on a Catalyst 9800 WLC and ISE.

Prerequisites

Requirements

Cisco recommends that you have knowledge of 9800 Wireless LAN Controllers (WLC) configuration.

Components Used

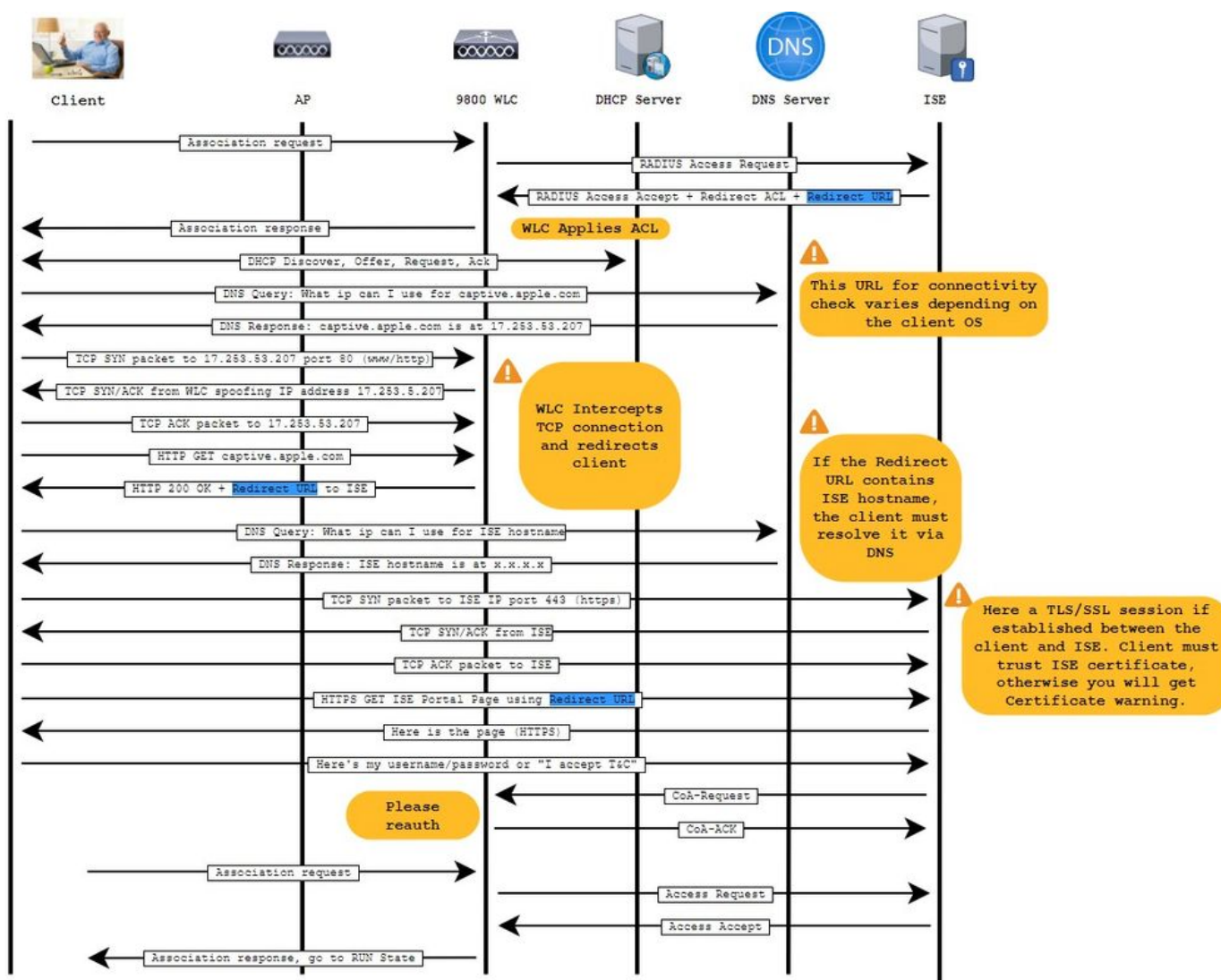
The information in this document is based on these software and hardware versions:

- 9800 WLC Cisco IOS® XE Gibraltar v17.6.x
- Identity Service Engine (ISE) v3.0

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.

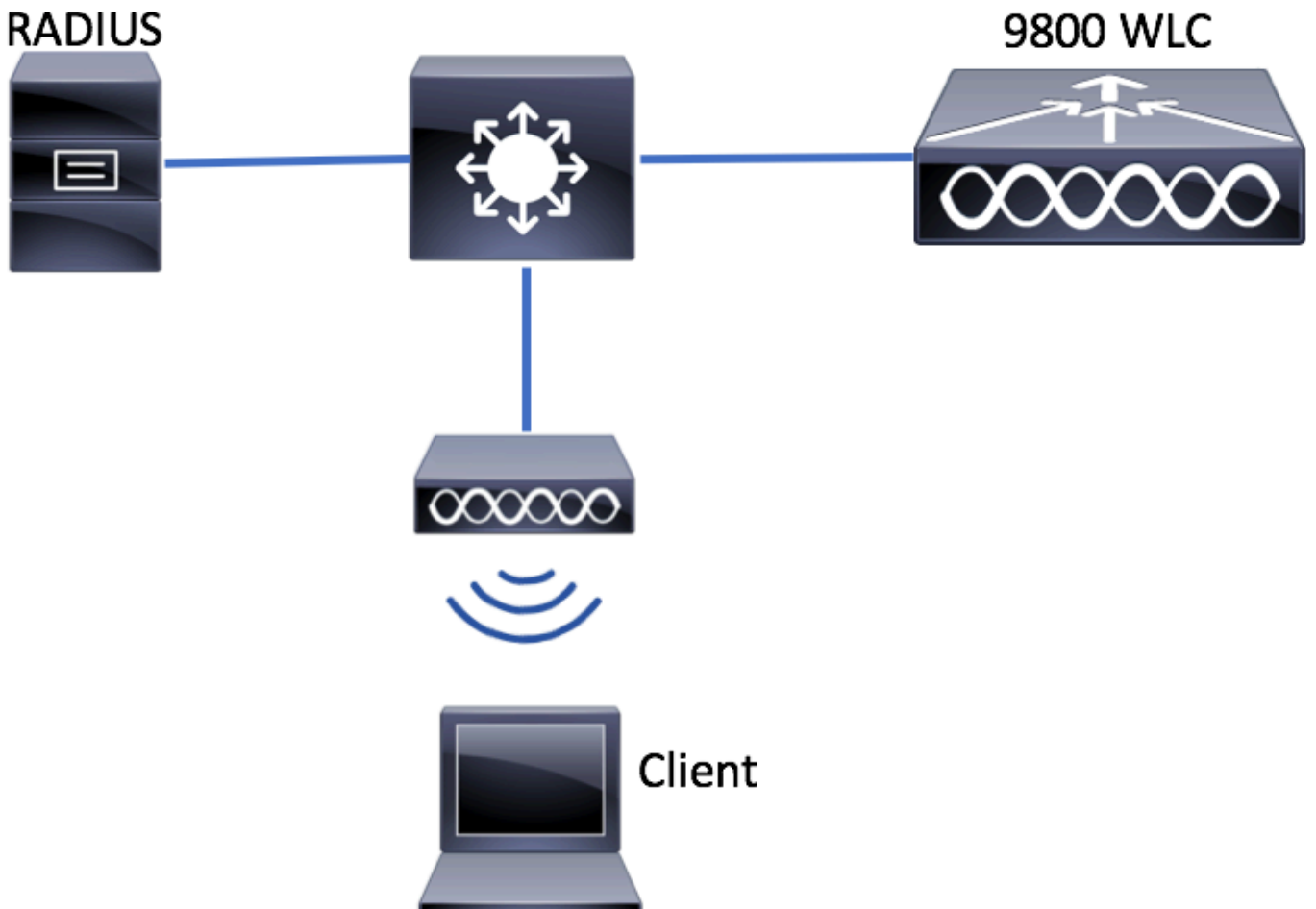
Background Information

The CWA process is shown here where you can see the CWA process of an Apple device as an example:



Configure

Network Diagram



AAA Configuration on 9800 WLC

Step 1. Add the ISE server to the 9800 WLC configuration.

Navigate to **Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add** and enter the RADIUS server information as shown in the images.

The screenshot shows the Cisco ISE configuration interface. The navigation path is highlighted in red: **Configuration > Security > AAA**. Below this, the **Servers / Groups** tab is selected. The **RADIUS** server type is highlighted. The interface shows a table with columns for Name and Address, and a pagination control showing 0 items per page.

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 ✕

Name*	<input type="text" value="ISE-server"/>	Support for CoA ⓘ	ENABLED <input checked="" type="checkbox"/>
Server Address*	<input type="text" value=""/>	CoA Server Key Type	<input type="text" value="Clear Text"/>
PAC Key	<input type="checkbox"/>	CoA Server Key ⓘ	<input type="password" value=""/>
Key Type	<input type="text" value="Clear Text"/>	Confirm CoA Server Key	<input type="password" value=""/>
Key* ⓘ	<input type="password" value=""/>	Automate Tester	<input type="checkbox"/>
Confirm Key*	<input type="password" value=""/>		
Auth Port	<input type="text" value="1812"/>		
Acct Port	<input type="text" value="1813"/>		
Server Timeout (seconds)	<input type="text" value="1-1000"/>		
Retry Count	<input type="text" value="0-100"/>		



Note: On version 17.4.X and later, ensure to also configure the CoA server key when you configure the RADIUS server. Use the same key as the shared secret (they are the same by default on ISE). The purpose is to optionally configure a different key for CoA than the shared secret if that is what your RADIUS server configured. In Cisco IOS XE 17.3, the web UI simply used the same shared secret as CoA key.

Step 2. Create an authorization method list.

Navigate to Configuration > Security > AAA > AAA Method List > Authorization > + Add as shown in the image.

Search Menu Items

- Dashboard
- Monitoring
- Configuration**
- Administration
- Troubleshooting

Authentication Authorization and Accounting

+ AAA Wizard

AAA Method List Servers / Groups AAA Advanced

General

Authentication

Authorization

Accounting

+ Add **x Delete**

Name	Type	Group Type	Group
<input type="checkbox"/> default	network	local	N/A

10 items per page

Quick Setup: AAA Authorization

Method List Name*

Type*

Group Type

Fallback to local

Authenticated

Available Server Groups **Assigned Server Groups**

ldap
tacacs+

radius

Step 3. (Optional) Create an accounting method list as shown in the image.

Quick Setup: AAA Accounting ✕

Method List Name*

Type*

Available Server Groups Assigned Server Groups

ldap tacacs+	<input type="button" value=">"/> <input type="button" value="<"/> <input type="button" value="»"/> <input type="button" value="«"/>	radius	<input type="button" value="↖"/> <input type="button" value="↗"/> <input type="button" value="⏴"/> <input type="button" value="⏵"/>
-----------------	--	--------	--

Note: CWA does not work if you decide to load-balance (from the Cisco IOS XE CLI configuration) your radius servers due to Cisco bug ID [CSCvh03827](#). The usage of external load balancers is fine. However, make sure your load balancer works on a per-client basis by using the calling-station-id RADIUS attribute. Relying on UDP source port is not a supported mechanism for balancing RADIUS requests from the 9800.

Step 4. (Optional) You can define the AAA policy to send the SSID name as a Called-station-id attribute, which can be useful if you want to leverage this condition on ISE later in the process.

Navigate to Configuration > Security > Wireless AAA Policy and either edit the default AAA policy or create a new one.

- ☰ Dashboard
- 🕒 Monitoring >
- 🔧 **Configuration** >
- ⚙️ Administration >
- 🔧 Troubleshooting

Configuration > Security > **Wireless AAA Policy**

+ Add
× Delete

Policy Name
<input type="checkbox"/> default-aaa-policy

⏪
⏩
1
⏪
⏩

10

items per page

You can choose SSID as Option 1. Be mindful that even when you choose SSID only, the called station id does still append the AP MAC address to the SSID name.

Edit Wireless AAA Policy

Policy Name*

default-aaa-policy

Option 1

SSID ▼

Option 2

Not Configured ▼

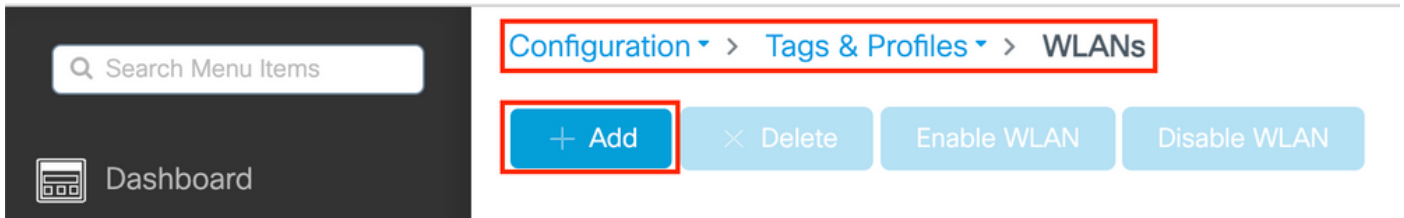
Option 3

Not Configured ▼

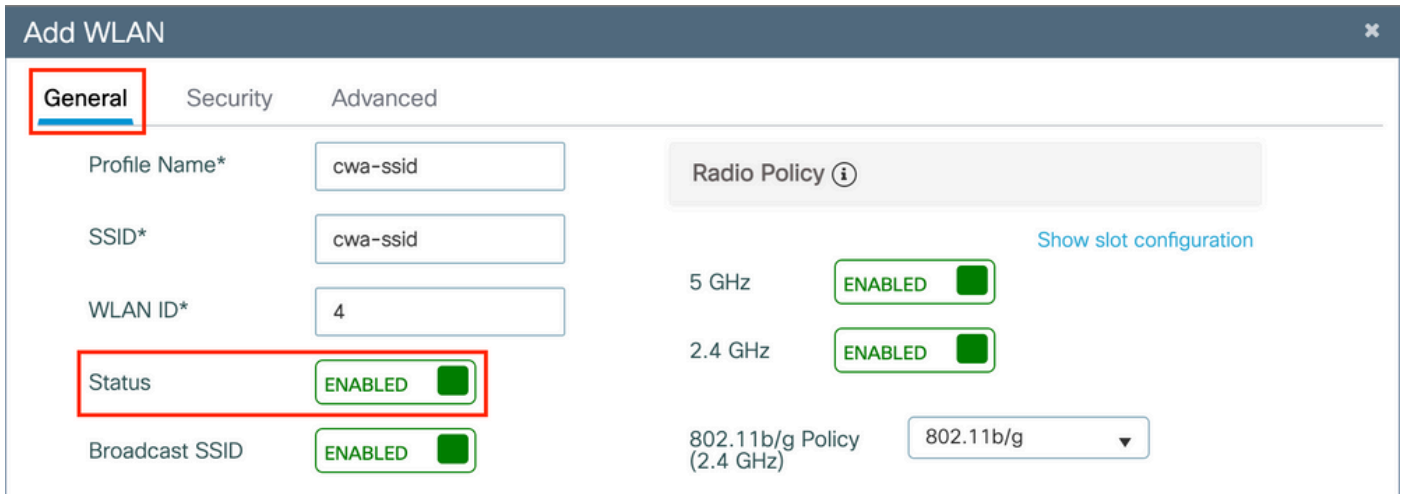
WLAN Configuration

Step 1. Create the WLAN.

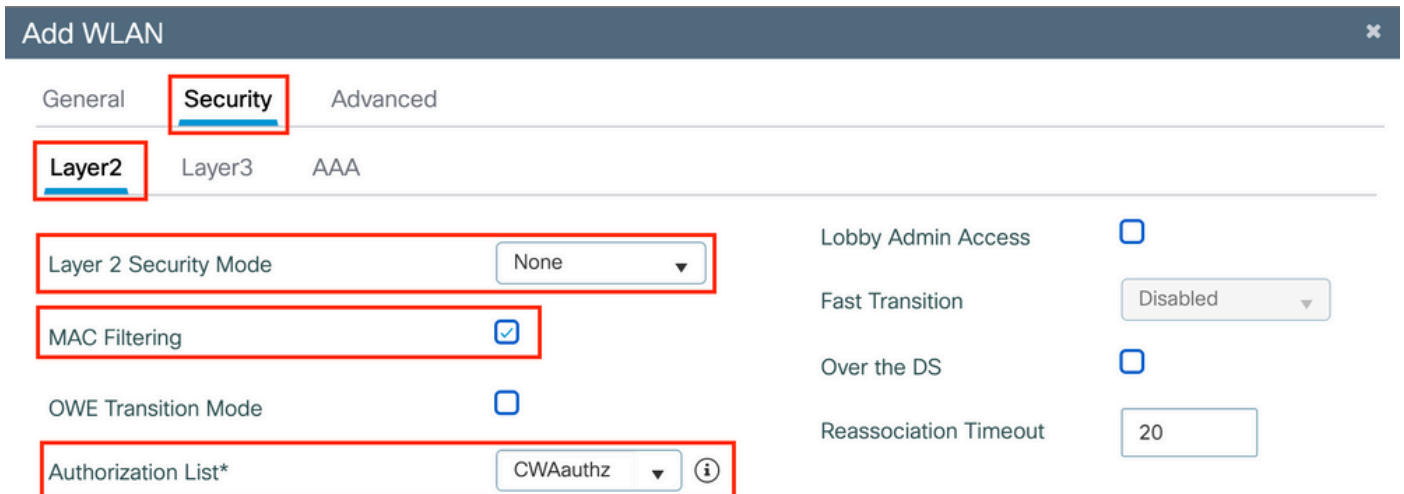
Navigate to Configuration > Tags & Profiles > WLANs > + Add and configure the network as needed.



Step 2. Enter the WLAN general information.



Step 3. Navigate to the Security tab and choose the needed security method. In this case, only 'MAC Filtering' and the AAA authorization list (that you created in Step 2. in the AAA Configuration section) are needed.



CLI:

```
#config t
(config)#wlan cwa-ssid 4 cwa-ssid
(config-wlan)#mac-filtering CWAauthz
(config-wlan)#no security ft adaptive
(config-wlan)#no security wpa
(config-wlan)#no security wpa wpa2
(config-wlan)#no security wpa wpa2 ciphers aes
```

```
(config-wlan)#no security wpa akm dot1x
(config-wlan)#no shutdown
```

Policy Profile Configuration

Inside a Policy Profile, you can decide to assign the clients to which VLAN, 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 one.

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.

The screenshot displays the 'Policy Profile' configuration interface. On the left, a dark sidebar contains menu items: 'Dashboard', 'Monitoring', 'Configuration' (highlighted), and 'Administration'. The main content area is titled 'Policy Profile' and features two buttons: a blue '+ Add' button (highlighted with a red box) and a grey 'x Delete' button. Below these buttons is a table with two columns: 'Policy Profile Name' and 'Description'. The table contains two entries: 'voice' and 'default-policy-profile'. The 'default-policy-profile' row is highlighted with a red box and includes a checkbox on the left. Below the table, there is a pagination control showing '1' items per page and a dropdown menu set to '10 items per page'.

Ensure the profile is enabled.

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

Description

Status ENABLED

Passive Client DISABLED

Encrypted Traffic Analytics DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

WLAN Switching Policy

Central Switching ENABLED

Central Authentication ENABLED

Central DHCP ENABLED

Flex NAT/PAT DISABLED

Step 2. Choose the VLAN.

Navigate to the **Access Policies** tab and choose the VLAN name from the drop-down or manually type the VLAN-ID. Do not configure an ACL in the policy profile.

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select ▼

VLAN

VLAN/VLAN Group

VLAN1416 ▼

Multicast VLAN

Enter Multicast VLAN

WLAN ACL

IPv4 ACL

Search or Select ▼

IPv6 ACL

Search or Select ▼

URL Filters

Pre Auth

Search or Select ▼

Post Auth

Search or Select ▼

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 accounting method too.

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

DHCP

IPv4 DHCP Required

DHCP Server IP Address

[Show more >>>](#)

AAA Policy

Allow AAA Override

NAC State

NAC Type

Policy Name

Accounting List ⓘ ✕

WGB Parameters

Broadcast Tagging

WGB VLAN

Policy Proxy Settings

ARP Proxy DISABLED

IPv6 Proxy

Fabric Profile

Link-Local Bridging

mDNS Service Policy [Clear](#)

Hotspot Server

User Defined (Private) Network

Status

Drop Unicast

DNS Layer Security

DNS Layer Security Parameter Map [Clear](#)

Flex DHCP Option for DNS ENABLED

Flex DNS Traffic Redirect IGNORE

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Air Time Fairness Policies

2.4 GHz Policy

5 GHz Policy

EoGRE Tunnel Profiles


Tunnel Profile

CLI:

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

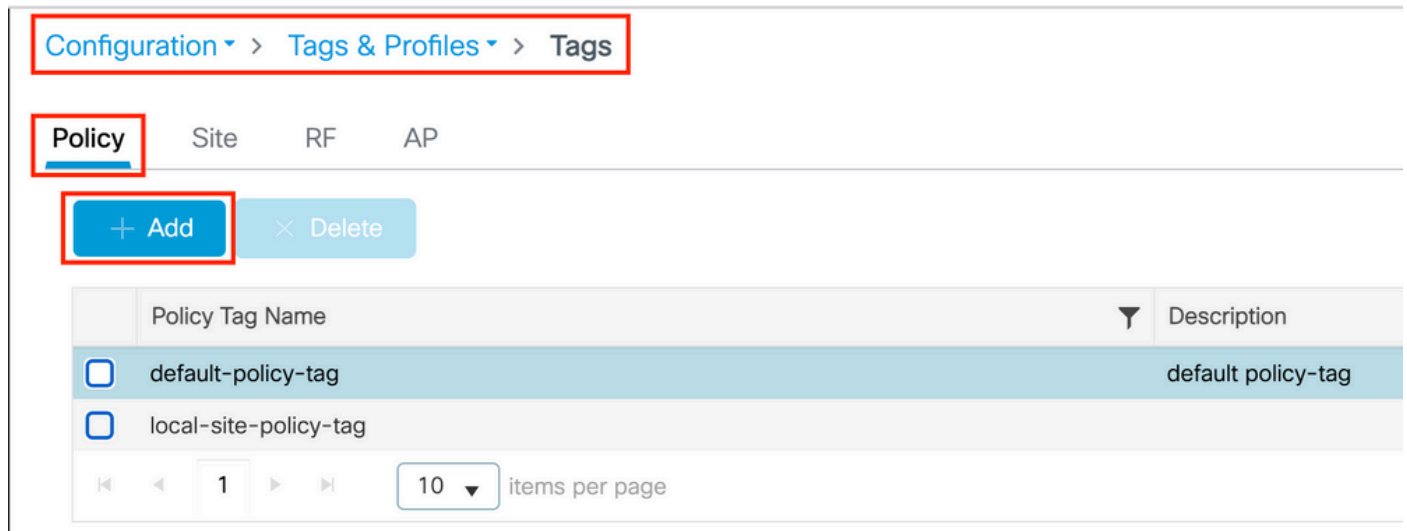
Policy Tag Configuration

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 can not be modified or deleted. If you have a WLAN with ID 17 or later the default-policy tag can not be used.

GUI:

Navigate to [Configuration > Tags & Profiles > Tags > Policy](#) and add a new one if needed as shown in the image.



Configuration > Tags & Profiles > Tags

Policy Site RF AP

+ Add × Delete

Policy Tag Name	Description
<input type="checkbox"/> default-policy-tag	default policy-tag
<input type="checkbox"/> local-site-policy-tag	

1 10 items per page

Link your WLAN Profile to the desired Policy Profile.

Add Policy Tag ✕

Name*

Description

▼ **WLAN-POLICY Maps: 1**

+ Add
✕ Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> cwa-ssid	default-policy-profile

⏪ ⏩ 1 10 items per page 1 - 1 of 1 items

➤ **RLAN-POLICY Maps: 0**

↶ Cancel
📄 Apply to Device

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:

In order 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`.

Edit AP

- General**
- Interfaces
- High Availability
- Inventory
- ICap
- Advanced
- Support Bundle

General	Tags
AP Name*	⚠ Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.
Location*	
Base Radio MAC	Policy <input type="text" value="cwa-policy-tag"/>
Ethernet MAC	Site <input type="text" value="default-site-tag"/>
Admin Status <input checked="" type="checkbox"/> ENABLED	RF <input type="text" value="default-rf-tag"/>
AP Mode <input type="text" value="Local"/>	Write Tag Config to AP <input type="checkbox"/> ⓘ
Operation Status Registered	

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

In order to assign the same Policy Tag to several APs, navigate to [Configuration > Wireless > Wireless Setup > Advanced > Start Now](#).

Start

Tags & Profiles



WLAN Profile



Policy Profile



Policy Tag



AP Join Profile



Flex Profile



Site Tag



RF Profile



RF Tag



Apply

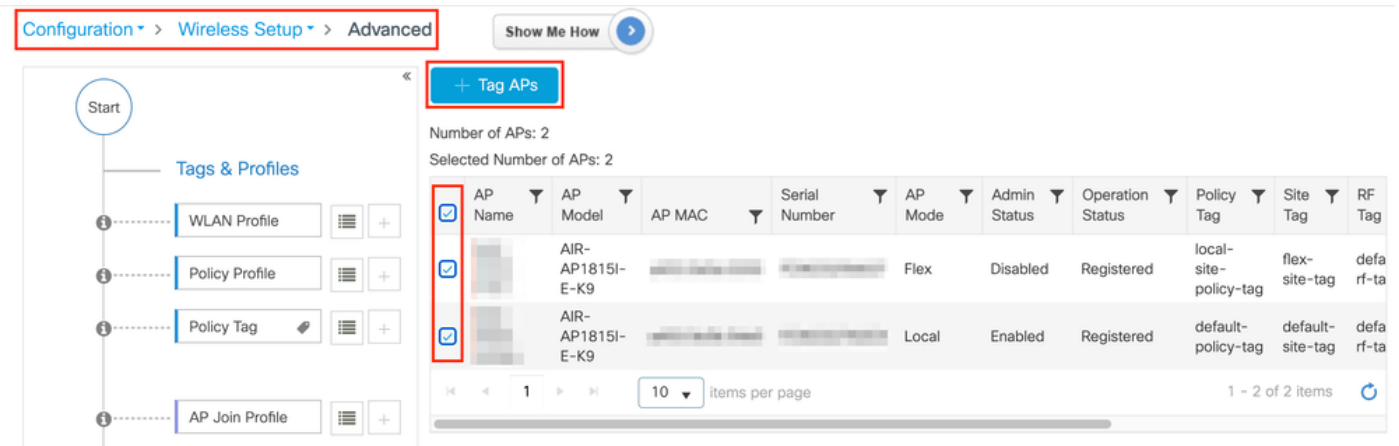


Tag APs

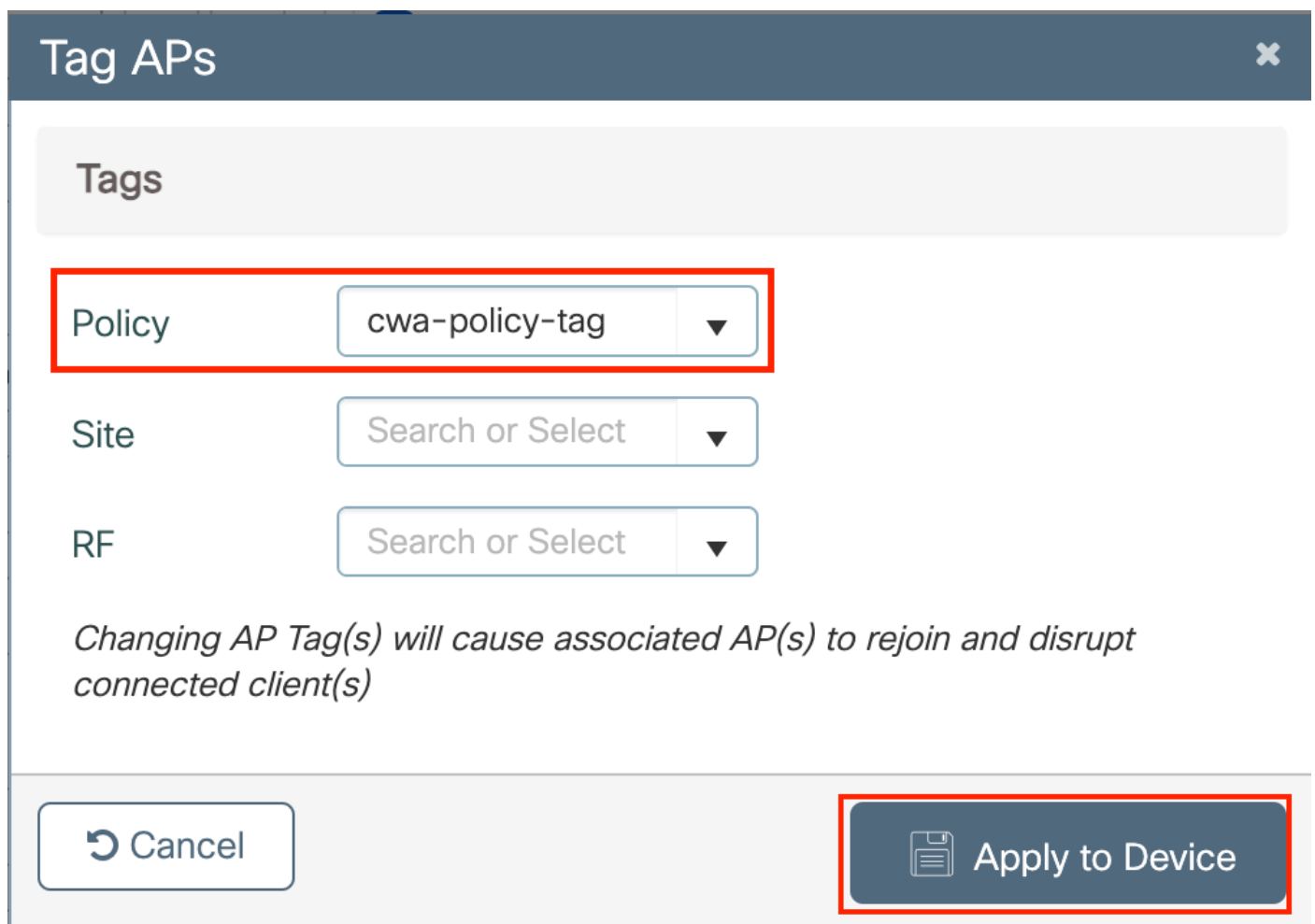


Start Now →

Done



Choose the wished Tag and click Save & Apply to Device as shown in the image.



CLI:

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

end

Redirect ACL Configuration

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

Choose a name for the ACL, and make it IPv4 Extended type and add every rule as a sequence as shown in the image.

ACL Name* REDIRECT ACL Type IPv4 Extended

Rules

Sequence* 1 Action deny

Source Type any

Destination Type Host Host Name* <ISE-ip> **This field is mandatory**

Protocol ip

Log DSCP None

+ Add × Delete

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
0										

10 items per page No items to display

Cancel Apply to Device

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 defines what traffic goes to the CPU (on permits) for further treatment (like redirection) and what traffic stays on the data plane (on deny) and avoids redirection.

The ACL must look like this (replace 10.48.39.28 with your ISE IP address in this example):


Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
<input type="checkbox"/> 10	deny	any		10.48.39.28		ip			None	Disabled
<input type="checkbox"/> 20	deny	10.48.39.28		any		ip			None	Disabled
<input type="checkbox"/> 30	deny	any		any		udp		eq domain	None	Disabled
<input type="checkbox"/> 40	deny	any		any		udp	eq domain		None	Disabled
<input type="checkbox"/> 50	permit	any		any		tcp		eq www	None	Disabled

1 items per page 1 - 5 of 5 items

Note: For the redirection ACL, think of the deny action as a deny redirection (not deny traffic) and the permit action as permit redirection. The WLC only looks into traffic that it can redirect (ports 80 and 443 by default).

CLI:

```
ip access-list extended REDIRECT
deny ip any host <ISE-IP>
deny ip host<ISE-IP> any
deny udp any any eq domain
deny udp any eq domain any
permit 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 also redirects HTTPS, which is often undesirable as it has to provide its own certificate and always creates a certificate violation. This is the exception to the previous statement that says you do not need a certificate on the WLC in case of CWA: you need one if you have HTTPS interception enabled but it is never considered valid anyway.

You can improve the ACL by action to deny only the guest port 8443 to the ISE server.

Enable Redirection for HTTP or HTTPS

The web admin portal configuration is tied with the web authentication portal configuration and it needs to listen on port 80 in order to redirect. Therefore, HTTP has to be enabled for the redirection to work properly. You can either choose to enable it globally (with the use of the command `ip http server`) or you can enable HTTP for the web authentication module only (with the use of the command `webauth-http-enable` under the parameter map).



Note: The redirection of the HTTP traffic happens inside CAPWAP, even in case of FlexConnect Local Switching. Since it is the WLC doing the interception work, the AP sends the HTTP(S) packets inside the CAPWAP tunnel and receive the redirection from the WLC back in CAPWAP

If you want to be redirected when you try to access an HTTPS URL, then add the command `intercept-https-enable` under the parameter map but note this is not an optimal configuration, that it has an impact on the WLC CPU and generates certificate errors anyway:

```
<#root>
```

```
parameter-map type webauth global  
type webauth
```

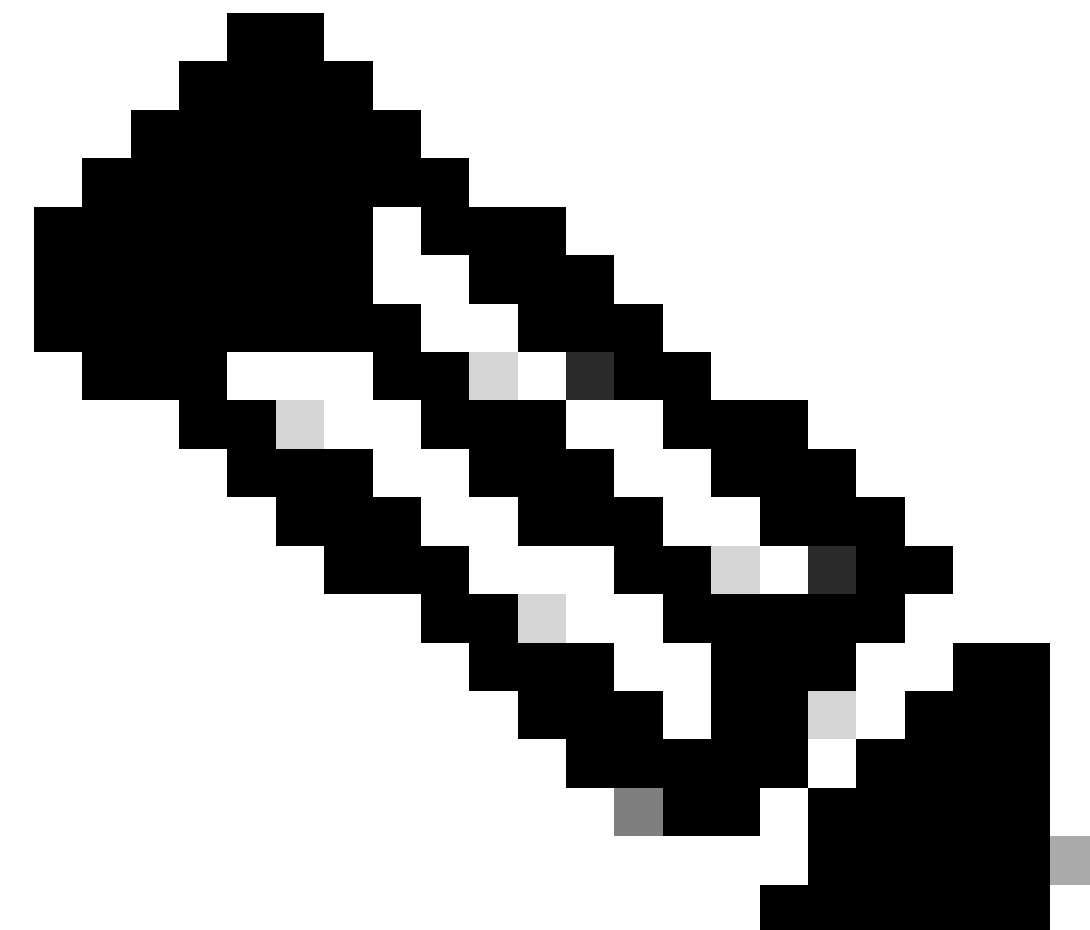
```
intercept-https-enable
```

```
trustpoint xxxx
```

You can also do it via the GUI with the option 'Web Auth intercept HTTPS' checked in the Parameter Map (Configuration > Security > Web Auth).

The screenshot shows the 'Edit Web Auth Parameter' configuration page. On the left is a navigation sidebar with options: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled 'Configuration > Security > Web Auth' and contains a table of parameter maps. The table has one entry named 'global' with a checkbox selected. Below the table is a pagination control showing '1' of 10 items per page. To the right is the 'Edit Web Auth Parameter' form with the following fields:

- Maximum HTTP connections: 100
- Init-State Timeout(secs): 120
- Type: webauth
- Virtual IPv4 Address: (empty)
- Trustpoint: --- Select ---
- Virtual IPv6 Address: x:x:x:x:x
- Web Auth intercept HTTPS: (highlighted with a red box)
- Captive Bypass Portal:



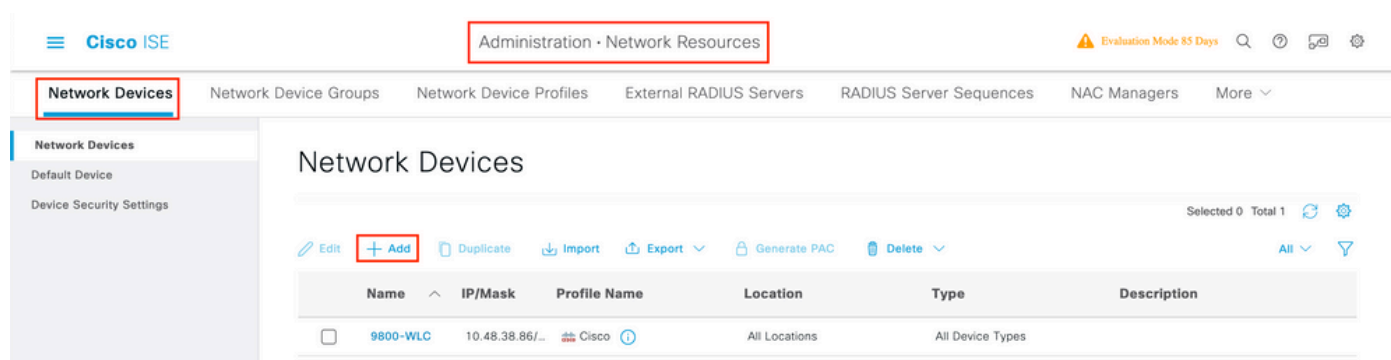
Note: By default, browsers use an HTTP website to initiate the redirection process, if HTTPS

redirection is needed then Web Auth intercept HTTPS has to be checked; however, this configuration is not recommended as it increases CPU usage.

ISE Configuration

Add 9800 WLC to ISE

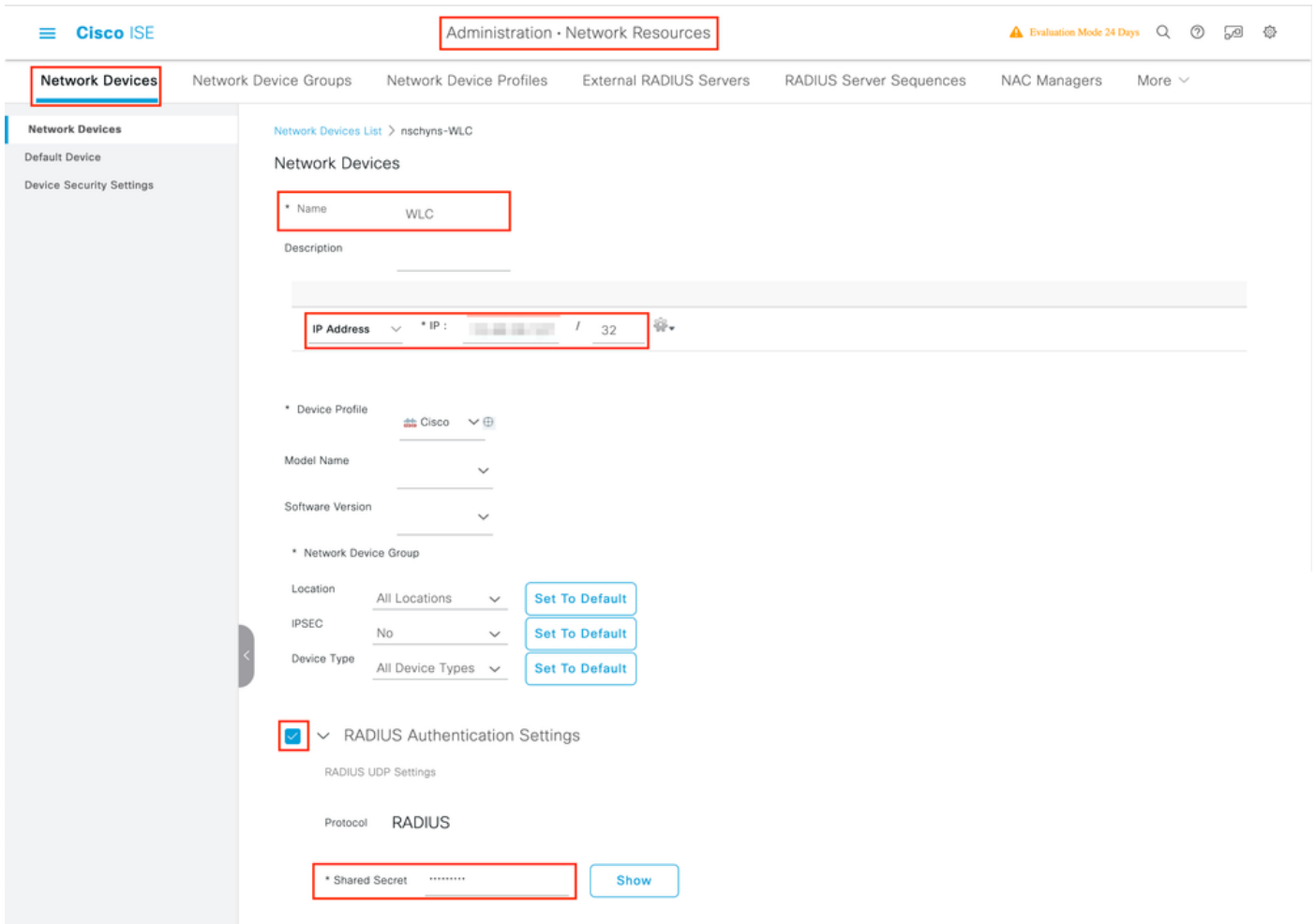
Step 1. Open the ISE console and navigate to Administration > Network Resources > Network Devices > Add as shown in the image.



Step 2. Configure the network device.

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

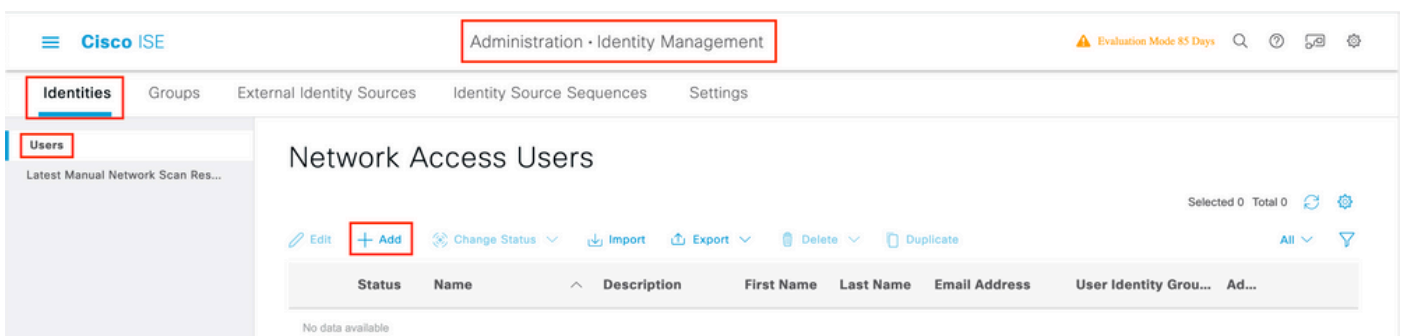
The IP address here corresponds to the WLC interface that sends the authentication requests. By default it is the management interface as shown in the image:



For more information about Network Device Groups, review the ISE admin guide Chapter: Manage Network Devices: [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.

Cisco ISE Administration - Identity Management

Evaluation Mode 85 Days

Identities | Groups | External Identity Sources | Identity Source Sequences | Settings

Users

Latest Manual Network Scan Res...

Network Access Users List > New Network Access User

Network Access User

* Name user1

Status Enabled

Email

Passwords

Password Type: Internal Users

* Login Password Password Re-Enter Password

Generate Password

Enable Password

> User Information

> Account Options

> Account Disable Policy

User Groups

ALL_ACCOUNTS (default)

Create Authorization Profile

The policy profile is the result assigned to a client based on its parameters (such 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.

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

Step 1. Navigate to Policy > Policy Elements > Results > Authorization > Authorization Profiles. Click add in order to create your own or edit the Cisco_Webauth default result.

Cisco ISE Policy - Policy Elements

Evaluation Mode 24 Days

Dictionarys | Conditions | Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Standard Authorization Profiles

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Selected 0 Total 11

Edit + Add Duplicate Delete

Name	Profile	Description
Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices. Ensure that you config
Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
Cisco_Temporal_Onboard	Cisco	Onboard the device with Cisco temporal agent
Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA portal.

Step 2. Enter the redirection information. Ensure that the ACL name is the same as that was configured on the 9800 WLC.

The screenshot shows the Cisco ISE interface for configuring an Authorization Profile. The breadcrumb navigation is "Policy > Policy Elements". The left sidebar shows "Authentication" > "Authorization" > "Authorization Profiles" selected. The main content area is titled "Authorization Profile" and shows the following configuration:

- Name: Cisco_WebAuth
- Description: Default Profile used to redirect users to the CWA portal.
- Access Type: ACCESS_ACCEPT
- Network Device Profile: Cisco
- Service Template:
- Track Movement:
- Agentless Posture:
- Passive Identity Tracking:

Under "Common Tasks", the "Web Redirection (CWA, MDM, NSP, CPP)" checkbox is checked. Below it, the configuration is: Centralized Web Auth > ACL REDIRECT > Value Self-Registered Guest Portal (c).

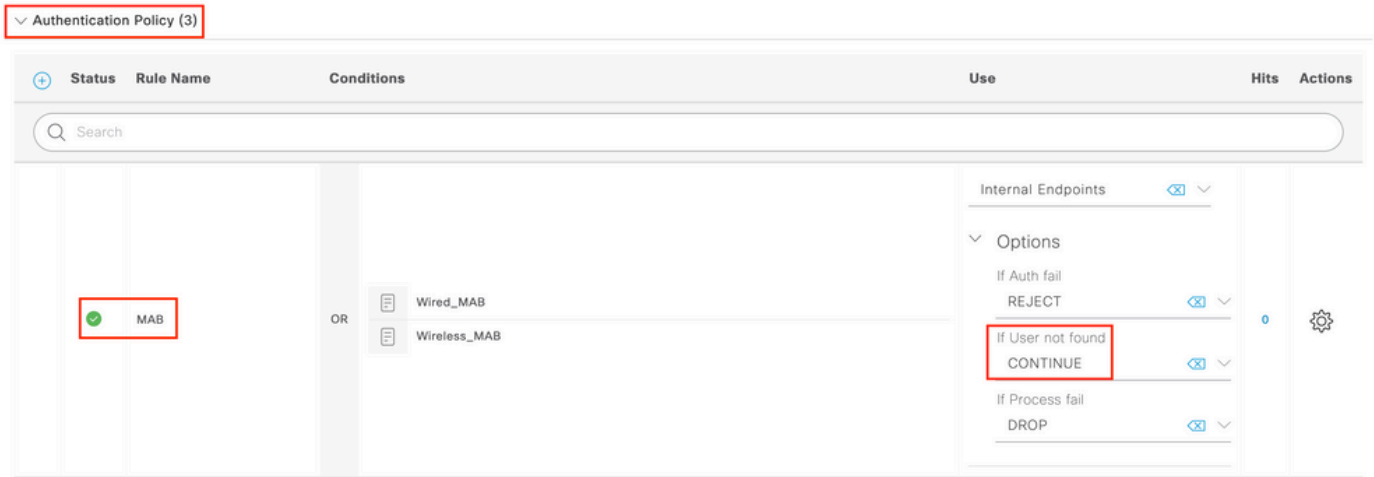
Configure Authentication Rule

Step 1. A Policy Set defines a collection of Authentication and Authorization rules. To create one, navigate to Policy > Policy Sets, click on the gear of the first Policy Set in the list and choose Insert new row or click the blue arrow on the right to choose the default Policy Set.

The screenshot shows the Cisco ISE interface for the "Policy Sets" configuration page. The breadcrumb navigation is "Policy > Policy Sets". The page title is "Policy Sets". There are buttons for "Reset", "Reset Policyset Hitcounts", and "Save". Below the buttons is a table with the following columns: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, Hits, Actions, and View.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<input checked="" type="checkbox"/>	Default	Default policy set		Default Network Access	70		

Step 2. Expand Authentication policy. For the MAB rule (match on wired or wireless MAB), expand Options, and choose the CONTINUE option in case you see 'If User not found'.



Step 3. Click **Save** in order to save the changes.

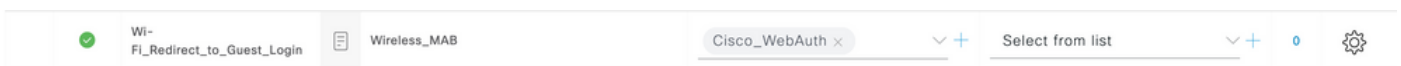
Configure Authorization Rules

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

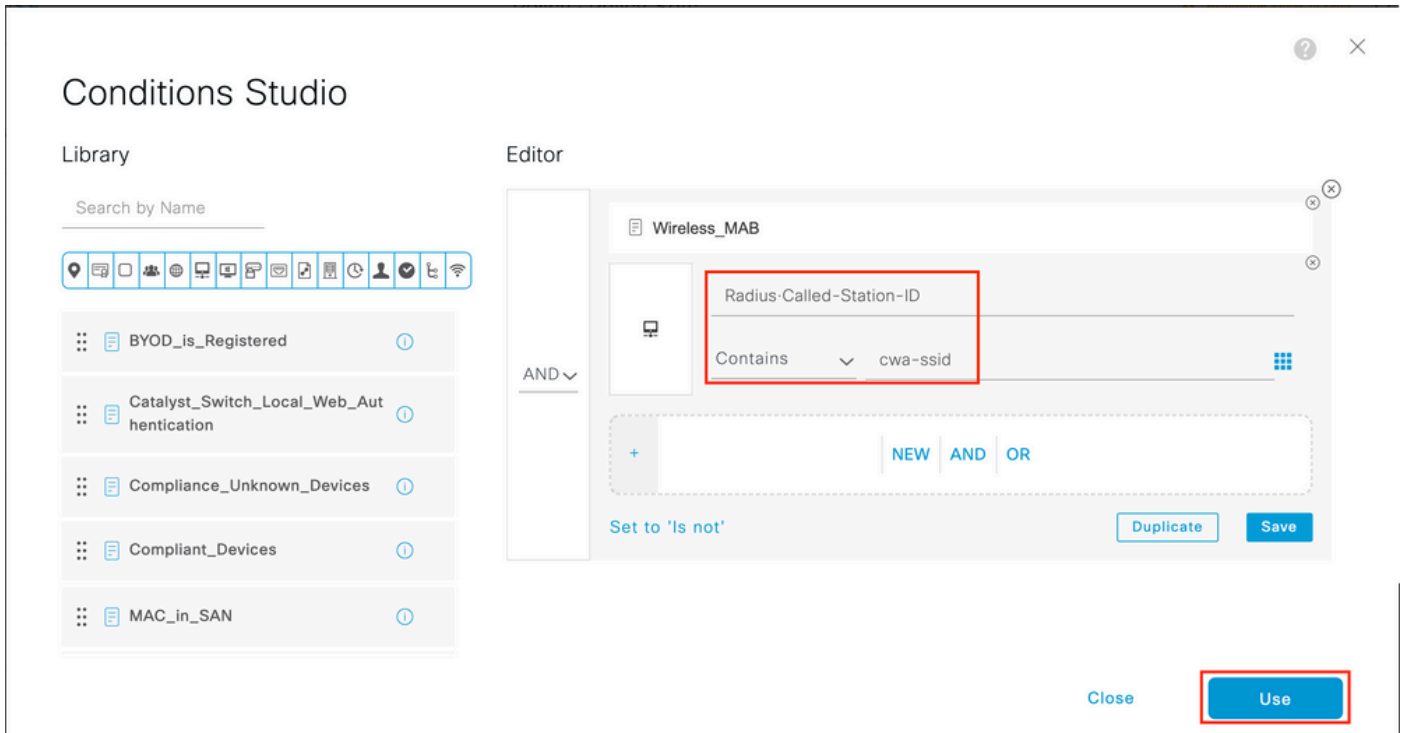
Step 1. On the same Policy set page, close down the **Authentication Policy** and expand **Authorziation Policy** as shown in the image.



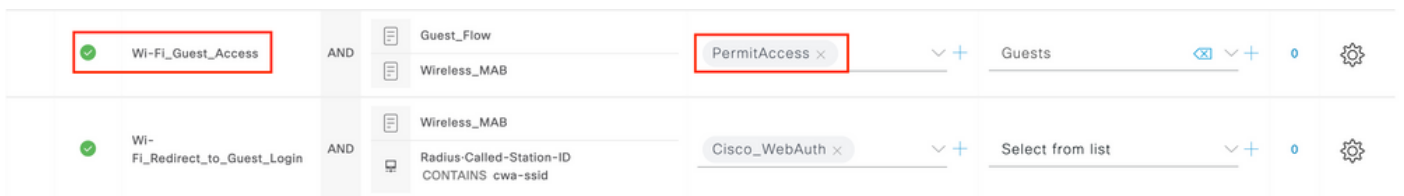
Step 2. Recent ISE versions start with a pre-created rule called **Wifi_Redirect_to_Guest_Login** which matches mostly our needs. Turn the grey sign on the left to **enable**.



Step 3. That rule matches **Wireless_MAB** only and returns the CWA redirection attributes. Now, you can optionally add a little twist and make it match only the specific SSID. Choose 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 with the **Use** at the bottom of the screen as shown in the image.



Step 4. You now need a second rule, defined with a higher priority, that matches 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 list restrictions.



Step 5. Save the rules.

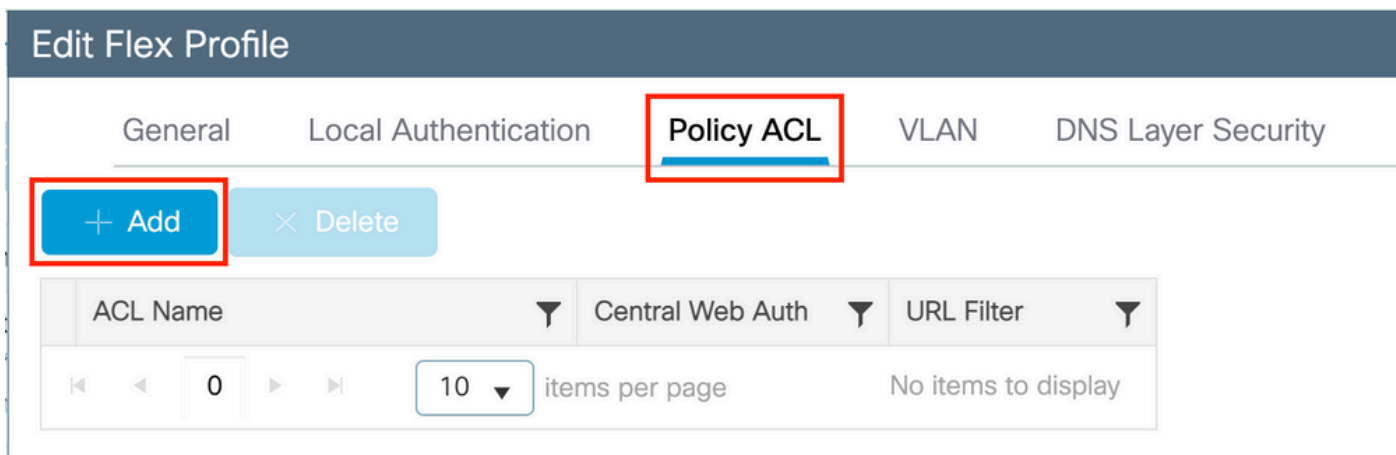
Click **Save** at the bottom of the rules.

Flexconnect Local Switching Access Points Only

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

Navigate to **Configuration > Tags & Profiles > Flex** and choose your Flex profile. Then, navigate to the **Policy ACL** tab.

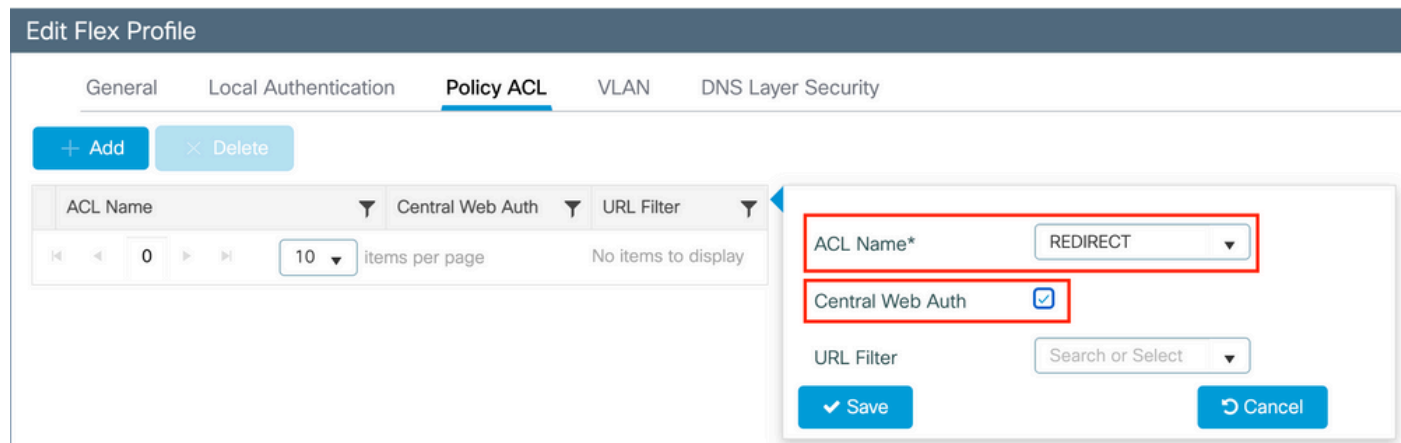
Click **Add** as shown in the image.



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 Cisco IOS XE. However, on the AP the 'deny' statement means the opposite. So, this checkbox automatically swaps all permits and denies them when it does the push to the AP. You can verify this with a `show ip access list` from the AP CLI).

Note: In Flexconnect local switching scenario, the ACL must specifically mention return statements (which is not necessarily required in local mode), so ensure that all your ACL rules cover both ways of traffic (to and from the ISE for example).

Do not forget to hit `Save` and then `Update` and apply to the device.



Certificates

In order 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 is the ISE certificate (which has to be trusted by the client).

Verify

You can use these commands to verify the 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 that corresponds to this example:

```
aaa new-model
!
aaa authorization network CWAauthz group radius
aaa accounting identity CWAacct start-stop group radius
!
aaa server radius dynamic-author
  client <ISE-IP> server-key cisco123
!
aaa session-id common
!
!
radius server ISE-server
  address ipv4 <ISE-IP> auth-port 1812 acct-port 1813
  key cisco123
!
!
wireless aaa policy default-aaa-policy
wireless cts-sxp profile default-sxp-profile

wireless profile policy default-policy-profile
  aaa-override
  nac
  vlan 1416
  no shutdown
wireless tag policy cwa-policy-tag
  wlan cwa-ssid policy default-policy-profile
wlan cwa-ssid 4 cwa-ssid
  mac-filtering CWAauthz
  no security ft adaptive
  no security wpa
  no security wpa wpa2
  no security wpa wpa2 ciphers aes
  no security wpa akm dot1x
  no shutdown

ip http server (or "webauth-http-enable" under the parameter map)
ip http secure-server
```

Troubleshoot

Checklist

- Ensure the client connects and gets a valid IP address.
- If the redirection is not automatic, open a browser and try a random IP address. For example, 10.0.0.1. If redirection works, it is possible that you have a DNS resolution problem. Verify that you have a valid DNS server provided via DHCP and that it can resolve hostnames.
- Ensure that you have the command `ip http server` configured for redirection on HTTP to work. The web admin portal configuration is tied with the web authentication portal configuration and it needs to be listed on port 80 in order to redirect. You can either choose to enable it globally (with the use of the command `ip http server`) or you can enable HTTP for the web authentication module only (with the use of the command `webauth-http-enable` under the parameter map).
- If you are not redirected when you try to access an HTTPS URL and that is required, then verify that you have the command `intercept-https-enable` under the parameter map:

```
<#root>
```

```
parameter-map type webauth global  
type webauth
```

```
intercept-https-enable
```

```
trustpoint xxxxx
```

You can also check via the GUI that you have the option 'Web Auth intercept HTTPS' checked in the Parameter Map:

The screenshot shows the Cisco Catalyst 9800 Series Wireless Controller GUI. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled 'Configuration > Security > Web Auth'. It shows a list of Parameter Map Names with 'global' selected. The right pane is titled 'Edit Web Auth Parameter' and contains the following configuration options:

Maximum HTTP connections	100
Init-State Timeout(secs)	120
Type	webauth
Virtual IPv4 Address	
Trustpoint	--- Select ---
Virtual IPv6 Address	XXXX:XX:XX:XX
Web Auth intercept HTTPS	<input checked="" type="checkbox"/>
Captive Bypass Portal	<input type="checkbox"/>

Service Port Support for RADIUS

The Cisco Catalyst 9800 Series Wireless Controller has a service port that is referred to as GigabitEthernet opport. As from version 17.6.1, RADIUS (that includes CoA) is supported through this port.

If you want to use the Service Port for RADIUS, then you need this configuration:

```
<#root>

aaa server radius dynamic-author
client 10.48.39.28

vrf Mgmt-intf

  server-key cisco123

interface GigabitEthernet0

vrf forwarding Mgmt-intf

  ip address x.x.x.x x.x.x.x


!if using aaa group server:
aaa group server radius group-name
server name nicoISE

ip vrf forwarding Mgmt-intf

ip radius source-interface GigabitEthernet0
```

Collect Debugs

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

 **Note:** You can go back a few hours to several days in the logs but it depends on the volume of logs generated.

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

Step 1. Check the WLC 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 WLC buffer or the external syslog as dictated by the system configuration. This provides a quick view into the health of the system and errors if any.


```
# show logging
```

Step 3. Verify if any debug conditions are enabled.

```
# show debugging
```


```
Cisco IOS XE Conditional Debug Configs:
```

```
Conditional Debug Global State: Stop
```

```
Cisco IOS XE Packet Tracing Configs:
```

```
Packet Infra debugs:
```

```
Ip Address _____ Port  
-----|-----
```

 **Note:** If you see any condition listed, it means the traces are logged up to debug level for all the processes that encounter the enabled conditions (mac address, IP address, and so on). This increases the volume of logs. Therefore, it is recommended to clear all conditions when you do not actively debug.

Step 4. With the assumption that the 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-
```

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 provides debug-level traces for all processes that interact with the specified condition (client mac address in this case). In order to enable conditional debugging, proceed with these steps.


Step 5. Ensure there are no debug conditions enabled.

```
# clear platform condition all
```

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

These 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 the 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_aaaabbbccccc_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.
```

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 take only 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 r
```

 **Note:** This command output returns traces for all log levels for all processes and is quite voluminous. 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 troubleshoot session.

Examples

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

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

In the next example, ISE rejected authentication because no authorization rule matched. This is because you see the Called-station-ID attribute sent as the SSID name appended to the AP mac address, while the authorization is an exact match to the SSID name. It gets fixed with the change of that rule to 'contains' instead of 'equal'.

Event	5400 Authentication failed
Failure Reason	15039 Rejected per authorization profile
Resolution	Authorization Profile with ACCESS_REJECT attribute was selected as a result of the matching authorization rule. Check the appropriate Authorization policy rule-results.
Root cause	Selected Authorization Profile contains ACCESS_REJECT attribute
Username	E8:36:17:1F:A1:62

```
15048 Queried PIP - Radius.NAS-Port-Type
15048 Queried PIP - Network Access.UserName
15048 Queried PIP - IdentityGroup.Name (2 times)
15048 Queried PIP - EndPoints.LogicalProfile
15048 Queried PIP - Radius.Called-Station-ID
15048 Queried PIP - Network Access.AuthenticationStatus
15016 Selected Authorization Profile - DenyAccess
15039 Rejected per authorization profile
11003 Returned RADIUS Access-Reject
```

Other Attributes

ConfigVersionId	140
Device Port	58209
DestinationPort	1812
RadiusPacketType	AccessRequest
Protocol	Radius
NAS-Port	71111
Framed-MTU	1485
OriginalUserName	e836171fa162
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	nicolse26/356963261/1
UseCase	Host Lookup
SelectedAuthenticationIdentityStores	Internal Endpoints
IdentityPolicyMatchedRule	MAB
AuthorizationPolicyMatchedRule	Default
EndPointMACAddress	E8-36-17-1F-A1-62
ISEPolicySetName	Default
IdentitySelectionMatchedRule	MAB
DTLSSupport	Unknown
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
RADIUS Username	E8:36:17:1F:A1:62
NAS-Identifler	cwa-ssid
Device IP Address	10.48.71.120
CPMSessionID	7847300A0000012DFC227BF1
Called-Station-ID	00-27-e3-8f-33-a0:cwa-ssid
CiscoAVPair	service-type=Call Check, audit-session-id=7847300A0000012DFC227BF1, method=mab, client-if-id=3003124185, vlan-id=1468, cisco-wlan-ssid=cwa-ssid

Troubleshooting > Radioactive Trace

Conditional Debug Global State: **Stopped**

MAC/IP Address	Trace file	
<input type="checkbox"/> e836.171f.a162	debugTrace_e836.171f.a162.txt ↓	<input type="button" value="Generate"/>

< 1 > 10 items per page 1 - 1 of 1 items

In this case, the problem lies with the fact that you made a typo when you created the ACL name and it does not match the ACL name returned by ISEs or the WLC complains there is no such ACL as the one requested by ISE:

```

2019/09/04 12:00:06.507 {wncd_x_R0-0}{1}: [client-auth] [24264]: (ERR): MAC: e836.171f.a162 client aut
2019/09/04 12:00:06.516 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [24264]: (ERR): SANET_AUTHZ_FAILURE - Redire
2019/09/04 12:00:06.518 {wncd_x_R0-0}{1}: [errmsg] [24264]: (note): %SESSION_MGR-5-FAIL: Authorization
  
```