

Configure Central Web Authentication on SD-Access

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Topology](#)

[Overview](#)

[Configure CWA on Cisco Catalyst Center](#)

[Create the Network Profile](#)

[Create the SSID](#)

[Fabric Provisioning](#)

[Review the Configuration Provisioned to Cisco ISE](#)

[Authorization Profile](#)

[Policy Sets](#)

[Guest Portal Configuration](#)

[Review the Configuration Provisioned to the WLC](#)

[SSID Configuration](#)

[Wireless Policy Profile Configuration](#)

[Policy Tag Configuration](#)

[Redirect ACL Configuration](#)

[Redirect ACL on the Access Point](#)

Introduction

This document describes a step-by-step guide to configure Central Web Authentication (CWA) and outlines verification procedures across all components.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Catalyst Center
- Cisco Identity Services Engine (ISE)
- Catalyst 9800 Wireless Controller Architecture
- Authentication, Authorization, and Accounting (AAA)

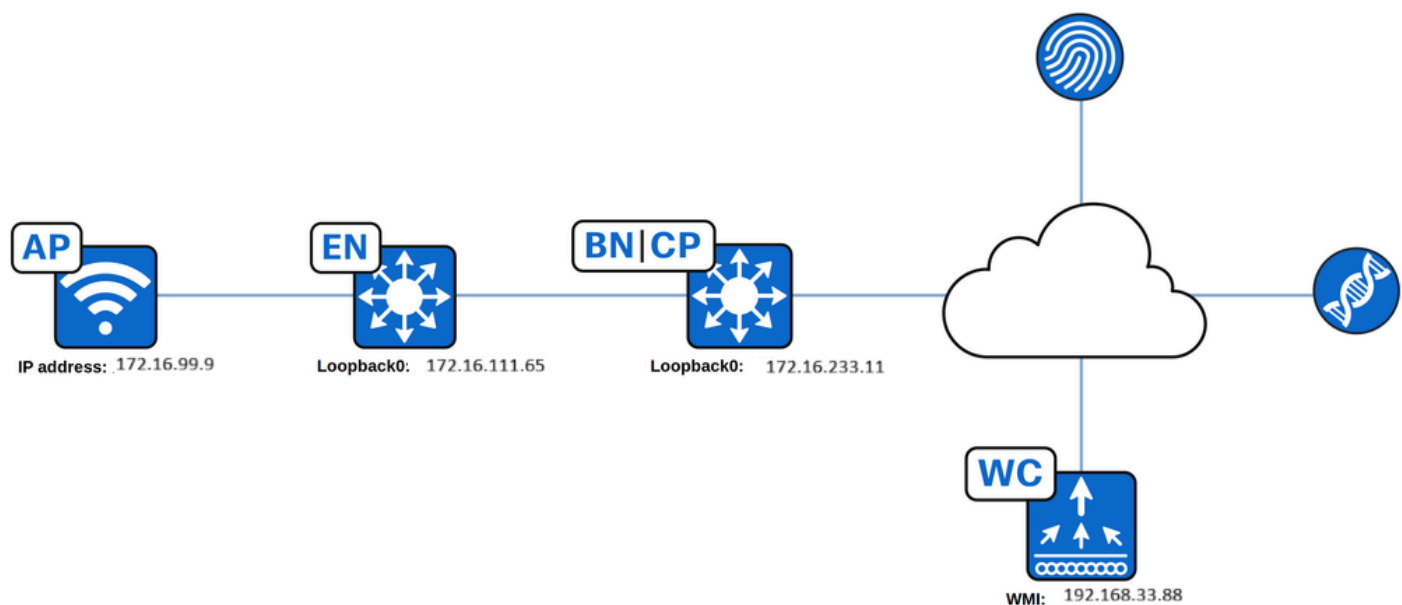
Components Used

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

- Cisco Wireless LAN Controller (WLC) - C9800-CL, Cisco IOS® XE 17.12.04
- Cisco Catalyst Center - Version 2.3.7.7
- Cisco Identity Services Engine (ISE) - Version 3.0.0.458
- SDA Edge Node - C9300-48P, Cisco IOS® XE 17.12.05
- SDA Border Node/Control Plane - C9500-48P, Cisco IOS® XE 17.12.05
- Cisco Access Point - C9130AXI-A, version 17.9.5.47

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.

Topology



Overview

Central Web Authentication (CWA) uses a guest-type SSID to redirect the user's web browser to a captive portal hosted by Cisco ISE, using a configured redirection ACL. The captive portal enables the user to register and authenticate, and after successful authentication, the Wireless LAN Controller (WLC) applies the appropriate authorization to grant full network access. This guide provides step-by-step instructions for configuring CWA using Cisco Catalyst Center.

Configure CWA on Cisco Catalyst Center

Create the Network Profile

A network profile allows configuration of settings that can be applied to a specific site. Network profiles can be created for various elements in Cisco Catalyst Center, including:

- Assurance
- Firewall
- Routing
- Switching
- Telemetry Appliance

- Wireless

For CWA, a wireless profile must be configured.

To configure a wireless profile, navigate to **Design > Network Profiles**, click **Add Profile** and select **Wireless**.

Network Profiles

Network Profiles (119)

Search Table

Profile Name	Type ▴	Sites	Action
+ Add Profile Assurance Firewall Routing Switching Wireless			

Name the profile as required. In this example, the wireless profile is named **CWA_Cisco_Wireless_Profile**. You can add any existing SSIDs to this profile by selecting **Add SSID**. SSID creation is covered in next section.

Add a Network Profile

Following tasks must be completed before creating a Wireless Network Profile.

1. Define SSIDs, Interface, RF Profiles and AP Profiles under [Network Settings > Wireless](#)
2. Define CLI Templates under [CLI Templates](#) (Optional)
3. Define Feature Templates under [Feature Templates](#) (Optional)

Note: Changes in SSIDs, AP Zones, Feature Templates, CLI Templates sections require Controller provisioning. Changes in Custom Tags/Groups require Access Point provisioning.

Profile Name*
CWA_Cisco_Wireless_Profile

Site: [Assign](#)

SSIDs AP Zones Feature Templates CLI Templates Advanced Settings ▾

Add SSID

Select **Assign** to choose the site where this profile is to be applied, and then select the desired **site**. After you select the sites click **Save**.

Profile Name*
CWA_Cisco_Wireless_Profile

Site: [Assign](#)

SSIDs AP Zones Feature Templates CLI Templates Advanced Settings ▾

Add SSID

Create the SSID

Navigate to **Design > Network Settings > Wireless > SSIDs** and click **Add**.

SSIDs

Configure SSIDs for enterprise and guest wireless networks. You can assign them to sites via Wireless Network Profiles.

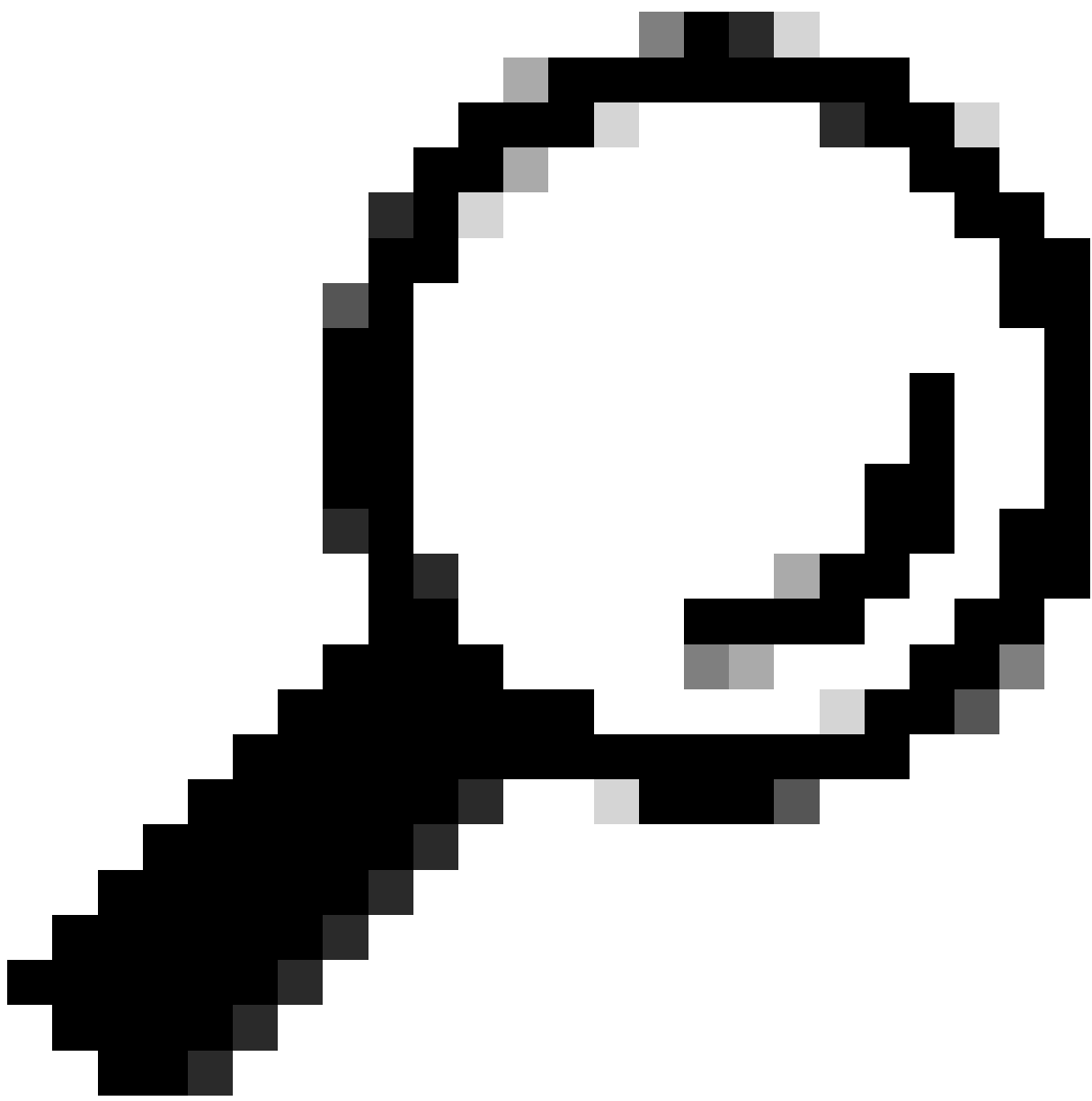
SSID (79)

+ Add

Search Table

Edit Delete SSID Scheduler ⓘ 0 Selected

	Network Name (SSID) ▾	WLAN Profile Name	Policy Profile Name	SSID Type	L2 Security	L3 Security	Wireless Profiles	Portal Name	AAA Servers
☐	1865test	1865test_... (2)	1865test_... (2)	Enterprise	wpa3_personal	open	fernarom_wireless, J... See all	N/A	Configure AAA



Tip: When creating an SSID for CWA, it is essential to select the **Guest type**. This selection adds a command to the SSID's wireless policy profile on the WLC - the **nac** command - which allows

CoA to be used for reauthentication after the user registers on the captive portal. Without this configuration, users can experience an endless loop of registering and being redirected to the portal repeatedly.

After selecting **Add**, proceed through the SSID configuration workflow. On the first page, configure the **SSID name**, you can also select the **radio policy band**, and define the **SSID state**, including **administrative status** and **broadcast settings**. For this configuration guide, the SSID is named CWA_Cisco.

Wireless Network Name (SSID)* CWA_Cisco	WLAN Profile Name* CWA_Cisco_profile	Policy Profile Name CWA_Cisco_profile
--	---	--

Radio Policy

☒ 2.4GHz ☒ 5GHz ☒ 6GHz ⓘ

802.11b/g Policy
802.11bg ▼ ☐ Band Select ⓘ ☐ 6 GHz Client Steering

☐ Fast Lane ⓘ

Quality of Service(QoS) ⓘ

Egress
VoIP (Platinum) ⓘ ▼ Ingress
VoIP (Platinum) Up ⓘ ▼ ⓘ

SSID STATE

☒ Admin Status ☐ Broadcast SSID

After entering the SSID name, the WLAN profile name and policy profile name are automatically generated. Select **Next** to proceed.

At least one AAA/PSN must be configured for CWA SSIDs. If none is configured, select **Configure AAA** and choose the **PSN IP address** from the drop-down list.

Authentication, Authorization, and Accounting Configuration

Atleast one AAA/PSN is required for CWA SSIDs. Configure AAA to add one.

 [Configure AAA](#)

☐ AAA Override	☒ MAC Filtering	☐ Deny RCM Clients ⓘ
---------------------------------------	---	---

Pre-Auth ACL List Name ▼

After selecting the AAA server, set the **Layer 3 security parameters** and select the portal type: **Self-Registered** or **Hotspot**.

Hotspot guest portals: A hotspot guest portal provides network access for guests without the need for usernames and passwords. Here, users must accept an Acceptable Use Policy (AUP) to obtain access to the network, leading to subsequent internet access. **Credentialed guest portals:** Access through a credentialed guest portal requires guests to have a username and password.

L3 SECURITY

☒ Web Policy ☐ Open

Most secure
Guest users are redirected to a Web Portal for authentication

Authentication Server

Central Web Authentication

What kind of portal are you creating today ?

Self Registered

Self Registered

Hotspot

Where will your guests redirect after successful authentication ?

Original URL

The action that occurs after the user registers or accepts the use policy can also be configured. Three options are available: **Success Page**, **Original URL**, and **Custom URL**.

Authentication Server

Central Web Authentication

What kind of portal are you creating today ?

Self Registered

Where will your guests redirect after successful authentication ?

Original URL

Success Page

Original URL

Custom URL

The following describes the behavior of each option:

Success Page: Redirects the user to a confirmation page indicating that authentication was successful.

Original URL: Redirects the user to the original URL that was requested before being intercepted by the captive portal.

Custom URL: Redirects the user to a specified custom URL. Selecting this option enables an additional field to define the destination URL

On the same page, under Authentication, Authorization, and Accounting Configuration, a Pre-auth ACL can also be configured. This ACL allows the addition of extra entries for protocols beyond DHCP, DNS, or PSN IP addresses, which are obtained from the network settings and appended to the redirection ACL during provisioning. This feature is available in Cisco Catalyst Center version 2.3.3.x and later.

Authentication, Authorization, and Accounting Configuration

 AAA Configured (1)

☒ AAA Override

☒ MAC Filtering

☐ Deny RCM Clients 

Pre-Auth ACL List Name 

To configure a Pre-Auth ACL, navigate to **Design > Network Settings > Wireless > Security Settings**, and click **Add**.

Pre-Auth ACLs AP Authorization List AP Impersonation Configure DTLS Ciphersuites

Configure Pre-Auth Access Control Lists. You can assign them to SSIDs during SSID creation or modification.

Pre-Auth Access Control Lists (10)

 Add

The first name identifies the ACL in Catalyst Center, while the second name corresponds to the ACL name on the WLC. The second name can match the existing redirect ACL configured on the WLC. As a reference, Catalyst Center provisions the name Cisco DNA_ACL_WEBAUTH_REDIRECT to the WLC. Entries from the Pre-Auth ACL are appended after the existing entries.

New Pre-Auth ACL

Pre-Auth ACL List Name*
Name_on_Catalyst_Center 

Pre-Auth ACL Name*
DNAC_ACL_WEBAUTH_REDIRECT 

Returning to the SSID creation workflow, selecting **Next** displays the advanced settings, including fast transition, session timeout, client user timeout, and rate limiting. Adjust the parameters as required, then select **Next** to proceed. For the purpose of this configuration guide, the example retains the default settings.

Advanced Settings

Configure the advanced fields to complete SSID setup.

SSID Name: CWA_Cisco (Guest)

MFP Client Protection ⓘ

☒ Optional ☐ Required ☐ Disabled

Protected Management Frame (802.11w)

☐ Optional ☐ Required ☒ Disabled

☒ 11k - Neighbor List

☐ Radius Client Profiling ⓘ

☒ Coverage Hole Detection

WLAN Timeouts

☒ Session Timeout ⓘ

In (secs)*
28800
Range is from 1 to 86400

☒ Client Exclusion

In (secs)*
180
Range is from 0 to 2147483647

☒ Client User Idle Timeout

In (secs)*
300
Range is from 15 to 100000

11v BSS Transition Support

☒ BSS Max Idle Service

☒ Directed Multicast Service

After selecting Next, a prompt appears to associate any feature templates with the SSID. If applicable, select the desired **templates** by clicking **Add**, and when finished, click **Next**.

Associate Feature Templates to SSID

Select a design instance from the table or add new design instance to associate the Feature Templates to SSID.

Design Instances

Refresh

Export

Import

Add

Search Table

Associate the SSID with the previously created wireless profile. For reference, see the section **Create the Wireless Network Profile**. In this section you can also select if the SSID is fabric enabled or not. After you are finished, click **Associate profile**.

SSID Name: CWA_Cisco (Guest)

Add Profile

Search

100NG SOM RA

adortiz-test-profile

anarami-wireless

angel test

antvegaprofile

Cnicolet_Oeiras

CWA_Cisco_Wireless_P...

Associate Profile

Cancel

Profile Name

CWA_Cisco_Wireless_Profile

WLAN Profile Name

CWA_Cisco_profile ⓘ

Policy Profile Name

CWA_Cisco_profile ⓘ

Fabric

☒ Yes ☐ No

802.11be Profile Name

▼

show wireless management trustpoint

Once the profile is associated with the SSID, click **Next** to create and design the captive portal, to start,

click **Create Portal**.

SSID Name: CWA_Cisco (Guest)

No Self Registration Portal Available

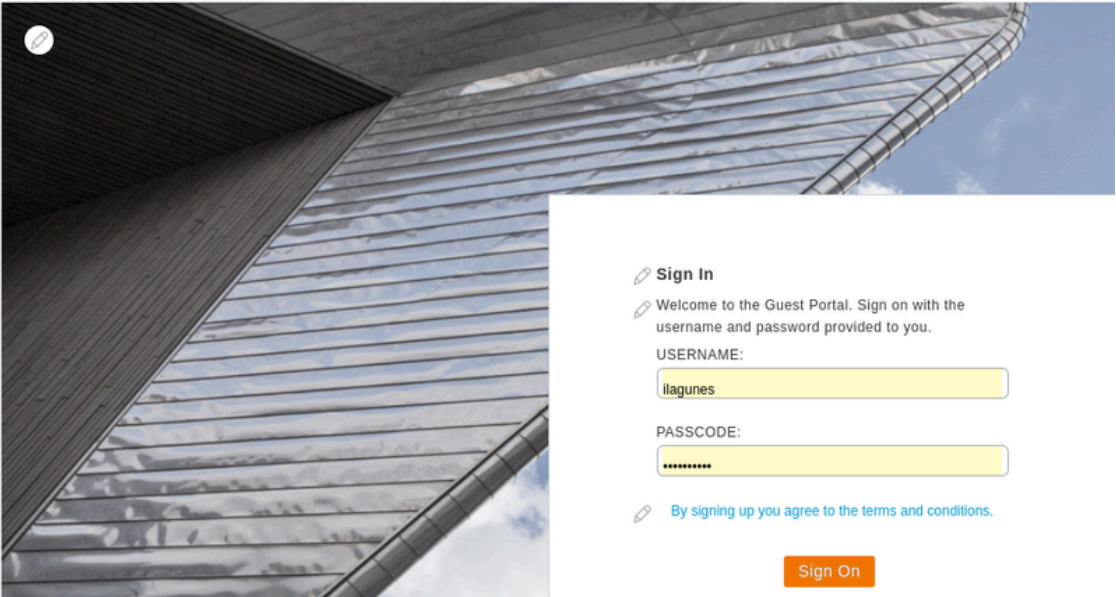
Use the create portal button to create a new portal

Create Portal

The portal name defines the domain name in the FQDN and the policy set name on ISE. Click **Save** when finished. The portal remains editable and can be deleted if necessary.

Portal

CWA_Cisco_Portal		Login Page
> Page Content		
Access Code		
Header Text		



 **Sign In**

 Welcome to the Guest Portal. Sign on with the username and password provided to you.

USERNAME:

PASSCODE:

 By signing up you agree to the terms and conditions.

Sign On

Select **Next** to display a summary of all configuration parameters defined in the previous steps.

Summary

Review all changes

SSID Name: CWA_Cisco (Guest)

> Basic Settings [Edit](#)

> Security Settings [Edit](#)

> Advanced Settings [Edit](#)

∨ Associate Feature Templates to SSID [Edit](#)

Design Instance	N/A
-----------------	-----

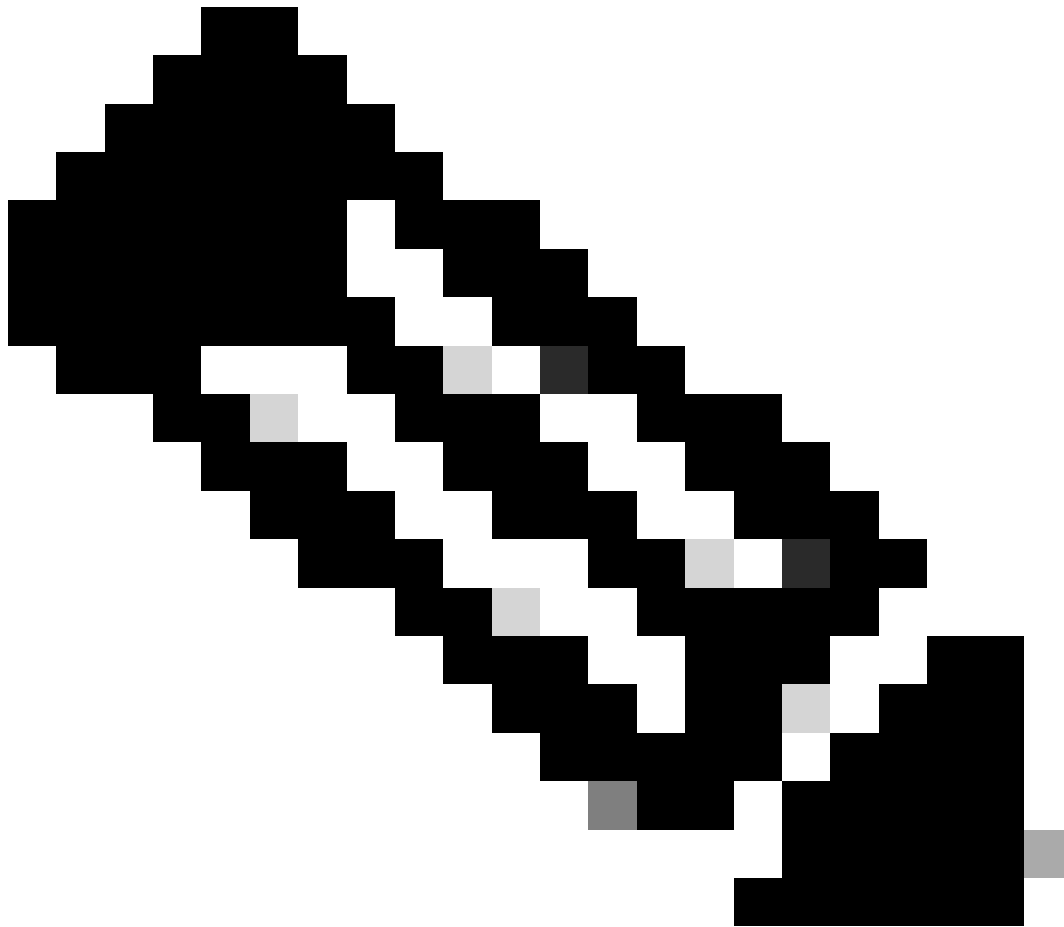
∨ Network Profile Settings [Edit](#)

CWA_Cisco_Wireless_Profile	Fabric (Associated)
----------------------------	-------------------------------------

Confirm the configuration details, and then select **Save** to apply the changes.

Fabric Provisioning

After associating the wireless network profile with the fabric site, the SSID appears under **Provision > Fabric Sites > (Your site) > Wireless SSIDs**.



Note: You need to provision the Wireless LAN Controller for the site for the SSIDs to show under Wireless SSIDs

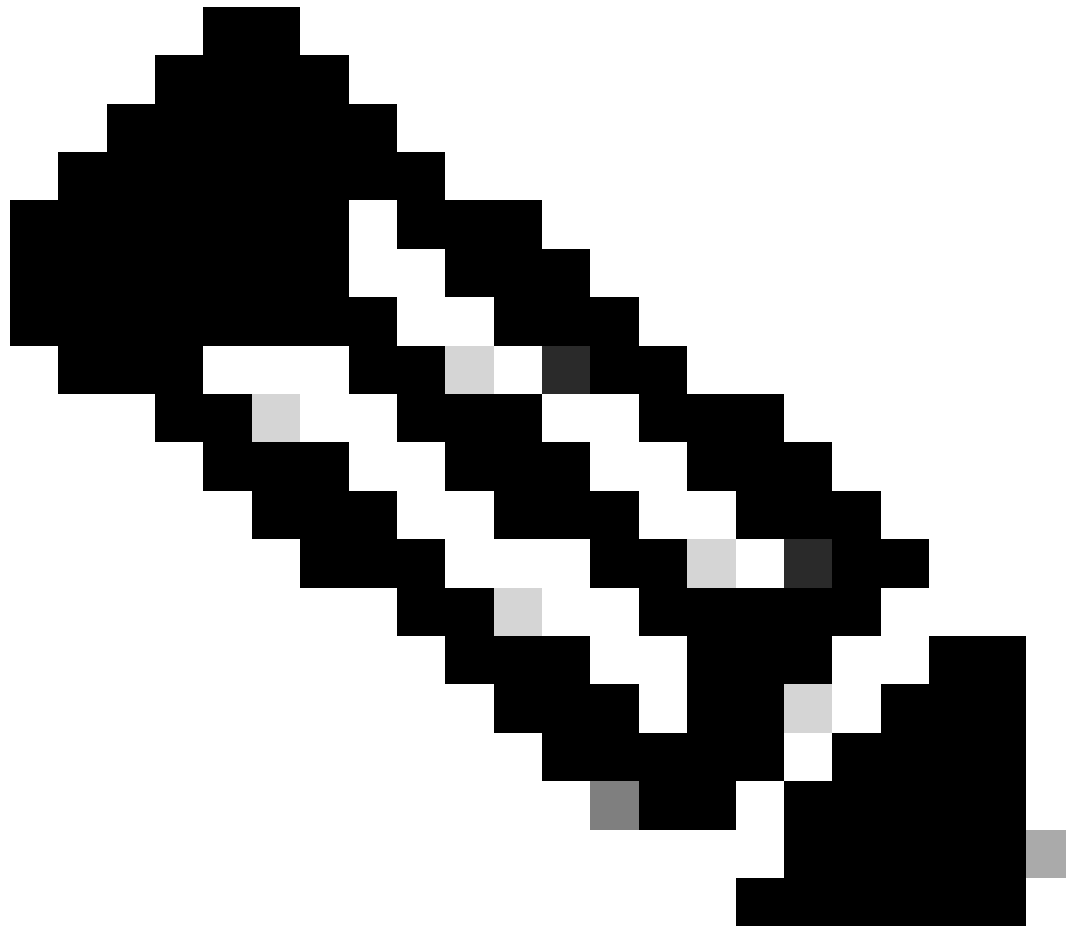
Choose the **SSID pool**, optionally associate a **Security Group Tag**, and click **Deploy**. The SSID is broadcast by access points only if a pool is assigned.

☒ Enable Wireless Multicast ⓘ

SSID Name	Type	Security	Traffic Type	Address Pool	Security Group
CWA_Cisco	Guest	Open	Voice + Data	Choose Pool test ⓘ	Assign SGT

1 Record(s) Show Records: 25 1 - 1 ⓘ

On AireOS and Catalyst 9800 controllers, re-provision the Wireless LAN Controller after any SSID configuration changes in Network Settings.



Note: If no pool is assigned to the SSID, it is expected that the APs do not broadcast it. The SSID is broadcast only after a pool is assigned. Once the pool is assigned, the controller does not need to be re-provisioned.

Review the Configuration Provisioned to Cisco ISE

This section examines the configuration provisioned by Catalyst Center to Cisco ISE.

Authorization Profile

Part of the configuration that Catalyst Center provisions on Cisco ISE is an Authorization Profile. This profile defines the result assigned to a client based on its parameters and can include specific settings such as VLAN assignment, ACLs, or URL redirects.

To view the Authorization Profile in ISE, navigate to **Policy > Policy Elements > Results**. If the portal name is **CWA_Cisco_Portal**, the profile name is **CWA_Cisco_Portal_Profile**. The description field displays the text: DNA generated Authorization Profile for portal - CWA_Cisco_Portal.

Standard Authorization Profiles

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

Selected 0 Total 18

[Edit](#) [+ Add](#) [Duplicate](#) [Delete](#)

All [Filter](#)

☐	Name	Profile	Description
☐	AuthProfile-DNAC	Cisco	SGT Authentication Profile para DNACtl
☐	Block_Wireless_Access	Cisco	Default profile used to block wireless devices. Ensure that you configure a NULL RC
☐	CWA_Cisco_Portal_Profile	Cisco	DNA generated Authorization Profile for portal - CWA_Cisco_Portal

To view the attributes sent to the Wireless LAN Controller by this authorization profile, click the **Authorization Profile name** and refer to the **Common Tasks** section.

This Authorization Profile delivers the Redirect ACL and the Redirect URL.

Web Redirection attribute includes two parameters:

1. ACL Name: Set to Cisco DNA_ACL_WEBAUTH_REDIRECT.
2. Value: Refers to the name of the captive portal, in this example CWA_Cisco_Portal.

The Display Certificates Renewal Message option enables the portal to be used for renewing certificates that the endpoint is currently using.

An additional option, Static IP/Host Name/FQDN, is available under Display Certificates Renewal Message. This feature allows the delivery of the portal's IP address instead of its FQDN, which is useful when the captive portal fails to load due to the inability to reach the DNS server.

Common Tasks

☒ Web Redirection (CWA, MDM, NSP, CPP) [?](#)

Centralized Web Auth [v](#)

ACL

DNAC_ACL_WEBAUTH_RE... [v](#)

Value

CWA_Cisco_Portal [v](#)

☒ Display Certificates Renewal Message

☐ Static IP/Host name/FQDN

☐ Suppress Profiler CoA for endpoints in Logical Profile

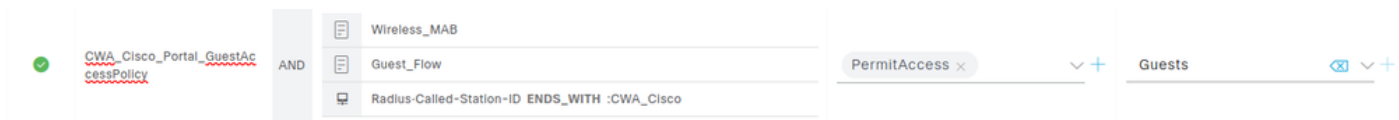
Policy Sets

Navigate to **Policy > Policy Sets > Default > Authorization Policy** to view the two policy sets created for the portal named CWA_Cisco_Portal. These policy sets are:

- CWA_Cisco_Portal_GuestAccessPolicy
- CWA_Cisco_Portal_RedirectPolicy

☒	<u>CWA_Cisco_Portal_GuestAccessPolicy</u>	AND	Wireless_MAB Guest_Flow Radius-Called-Station-ID ENDS_WITH :CWA_Cisco	PermitAccess x v +	Guests x v +
☒	<u>CWA_Cisco_Portal_RedirectPolicy</u>	AND	Wireless_MAB Radius-Called-Station-ID ENDS_WITH :CWA_Cisco	CWA_Cisco_Portal_Pr... x v +	Select from list v +

The CWA_Cisco_Portal_GuestAccessPolicy policy is applied when the client has already completed the web authentication process, either through self-registration or via the hotspot portal.



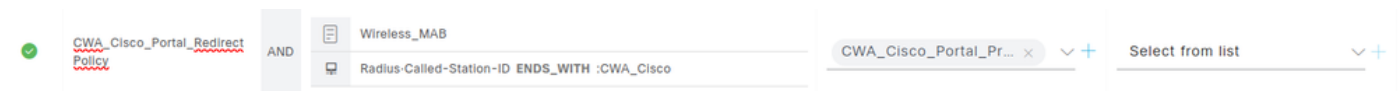
This policy set matches three criteria:

- **Wireless_MAB:** Used when Cisco ISE receives a MAC Authentication Bypass (MAB) authentication request from a Wireless LAN Controller.
- **Guest_Flow:** Refers to ISE checking the MAC address of the endpoint against the GuestEndpoints identity group. If the endpoint MAC address is not present in this group, the policy is not applied.
- **RADIUS Called-Station-ID ENDS_WITH :CWA_Cisco:** The Called-Station-ID is a RADIUS attribute in ISE that stores the bridge or Access Point MAC address in ASCII format and appends the SSID being accessed, separated by a semicolon (;). In this example, CWA_Cisco represents the SSID name.

Under the column profiles you see the name PermitAccess, this is a reserved authorization profile that cannot be edited, which gives full access to the network and you can also assign an SGT under the column Security Groups, which in this case is Guests.

The PermitAccess profile is used. This is a reserved authorization profile that cannot be edited and grants full access to the network. An SGT can also be assigned under the Security Groups column; in this case, the SGT is set to Guests.

The next policy to review is CWA_Cisco_Portal_RedirectPolicy.



This policy set matches the following two criteria:

- **Wireless_MAB:** Used when Cisco ISE receives a MAB authentication request from a Wireless LAN Controller.
- **RADIUS Called-Station-ID ENDS_WITH :CWA_Cisco:** The Called-Station-ID is a RADIUS attribute in ISE that stores the bridge or Access Point MAC address in ASCII format and appends the SSID being accessed, separated by a semicolon (;). In this example, :CWA_Cisco represents the SSID name.

The order of these policies is critical. If CWA_Cisco_Portal_RedirectPolicy appears first in the list, it matches only MAB authentication and the SSID name using the RADIUS attribute Called-Station-ID ENDS_WITH :CWA_Training. In this configuration, even if the endpoint has already authenticated through the portal, it will continue to match this policy indefinitely. As a result, full access is never granted via the PermitAccess profile, and the client remains stuck in a continuous loop of authentication and redirection to the portal.

Guest Portal Configuration

Navigate to **Work Centers > Guest Access > Portals & Components** to view the portal.

The Guest portal created here uses the same name as in Catalyst Center CWA_Cisco_Portal. Select the portal name to if you wish to view additional details.

Guest Portals

Choose one of the three pre-defined portal types, which you can edit, customize, and authorize for guest access.

Create Edit Duplicate Delete

CWA_Cisco_Portal
Wireless Setup Self-Registration Guest Portal
✔ Used in 1 rules in the Authorization policy

Deadpool_Site
Wireless Setup Self-Registration Guest Portal
✔ Used in 1 rules in the Authorization policy

Hotspot Guest Portal (default)
Guests do not require username and password credentials to access the network, but you can optionally require an access code
⚠ Authorization setup required

Review the Configuration Provisioned to the WLC

This section examines the configuration provisioned by Catalyst Center to the Wireless LAN Controller.

SSID Configuration

In the WLC GUI, navigate to **Configuration > Tags & Profiles > WLANs** to view the SSID configuration.

Selected WLANs : 0

☐	Status	Name	ID	SSID	2.4/5 GHz Security
☐	✔	CWA_Cisco_profile	21	CWA_Cisco	[open], MAC Filtering

1 10

The SSID CWA_Cisco is has the name CWA_Cisco_profile on the WLC, with ID 21 and an Open security type using MAC filtering. Double click the **SSID** to view its configuration.

General Security Advanced Add To Policy Tags

Profile Name* CWA_Cisco_profile

SSID* CWA_Cisco

WLAN ID* 21

Status **ENABLED**

Broadcast SSID **ENABLED**

Radio Policy ⓘ

Show slot configuration

6 GHz
Status **DISABLED**

5 GHz
Status **ENABLED**

2.4 GHz
Status **ENABLED**

802.11b/g Policy 802.11b/g

The SSID is UP and broadcasting on both 5 GHz and 2.4 GHz channels and is attached to the policy profile CWA_Cisco_Profile. Click the **Security** tab to view the settings.

☐ WPA + WPA2
 ☐ WPA2 + WPA3
 ☐ WPA3
 ☐ Static WEP
 ☒ None

MAC Filtering ☒

OWE Transition Mode ☐

Lobby Admin Access ☐

Authorization List*

co-0044d514

default
 dnac-cts-CWA_Cisco-0044d514

Fast Transition

Status Disabled

Over the DS ☐

Reassociation Timeout * 20

Key settings include the Layer 2 security method (MAC Filtering) and the AAA authorization list (Cisco DNA-cts-CWA_Cisco-0044d514). To review its configuration, navigate to **Configuration > Security > AAA > AAA Method List > Authorization**.

Servers / Groups AAA Method List AAA Advanced

	Name	Type	Group Type	Group1	Group2	Group3	Group4
☐	default	exec	local	N/A	N/A	N/A	N/A
☐	default	network	local	N/A	N/A	N/A	N/A
☐	dnac-cts-CWA_Traini-6a20f88c	network	group	dnac-rGrp-CWA_Traini-6a20f88c	N/A	N/A	N/A
☐	dnac-cts-Guest_pers-6fc56a40	network	group	dnac-rGrp-Guest_pers-6fc56a40	N/A	N/A	N/A
☐	dnac-cts-CWA_Cisco-0044d514	network	group	dnac-rGrp-CWA_Cisco-0044d514	N/A	N/A	N/A

The method list points to the RADIUS group Cisco DNA-rGrp-CWA_Cisco-0044d514 in the Group1 column. To view its configuration, navigate to **Configuration > Security > AAA > Server/Groups > Server Groups**.

Servers Server Groups

	Name	Server 1	Server 2	Server 3
☐	dnac-rGrp-CWA_Cisco-0044d514	dnac-radius_10.88.244.180	N/A	N/A

The server group group Cisco DNA-rGrp-CWA_Cisco-0044d514 points to Cisco DNA-radius_10.88.244.180 in the Server 1 column. View its configuration in the **Servers** tab.

Servers Server Groups

	Name	Address	Auth Port	Acct Port
☐	dnac-radius_10.88.244.180	10.88.244.180	1812	1813

The server Cisco DNA-radius_10.88.244.180 has the IP address 10.88.244.180, Click its **name** to view its configuration

Name*	dnac-radius_10.88.244.	Support for CoA ⓘ	ENABLED ☒
Server Address*	10.88.244.180	CoA Server Key Type	Hidden ▼
Set New Key	☐	CoA Server Key ⓘ	
Auth Port	1812	Automate Tester	☐
Acct Port	1813		
Server Timeout (seconds)	4		
Retry Count	3		

A critical configuration is Change of Authorization (CoA), which provides a mechanism to modify the attributes of an Authentication, Authorization, and Accounting (AAA) session after it has been authenticated on the captive portal. Without this feature, the endpoint remains in a web-auth pending state even after completing registration on the portal.

Wireless Policy Profile Configuration

Inside the Policy Profile, clients can be assigned settings such as VLAN, ACLs, QoS, Mobility Anchor, and timers. To view the configuration for the policy profile, navigate to **Configuration > Tags & Profiles > Policy**.

	Admin Status	Associated Policy Tags	Policy Profile Name	Description
☐	✓		CWA_Cisco_profile	CWA_Cisco_profile
☐	✓		default-policy-profile	default policy profile

Click the **policy name** to view its configuration.

General	Access Policies	QOS and AVC	Mobility	Advanced
---------	-----------------	-------------	----------	----------

Name*	CWA_Cisco_profile	WLAN Switching Policy	
Description	CWA_Cisco_profile	Central Switching	DISABLED ☐
Status	ENABLED ☒	Central Authentication	ENABLED ☒
Passive Client	DISABLED ☐	Central DHCP	DISABLED ☐
IP MAC Binding	ENABLED ☒	Flex NAT/PAT	DISABLED ☐
Encrypted Traffic Analytics	DISABLED ☐		

CTS Policy	
Inline Tagging	☐
SGACL Enforcement	☐
Default SGT	2-65519

The policy status is Enabled and as with any fabric SSID, central switching and central DHCP are disabled. Click **Advanced** tab, then navigate to the **AAA Policy** section to view additional configuration details.

AAA Policy

Allow AAA Override☒

NAC State☒

Policy Name

default-aaa-policy x ▼

Accounting List

Search or Select ▼

Interim Accounting

ENABLED

Both AAA Override and Network Access Control (NAC) can be enabled. AAA Override allows the controller to accept attributes returned by the RADIUS server, such as ACLs or URLs, and apply these attributes to clients. NAC enables Change of Authorization (CoA) after the client has registered on the portal.

This configuration can also be viewed through the CLI on the WLC.
To verify the policy profile, the SSID is attached to run the command:

<#root>

WLC#show fabric wlan summary

Number of Fabric wlan : 1

WLAN	Profile Name	SSID	Status

21	CWA_Cisco_profile		
	CWA_Cisco	UP	

To view the configuration for the policy profile CWA_Cisco_profile run the command:

<#root>

WLC#show running-config | section policy CWA_Cisco_profile

wireless profile policy CWA_Cisco_profile

```
aaa-override

no central dhcp

no central switching

description CWA_Cisco_profile
dhcp-tlv-caching
exclusionlist timeout 180
fabric CWA_Cisco_profile
http-tlv-caching

nac

service-policy input platinum-up
service-policy output platinum
no shutdown
```

Policy Tag Configuration

The policy tag is the way you link the WLAN with the Policy Profile, navigate to **Configuration > Tags & Profiles > WLANs**, click the **WLAN name**, and navigate to **Add to Policy Tags** to identify the policy tag assigned to the SSID.

General Security Advanced Add To Policy Tags

+ Add × Delete

☐	Policy Tag	Policy Profile
☐	PT_ilagu_TOYOT_Foor6_a5548	CWA_Cisco_profile

1

10

1 - 1 of 1 items

For the SSID CWA_Cisco_profile the policy tag PT_ilagu_TOYOT_Foor6_a5548 is used to verify tis configuration navigate to **Configuration > Tags & Profiles > Tags > Policy**.

	Policy Tag Name	Description
☐	default-policy-tag	default policy-tag
☐	PT_ilagu_TOYOT_Foor6_a5548	PolicyTagName PT_ilagu_TOYOT_Foor6_a55

Click the **name** to view its details. The policy tag PT_ilagu_TOYOT_Foor6_a5548 links the WLAN CWA_Cisco which is associated with the name CWA_Cisco_profile on the WLC (see the WLANs page for reference) to the Policy Profile CWA_Cisco_profile.

WLAN-POLICY Maps: 1

+ Add × Delete

WLAN Profile	Policy Profile
☐ CWA_Cisco_profile	CWA_Cisco_profile
1 - 1 of 1 items	

The WLAN name CWA_Cisco_profile references the WLAN CWA_Cisco.

Status	Name	ID	SSID
☐	CWA_Cisco_profile	21	CWA_Cisco

Redirect ACL Configuration

In CWA, a Redirect Access Control List defines which traffic is redirected to the WLC for further processing and which traffic bypasses redirection

This configuration is pushed to the WLC after creating the SSID and provisioning the WLC from Inventory. To view it, navigate to **Configuration > Security > ACL**, The name of the ACL that Catalyst Center uses for the redirect ACL is Cisco DNA_ACL_WEBAUTH_REDIRECT.

ACL Name	ACL Type	ACE Count	Downloaded ACL
☐ DNA_ACL_WEBAUTH_REDIRECT	IPv4 Extended	9	No

Click the **name** to view its configuration. The values are derived from the network settings of the network settings from the site on Catalyst Center.

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
☐ 1	deny	8.8.8.8		any		udp	eq bootps	eq bootpc	None	Disable
☐ 2	deny	any		8.8.8.8		udp	eq bootpc	eq bootps	None	Disable
☐ 3	deny	1.1.1.1		any		udp	eq bootps	eq bootpc	None	Disable
☐ 4	deny	any		1.1.1.1		udp	eq bootpc	eq bootps	None	Disable
☐ 5	deny	9.9.9.9		any		udp	eq bootps	eq bootpc	None	Disable
☐ 6	deny	any		9.9.9.9		udp	eq bootpc	eq bootps	None	Disable
☐ 7	deny	10.88.244.180		any		ip	None	None	None	Disable
☐ 8	deny	any		10.88.244.180		ip	None	None	None	Disable
☐ 9	permit	any		any		tcp	0 - 65535	eq www	None	Disable

Note: These values are obtained from the site's network settings configured in Catalyst Center, and DHCP/DNS values are sourced from the pool configured in the WLAN. The ISE PSN IP address is referenced in the AAA configuration within the SSID workflow.

To view the redirection ACL on the WLC CLI, run this command:

<#root>

WLC#show ip access-lists Cisco DNA_ACL_WEBAUTH_REDIRECT

Extended IP access list Cisco DNA_ACL_WEBAUTH_REDIRECT

```
1 deny udp host 8.8.8.8 eq bootps any eq bootpc
2 deny udp any eq bootpc host 8.8.8.8 eq bootps
3 deny udp host 1.1.1.1 eq bootps any eq bootpc
4 deny udp any eq bootpc host 1.1.1.1 eq bootps
5 deny udp host 9.9.9.9 eq bootps any eq bootpc
6 deny udp any eq bootpc host 9.9.9.9 eq bootps
7 deny ip host 10.88.244.180 any
8 deny ip any host 10.88.244.180
9 permit tcp any range 0 65535 any eq www
```

The redirect ACL can be applied to the Flex Profile so it can be sent to the access points. Run this command to confirm this configuration

```
<#root>
```

```
WLC#show running-config | section flex
```

```
wireless profile flex default-flex-profile
```

```
  acl-policy Cisco DNA_ACL_WEBAUTH_REDIRECT
```

```
central-webauth
```

```
urlfilter list Cisco DNA_ACL_WEBAUTH_REDIRECT
```

Redirect ACL on the Access Point

On the access point, the permit and deny values are reversed: permit indicates forwarding traffic, and deny indicates redirection. To review the configuration for the redirect ACL on the AP, run this command:

```
<#root>
```

```
AP#sh ip access-lists
```

```
Extended IP access list Cisco DNA_ACL_WEBAUTH_REDIRECT
```

```
1 permit udp 8.8.8.8 0.0.0.0 dhcp_server any eq 68
```

```
2 permit udp any dhcp_client 8.8.8.8 0.0.0.0 eq 67
```

```
3 permit udp 1.1.1.1 0.0.0.0 dhcp_server any eq 68
```

```
4 permit udp any dhcp_client 1.1.1.1 0.0.0.0 eq 67
```

```
5 permit udp 9.9.9.9 0.0.0.0 dhcp_server any eq 68
```

```
6 permit udp any dhcp_client 9.9.9.9 0.0.0.0 eq 67
```

```
7 permit ip 10.88.244.180 0.0.0.0 any
```

```
8 permit ip any 10.88.244.180 0.0.0.0
```

```
9 deny tcp any range 0 65535 any eq 80
```