Configure 9800 WLC and Aruba ClearPass - Guest Access & FlexConnect

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

- Traffic Flow for CWA Guest Enterprise Deployment
- Network Diagram

Configure

- Configure Guest Wireless Access C9800 Parameters
  - C9800 - AAA Configuration for Guest
  - C9800 - Configure Redirection ACL
  - C9800 - Guest WLAN Profile Configuration
  - C9800 - Guest Policy Profile Definition
- C9800 - Policy Tag
- C9800 - AP Join Profile
- C9800 - Flex Profile
- C9800 - Site Tag
- C9800 - RF Profile
- C9800 - Assign Tags to AP
- Configure Aruba CPPM Instance
  - Aruba ClearPass Server Initial Configuration
  - Apply for Licenses
  - Server Hostname
  - Generate CPPM Web Server Certificate (HTTPS)
  - Define C9800 WLC as a Network Device
- Guest Portal Page and CoA Timers
- ClearPass - Guest CWA Configuration
  - ClearPass Endpoint Metadata Attribute: Allow-Guest-Internet
  - ClearPass Reauthenticate Enforcement Policy Configuration
  - ClearPass Guest Portal Redirect Enforcement Profile Configuration
  - ClearPass Metadata Enforcement Profile Configuration
  - ClearPass Guest Internet Access Enforcement Policy Configuration
  - ClearPass Guest Post-AUP Enforcement Policy Configuration
  - ClearPass MAB Authentication Service Configuration
  - ClearPass Webauth Service Configuration
  - ClearPass - Web Login
- Verification - Guest CWA Authorization

Appendix

Related Information

Introduction

This document describes the integration of the Catalyst 9800 Wireless LAN Controller (WLC) with Aruba ClearPass.

Prerequisites

This guide assumes these components have been configured and verified:

- All pertinent components are synced to Network Time Protocol (NTP) and verified to have the correct time (required for certificate validation)
- Operational DNS Server (required for Guest traffic flows, Certificate Revocation List (CRL) validation)
- Operational DHCP Server
- An optional Certificate authority (CA) (required to sign the CPPM hosted Guest Portal)
- Catalyst 9800 WLC
- Aruba ClearPass Server (Requires Platform License, Access License, Onboard License)
- Vmware ESXi

Requirements

Cisco recommends that you have knowledge of these topics:

- C9800 deployment and New Configuration Model
- Flexconnect Switching on C9800
- 9800 CWA Authentication (refer to https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213920-central-web-authentication-cwa-on-cata.html)

Components Used

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

- Cisco Catalyst C9800-L-C that runs 17.3.4c
- Cisco Catalyst C9130AX
- Aruba ClearPass, 6-8-0-109592 and 6.8-3 patch
- MS Windows Server
  - Active Directory (GP configured for automated machine-based certificate issuance to managed endpoints)
  - DHCP Server with option 43 and option 60
  - DNS Server
  - NTP Server to time-sync all the components
  - The CA

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 integration of the Catalyst 9800 WLC implementation utilizes Central Web Authentication (CWA) for wireless clients in a Flexconnect mode of Access Point (AP) deployment.

Guest wireless authentication is supported by Guest Portal with an anonymous acceptable user policy (AUP) page, hosted on Aruba Clearpass in a secure demilitarized zone (DMZ) segment.

The diagram conveys the details of the Guest Wifi access exchanges before the guest user is allowed onto the network:

1. The guest user associates with the Guest Wifi in a remote office.

2. The initial RADIUS Access Request is proxied by C9800 to the RADIUS server.

3. The server looks up the supplied guest MAC address in the local MAC Endpoint Database.
If the MAC address is not found, then the server responds with a MAC Authentication Bypass (MAB) profile. This RADIUS response includes:

- URL Redirect Access Control List (ACL)
- URL Redirect

4. The client goes through the IP Learn process where it is assigned an IP address.

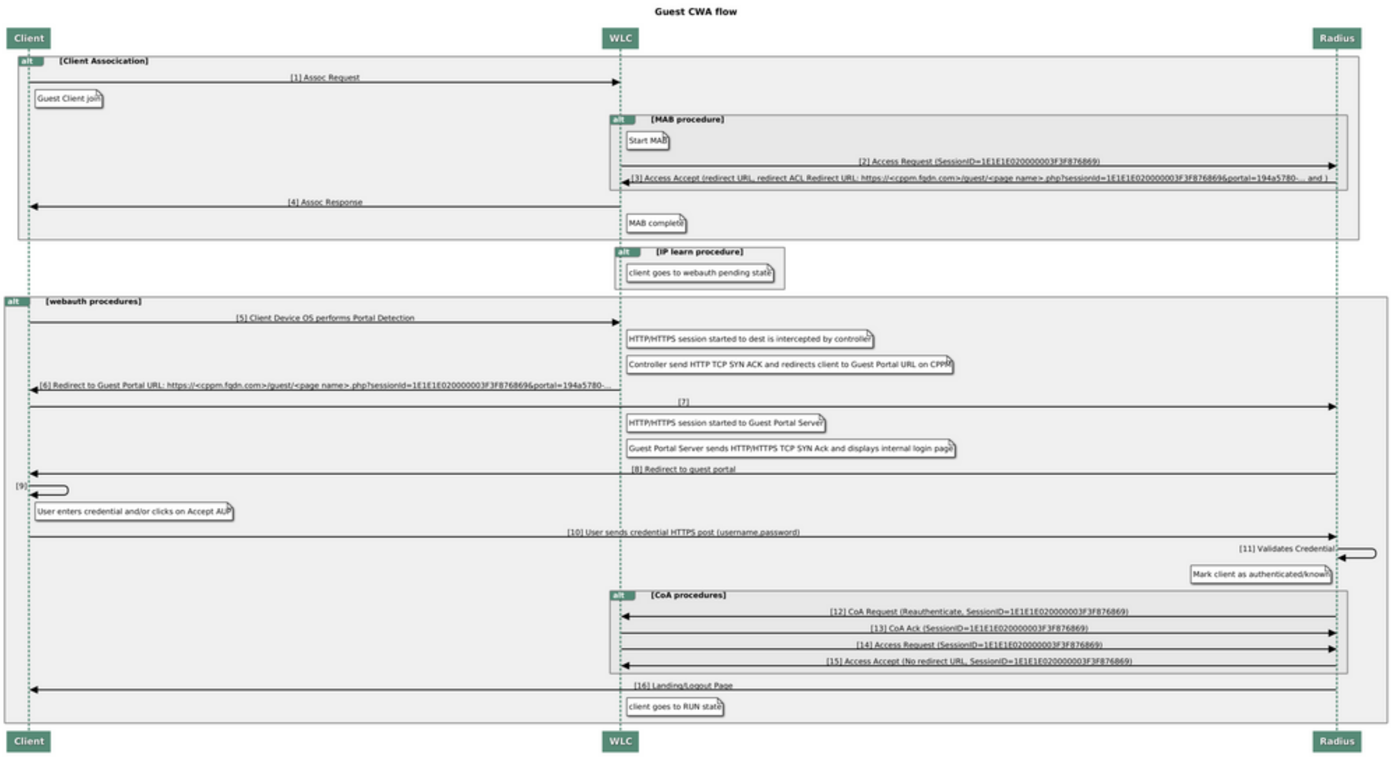
5. C9800 transitions the guest client (identified by its MAC address) to the 'Web Auth Pending' state.

6. Most modern device OS in association with guest WLANs perform some sort of captive portal detection. The exact detection mechanism is dependent on specific OS implementation. The client OS opens a pop-up (pseudo browser) dialog with a page redirected by C9800 to the guest portal URL hosted by the RADIUS server supplied as part of the RADIUS Access-Accept response.

7. Guest User accepts the Terms and Conditions on the presented pop-up ClearPass sets a flag for the client MAC address in its Endpoint Database (DB) to indicate the client has completed an authentication and initiates a RADIUS Change of Authorization (CoA), by the selection of an interface based on the routing table (if there are multiple interfaces present on ClearPass).

8. WLC transitions the Guest Client to the 'Run' State and the user is granted access to the Internet with no further redirects.

Note: For Cisco 9800 Foreign, Anchor Wireless Controller state flow diagram with RADIUS and externally hosted Guest Portal, refer to the Appendix section in this article.


Guest CWA flow
Client
WLC
Radius
alt
[Client Assocication]
[1] Assoc Request
Guest Client join
alt
[MAB procedure]
Start MAB
[2] Access Request (SessionID=1E1E1E020000003F3F876869)
[3] Access Accept (redirect URL, redirect ACL Redirect URL: https://<cppm.fqdn.com>/guest/<page name>.php?sessionId=1E1E1E020000003F3F876869&portal=194a5780-... and)
[4] Assoc Response
MAB complete
alt
[IP learn procedure]
client goes to webauth pending state
alt
[webauth procedures]
[5] Client Device OS performs Portal Detection
HTTP/HTTPS session started to dest is intercepted by controller
Controller send HTTP TCP SYN ACK and redirects client to Guest Portal URL on CPPM
[6] Redirect to Guest Portal URL: https://<cppm.fqdn.com>/guest/<page name>.php?sessionId=1E1E1E020000003F3F876869&portal=194a5780-...
[7]
HTTP/HTTPS session started to Guest Portal Server
Guest Portal Server sends HTTP/HTTPS TCP SYN Ack and displays internal login page
[8] Redirect to guest portal
[9]
User enters credential and/or clicks on Accept AUP
[10] User sends credential HTTPS post (username,password)
[11] Validates Credential
Mark client as authenticated/known
alt
[CoA procedures]
[12] CoA Request (Reauthenticate, SessionID=1E1E1E020000003F3F876869)
[13] CoA Ack (SessionID=1E1E1E020000003F3F876869)
[14] Access Request (SessionID=1E1E1E020000003F3F876869)
[15] Access Accept (No redirect URL, SessionID=1E1E1E020000003F3F876869)
[16] Landing/Logout Page
client goes to RUN state
Client
WLC
Radius

Guest Central Web Authentication (CWA) State Diagram

Traffic Flow for CWA Guest Enterprise Deployment

In a typical enterprise deployment with multiple branch offices, each branch office is set up to provide secure, segmented access to guests through a Guest Portal once the guest accepts EULA.

In this configuration example, 9800 CWA is used for guest access via integration to a separate ClearPass instance exclusively deployed for guest users in the secure DMZ of the network.

The guests must accept the terms and conditions laid out in the web-consent pop-up portal provided by the DMZ ClearPass server. This configuration example focuses on the Anonymous Guest Access method (that is, no guest username/password is required in order to authenticate to the Guest Portal).

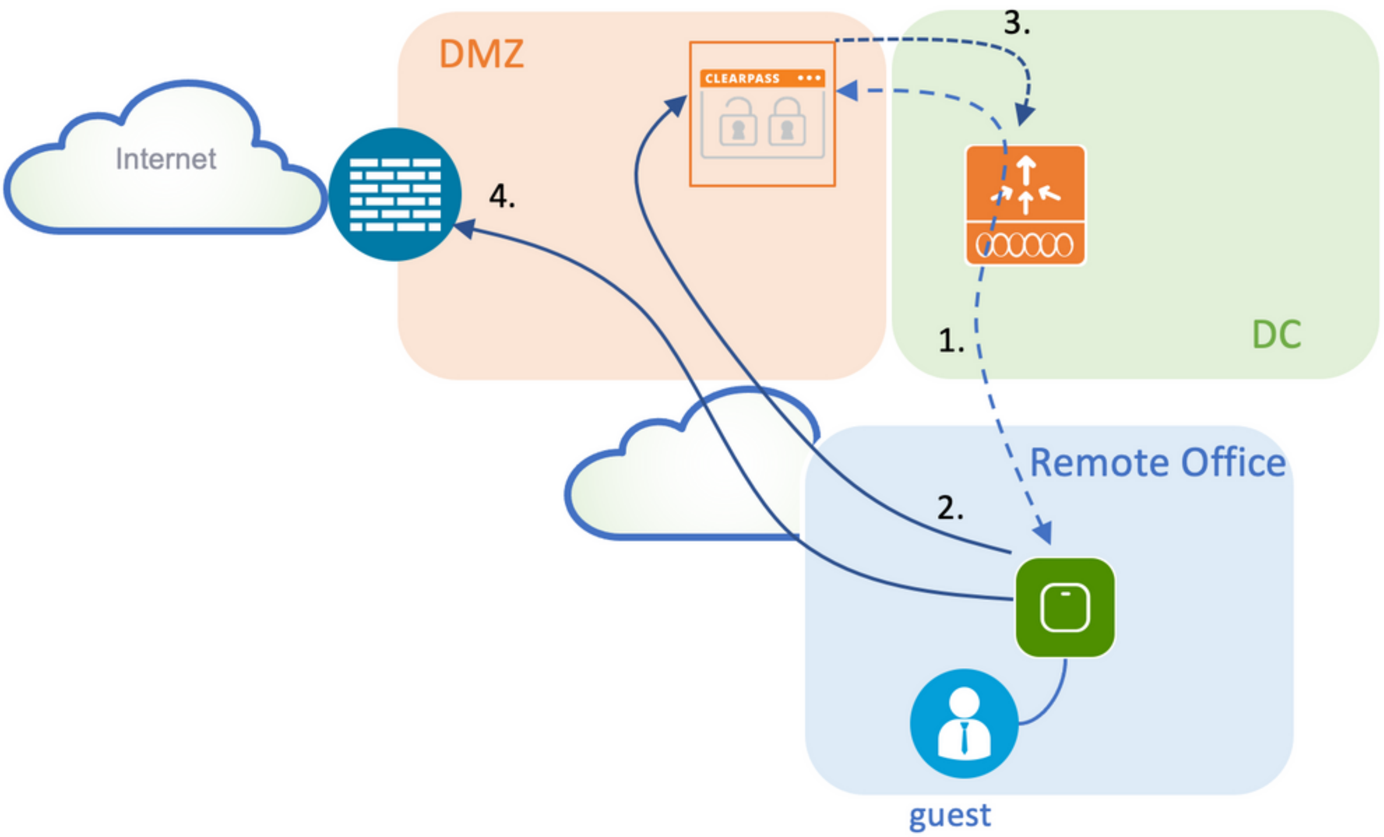
The traffic flow that corresponds to this deployment is shown in the image:

1. RADIUS - MAB phase

2. Guest Client URL redirect to Guest Portal

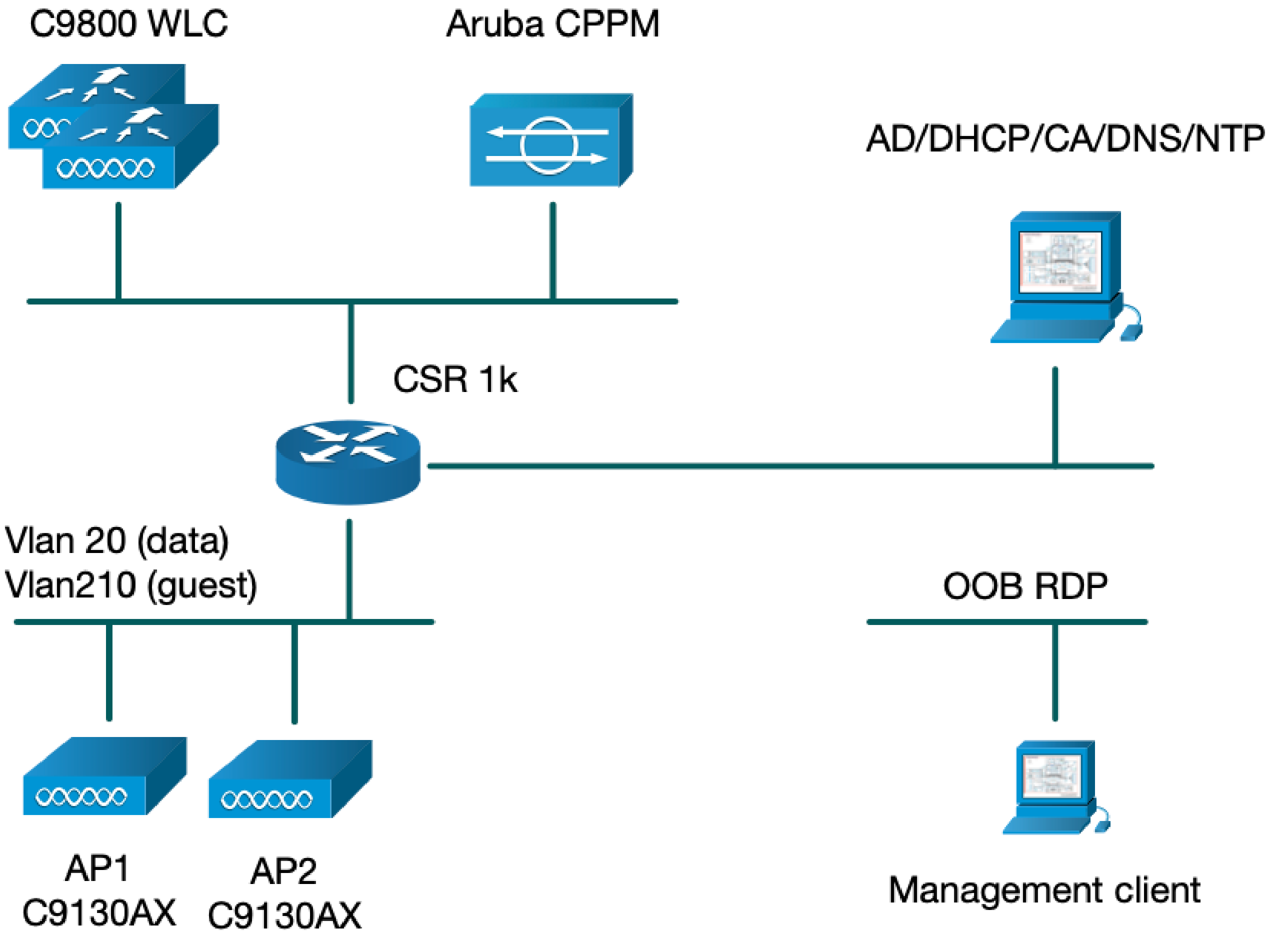
3. After guest acceptance of EULA on the Guest Portal, RADIUS CoA Reauthenticate is issued from CPPM to 9800 WLC

4. The guest is allowed access to the Internet



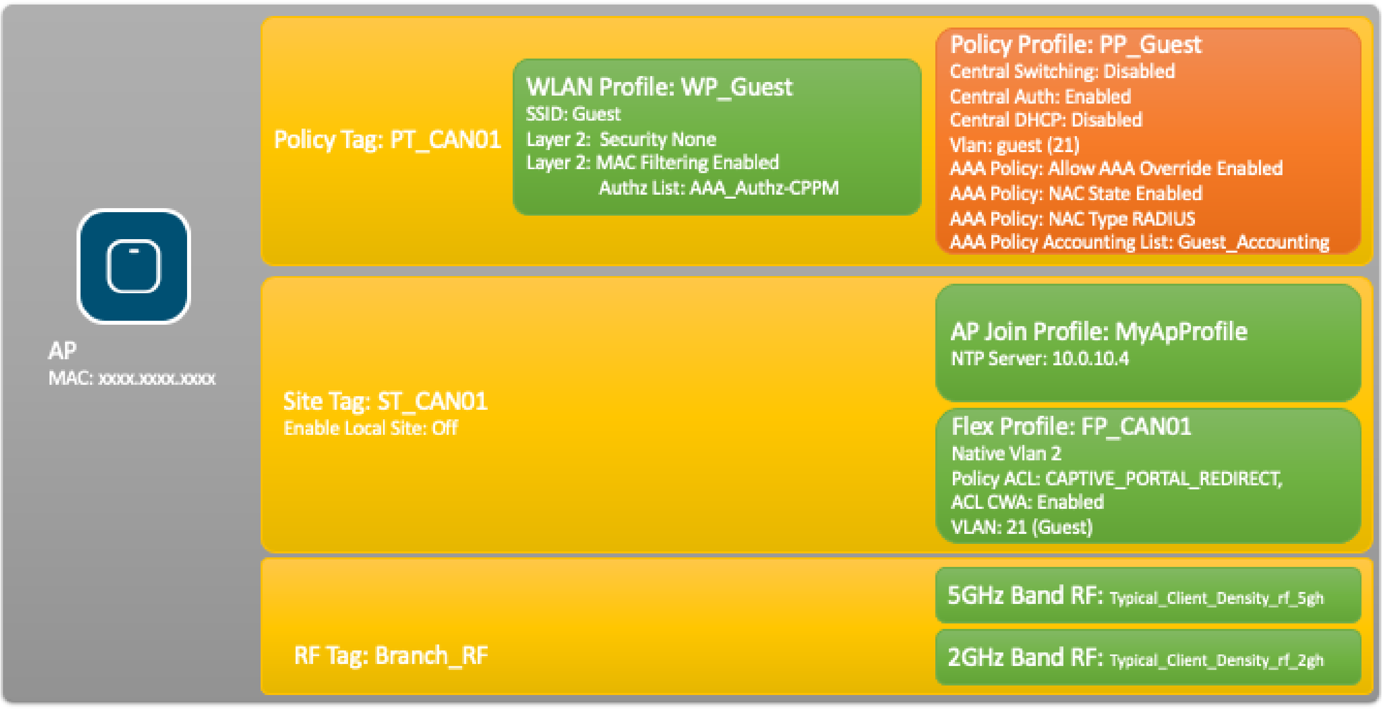
Network Diagram

Note: For lab demo purposes, a single/combined Aruba CPPM Server instance is used in order to serve both Guest and Corp SSID Network Access Server (NAS) functions. Best practice implementation suggests independent NAS instances.



Configure

In this configuration example, a new configuration model on C9800 is leveraged in order to create the necessary profiles and tags to provide dot1x Corporate Access and CWA guest Access to the enterprise branch. The resultant configuration is summarized in this image:

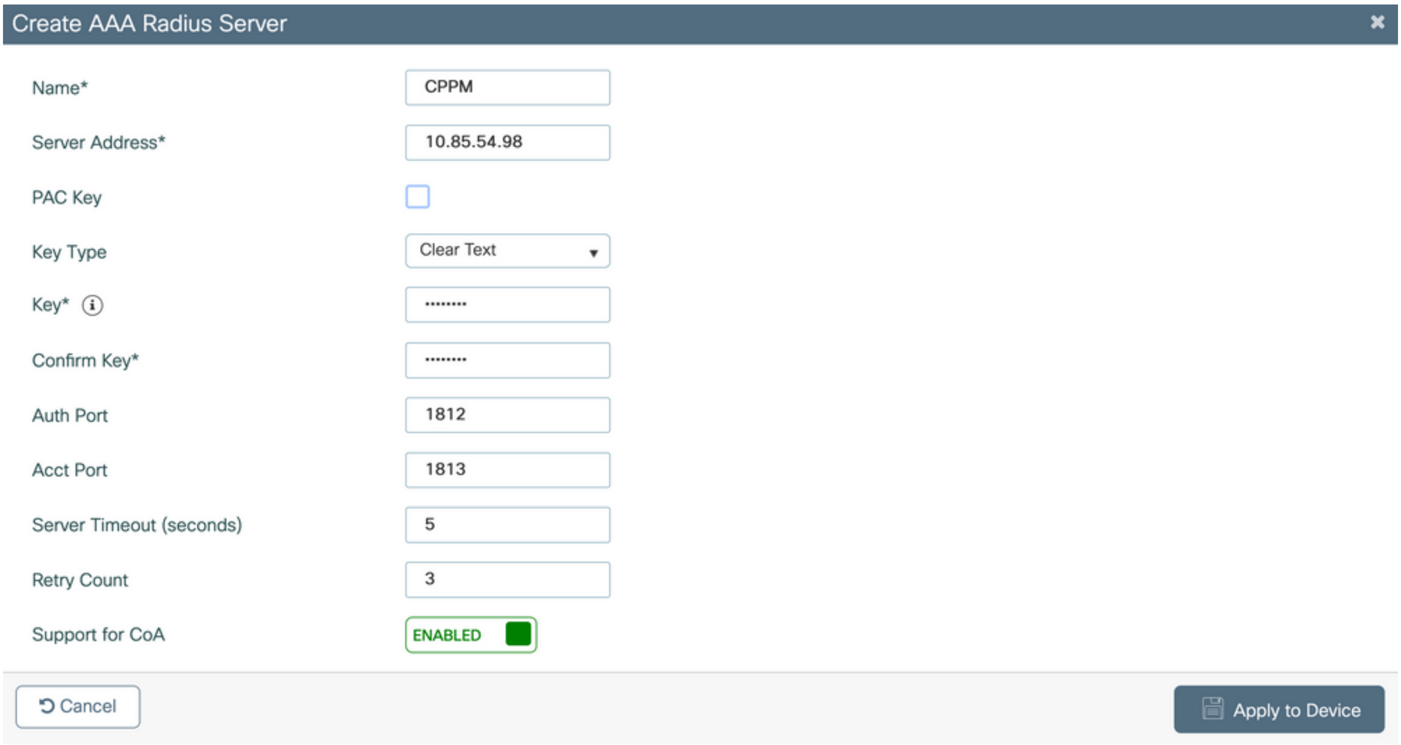

AP
MAC: xxxx.xxxx.xxxx
Policy Tag: PT_CAN01
WLAN Profile: WP_Guest
SSID: Guest
Layer 2: Security None
Layer 2: MAC Filtering Enabled
Authz List: AAA_Authz-CPPM
Policy Profile: PP_Guest
Central Switching: Disabled
Central Auth: Enabled
Central DHCP: Disabled
Vlan: guest (21)
AAA Policy: Allow AAA Override Enabled
AAA Policy: NAC State Enabled
AAA Policy: NAC Type RADIUS
AAA Policy Accounting List: Guest_Accounting
Site Tag: ST_CAN01
Enable Local Site: Off
AP Join Profile: MyApProfile
NTP Server: 10.0.10.4
Flex Profile: FP_CAN01
Native Vlan 2
Policy ACL: CAPTIVE_PORTAL_REDIRECT,
ACL CWA: Enabled
VLAN: 21 (Guest)
RF Tag: Branch_RF
5GHz Band RF: Typical_Client_Density_rf_5gh
2GHz Band RF: Typical_Client_Density_rf_2gh

Configure Guest Wireless Access C9800 Parameters

C9800 - AAA Configuration for Guest

Note: About Cisco bug ID CSCvh03827, ensure the defined Authentication, Authorization, and Accounting (AAA) servers are not load-balanced, as the mechanism relies on SessionID persistency in WLC to ClearPass RADIUS exchanges.

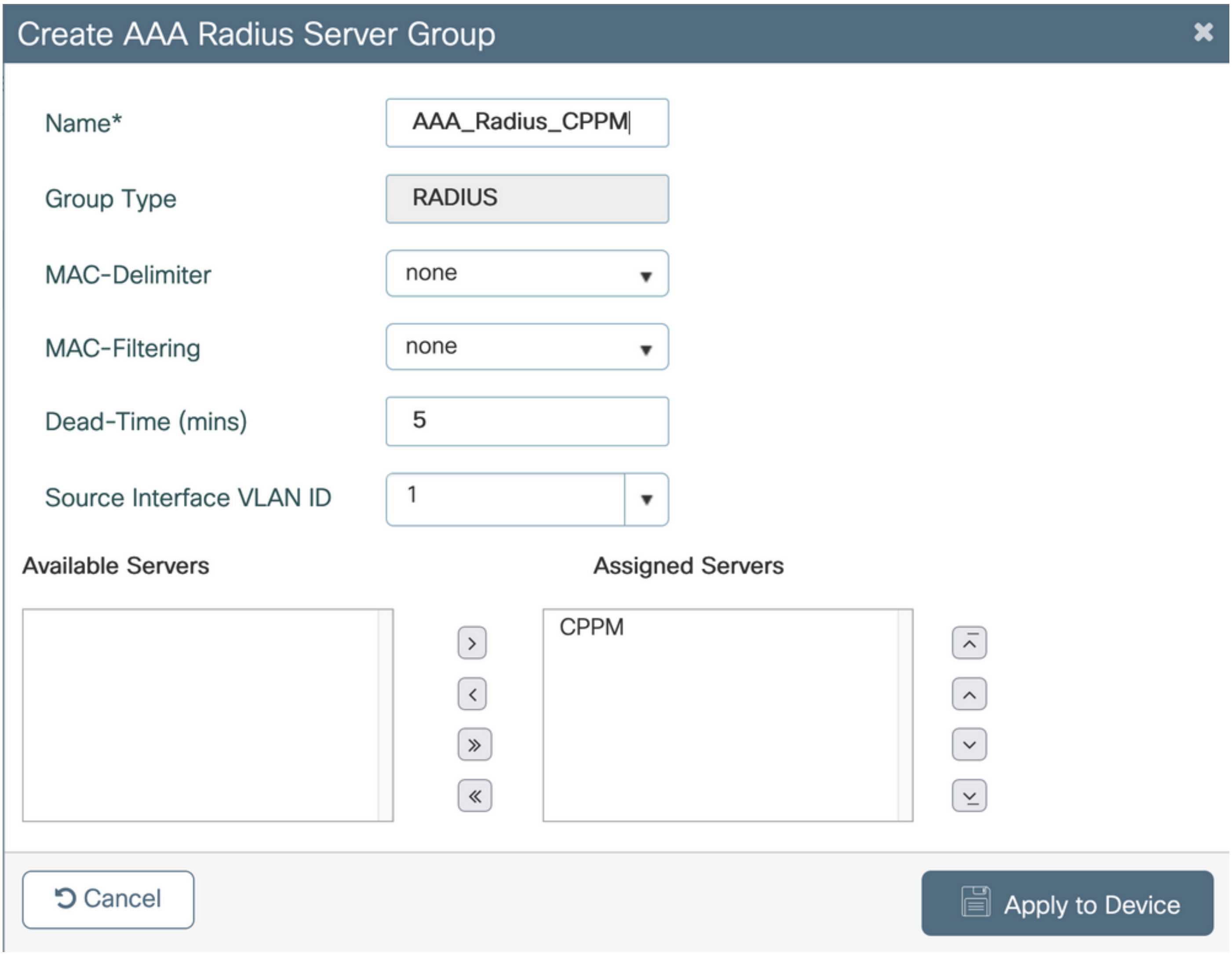
Step 1. Add the Aruba ClearPass DMZ server(s) to the 9800 WLC configuration and create an authentication method list. Navigate to Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > +Add and enter the RADIUS server information.



Create AAA Radius Server

Name*	CPPM
Server Address*	10.85.54.98
PAC Key	□
Key Type	Clear Text
Key*	••••••••
Confirm Key*	••••••••
Auth Port	1812
Acct Port	1813
Server Timeout (seconds)	5
Retry Count	3
Support for CoA	ENABLED

Step 2. Define AAA Server Group for guests and assign the server configured in Step 1. to this server group. Navigate to Configuration > Security > AAA > Servers/Groups > RADIUS > Groups > +Add.

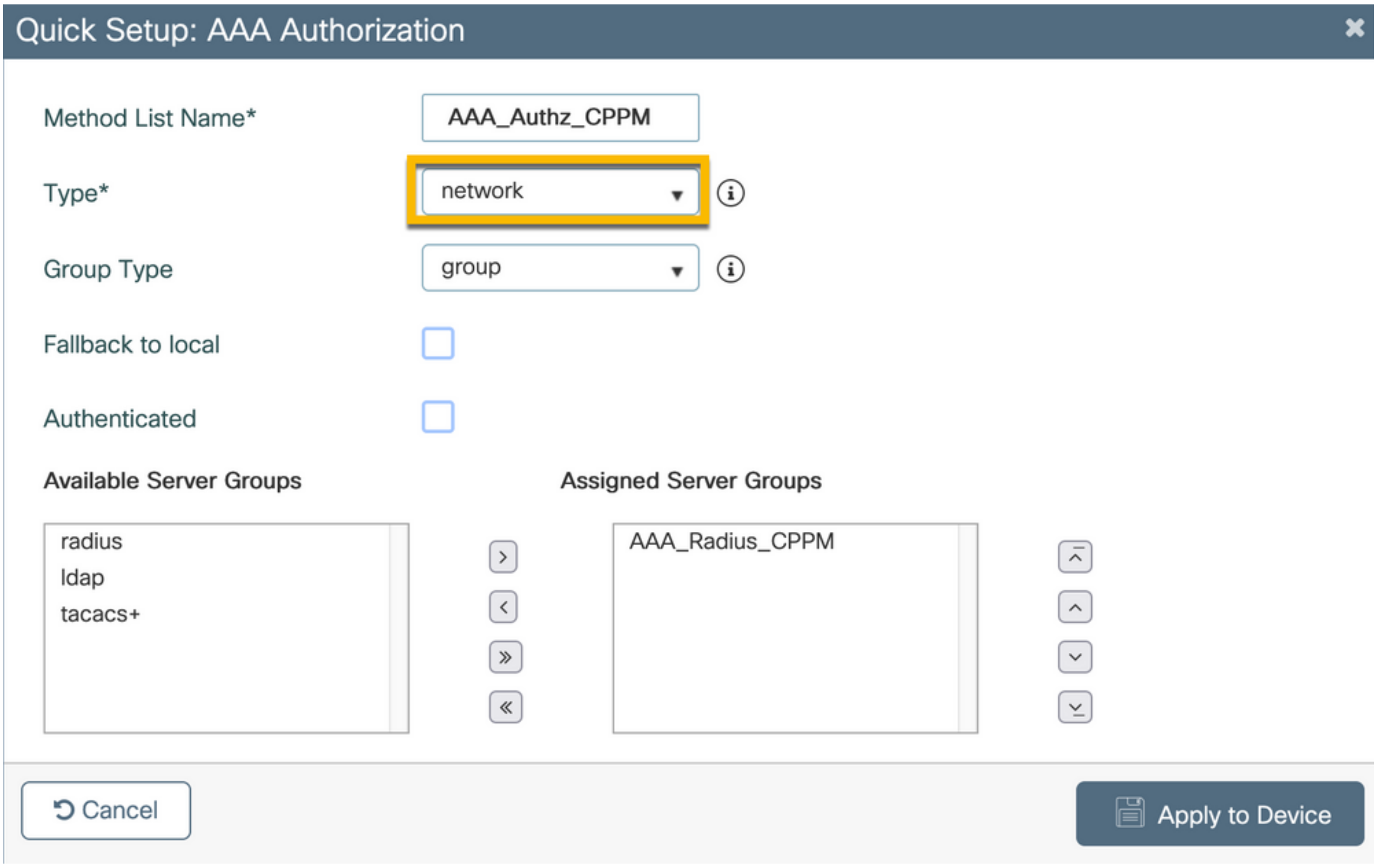


Create AAA Radius Server Group

Name*	AAA_Radius_CPPM
Group Type	RADIUS
MAC-Delimiter	none
MAC-Filtering	none
Dead-Time (mins)	5
Source Interface VLAN ID	1

Available Servers	Assigned Servers
	CPPM

Step 3. Define an Authorization method list for guest access and map the server group created in Step 2. Navigate to Configuration > Security > AAA > AAA Method List > Authorization > +Add. Choose Type Network and then AAA Server Group configured in Step 2.



Quick Setup: AAA Authorization

Method List Name* AAA_Authz_CPPM

Type* network

Group Type group

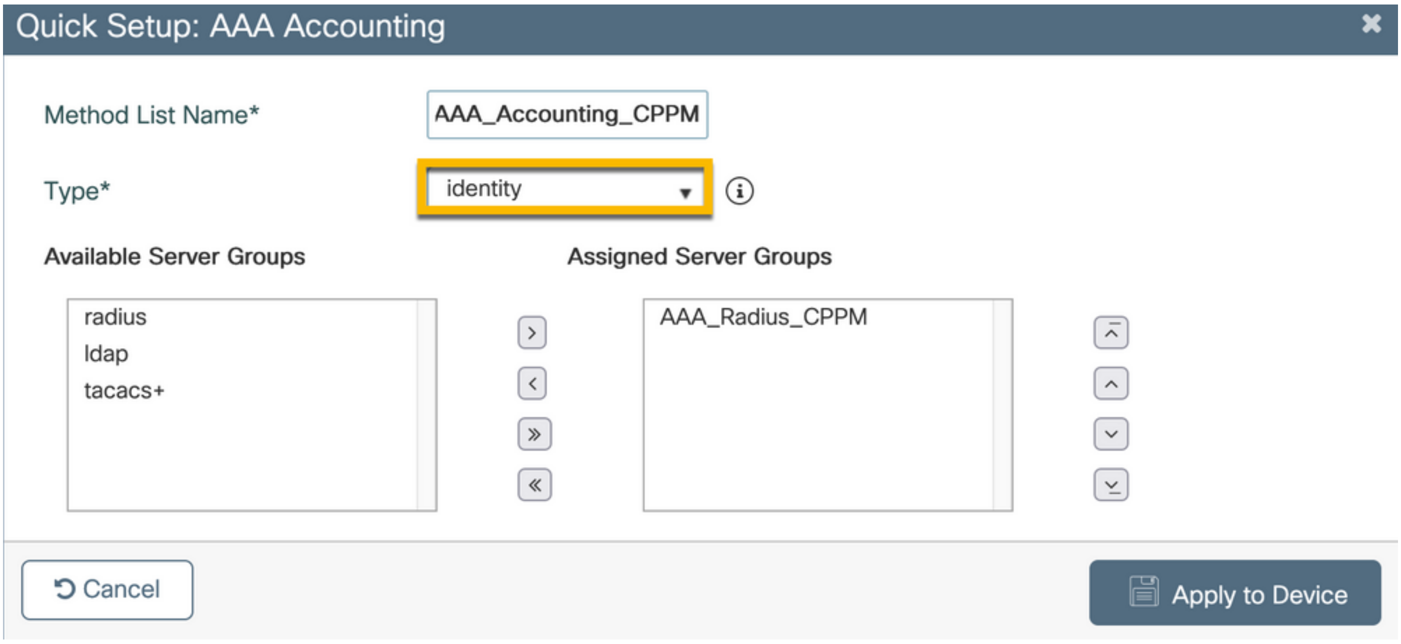
Fallback to local □

Authenticated □

Available Server Groups: radius, ldap, tacacs+

Assigned Server Groups: AAA_Radius_CPPM

Step 4. Create an Accounting method list for guest access and map the server group created in Step 2. Navigate to Configuration > Security > AAA > AAA Method List > Accounting > +Add. Choose Type Identity from the drop-down menu and then AAA Server Group configured in Step 2.



Quick Setup: AAA Accounting

Method List Name* AAA_Accounting_CPPM

Type* identity

Available Server Groups: radius, ldap, tacacs+

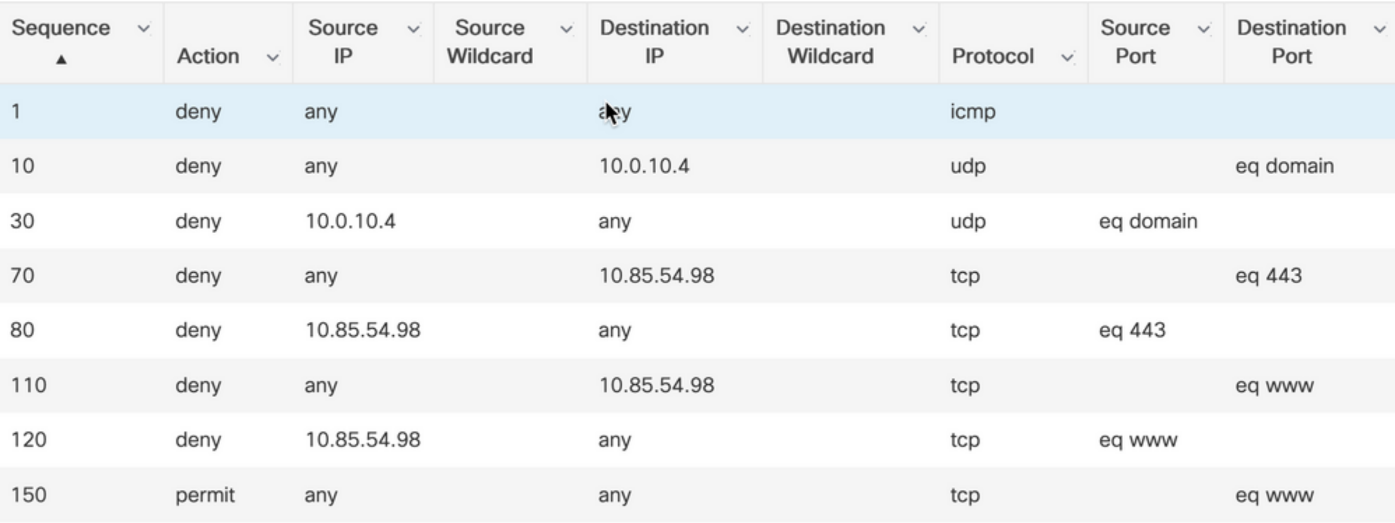
Assigned Server Groups: AAA_Radius_CPPM

C9800 - Configure Redirection ACL

The redirect ACL defines what traffic must be redirected to the Guest Portal versus allowed to pass with no redirection. Here, the ACL deny implies bypass redirect or pass through, while permit implies redirect to the portal. For each traffic class, you must consider the direction of traffic when you create Access Control Entries (ACEs) and create ACEs that match both ingress and egress traffic.

Navigate to Configuration > Security > ACL, and define a new ACL named CAPTIVE_PORTAL_REDIRECT. Configure the ACL with these ACEs:

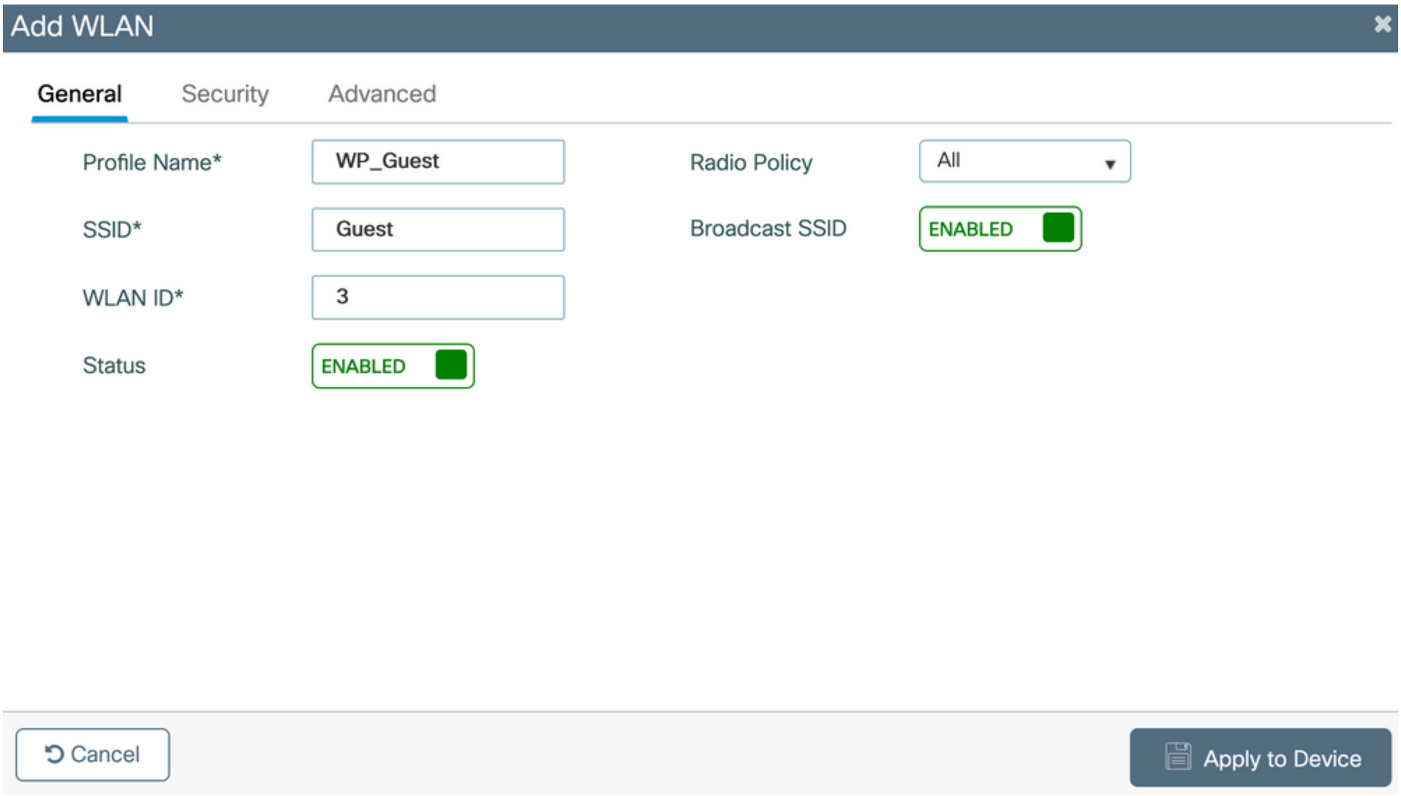
- ACE1: Allows bidirectional Internet Control Message Protocol (ICMP) traffic to bypass redirection and is primarily used to verify reachability.
- ACE10, ACE30: Allows bidirectional DNS traffic flow to DNS server 10.0.10.4 and not be redirected to the portal. A DNS lookup and interception for response are required to trigger the guest flow.
- ACE70, ACE80, ACE110, ACE120: Allows HTTP and HTTPS access to the guest captive portal for the user to be presented with the portal.
- ACE150: All HTTP traffic (UDP port 80) is redirected.



Sequence ▲	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port
1	deny	any		any		icmp		
10	deny	any		10.0.10.4		udp		eq domain
30	deny	10.0.10.4		any		udp	eq domain	
70	deny	any		10.85.54.98		tcp		eq 443
80	deny	10.85.54.98		any		tcp	eq 443	
110	deny	any		10.85.54.98		tcp		eq www
120	deny	10.85.54.98		any		tcp	eq www	
150	permit	any		any		tcp		eq www

C9800 - Guest WLAN Profile Configuration

Step 1. Navigate to Configuration > Tags & Profiles > Wireless > +Add. Create a new SSID Profile WP_Guest, with the broadcast of SSID 'Guest' that guest clients associate with.



Add WLAN

Profile Name* WP_Guest

SSID* Guest

WLAN ID* 3

Status ENABLED

Radio Policy All

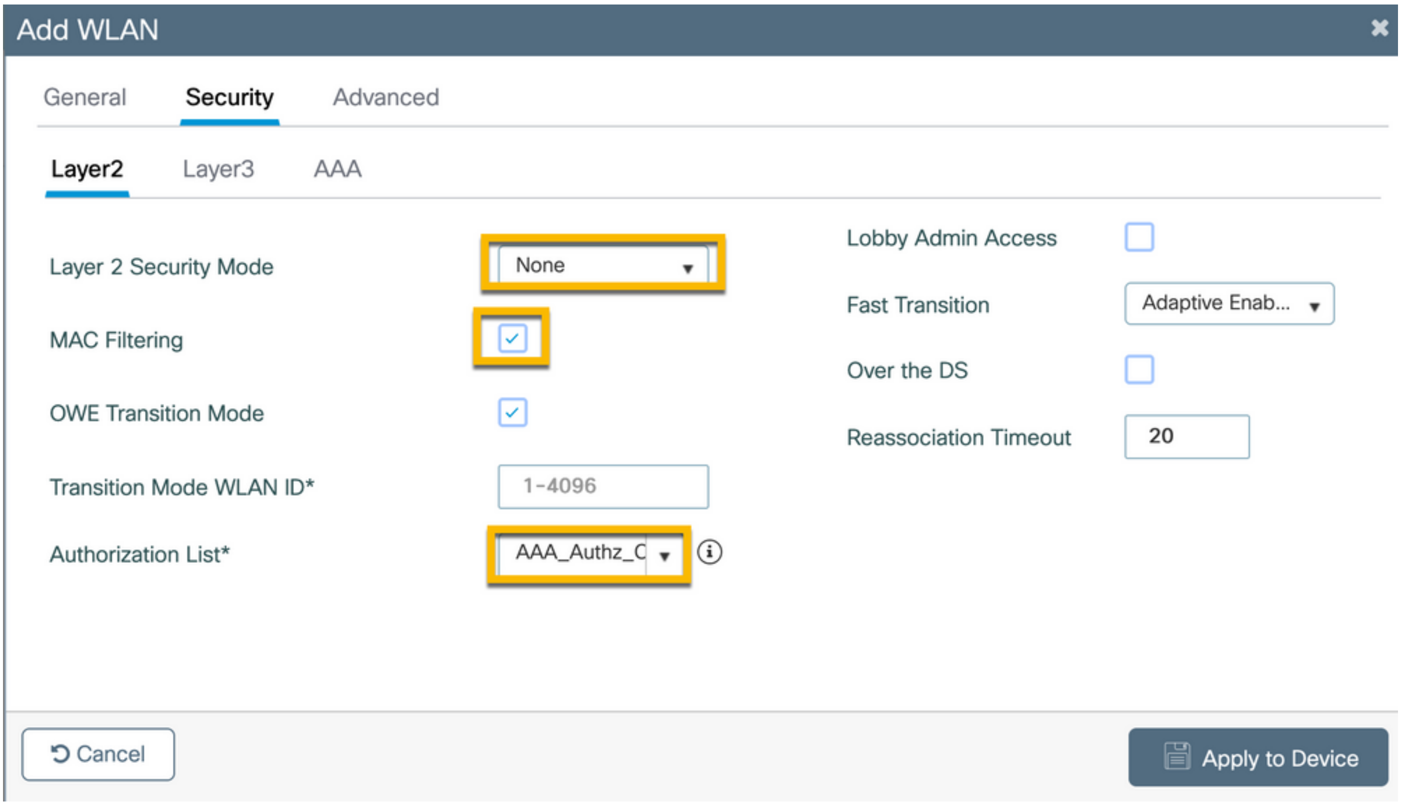
Broadcast SSID ENABLED

Under the same Add WLAN dialog, navigate to the Security > Layer 2 Tab.

- Layer 2 Security Mode: None

- MAC Filtering: Enabled

- Authorization list: AAA_Authz_CPPM from the drop-down menu (configured under Step 3. as part of AAA configuration)



Add WLAN

Layer 2 Security Mode None

MAC Filtering ☑

OWE Transition Mode ☑

Transition Mode WLAN ID* 1-4096

Authorization List* AAA_Authz_C

Lobby Admin Access □

Fast Transition Adaptive Enab...

Over the DS □

Reassociation Timeout 20

C9800 - Guest Policy Profile Definition

On C9800 WLC GUI, navigate to Configuration > Tags & Profiles > Policy > +Add.

Name: PP_Guest

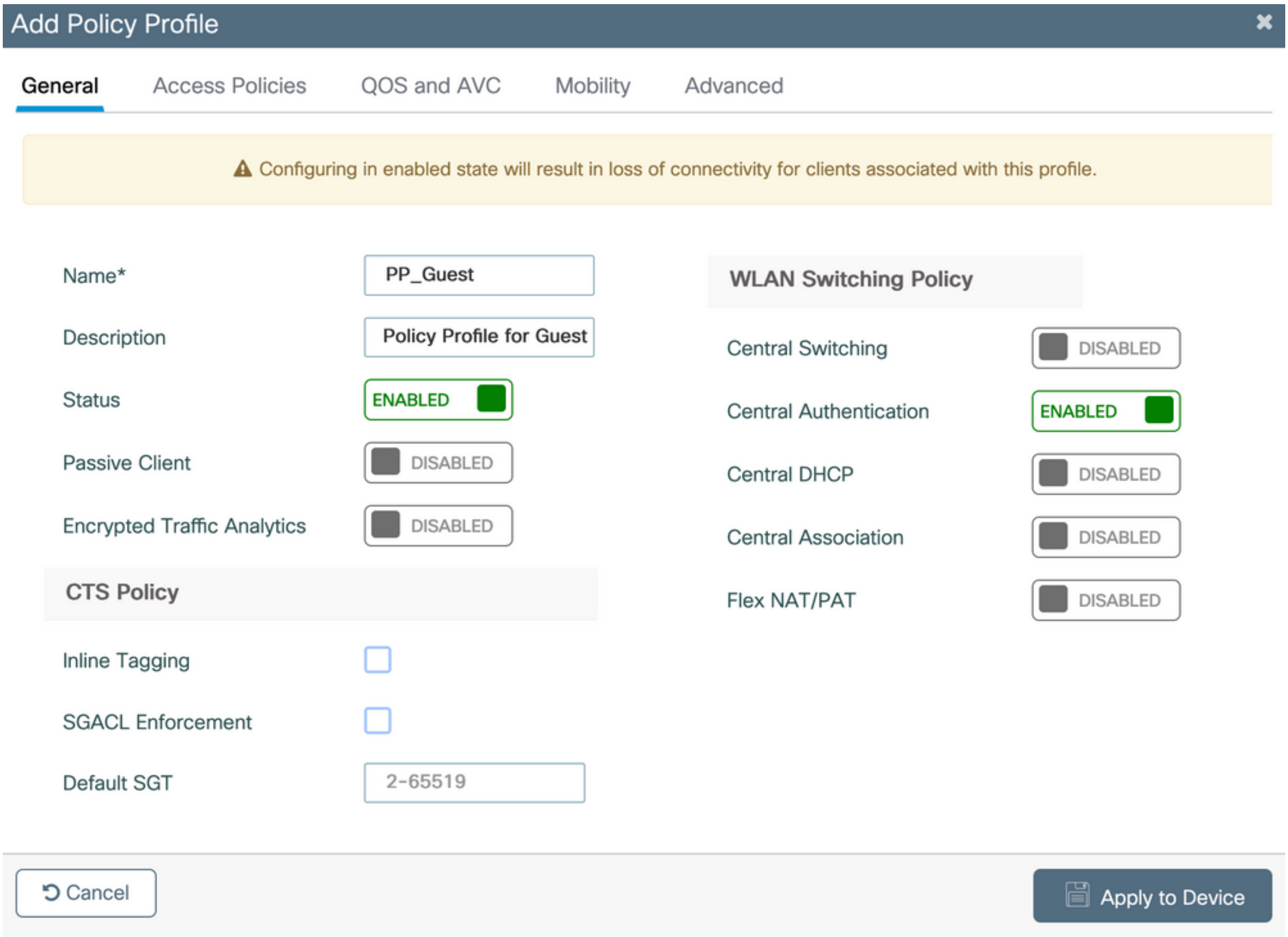
Status: Enabled

Central Switching: Disabled

Central Authentication: Enabled

Central DHCP: Disabled

Central Association: Disabled



⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

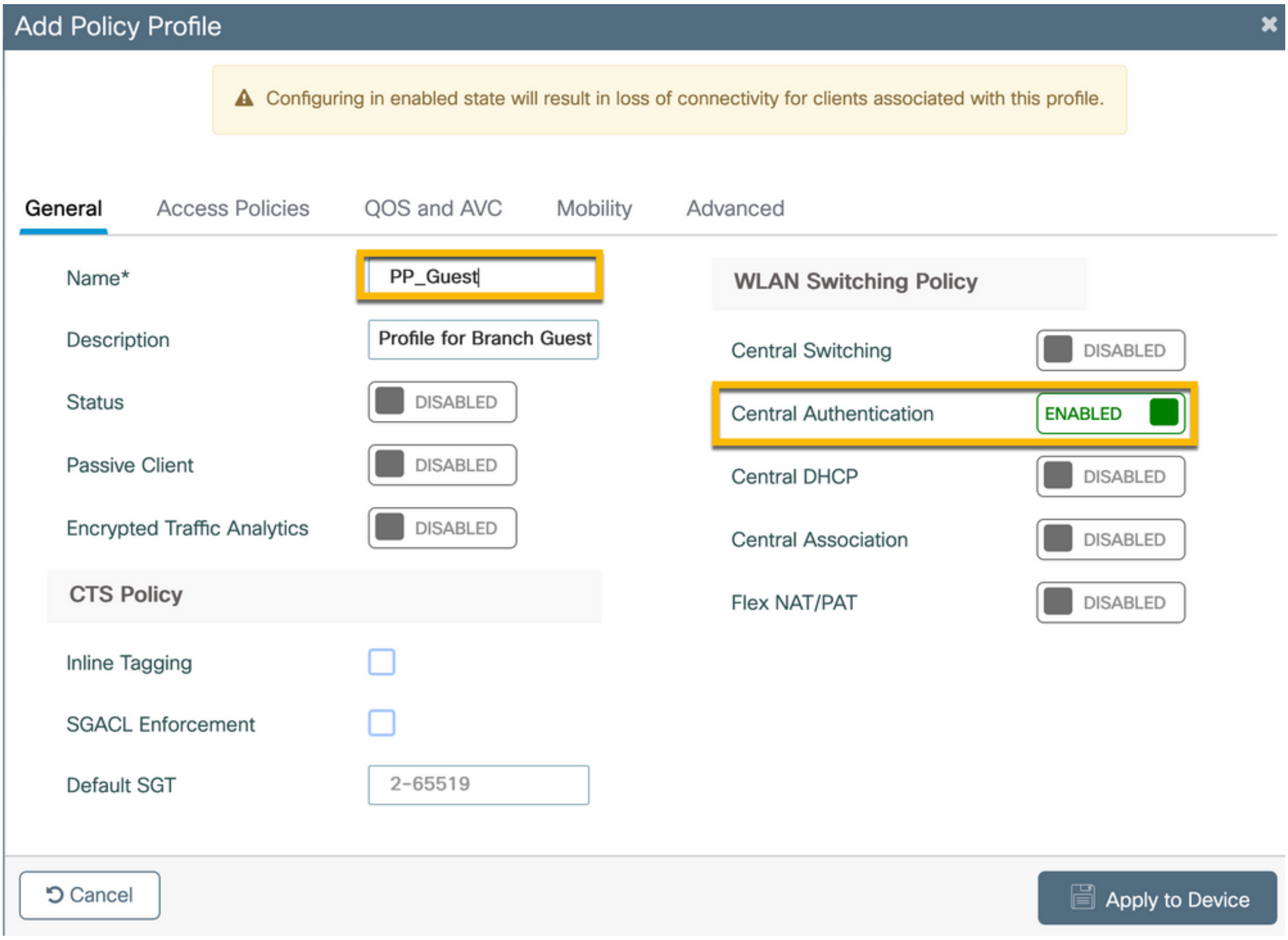
Name*	PP_Guest
Description	Policy Profile for Guest
Status	ENABLED
Passive Client	DISABLED
Encrypted Traffic Analytics	DISABLED

CTS Policy

Inline Tagging	□
SGACL Enforcement	□
Default SGT	2-65519

WLAN Switching Policy

Central Switching	DISABLED
Central Authentication	ENABLED
Central DHCP	DISABLED
Central Association	DISABLED
Flex NAT/PAT	DISABLED



Add Policy Profile

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name*: PP_Guest

Description: Profile for Branch Guest

Status: DISABLED

Passive Client: DISABLED

Encrypted Traffic Analytics: DISABLED

CTS Policy

Inline Tagging: □

SGACL Enforcement: □

Default SGT: 2-65519

WLAN Switching Policy

Central Switching: DISABLED

Central Authentication: ENABLED

Central DHCP: DISABLED

Central Association: DISABLED

Flex NAT/PAT: DISABLED

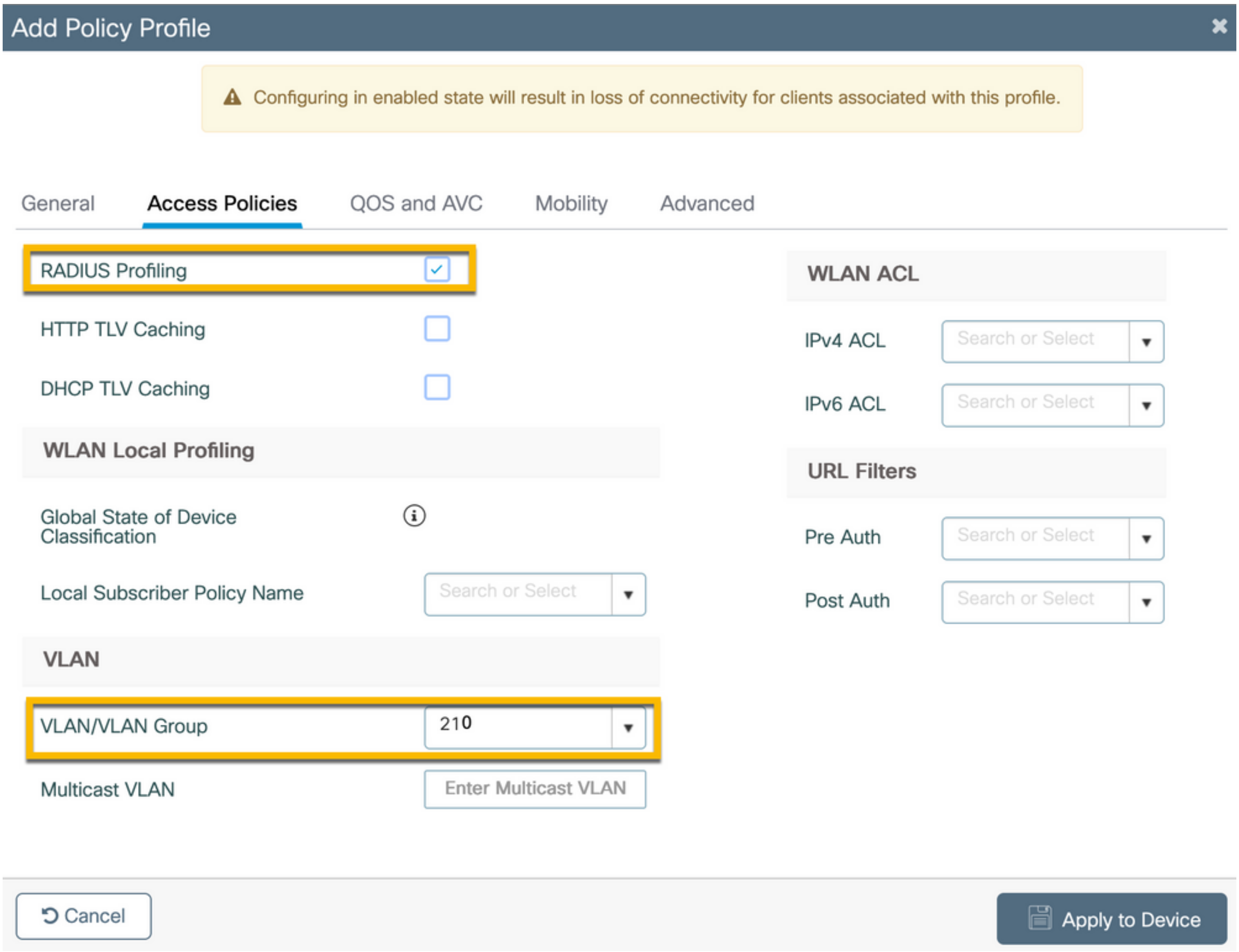
Navigate to the Access Policies tab in the same Add Policy Profile dialog.

- RADIUS Profiling: Enabled

- VLAN/VLAN Group: 210 (that is, VLAN 210 is the Guest local VLAN at each branch location)

Note: Guest VLAN for Flex must not have to be defined on the 9800 WLC under VLANs, in the VLAN/VLAN Group type VLAN number.

Known defect: Cisco bug ID CSCvn48234 causes SSID not to be broadcasted if the same Flex guest VLAN is defined under WLC and in the Flex Profile.



Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

RADIUS Profiling ☑

HTTP TLV Caching ☐

DHCP TLV Caching ☐

WLAN Local Profiling

Global State of Device Classification

Local Subscriber Policy Name: Search or Select

VLAN

VLAN/VLAN Group: 210

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

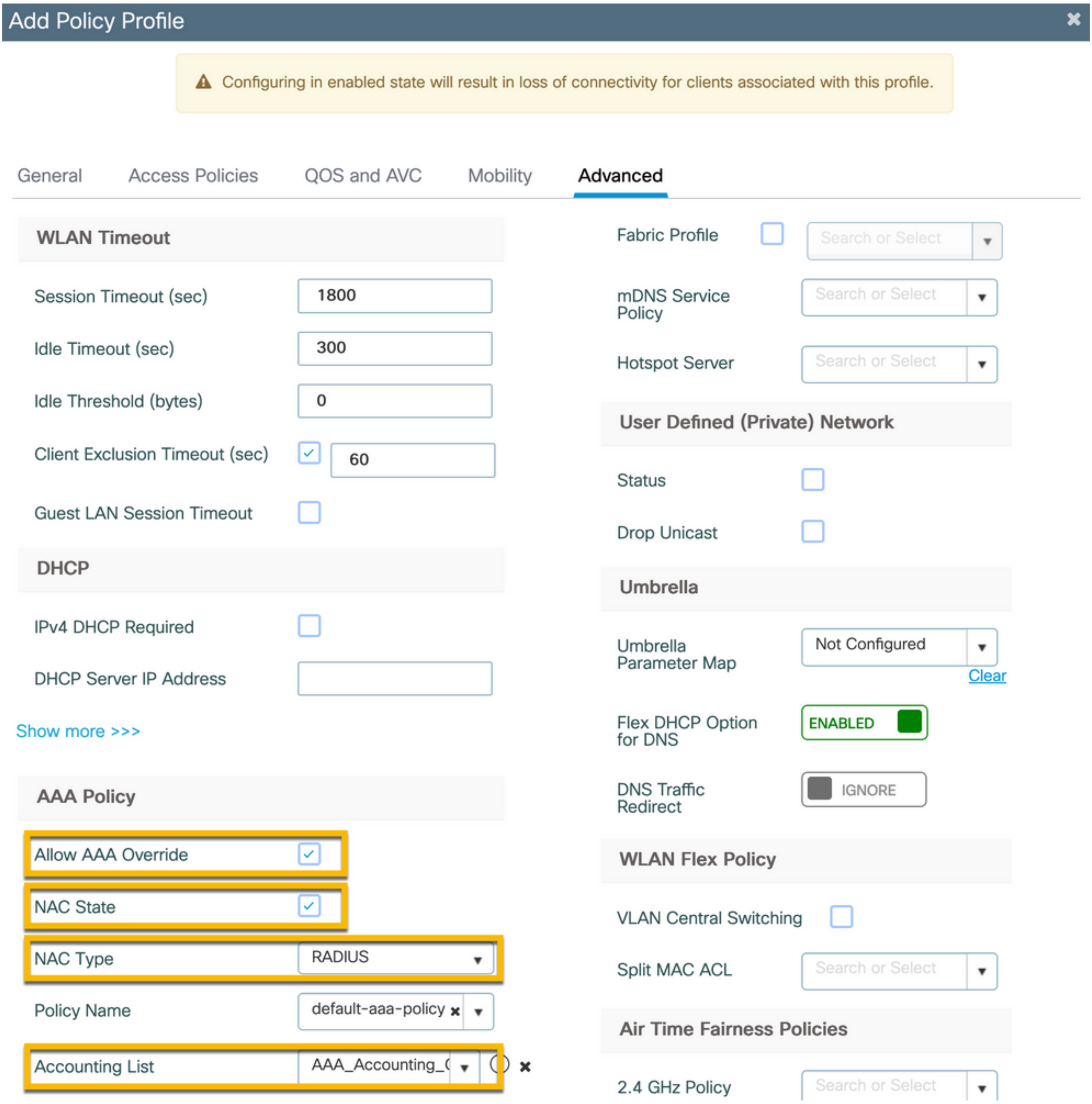
In the same Add Policy Profile dialog, navigate to the Advanced tab.

- Allow AAA Override: Enabled

- NAC State: Enabled

- NAC Type: RADIUS

- Accounting List: AAA_Accounting_CPPM (that is defined in Step 4. as part of AAA configuration)



Add Policy Profile

Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

WLAN Timeout

Session Timeout (sec): 1800

Idle Timeout (sec): 300

Idle Threshold (bytes): 0

Client Exclusion Timeout (sec): ☑ 60

Guest LAN Session Timeout: □

DHCP

IPv4 DHCP Required: □

DHCP Server IP Address:

Show more >>>

AAA Policy

Allow AAA Override: ☑

NAC State: ☑

NAC Type: RADIUS

Policy Name: default-aaa-policy

Accounting List: AAA_Accounting_(

Fabric Profile: □ Search or Select

mDNS Service Policy: Search or Select

Hotspot Server: Search or Select

User Defined (Private) Network

Status: □

Drop Unicast: □

Umbrella

Umbrella Parameter Map: Not Configured

Clear

Flex DHCP Option for DNS: ENABLED

DNS Traffic Redirect: IGNORE

WLAN Flex Policy

VLAN Central Switching: □

Split MAC ACL: Search or Select

Air Time Fairness Policies

2.4 GHz Policy: Search or Select

Note: 'Network Admission Control (NAC) State - Enable' is required in order to enable C9800 WLC to accept RADIUS CoA messages.

C9800 - Policy Tag

On C9800 GUI, navigate to Configuration > Tags & Profiles > Tags > Policy > +Add.

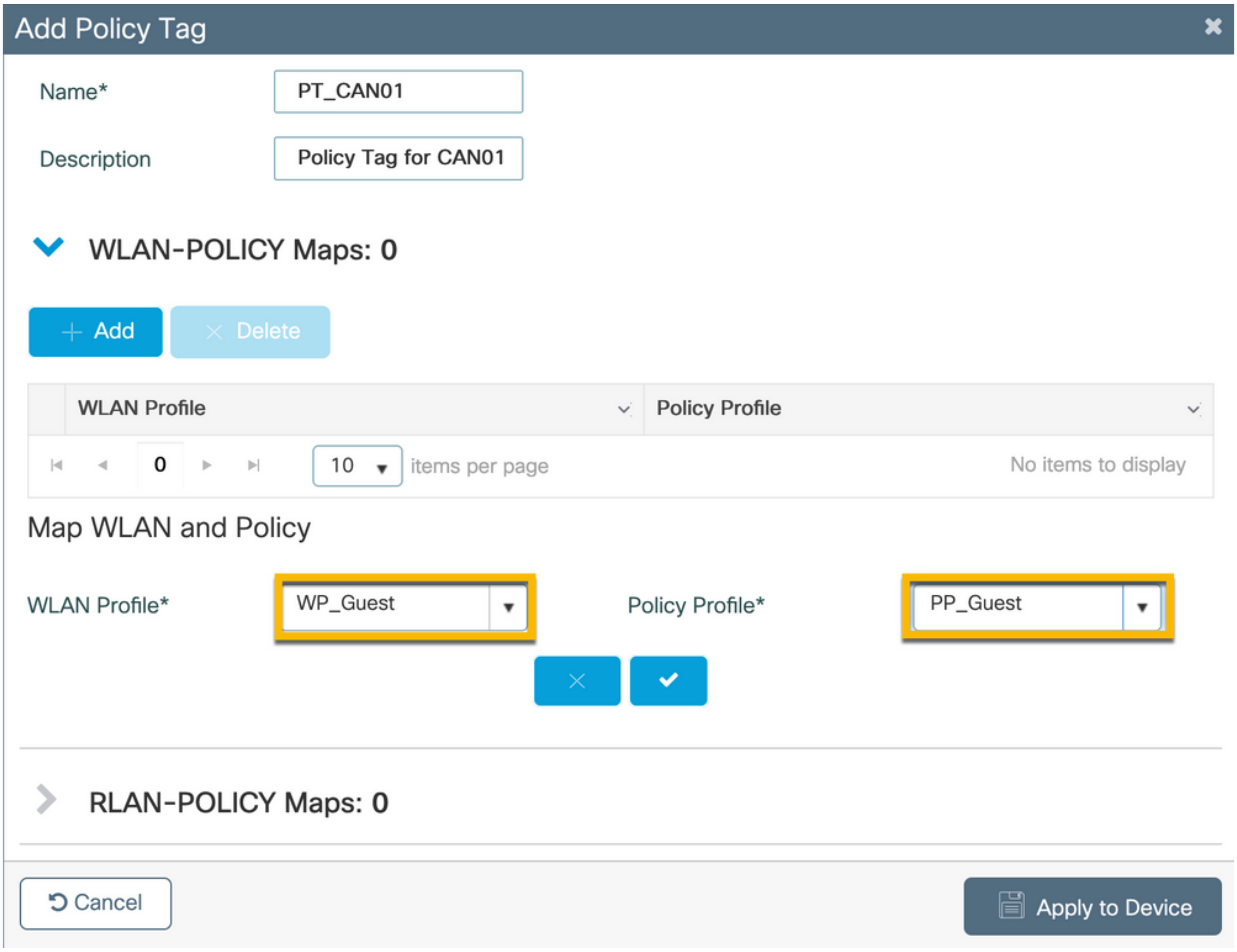
- Name: PT_CAN01

- Description: Policy Tag for CAN01 Branch Site

In the same dialog Add Policy Tag, under WLAN-POLICY MAPS, click +Add, and map the previously created WLAN Profile to the Policy Profile:

- WLAN Profile: WP_Guest

- Policy Profile: PP_Guest



Add Policy Tag

Name*: PT_CAN01

Description: Policy Tag for CAN01

WLAN-POLICY Maps: 0

WLAN Profile	Policy Profile

0 | 10 items per page | No items to display

Map WLAN and Policy

WLAN Profile*: WP_Guest

Policy Profile*: PP_Guest

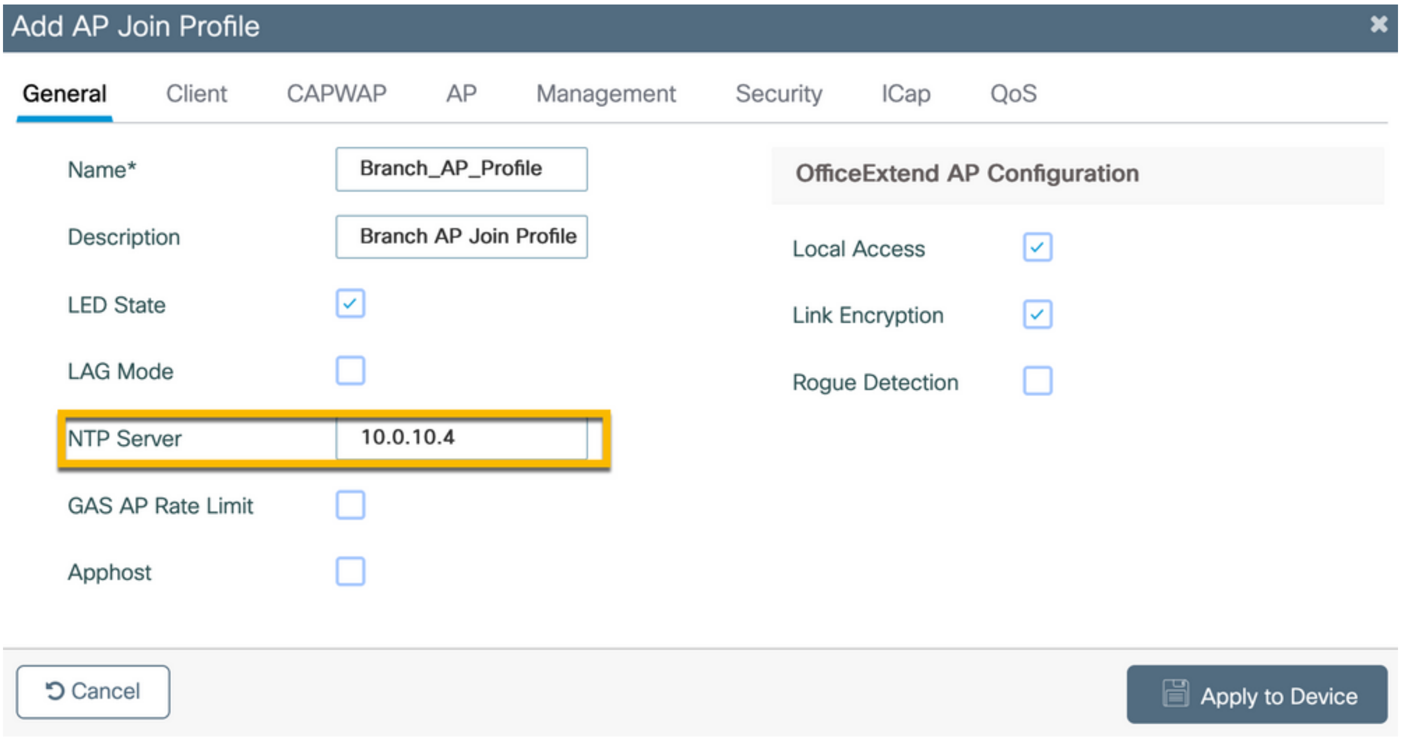
RLAN-POLICY Maps: 0

C9800 - AP Join Profile

On C9800 WLC GUI, navigate to Configuration > Tags & Profiles > AP Join > +Add.

- Name: Branch_AP_Profile

- NTP Server: 10.0.10.4 (refer to the lab topology diagram). This is the NTP server that is used by APs in Branch to synchronize.


Add AP Join Profile

Name*: Branch_AP_Profile

Description: Branch AP Join Profile

LED State: ☑

LAG Mode: □

NTP Server: 10.0.10.4

GAS AP Rate Limit: □

Apphost: □

OfficeExtend AP Configuration

Local Access: ☑

Link Encryption: ☑

Rogue Detection: □

C9800 - Flex Profile

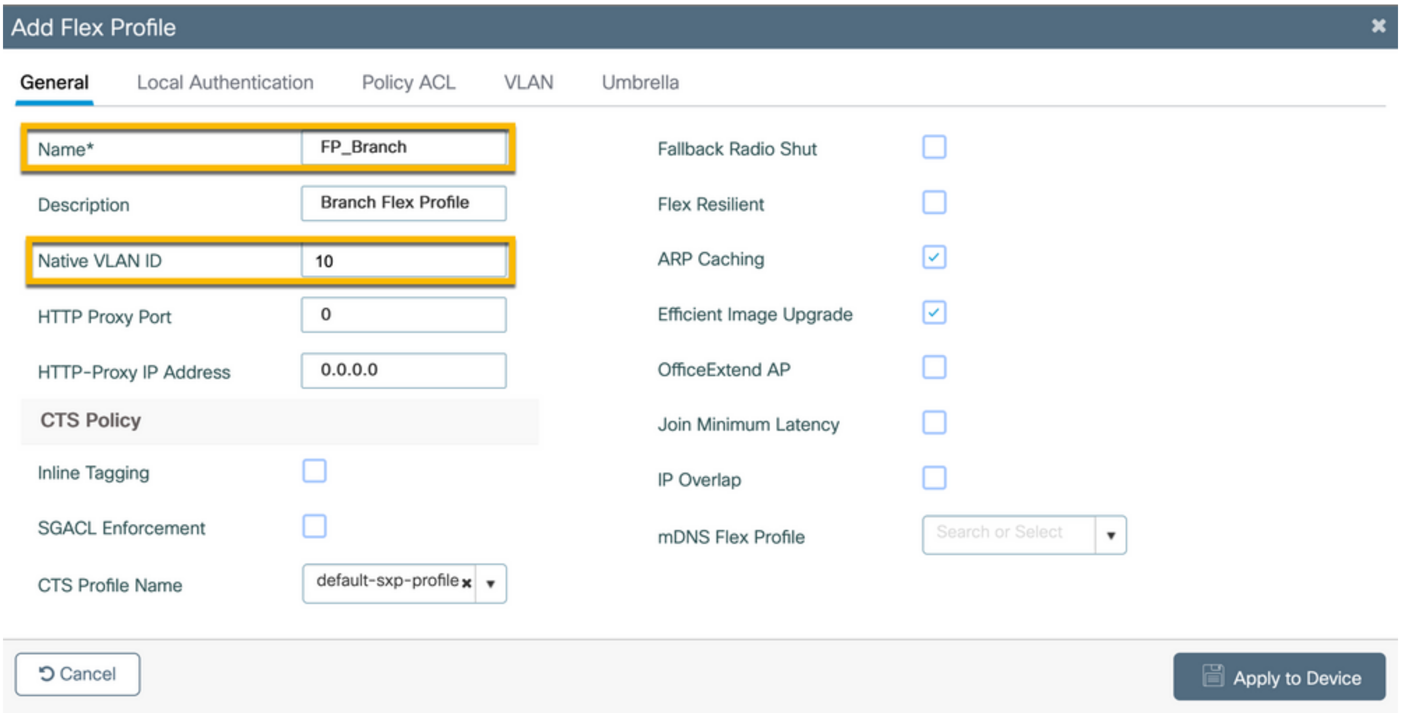
The profiles and tags are modular and can be reused for multiple sites.

In the case of FlexConnect deployment, if the same VLAN IDs are used at all of the branch sites, you can re-use the same flex profile.

Step 1. On a C9800 WLC GUI, navigate to Configuration > Tags & Profiles > Flex > +Add.

- Name: FP_Branch

- Native VLAN ID: 10 (only required if you have a non-default native VLAN where you want to have an AP management interface)


Add Flex Profile

Name*: FP_Branch

Description: Branch Flex Profile

Native VLAN ID: 10

HTTP Proxy Port: 0

HTTP-Proxy IP Address: 0.0.0.0

CTS Policy

Inline Tagging: □

SGACL Enforcement: □

CTS Profile Name: default-sxp-profile

Fallback Radio Shut: □

Flex Resilient: □

ARP Caching: ☑

Efficient Image Upgrade: ☑

OfficeExtend AP: □

Join Minimum Latency: □

IP Overlap: □

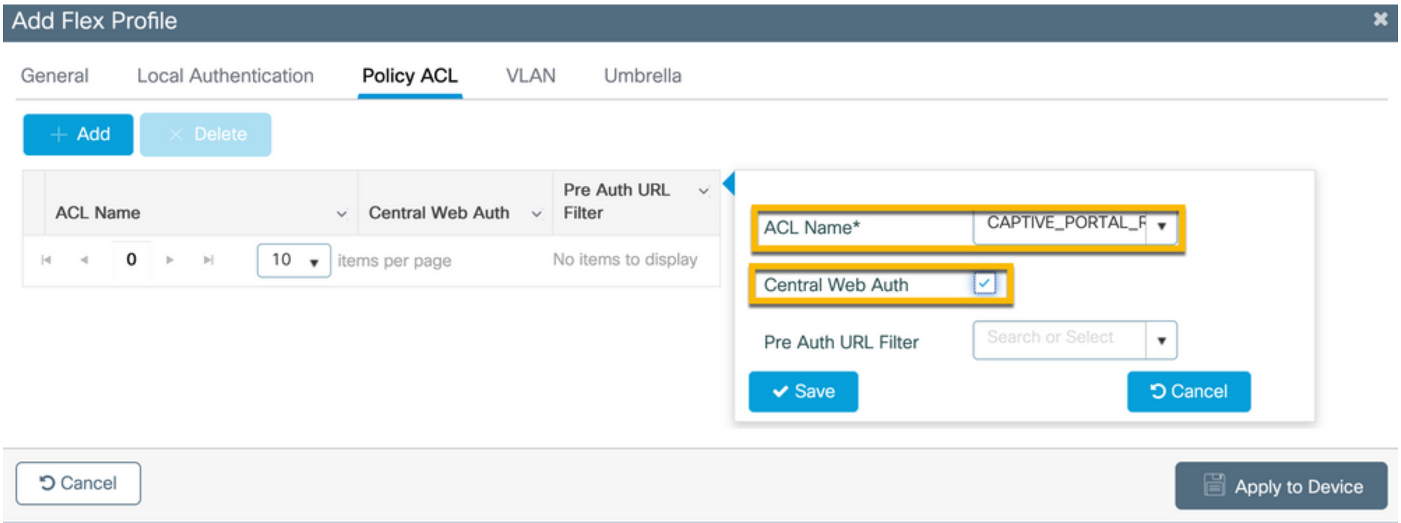
mDNS Flex Profile: Search or Select

On the same Add Flex Profile dialogue, navigate to the Policy ACL tab and click +Add.

- ACL Name: CAPTIVE_PORTAL_REDIRECT

- Central Web Auth: Enabled

On a Flexconnect deployment, each managed AP is expected to download the redirect ACL locally as redirection happens at the AP and not on the C9800.



Add Flex Profile

ACL Name*: CAPTIVE_PORTAL_R

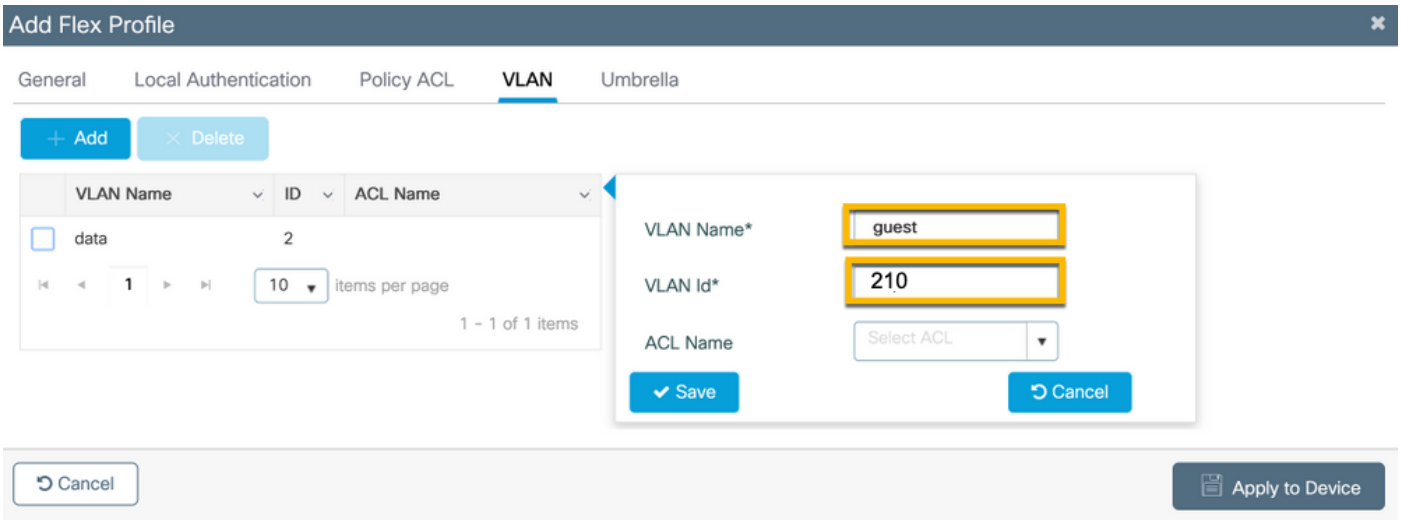
Central Web Auth: ☑

Pre Auth URL Filter: Search or Select

On the same Add Flex Profile dialogue, navigate to the VLAN tab and click +Add (refer to the lab topology diagram).

- VLAN Name: guest

- VLAN Id: 210



Add Flex Profile

VLAN Name	ID	ACL Name
□ data	2	

VLAN Name*: guest

VLAN Id*: 210

ACL Name: Select ACL

C9800 - Site Tag

On 9800 WLC GUI, navigate to Configuration > Tags & Profiles > Tags > Site > Add.

Note: Create a unique Site Tag for each Remote Site that must support the two wireless SSIDs as described.

There is a 1-1 mapping between a geographical location, Site Tag, and a Flex Profile configuration.

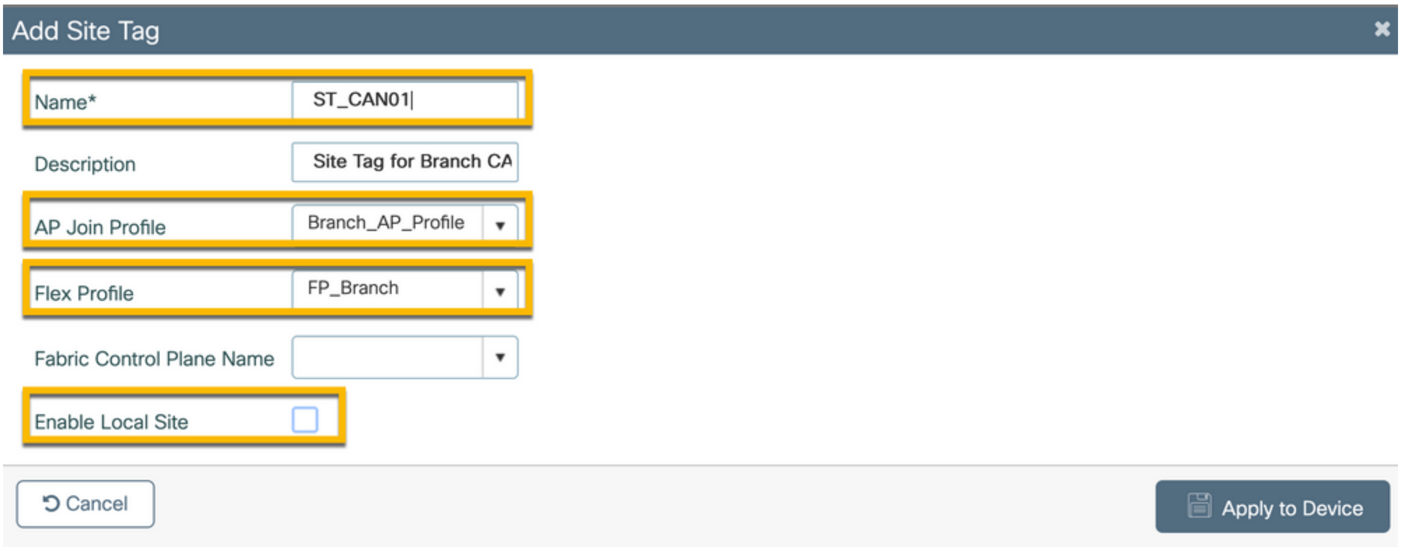
A flex connect site must have a flex connect profile associated with it. You can have a maximum of 100 access points for each Flex Connect site.

- Name: ST_CAN01

- AP Join Profile: Branch_AP_Profile

- Flex Profile: FP_Branch

- Enable Local Site: Disabled



Add Site Tag

Name*	ST_CAN01
Description	Site Tag for Branch CA
AP Join Profile	Branch_AP_Profile ▾
Flex Profile	FP_Branch ▾
Fabric Control Plane Name	▾
Enable Local Site	☐

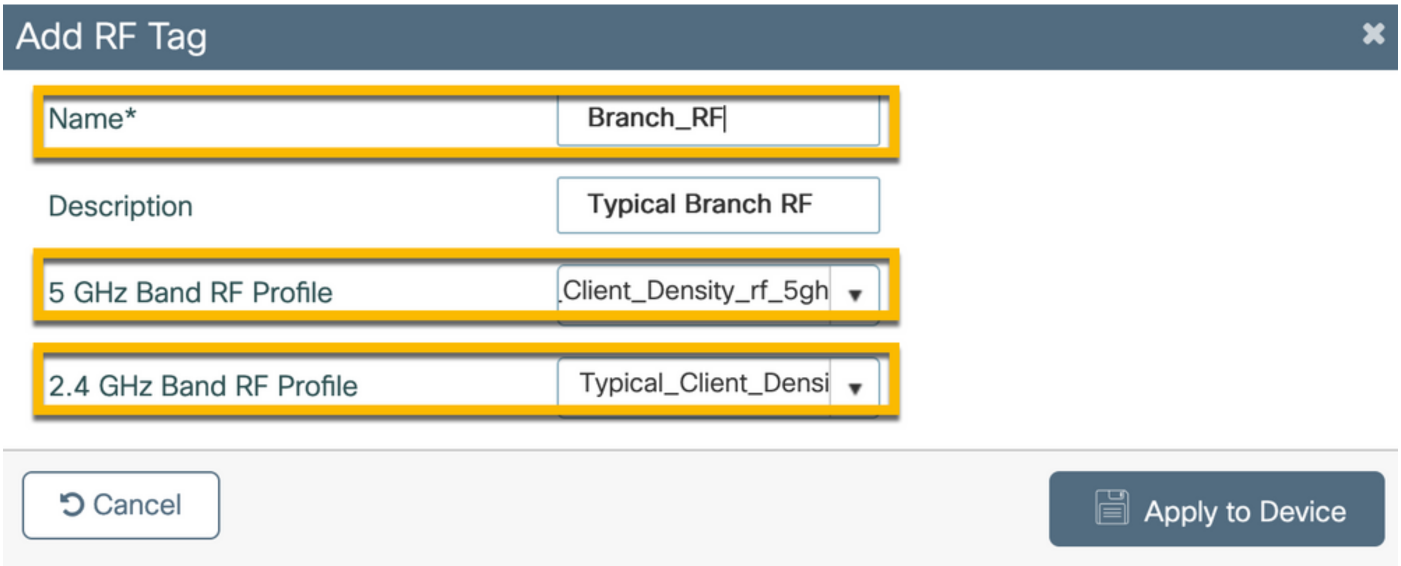
C9800 - RF Profile

On 9800 WLC GUI, navigate to Configuration > Tags & Profiles > Tags > RF > Add.

- Name: Branch_RF

- 5 GHz Band Radio Frequency (RF) Profile: Typical_Client_Density_5gh (system-defined option)

- 2.4 GHz Band RF Profile: Typical_Client_Density_2gh (system-defined option)



Add RF Tag

Name*	Branch_RF
Description	Typical Branch RF
5 GHz Band RF Profile	Client_Density_rf_5gh ▾
2.4 GHz Band RF Profile	Typical_Client_Densi ▾

C9800 - Assign Tags to AP

There are two options available in order to assign defined Tags to individual APs in the deployment:

- AP name-based assignment, which leverages regex rules that match patterns in the AP Name field (Configure > Tags & Profiles > Tags > AP > Filter)

- AP Ethernet MAC address based assignment (Configure > Tags & Profiles > Tags > AP > Static)

In production deployment with the Cisco DNA Center, it is highly recommended to either use DNAC and AP PNP Workflow or use a static bulk Comma-Separated Values (CSV) upload method available in 9800 in order to avoid manual per-AP assignment. Navigate to Configure > Tags & Profiles > Tags > AP > Static > Add (Note the Upload File option).

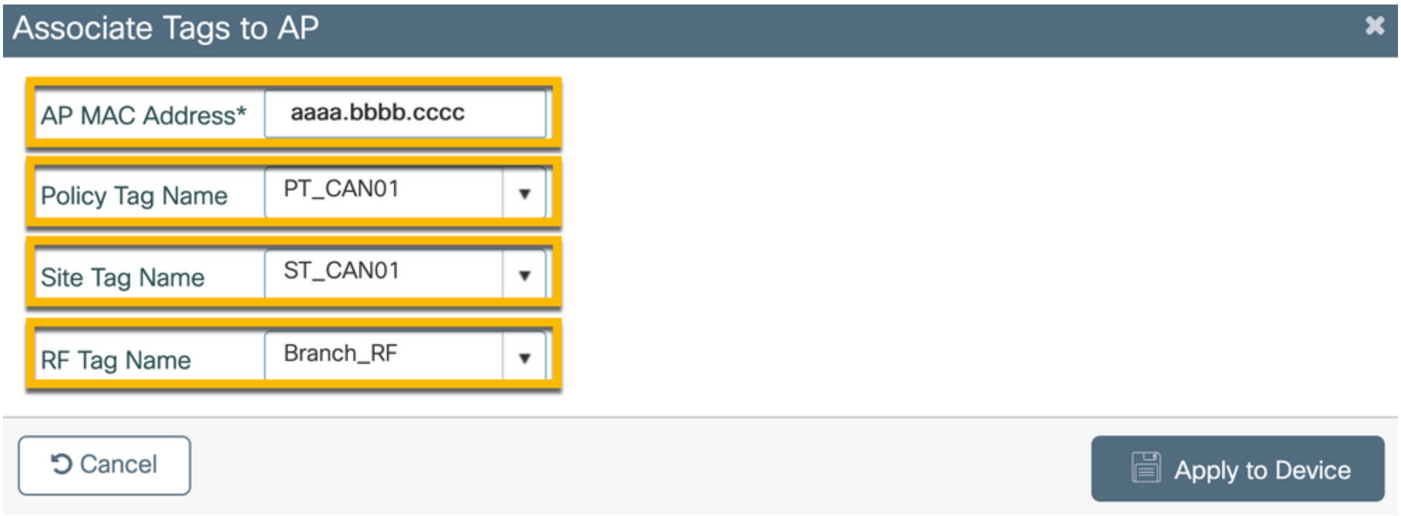
- AP MAC Address: <AP_ETHERNET_MAC>

- Policy Tag Name: PT_CAN01

- Site Tag Name: ST_CAN01

- RF Tag Name: Branch_RF

Note: As of Cisco IOS® XE 17.3.4c there is a maximum of 1,000 regex rules per controller limitation. If the number of sites in the deployment exceeds this number, the static per-MAC assignment must be leveraged.



Associate Tags to AP

AP MAC Address*	aaaa.bbbb.cccc
Policy Tag Name	PT_CAN01
Site Tag Name	ST_CAN01
RF Tag Name	Branch_RF

Note: Alternatively, to leverage the AP-name regex-based tag assignment method, navigate to Configure > Tags & Profiles > Tags > AP > Filter > Add.

- Name: BR_CAN01

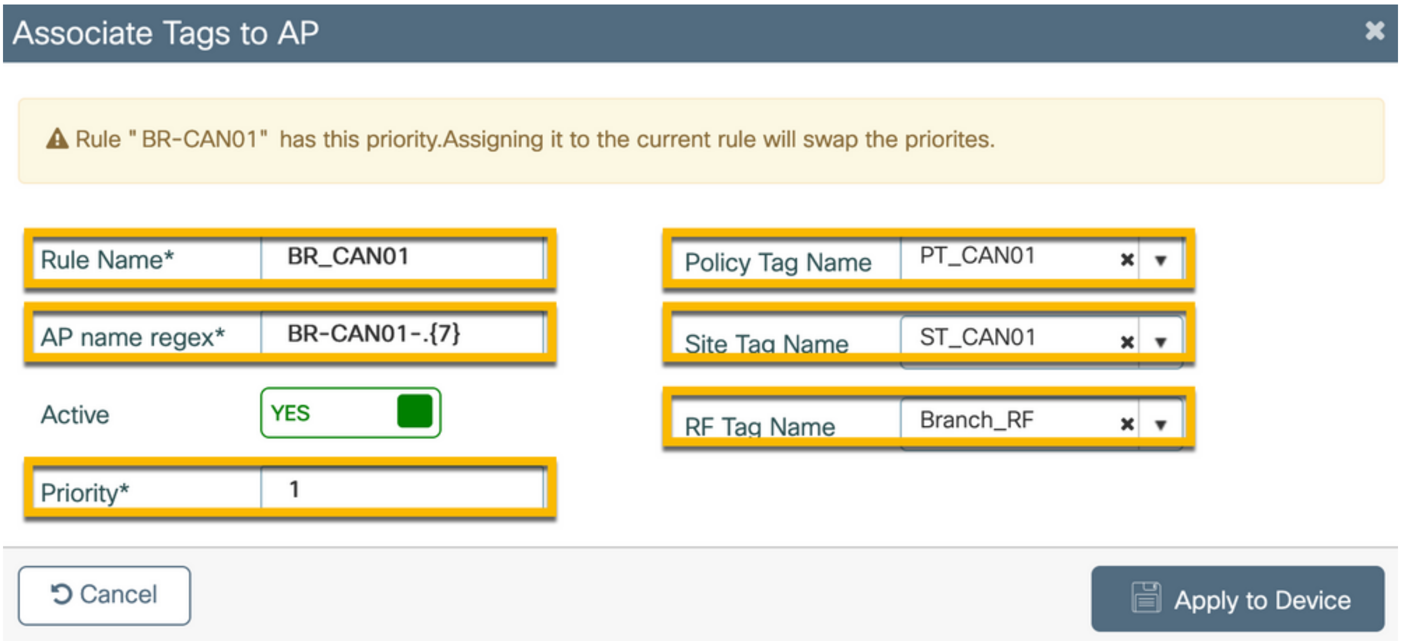
- AP name regex: BR-CAN01-.(7) (This rule matches on AP name convention adopted within the organization. In this example, the Tags are assigned to APs that have an AP Name field that contains 'BR_CAN01-' followed by any seven characters.)

- Priority: 1

- Policy Tag Name: PT_CAN01 (as defined)

- Site Tag Name: ST_CAN01

- RF Tag Name: Branch_RF



Associate Tags to AP

Rule " BR-CAN01" has this priority.Assigning it to the current rule will swap the priorites.

Rule Name*	BR_CAN01
AP name regex*	BR-CAN01-.{7}
Active	YES
Priority*	1
Policy Tag Name	PT_CAN01
Site Tag Name	ST_CAN01
RF Tag Name	Branch_RF

Configure Aruba CPPM Instance

For production/best practices based on Aruba CPPM configuration, contact your local HPE Aruba SE resource.

Aruba ClearPass Server Initial Configuration

Aruba ClearPass is deployed with the use of the Open Virtualization Format (OVF) template on the ESXi <> server that allocates these resources:

- Two reserved virtual CPUs
- 6 GB RAM
- 80 GB disk (must be added manually after initial VM deployment before the machine is powered on)

Apply for Licenses

Apply for a platform license via Administration > Server Manager > Licensing. Add Platform, Access, and Onboard licenses.

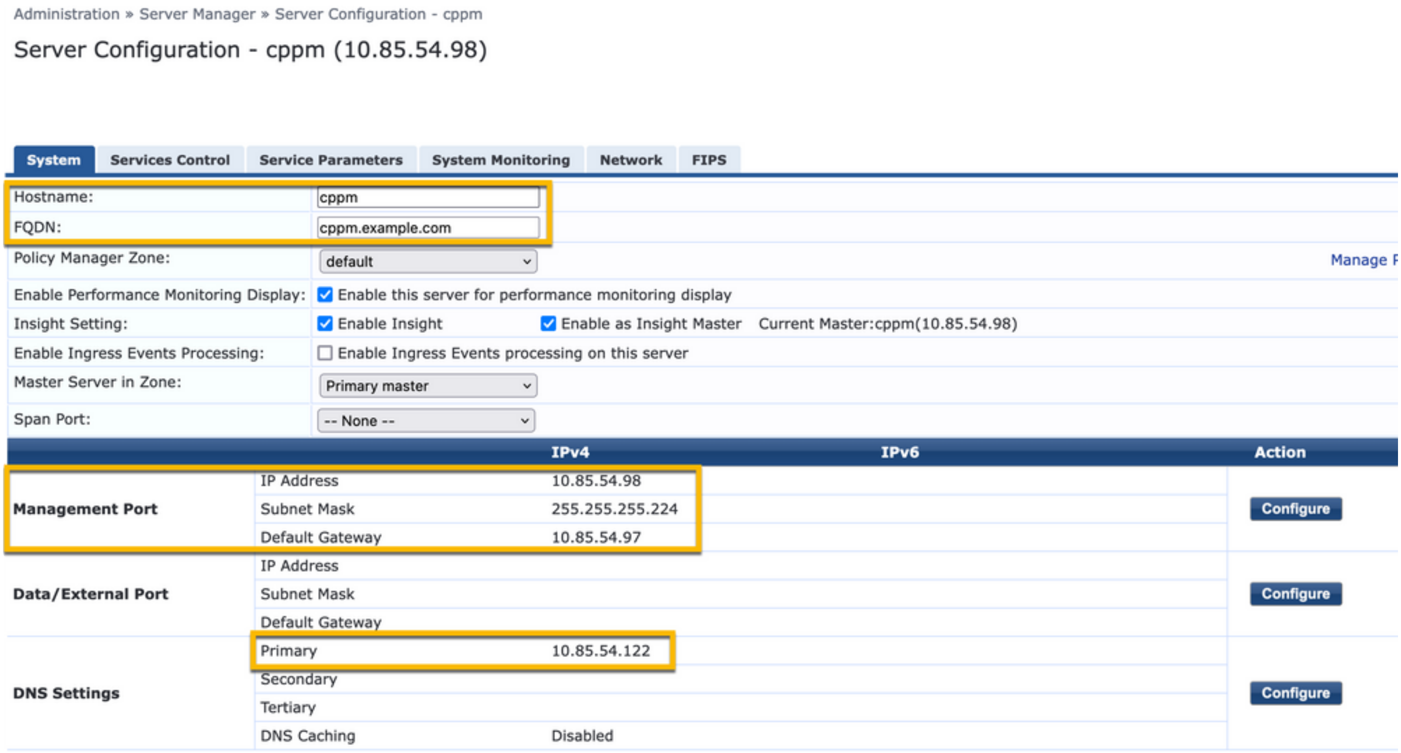
Server Hostname

Navigate to Administration > Server Manager > Server Configuration and choose the newly provisioned CPPM server.

- Hostname: cppm

- FQDN: cppm.example.com

- Verify Management Port IP Addressing and DNS



Administration » Server Manager » Server Configuration - cppm

Server Configuration - cppm (10.85.54.98)

Hostname:	cppm
FQDN:	cppm.example.com
Policy Manager Zone:	default
Enable Performance Monitoring Display:	☑ Enable this server for performance monitoring display
Insight Setting:	☑ Enable Insight ☑ Enable as Insight Master Current Master:cppm(10.85.54.98)
Enable Ingress Events Processing:	□ Enable Ingress Events processing on this server
Master Server in Zone:	Primary master
Span Port:	-- None --

		IPv4	IPv6	Action
Management Port	IP Address	10.85.54.98		Configure
	Subnet Mask	255.255.255.224		
	Default Gateway	10.85.54.97		
Data/External Port	IP Address			Configure
	Subnet Mask			
	Default Gateway			
DNS Settings	Primary	10.85.54.122		Configure
	Secondary			
	Tertiary			
	DNS Caching	Disabled		

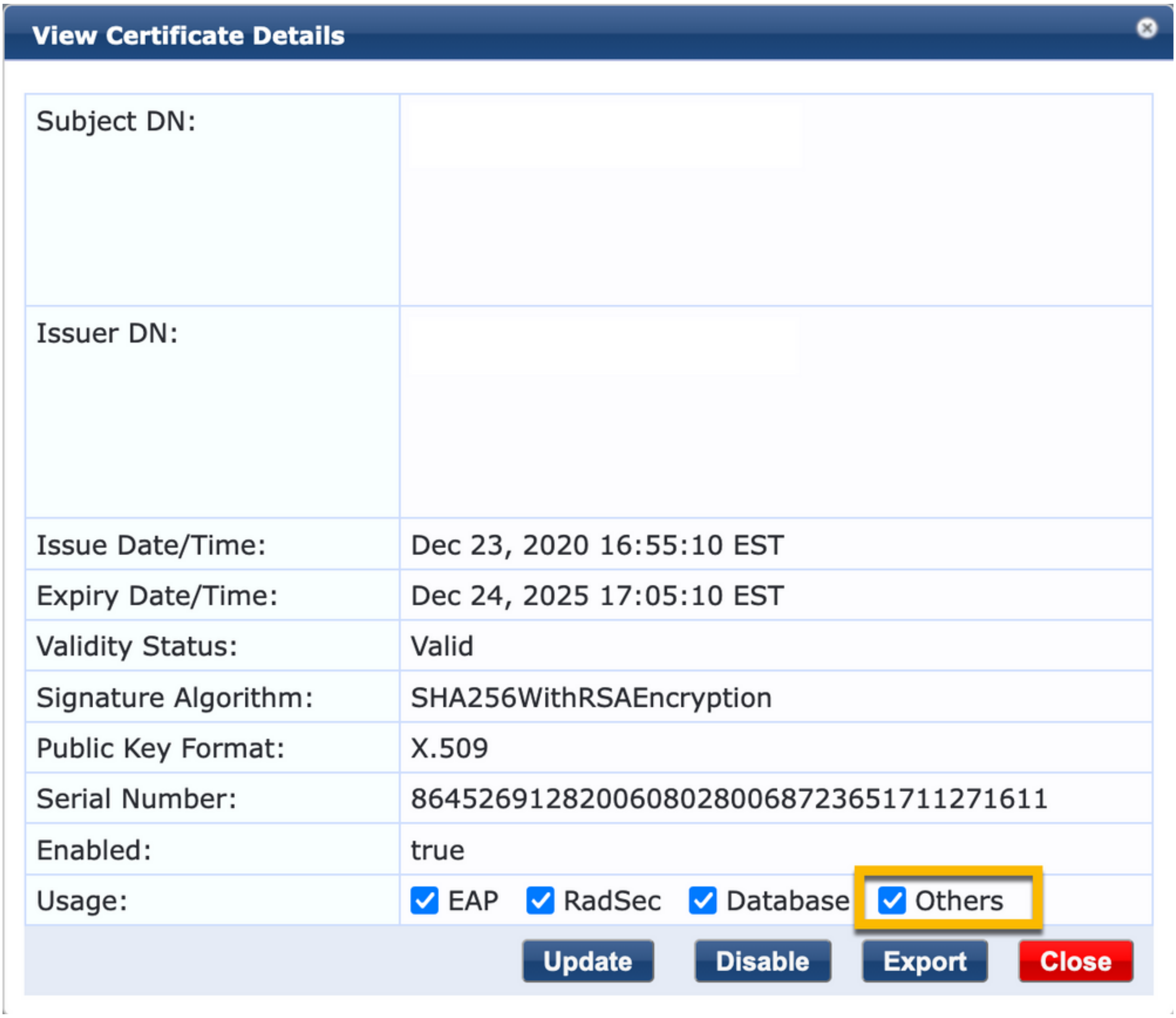
Generate CPPM Web Server Certificate (HTTPS)

This certificate is used when the ClearPass Guest Portal page is presented via HTTPS to guest clients who connect to the Guest Wifi in the Branch.

Step 1. Upload the CA pub chain certificate.

Navigate to Administration > Certificates > Trust List > Add.

- Usage: Enable Others



View Certificate Details

Subject DN:	
Issuer DN:	
Issue Date/Time:	Dec 23, 2020 16:55:10 EST
Expiry Date/Time:	Dec 24, 2025 17:05:10 EST
Validity Status:	Valid
Signature Algorithm:	SHA256WithRSAEncryption
Public Key Format:	X.509
Serial Number:	86452691282006080280068723651711271611
Enabled:	true
Usage:	☑ EAP ☑ RadSec ☑ Database ☑ Others

Step 2. Create Certificate Signing Request.

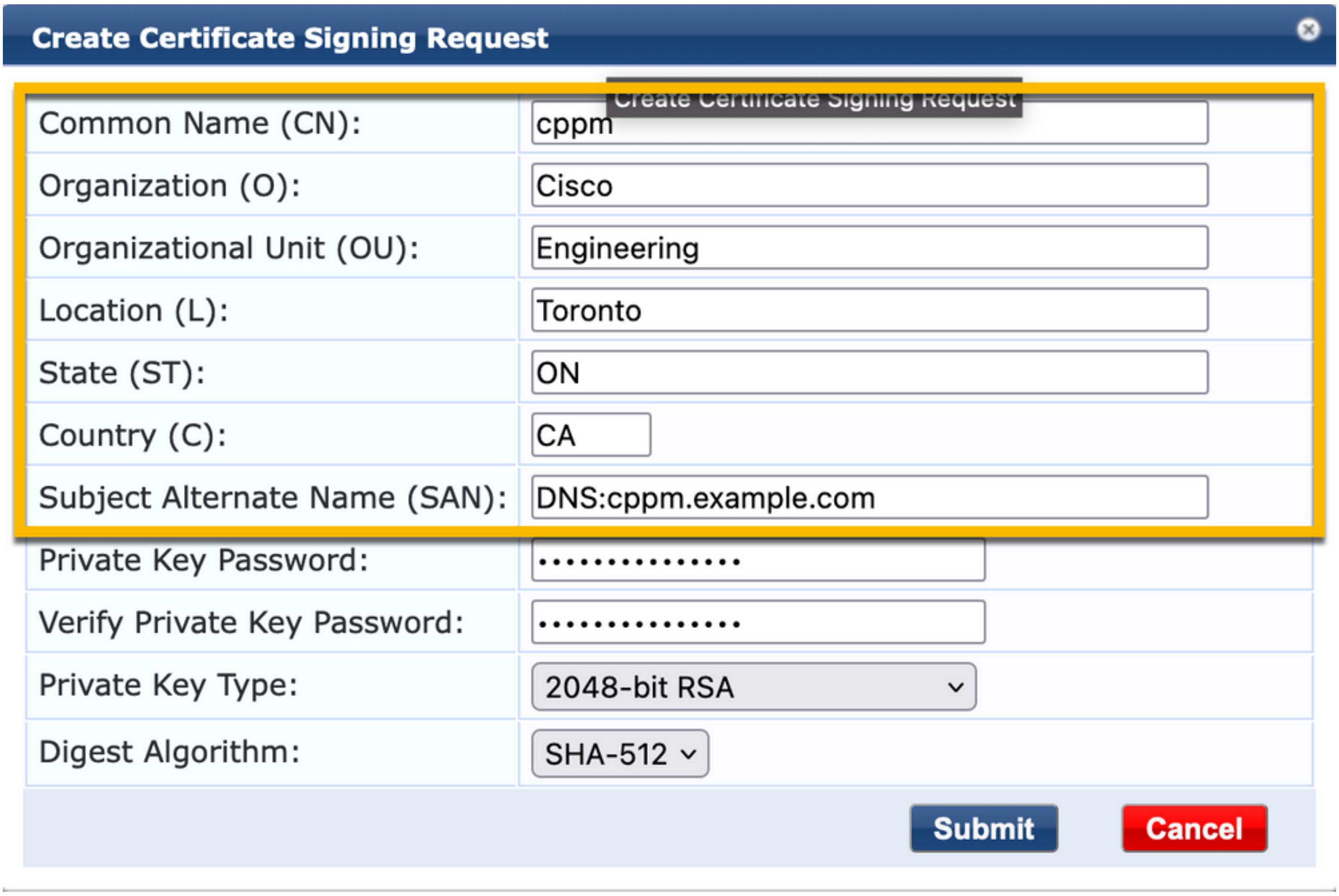
Navigate to Administration > Certificates > Certificate Store > Server Certificates > Usage: HTTPS Server Certificate.

- Click the Create Certificate Signing Request

- Common Name: CPPM

- Organization: cppm.example.com

Ensure to populate the SAN field (a common name must be present in SAN as well as IP and other FQDNs as needed). The format is DNS <fqdn1>,DNS:<fqdn2>,IP<ip1>.



Create Certificate Signing Request

Common Name (CN):	cppm
Organization (O):	Cisco
Organizational Unit (OU):	Engineering
Location (L):	Toronto
State (ST):	ON
Country (C):	CA
Subject Alternate Name (SAN):	DNS:cppm.example.com
Private Key Password:	•••••••••••••••
Verify Private Key Password:	•••••••••••••••
Private Key Type:	2048-bit RSA
Digest Algorithm:	SHA-512

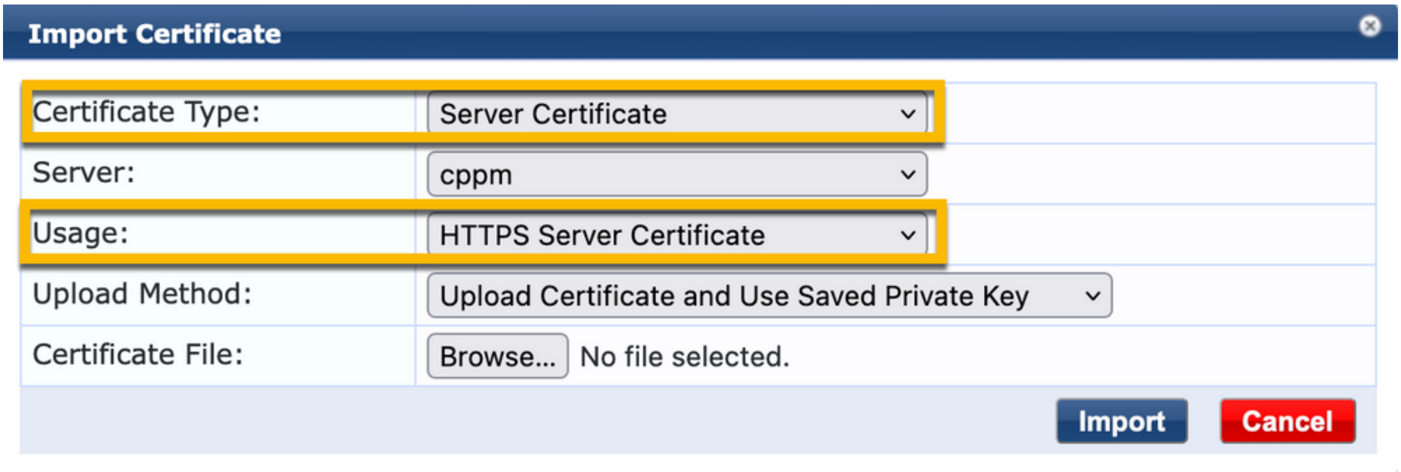
Step 3. In your CA of choice, sign the newly generated CPPM HTTPS Service CSR.

Step 4. Navigate to Certificate Template > Web Server > Import Certificate.

- Certificate Type: Server Certificate

- Usage: HTTP Server Certificate

- Certificate File: Browse, and choose CA signed CPPM HTTPS Service certificate



Import Certificate

Certificate Type:	Server Certificate
Server:	cppm
Usage:	HTTPS Server Certificate
Upload Method:	Upload Certificate and Use Saved Private Key
Certificate File:	Browse... No file selected.

Define C9800 WLC as a Network Device

Navigate to Configuration > Network > Devices > Add.

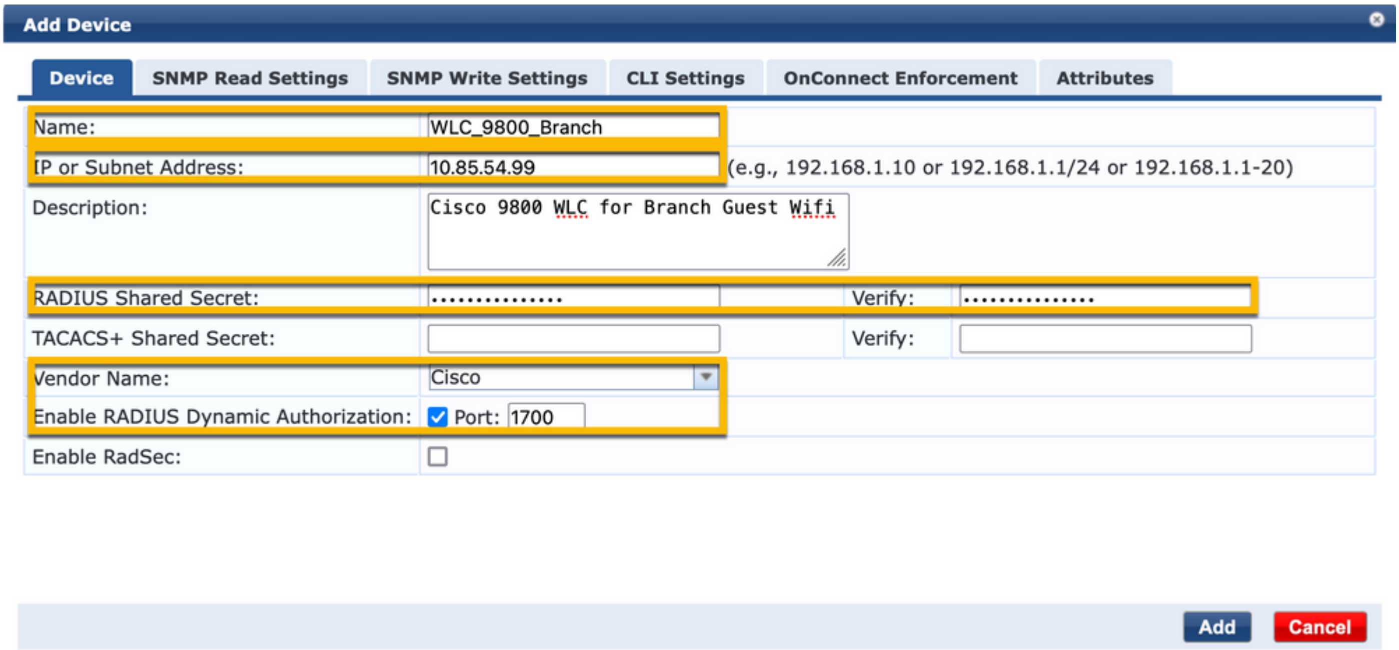
- Name: WLC_9800_Branch

- IP or Subnet Address: 10.85.54.99 (refer to lab topology diagram)

- RADIUS Shared Cisco: <WLC RADIUS password>

- Vendor Name: Cisco

- Enable RADIUS Dynamic Authorization: 1700



Name: WLC_9800_Branch

IP or Subnet Address: 10.85.54.99 (e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20)

Description: Cisco 9800 WLC for Branch Guest Wifi

RADIUS Shared Secret: ••••••••••••••• Verify: •••••••••••••••

TACACS+ Shared Secret: Verify:

Vendor Name: Cisco

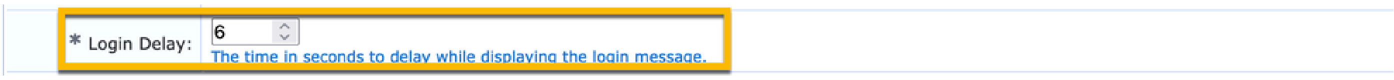
Enable RADIUS Dynamic Authorization: ☑ Port: 1700

Enable RadSec: □

Guest Portal Page and CoA Timers

It is very important to set the correct timer values throughout the configuration. If timers are not tuned, you are likely to run into a cycling Web Portal redirect with the client, not in 'Run State'.
Timers to pay attention to:

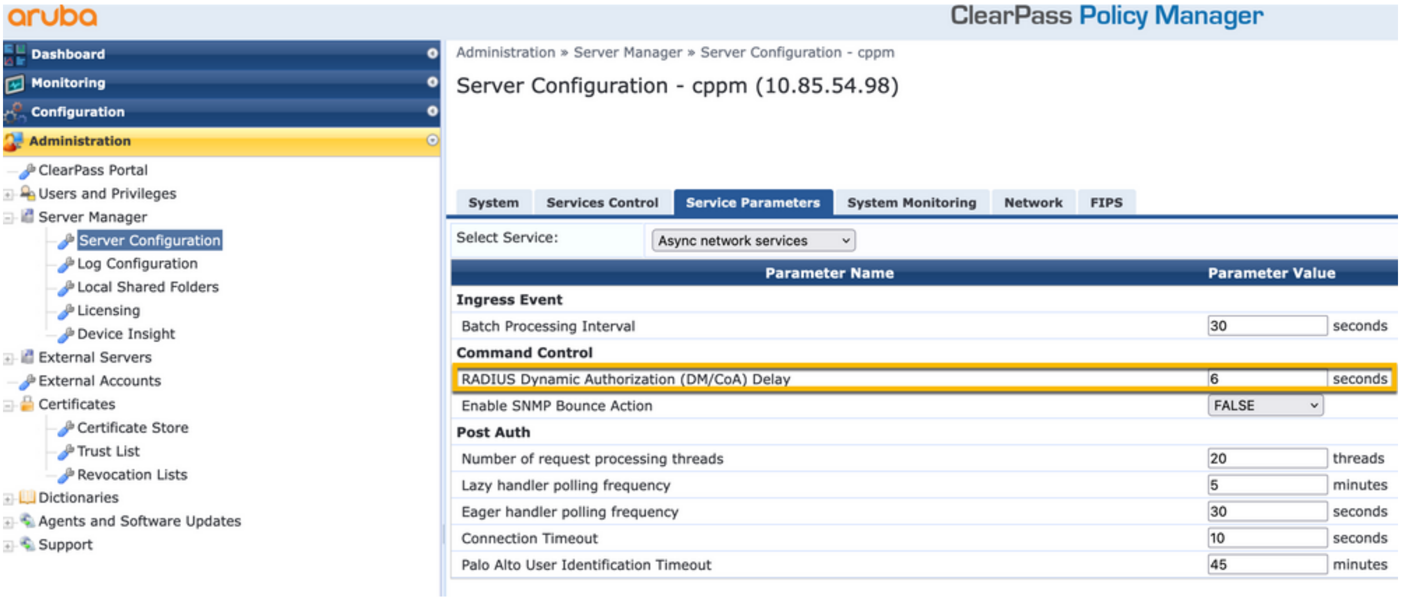
- Portal Web Login timer: This timer delays your redirect page before it allows access to the guest portal page to notify the CPPM service of state transition, register the Endpoint custom attribute 'Allow-Guest-Internet' value, and trigger the CoA process from CPPM to WLC. Navigate to Guest > Configuration > Pages > Web Logins.
  - Choose Guest Portal Name: Lab Anonymous Guest Registration (this Guest Portal page configuration is detailed as shown)
  - Click Edit
  - Login Delay: 6 seconds



* Login Delay: 6
The time in seconds to delay while displaying the login message.

- ClearPass CoA delay timer: This delays the origination of CoA messages from ClearPass to WLC. This is required for CPPM to successfully transition the state of the Client Endpoint internally before CoA Acknowledgement (ACK) comes back from WLC. Lab tests show the sub-millisecond response times from WLC, and if CPPM has not finished updating the Endpoint attributes, the new RADIUS session from WLC is matched to the Unauthenticated MAB Service enforcement policy, and the client is given a redirect page again. Navigate to CPPM > Administration > Server Manager > Server Configuration and choose CPPM Server > Service Parameters.

- RADIUS Dynamic Authorization (DM/CoA) Delay - Set to six seconds



Administration » Server Manager » Server Configuration - cppm

Server Configuration - cppm (10.85.54.98)

Select Service: Async network services

Parameter Name	Parameter Value	
Ingress Event		
Batch Processing Interval	30	seconds
Command Control		
RADIUS Dynamic Authorization (DM/CoA) Delay	6	seconds
Enable SNMP Bounce Action	FALSE	
Post Auth		
Number of request processing threads	20	threads
Lazy handler polling frequency	5	minutes
Eager handler polling frequency	30	seconds
Connection Timeout	10	seconds
Palo Alto User Identification Timeout	45	minutes

ClearPass - Guest CWA Configuration

ClearPass-side CWA Configuration is composed of (3) Service Points/Stages:

ClearPass Component	Service Type	Purpose
1. Policy Manager	Service: Mac Authentication	If the custom attribute Allow-Guest-Internet = TRUE, allow it onto the network. Else, trigger Redirect and COA: Reauthenticate.
2. Guest	Web Logins	Present Anonymous login AUP page. Post-auth set a custom attribute Allow-Guest-Internet = TRUE.
3. Policy Manager	Service: Web-based Authentication	Update Endpoint to Known Set custom attribute Allow-Guest-Internet = TRUE COA: Reauthenticate

ClearPass Endpoint Metadata Attribute: Allow-Guest-Internet

Create a metadata attribute of type Boolean in order to track the Guest Endpoint state as the client transitions between the 'Webauth Pending' and 'Run' state:

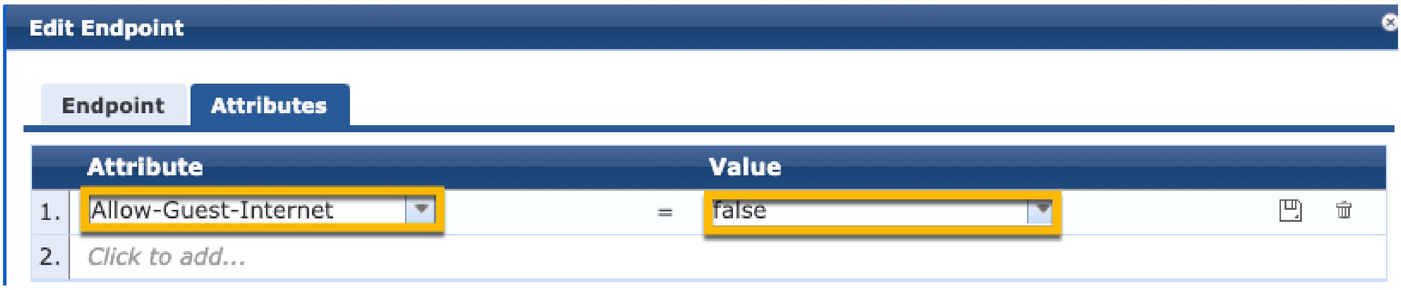
- New guests that connect to Wifi have a default metadata attribute set in order to Allow-Guest-Internet=false. Based on this attribute the client auth goes through the MAB service

- Guest client when you click the AUP Accept button, has its metadata attribute updated in order to Allow-

Guest-Internet=true. Subsequent MAB based on this attribute set to True allows non-redirected access to the Internet

Navigate to ClearPass > Configuration > Endpoints, pick any endpoint from the list, click the Attributes tab, add Allow-Guest-Internet with the value false and Save.

Note: You can also edit the same endpoint, and delete this attribute right after - this step simply creates a field in the Endpoints metadata DB that can be used in policies.



Edit Endpoint

	Attribute		Value
1.	Allow-Guest-Internet	=	false
2.	Click to add...		

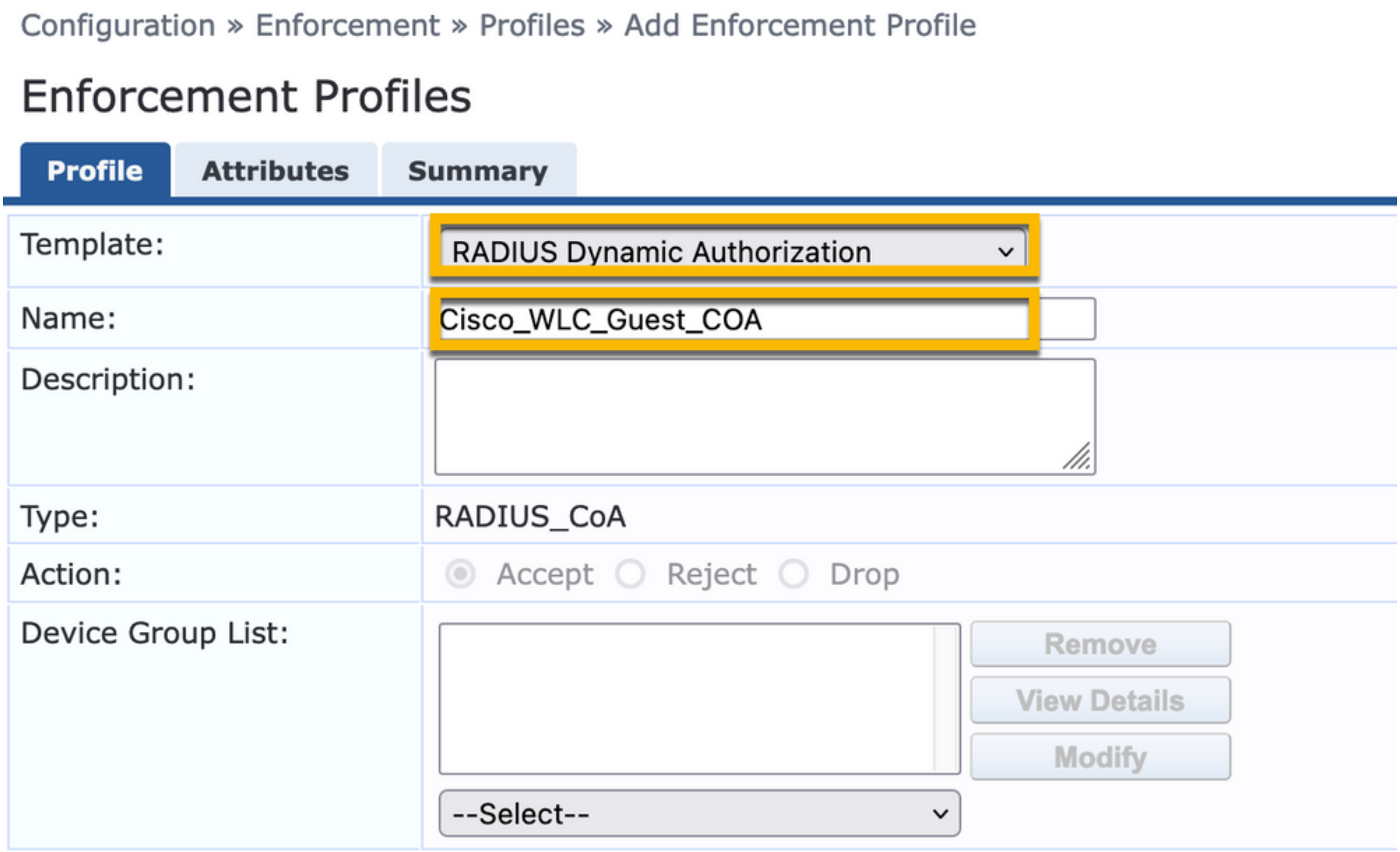
ClearPass Reauthenticate Enforcement Policy Configuration

Create an Enforcement Profile that is assigned to the guest client immediately after the client accepts AUP on the Guest Portal page.

Navigate to ClearPass > Configuration > Profiles > Add.

- Template: RADIUS Dynamic Authorization

- Name: Cisco_WLC_Guest_COA



Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Template:	RADIUS Dynamic Authorization
Name:	Cisco_WLC_Guest_COA
Description:	
Type:	RADIUS_CoA
Action:	● Accept ○ Reject ○ Drop
Device Group List:	--Select--

Radius:IETF	Calling-Station-Id	%{Radius:IETF:Calling-Station-Id}
Radius:Cisco	Cisco-AVPair	subscriber:command=reauthenticate
Radius:Cisco	Cisco-AVPair	%{Radius:Cisco:Cisco-AVPair:subscriber:audit-session-id}
Radius:Cisco	Cisco-AVPair	subscriber:reauthenticate-type=last-type=last

ClearPass Guest Portal Redirect Enforcement Profile Configuration

Create an Enforcement Profile that is applied to the Guest during the initial MAB phase, when the MAC address is not found in the CPPM Endpoint Database with 'Allow-Guest-Internet' set to 'true'.

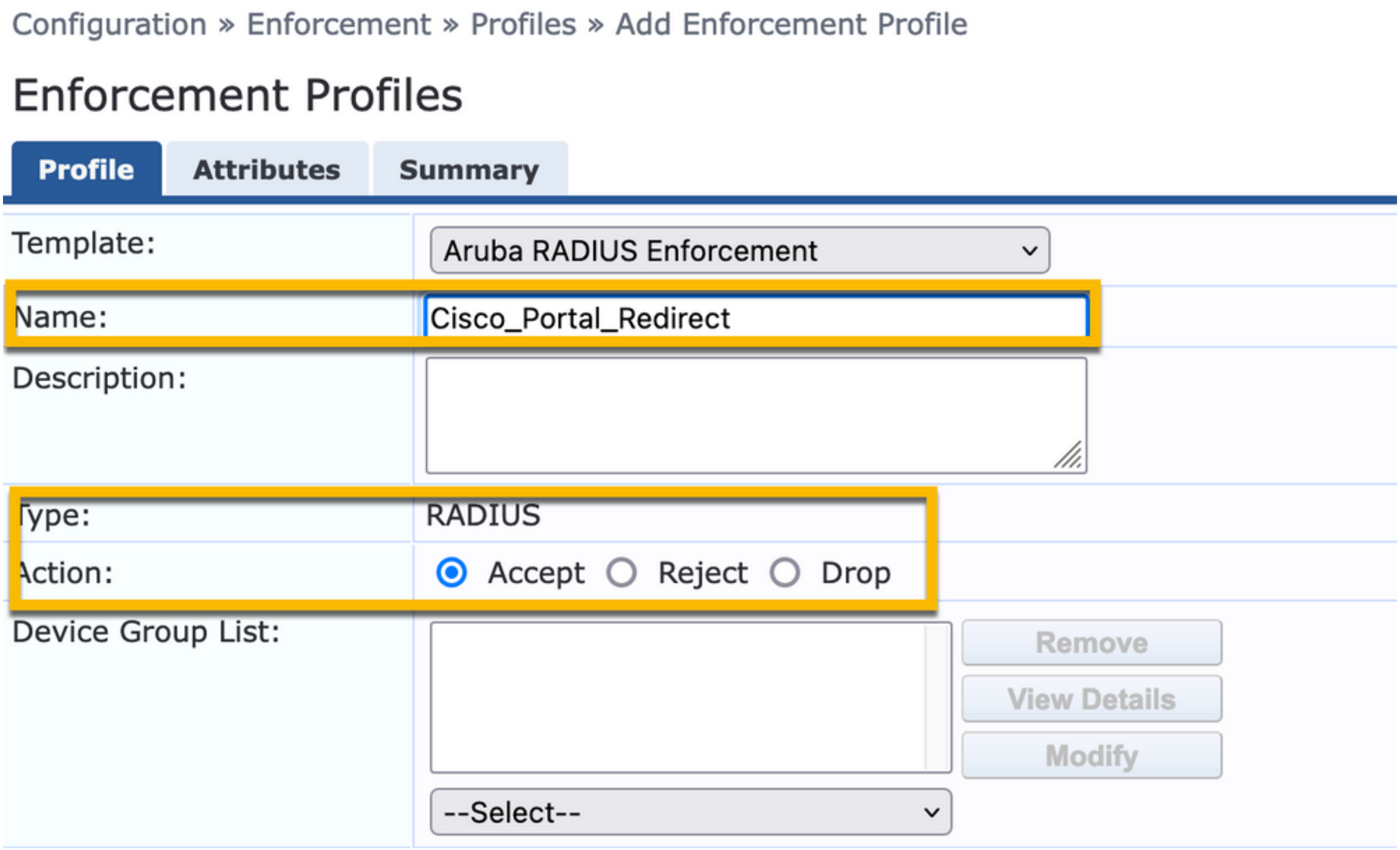
This causes the 9800 WLC to redirect the Guest client to the CPPM Guest Portal for external authentication.

Navigate to ClearPass > Enforcement > Profiles > Add.

- Name: Cisco_Portal_Redirect

- Type: RADIUS

- Action: Accept



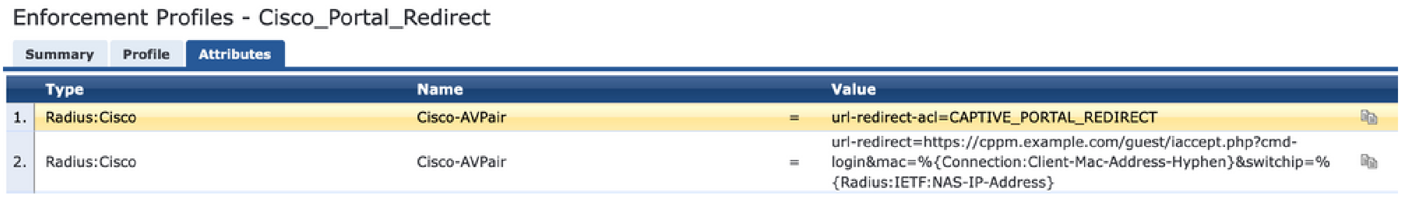
Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Template:	Aruba RADIUS Enforcement
Name:	Cisco_Portal_Redirect
Description:	
Type:	RADIUS
Action:	● Accept ○ Reject ○ Drop
Device Group List:	--Select--

ClearPass Redirect Enforcement Profile

In the same dialogue, under the Attributes tab, configure two Attributes as per this image:


Enforcement Profiles - Cisco_Portal_Redirect

	Type	Name		Value
1.	Radius:Cisco	Cisco-AVPair	=	url-redirect-acl=CAPTIVE_PORTAL_REDIRECT
2.	Radius:Cisco	Cisco-AVPair	=	url-redirect=https://cppm.example.com/guest/iaccept.php?cmd-login&mac=%{Connection:Client-Mac-Address-Hyphen}&switchip=%{Radius:IETF:NAS-IP-Address}

ClearPass Redirect Profile Attributes

The url-redirect-acl attribute is set to CAPTIVE-PORTAL-REDIRECT, which is the name of the ACL created on C9800.

Note: Only the reference to the ACL is passed in the RADIUS message, and not the ACL contents. It is important that the name of the ACL created on 9800 WLC matches exactly with the value of this RADIUS attribute as shown.

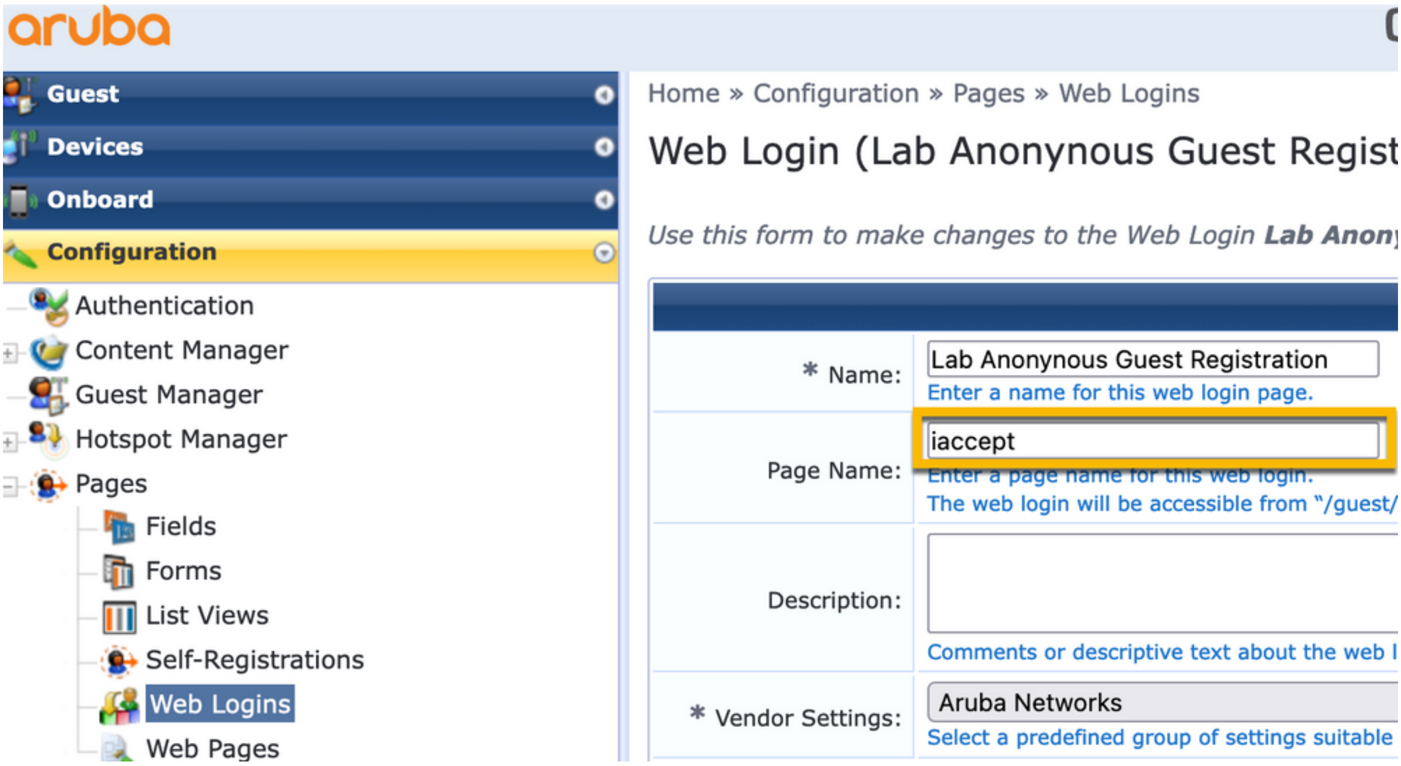
The url-redirect attribute is composed of several parameters:

- **The target URL** where the Guest Portal is hosted, https://cppm.example.com/guest/iaccept.php
- **Guest Client MAC**, macro %{Connection:Client-Mac-Address-Hyphen}
- **Authenticator IP** (9800 WLC triggers the redirect), macro %{Radius:IETF:NAS-IP-Address}
- **cmd-login** action

The URL of the ClearPass Guest Web Login Page is seen when you navigate to CPPM > Guest > Configuration > Pages > Web Logins > Edit.

In this example, the Guest Portal page name in CPPM is defined as iaccept.

Note: The configuration steps for the Guest Portal page are as described.



Home » Configuration » Pages » Web Logins

Web Login (Lab Anonynous Guest Regist

*Use this form to make changes to the Web Login **Lab Anony***

* Name:	Lab Anonynous Guest Registration Enter a name for this web login page.
Page Name:	iaccept Enter a page name for this web login. The web login will be accessible from "/guest/
Description:	 Comments or descriptive text about the web l
* Vendor Settings:	Aruba Networks Select a predefined group of settings suitable

Note: For Cisco devices, normally audit_session_id is used, but, that is not supported by other vendors.

ClearPass Metadata Enforcement Profile Configuration

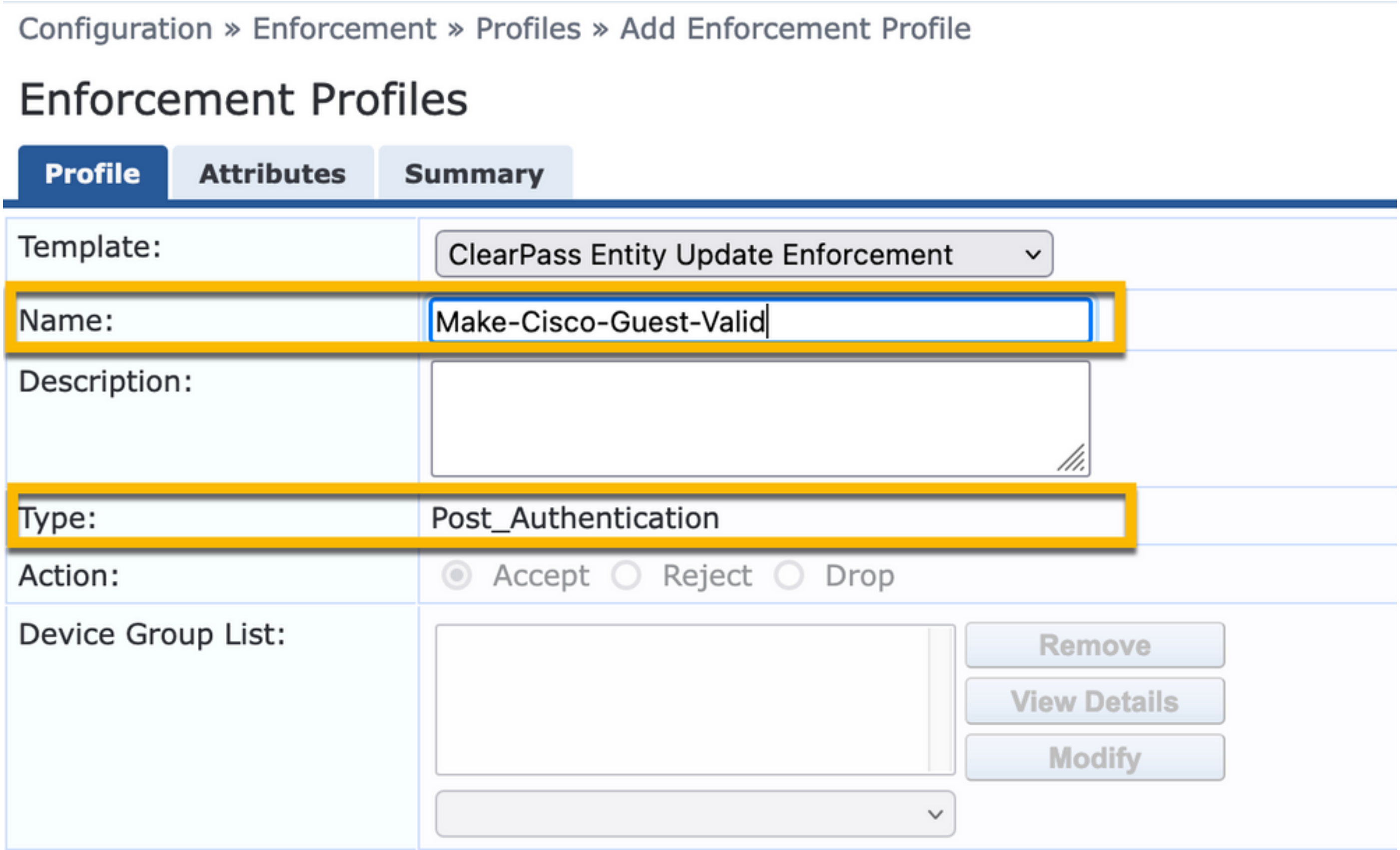
Configure Enforcement Profile in order to update Endpoint metadata attribute that is used for state transition tacking by CPPM.

This profile is applied to the MAC Address entry of the Guest Client in the Endpoint database and sets the Allow-Guest-Internet argument to 'true'.

Navigate to ClearPass > Enforcement > Profiles > Add.

- Template: ClearPass Entity Update Enforcement

- Type: Post_Authentication



Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Template:	ClearPass Entity Update Enforcement
Name:	Make-Cisco-Guest-Valid
Description:	
Type:	Post_Authentication
Action:	● Accept ○ Reject ○ Drop
Device Group List:	

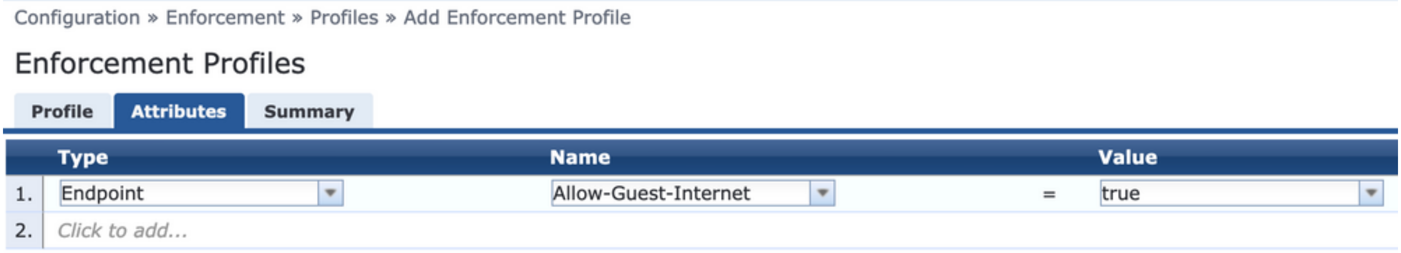
In the same dialogue, the Attributes tab.

- Type: Endpoint

- Name: Allow-Guest-Internet

Note: For this name to appear in the dropdown menu, you must manually define this field for at least one Endpoint as described in the steps.

- Value: true



Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

	Type	Name		Value
1.	Endpoint	Allow-Guest-Internet	=	true
2.	Click to add...			

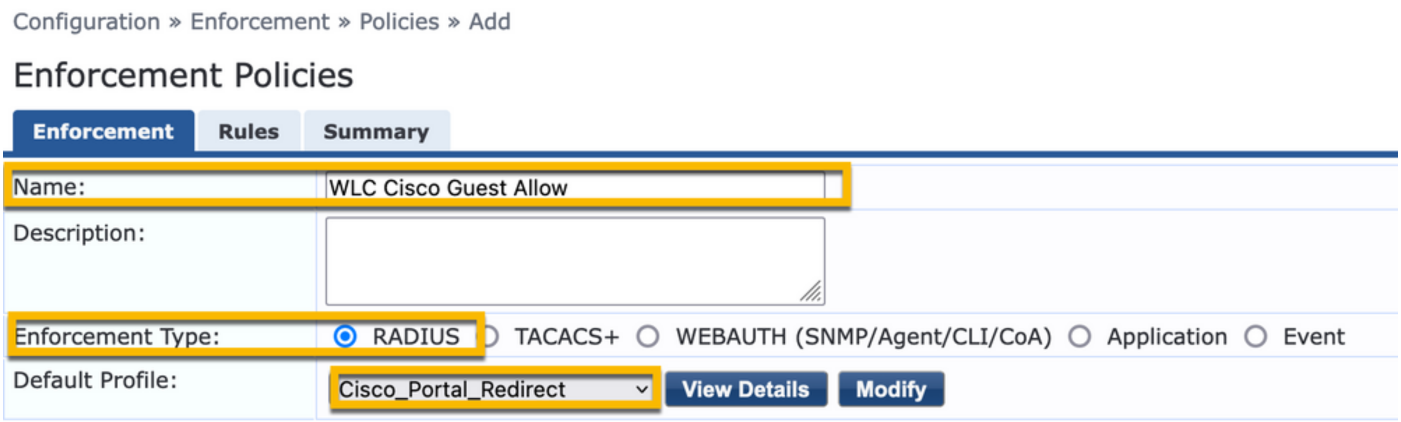
ClearPass Guest Internet Access Enforcement Policy Configuration

Navigate to ClearPass > Enforcement > Policies > Add.

- Name: WLC Cisco Guest Allow

- Enforcement Type: RADIUS

- Default Profile: Cisco_Portal_Redirect



Configuration » Enforcement » Policies » Add

Enforcement Policies

Name:	WLC Cisco Guest Allow
Description:	
Enforcement Type:	● RADIUS ○ TACACS+ ○ WEBAUTH (SNMP/Agent/CLI/CoA) ○ Application ○ Event
Default Profile:	Cisco_Portal_Redirect

In the same dialogue, navigate to the Rules tab and click Add Rule.

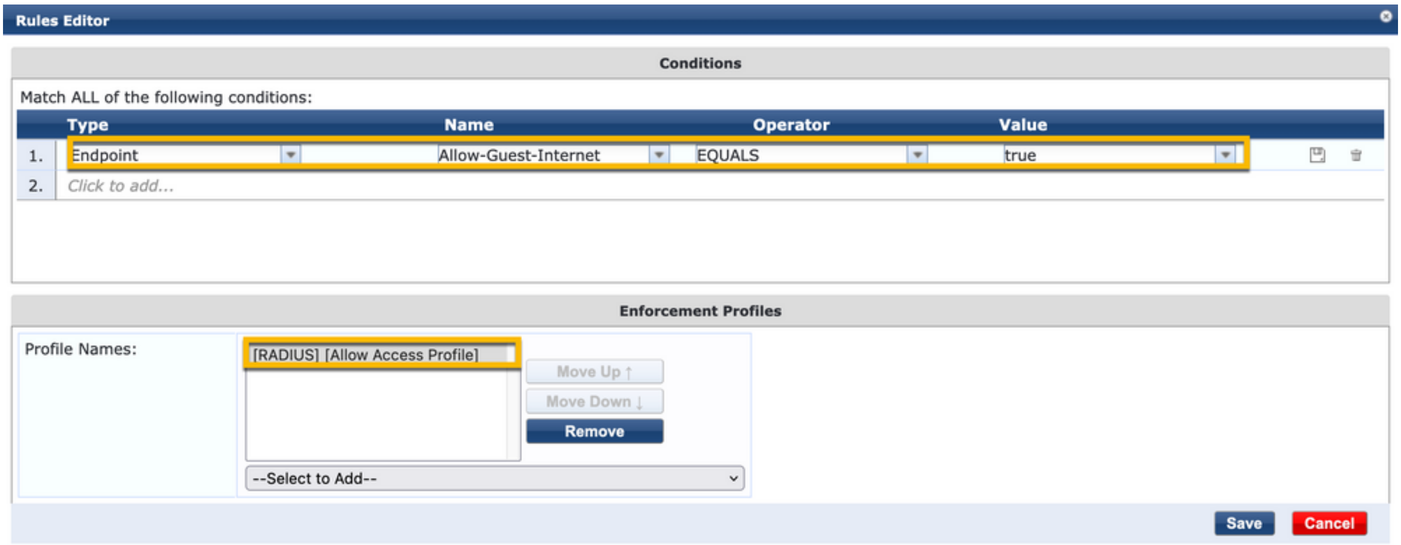
- Type: Endpoint

- Name: Allow-Guest-Internet

- Operator: EQUALS

- Value True

- Profile Names / Choose to Add: [RADIUS] [Allow Access Profile]



Rules Editor

Conditions

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Endpoint	Allow-Guest-Internet	EQUALS	true
2.	Click to add...			

Enforcement Profiles

Profile Names: [RADIUS] [Allow Access Profile]

--Select to Add--

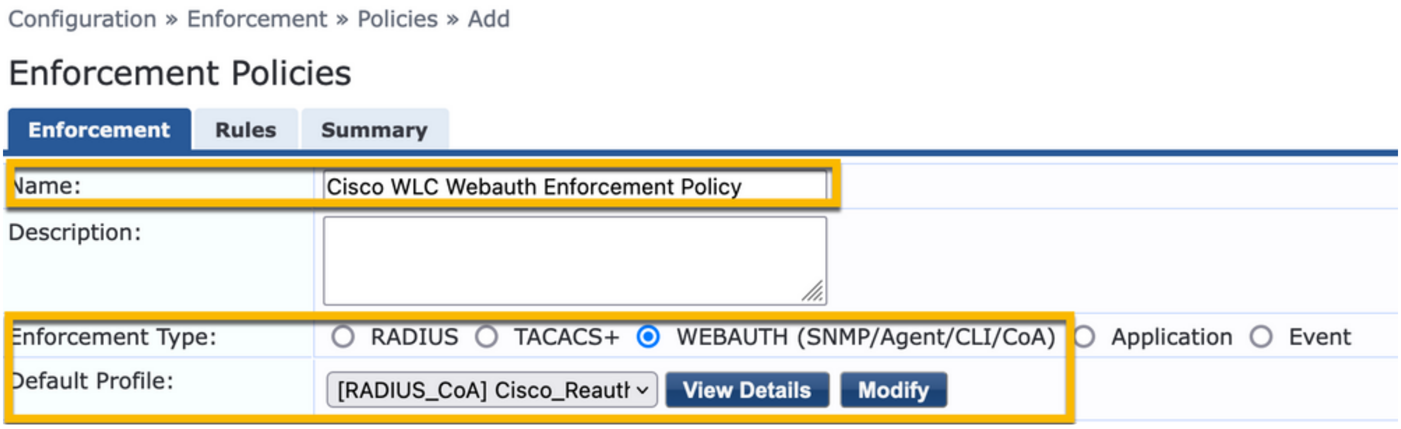
ClearPass Guest Post-AUP Enforcement Policy Configuration

Navigate to ClearPass > Enforcement > Policies > Add.

- Name: Cisco WLC Webauth Enforcement Policy

- Enforcement Type: WEBAUTH (SNMP/Agent/CLI/CoA)

- Default Profile: [RADIUS_CoA] Cisco_Reauthenticate_Session



Configuration » Enforcement » Policies » Add

Enforcement Policies

Name:	Cisco WLC Webauth Enforcement Policy
Description:	
Enforcement Type:	○ RADIUS ○ TACACS+ ● WEBAUTH (SNMP/Agent/CLI/CoA) ○ Application ○ Event
Default Profile:	[RADIUS_CoA] Cisco_Reautl

In the same dialogue, navigate to Rules > Add.

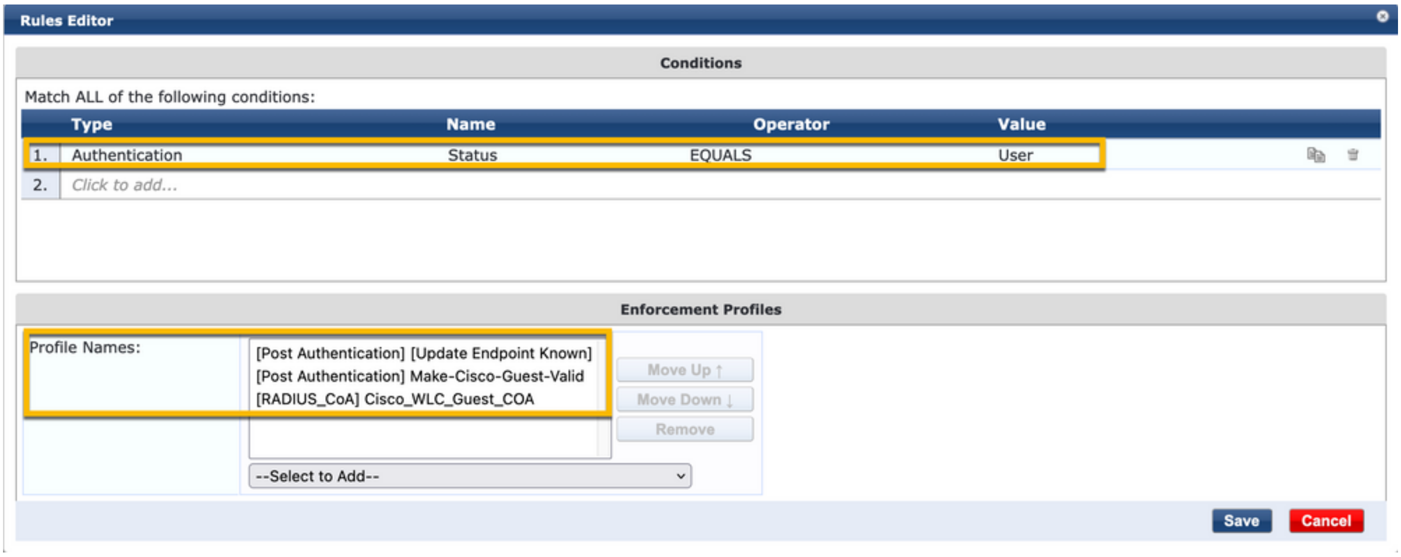
- Conditions: Authentication

- Name: Status

- Operator: EQUALS

- Value: User

- Profile Names: <add each>:
- [Post Authentication] [Update Endpoint Known]
- [Post Authentication] [Make-Cisco-Guest-Valid]
- [RADIUS_CoA] [Cisco_WLC_Guest_COA]



Rules Editor

Conditions

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Authentication	Status	EQUALS	User
2.	Click to add...			

Enforcement Profiles

Profile Names:
[Post Authentication] [Update Endpoint Known]
[Post Authentication] Make-Cisco-Guest-Valid
[RADIUS_CoA] Cisco_WLC_Guest_COA

Note: If you run into a scenario with a continuous Guest Portal redirect pseudo browser pop-up, it is indicative that either the CPPM Timers require adjustments or that the RADIUS CoA messages are not properly exchanged between CPPM and 9800 WLC. Verify these sites.

- Navigate to CPPM > Monitoring > Live Monitoring > Access Tracker, and ensure the RADIUS log entry contains RADIUS CoA details.

- On 9800 WLC, navigate to Troubleshooting > Packet Capture, enable PCAP on the interface where the arrival of RADIUS CoA packets is expected, and verify RADIUS CoA messages are received from the CPPM.

ClearPass MAB Authentication Service Configuration

The service is matched on Attribute Value (AV) pair Radius: Cisco | CiscoAVPair | cisco-wlan-ssid

Navigate to ClearPass > Configuration > Services > Add.

Service Tab:

- Name: GuestPortal - Mac Auth

- Type: MAC Authentication

- More Options: Choose Authorization, Profile Endpoints

Add match rule:

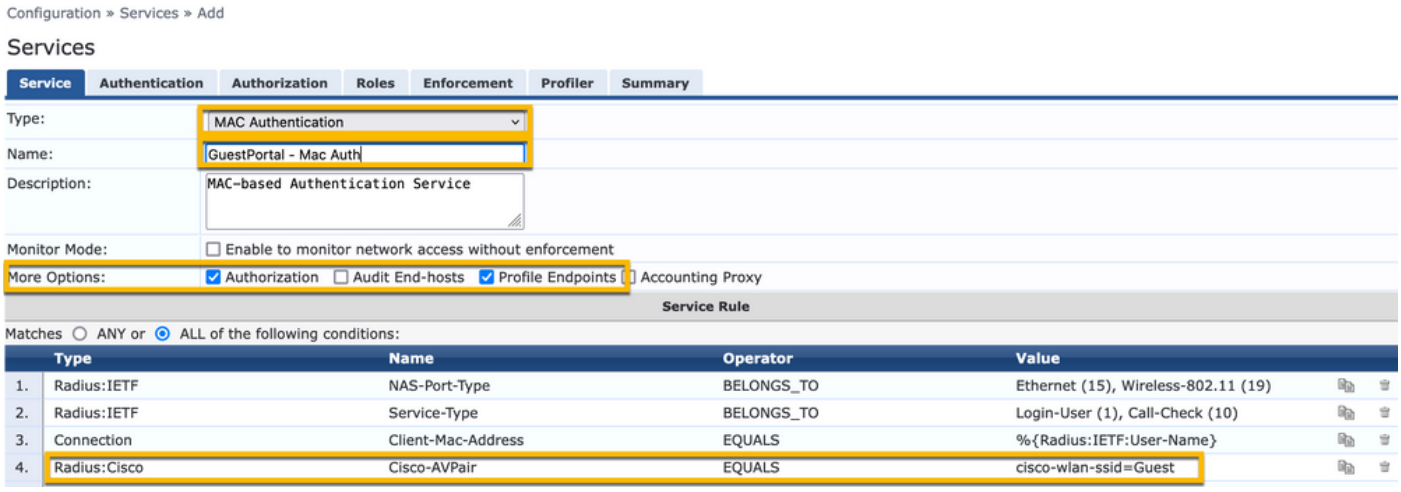
- Type: Radius: Cisco

- Name: Cisco-AVPair

- Operator: EQUALS

- Value: cisco-wlan-ssid=Guest (match your configured Guest SSID name)

Note: 'Guest' is the name of the broadcasted Guest SSID by 9800 WLC.



Type: MAC Authentication

Name: GuestPortal - Mac Auth

Description: MAC-based Authentication Service

Monitor Mode: □ Enable to monitor network access without enforcement

More Options: ☑ Authorization □ Audit End-hosts ☑ Profile Endpoints □ Accounting Proxy

Service Rule

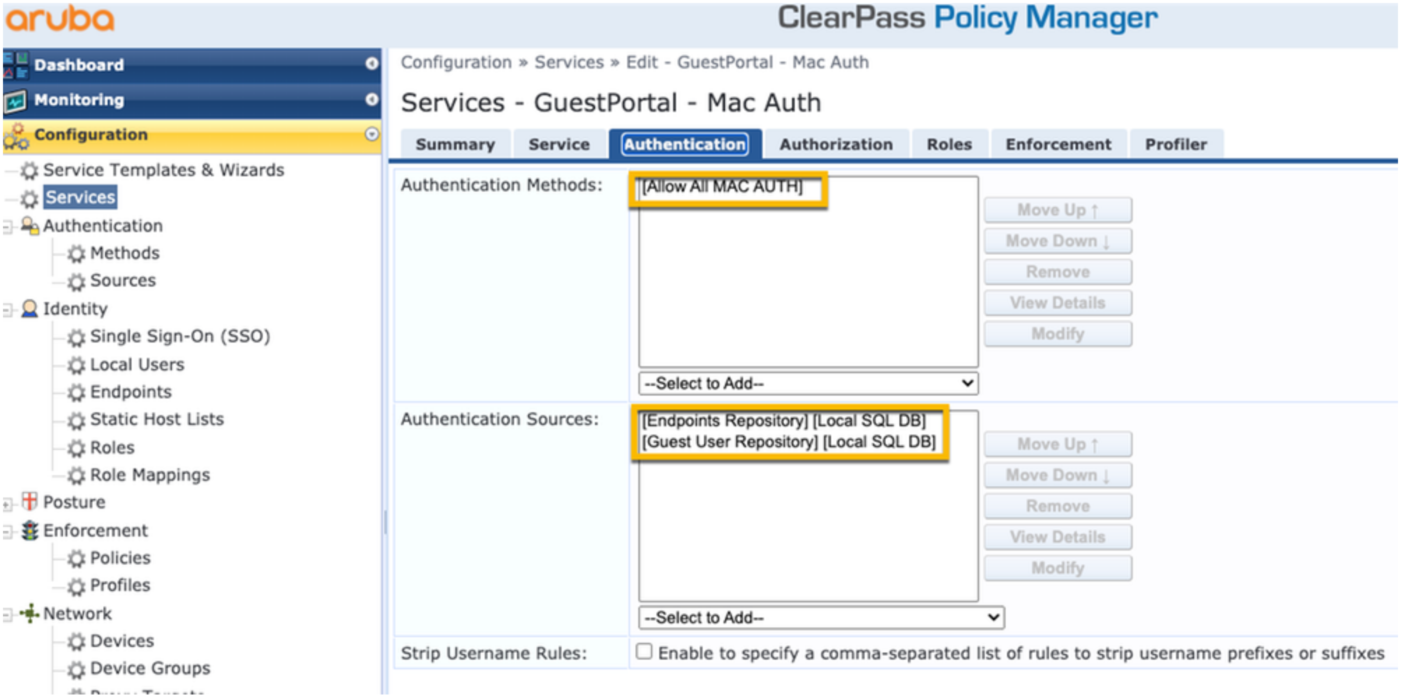
Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet (15), Wireless-802.11 (19)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Call-Check (10)
3.	Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}
4.	Radius:Cisco	Cisco-AVPair	EQUALS	cisco-wlan-ssid=Guest

While in the same dialogue, choose the Authentication Tab.

- Authentication Methods: Remove [MAC AUTH], Add [Allow All MAC AUTH]

- Authentication Sources: [Endpoints Repository][Local SQL DB], [Guest User Repository][Local SQL DB]



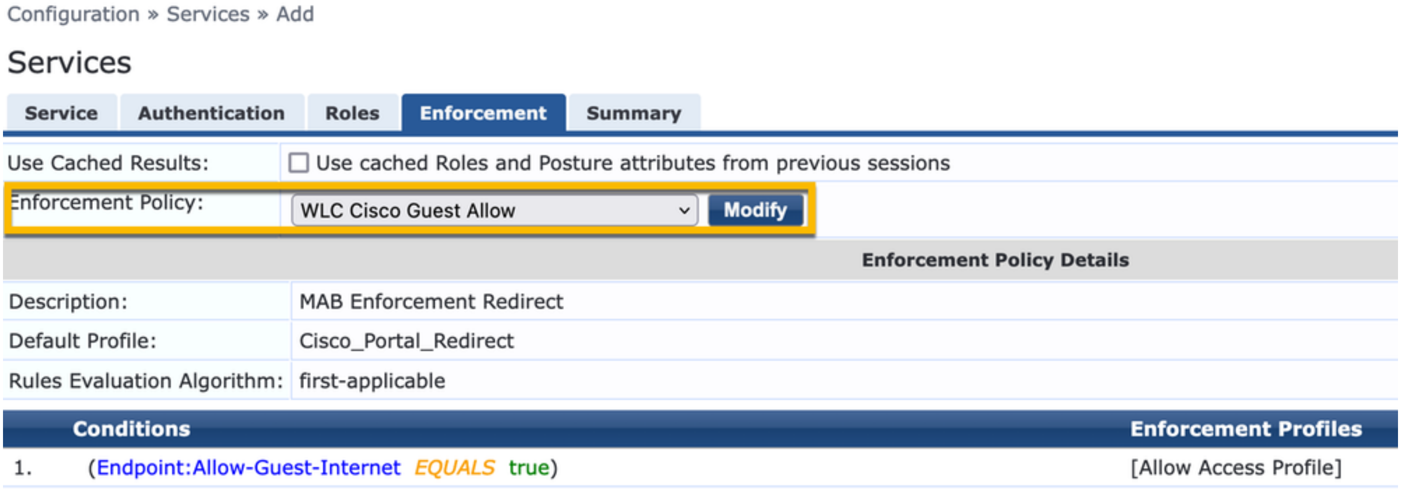
Configuration » Services » Edit - GuestPortal - Mac Auth

Services - GuestPortal - Mac Auth

Authentication Methods:	[Allow All MAC AUTH] --Select to Add--
Authentication Sources:	[Endpoints Repository] [Local SQL DB] [Guest User Repository] [Local SQL DB] --Select to Add--
Strip Username Rules:	□ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

While in the same dialogue, choose the Enforcement Tab.

- Enforcement Policy: WLC Cisco Guest Allow



Configuration » Services » Add

Services

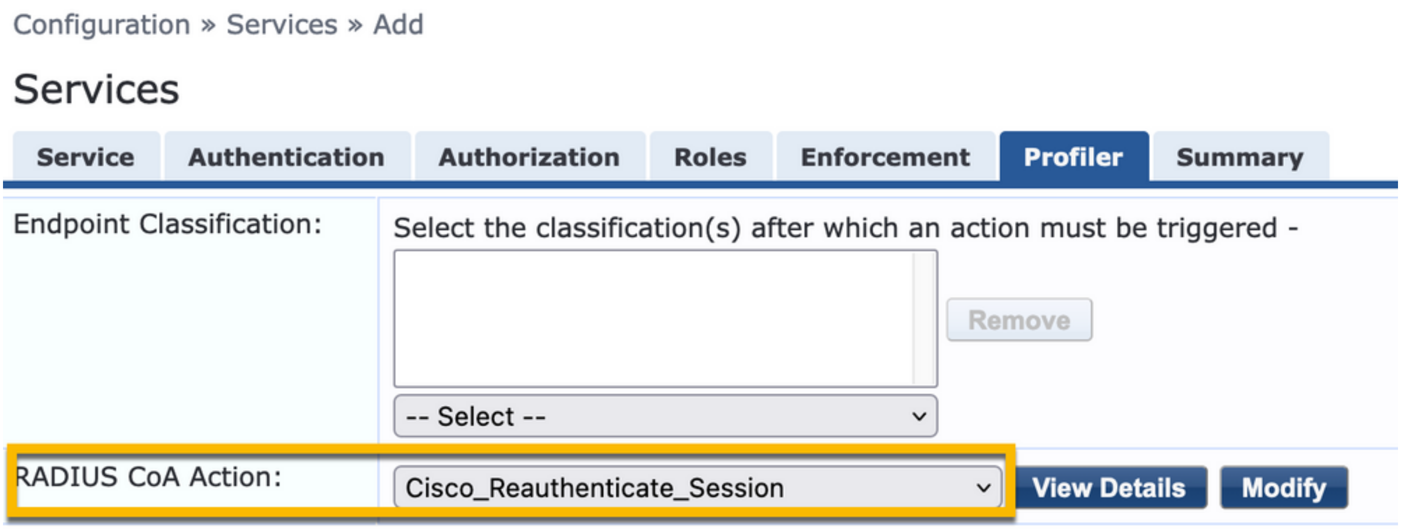
Use Cached Results:	□ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	WLC Cisco Guest Allow

Enforcement Policy Details

Description:	MAB Enforcement Redirect
Default Profile:	Cisco_Portal_Redirect
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Endpoint:Allow-Guest-Internet EQUALS true)	[Allow Access Profile]

While in the same dialogue, choose the Enforcement Tab.


Configuration » Services » Add

Services

Endpoint Classification: Select the classification(s) after which an action must be triggered -

-- Select --

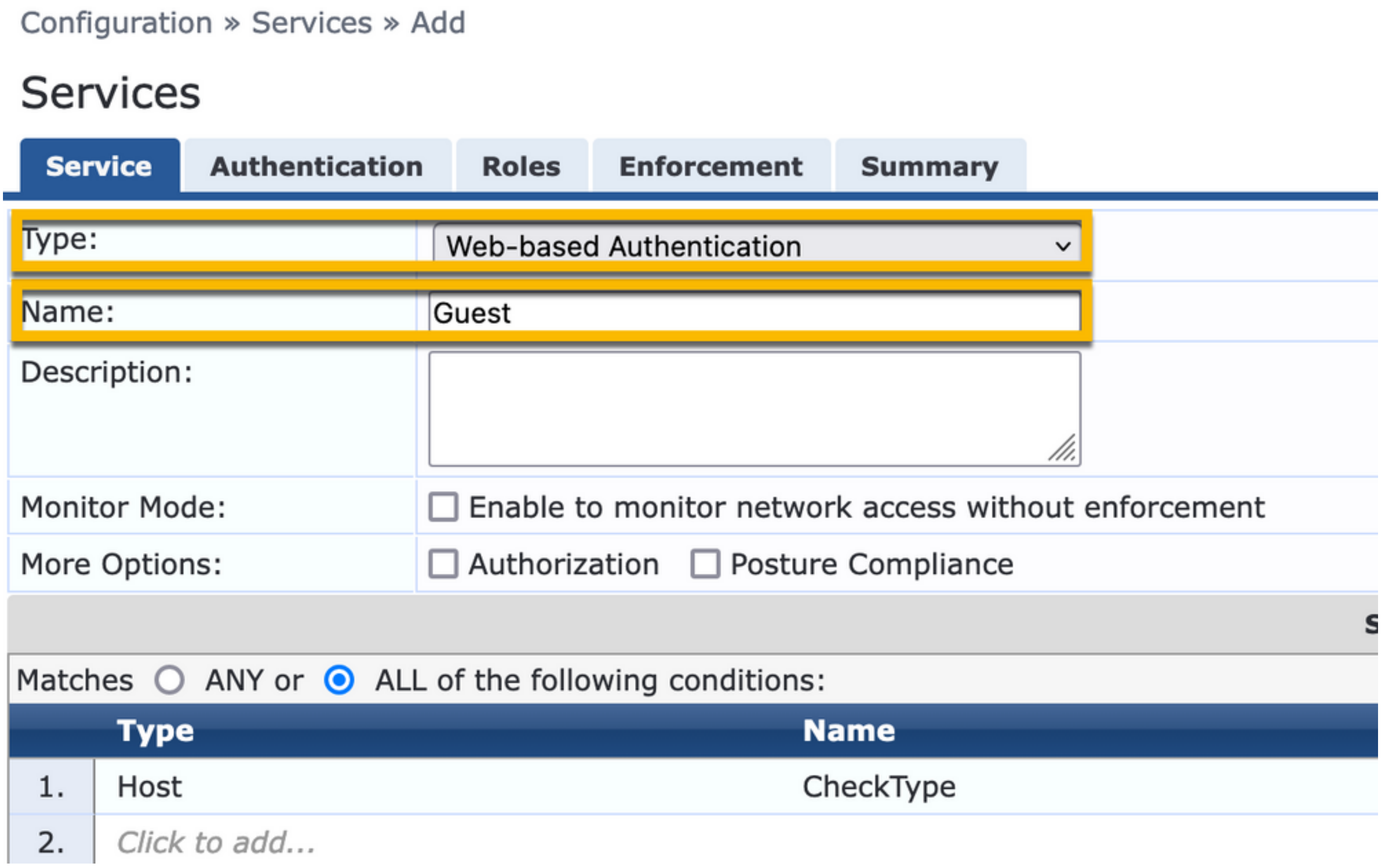
RADIUS CoA Action: Cisco_Reauthenticate_Session

ClearPass Webauth Service Configuration

Navigate to ClearPass > Enforcement > Policies > Add.

- Name: Guest_Portal_Webauth

- Type: Web-based Authentication


Configuration » Services » Add

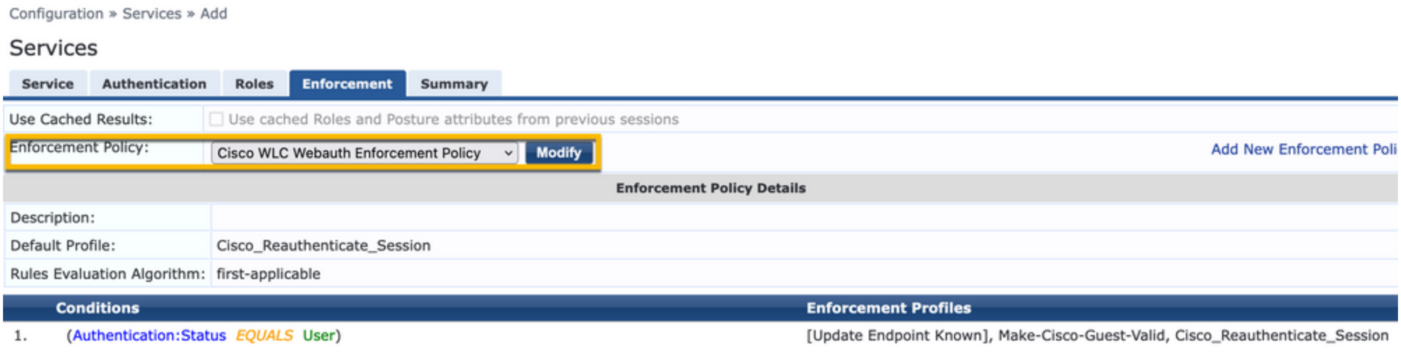
Services

Type:	Web-based Authentication
Name:	Guest
Description:	
Monitor Mode:	□ Enable to monitor network access without enforcement
More Options:	□ Authorization □ Posture Compliance

Matches ○ ANY or ● ALL of the following conditions:

	Type	Name
1.	Host	CheckType
2.	*Click to add...*	

While in the same dialogue, under the Enforcement tab, the Enforcement Policy: Cisco WLC Webauth Enforcement Policy.



Use Cached Results: □ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Cisco WLC Webauth Enforcement Policy

Enforcement Policy Details

Description:

Default Profile: Cisco_Reauthenticate_Session

Rules Evaluation Algorithm: first-applicable

	Conditions	Enforcement Profiles
1.	(Authentication:Status *EQUALS* User)	[Update Endpoint Known], Make-Cisco-Guest-Valid, Cisco_Reauthenticate_Session

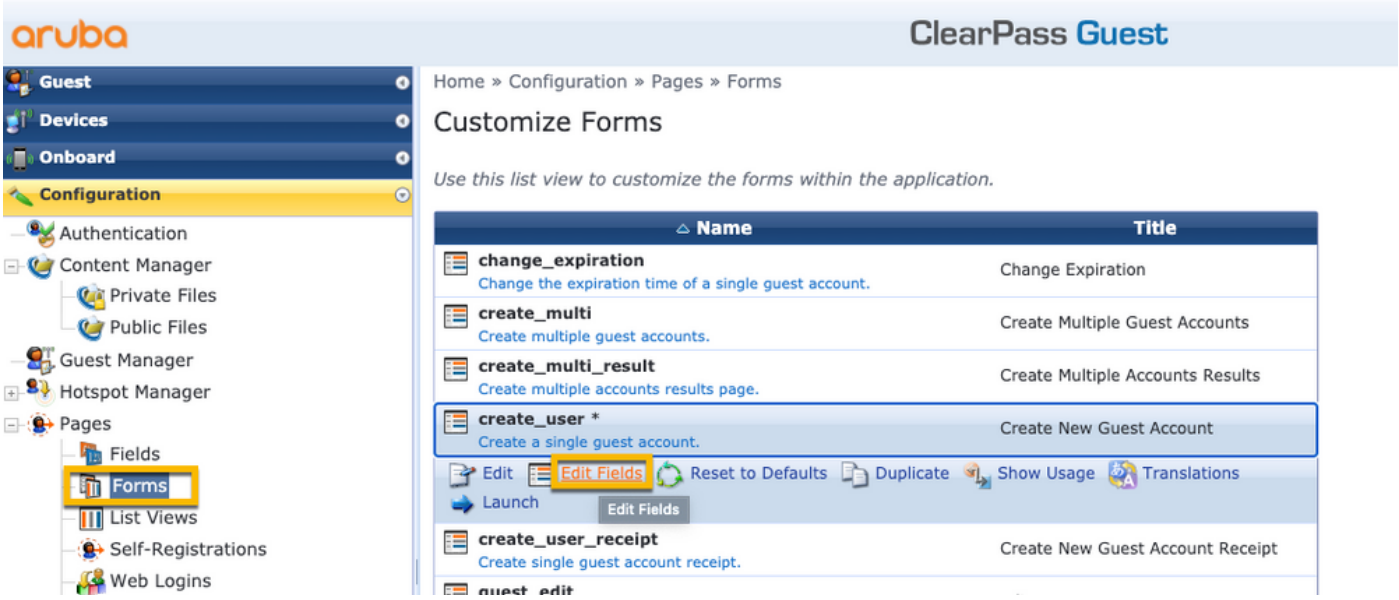
ClearPass - Web Login

For the Anonymous AUP Guest Portal page, use a single username with no password field.

The username that is used must have these fields defined/set:

username_auth | Username Authentication: | 1

In order to set the 'username_auth' field for a user, that field must be first exposed in the 'edit user' form. Navigate to ClearPass > Guest > Configuration > Pages > Forms, and choose create_user form.



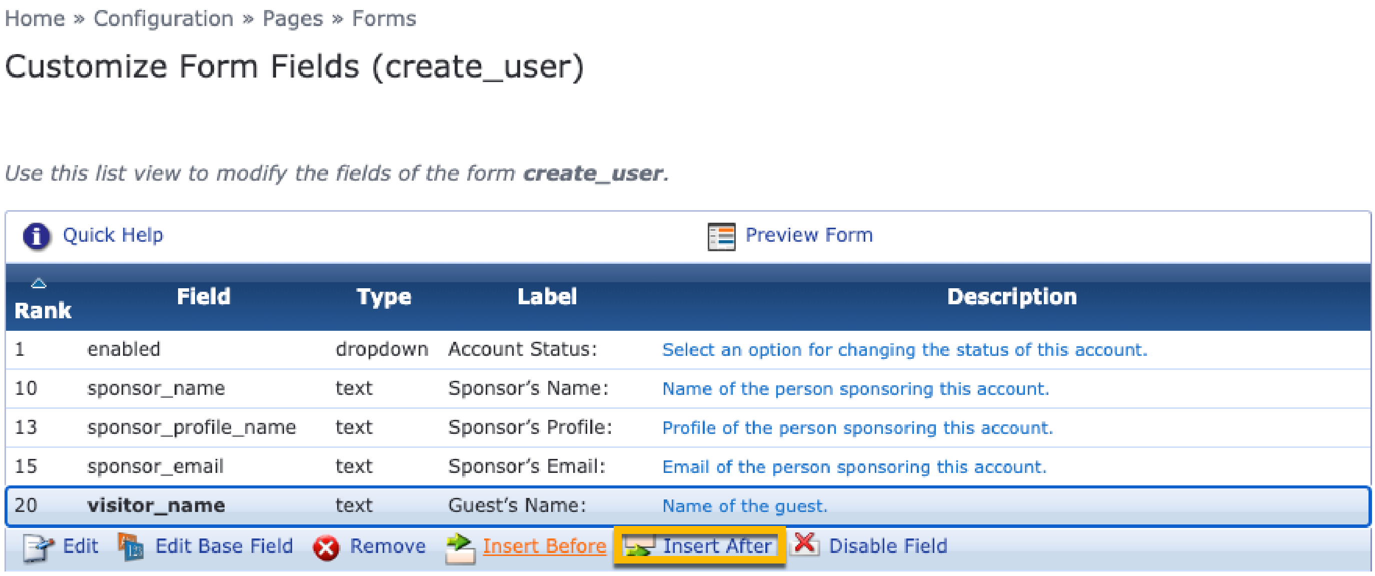
Home » Configuration » Pages » Forms

Customize Forms

Use this list view to customize the forms within the application.

Name	Title
change_expiration Change the expiration time of a single guest account.	Change Expiration
create_multi Create multiple guest accounts.	Create Multiple Guest Accounts
create_multi_result Create multiple accounts results page.	Create Multiple Accounts Results
create_user * Create a single guest account.	Create New Guest Account
create_user_receipt Create single guest account receipt.	Create New Guest Account Receipt
guest_edit	

Choose visitor_name (row 20), and click Insert After.

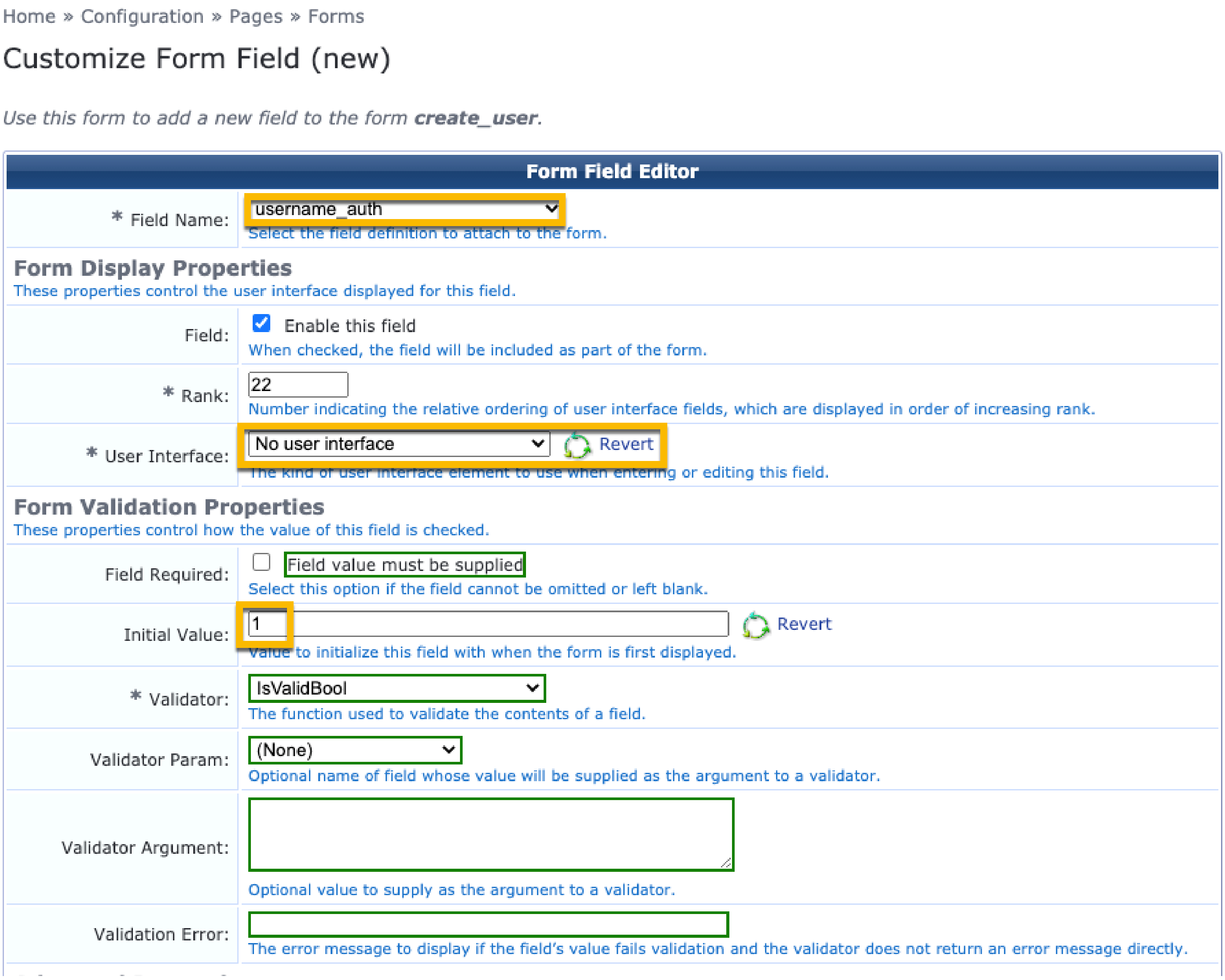


Home » Configuration » Pages » Forms

Customize Form Fields (create_user)

*Use this list view to modify the fields of the form **create_user**.*

Rank	Field	Type	Label	Description
1	enabled	dropdown	Account Status:	Select an option for changing the status of this account.
10	sponsor_name	text	Sponsor's Name:	Name of the person sponsoring this account.
13	sponsor_profile_name	text	Sponsor's Profile:	Profile of the person sponsoring this account.
15	sponsor_email	text	Sponsor's Email:	Email of the person sponsoring this account.
20	**visitor_name**	text	Guest's Name:	Name of the guest.



Home » Configuration » Pages » Forms

Customize Form Field (new)

*Use this form to add a new field to the form **create_user**.*

Form Field Editor

* Field Name: username_auth
Select the field definition to attach to the form.

Form Display Properties
These properties control the user interface displayed for this field.

Field: ☑ Enable this field
When checked, the field will be included as part of the form.

* Rank: 22
Number indicating the relative ordering of user interface fields, which are displayed in order of increasing rank.

* User Interface: No user interface — Revert
The kind of user interface element to use when entering or editing this field.

Form Validation Properties
These properties control how the value of this field is checked.

Field Required: ☐ Field value must be supplied
Select this option if the field cannot be omitted or left blank.

Initial Value: 1 — Revert
Value to initialize this field with when the form is first displayed.

* Validator: IsValidBool
The function used to validate the contents of a field.

Validator Param: (None)
Optional name of field whose value will be supplied as the argument to a validator.

Validator Argument:
Optional value to supply as the argument to a validator.

Validation Error:
The error message to display if the field's value fails validation and the validator does not return an error message directly.

Now create the username in order to use behind the AUP Guest Portal page.

Navigate to CPPM > Guest > Guest > Manage Accounts > Create.

- Guest Name: GuestWiFi

- Company Name: Cisco

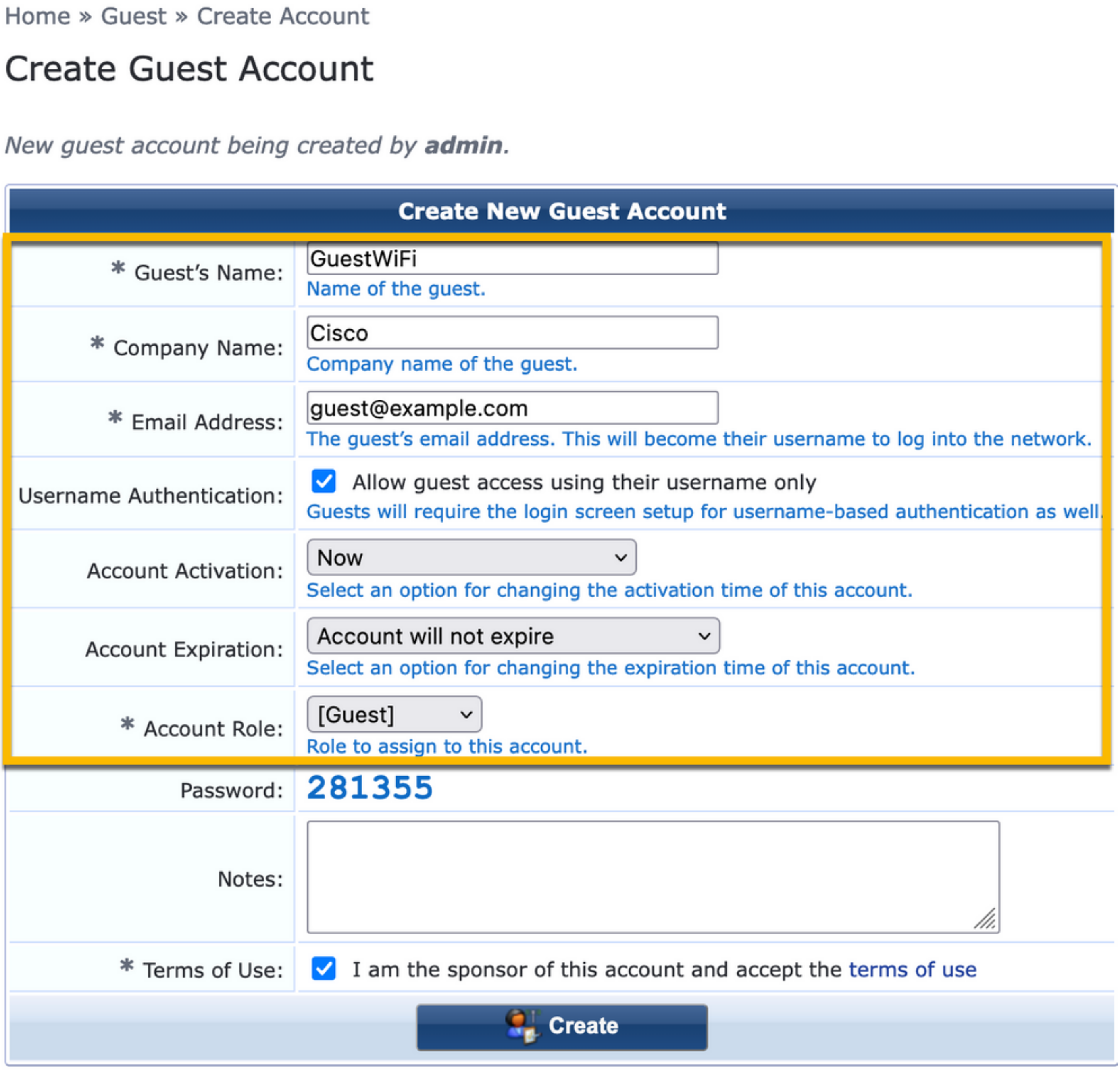
- Email Address: guest@example.com

- Username Authentication: Allow guest access with the use of their username only: Enabled

- Account Activation: Now

- Account Expiration: The account does not expire

- Terms of Use: I am the sponsor: Enabled



Home » Guest » Create Account

Create Guest Account

*New guest account being created by **admin**.*

Create New Guest Account

* Guest's Name:	GuestWiFi Name of the guest.
* Company Name:	Cisco Company name of the guest.
* Email Address:	guest@example.com The guest's email address. This will become their username to log into the network.
Username Authentication:	☑ Allow guest access using their username only Guests will require the login screen setup for username-based authentication as well.
Account Activation:	Now Select an option for changing the activation time of this account.
Account Expiration:	Account will not expire Select an option for changing the expiration time of this account.
* Account Role:	[Guest] Role to assign to this account.
Password:	281355
Notes:	
* Terms of Use:	☑ I am the sponsor of this account and accept the terms of use

Create a Web Login Form. Navigate to CPPM > Guest > Configuration > Web Logins.

Name: Lab Anonymous Guest Portal
Page Name: iaccept
Vendor Settings: Aruba Networks

Login Method: Server-initiated - Change of authorization (RFC 3576) sent to the controller
Authentication: Anonymous - Does not require a username or password
Anonymous User: GuestWifi
Terms: require a Terms and Conditions confirmation
Log In Label: accept and connect
Default URL: www.example.com
Login Delay: 6
Update Endpoint: Mark the MAC address of the user as a known endpoint
Advanced: Customize attributes stored with the endpoint, the Endpoint Attributes in the post-auth section:

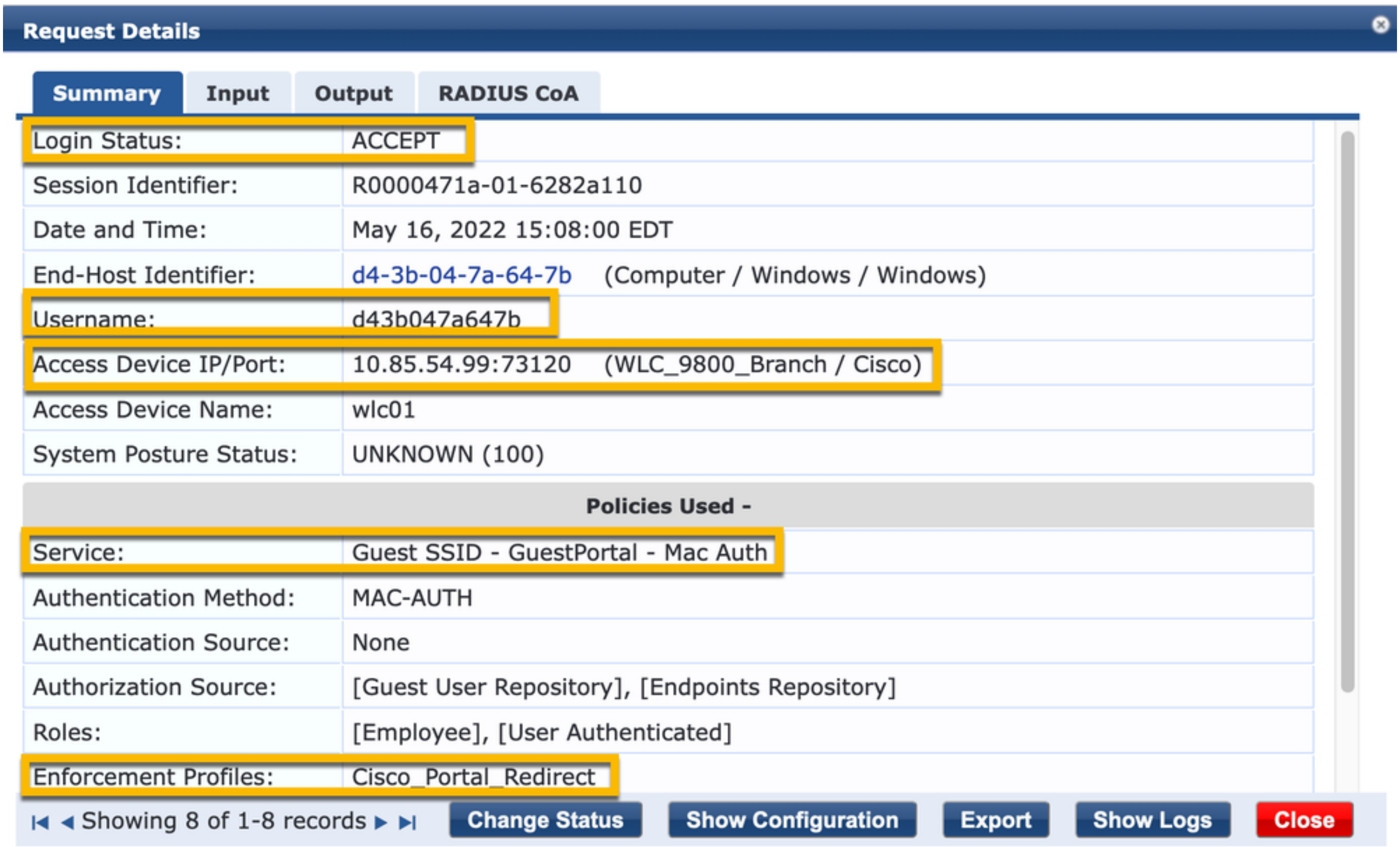
username | Username
visitor_name | Visitor Name
cn | Visitor Name
visitor_phone | Visitor Phone
email | Email
mail | Email
sponsor_name | Sponsor Name
sponsor_email | Sponsor Email
Allow-Guest-Internet | true

Verification - Guest CWA Authorization

In the CPPM, navigate to Live Monitoring > Access Tracker.

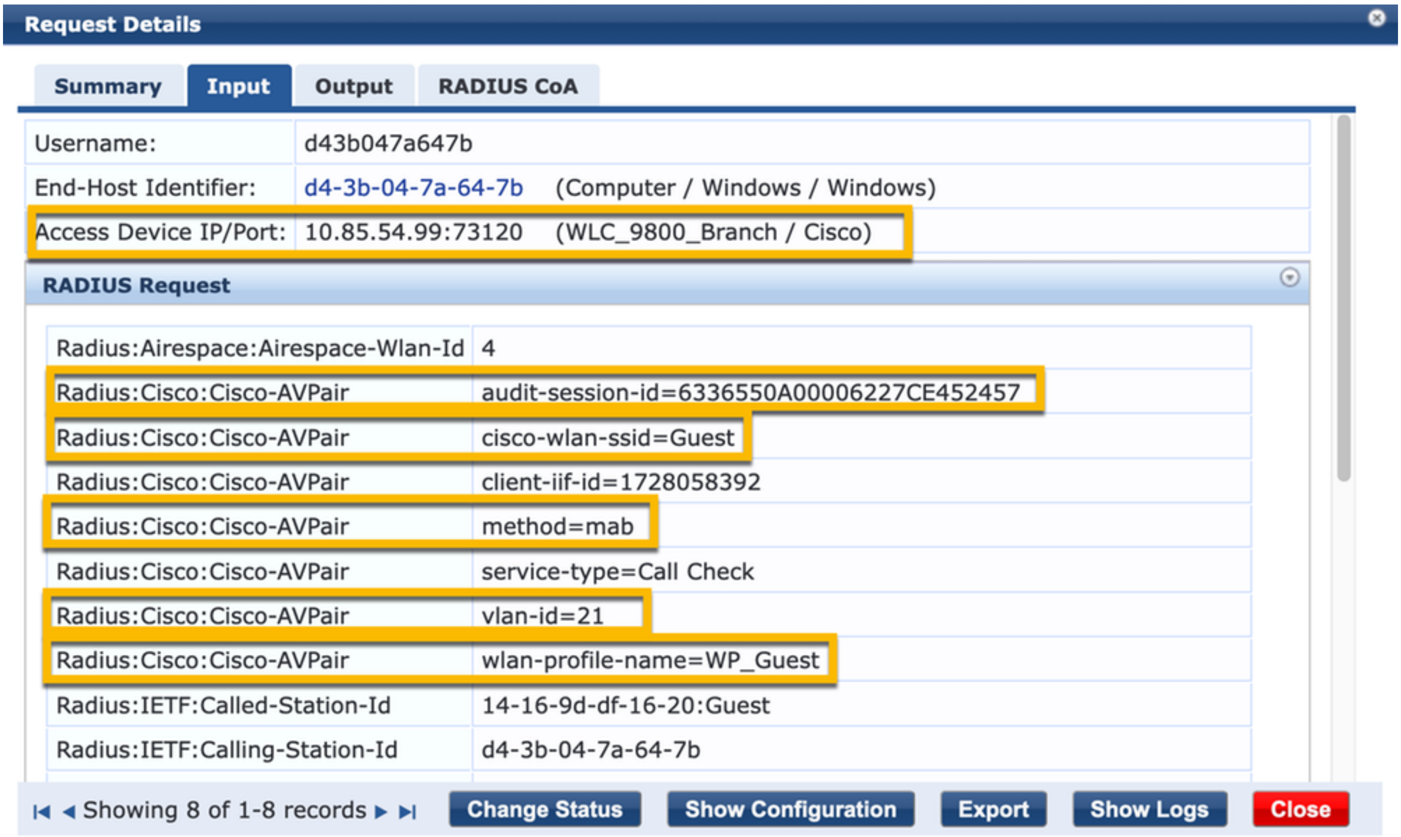
The New Guest user connects and triggers MAB Service.

Summary Tab:



Login Status:	ACCEPT
Session Identifier:	R0000471a-01-6282a110
Date and Time:	May 16, 2022 15:08:00 EDT
End-Host Identifier:	d4-3b-04-7a-64-7b (Computer / Windows / Windows)
Username:	d43b047a647b
Access Device IP/Port:	10.85.54.99:73120 (WLC_9800_Branch / Cisco)
Access Device Name:	wlc01
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	Guest SSID - GuestPortal - Mac Auth
Authentication Method:	MAC-AUTH
Authentication Source:	None
Authorization Source:	[Guest User Repository], [Endpoints Repository]
Roles:	[Employee], [User Authenticated]
Enforcement Profiles:	Cisco_Portal_Redirect

In the same dialogue, navigate to the Input Tab.

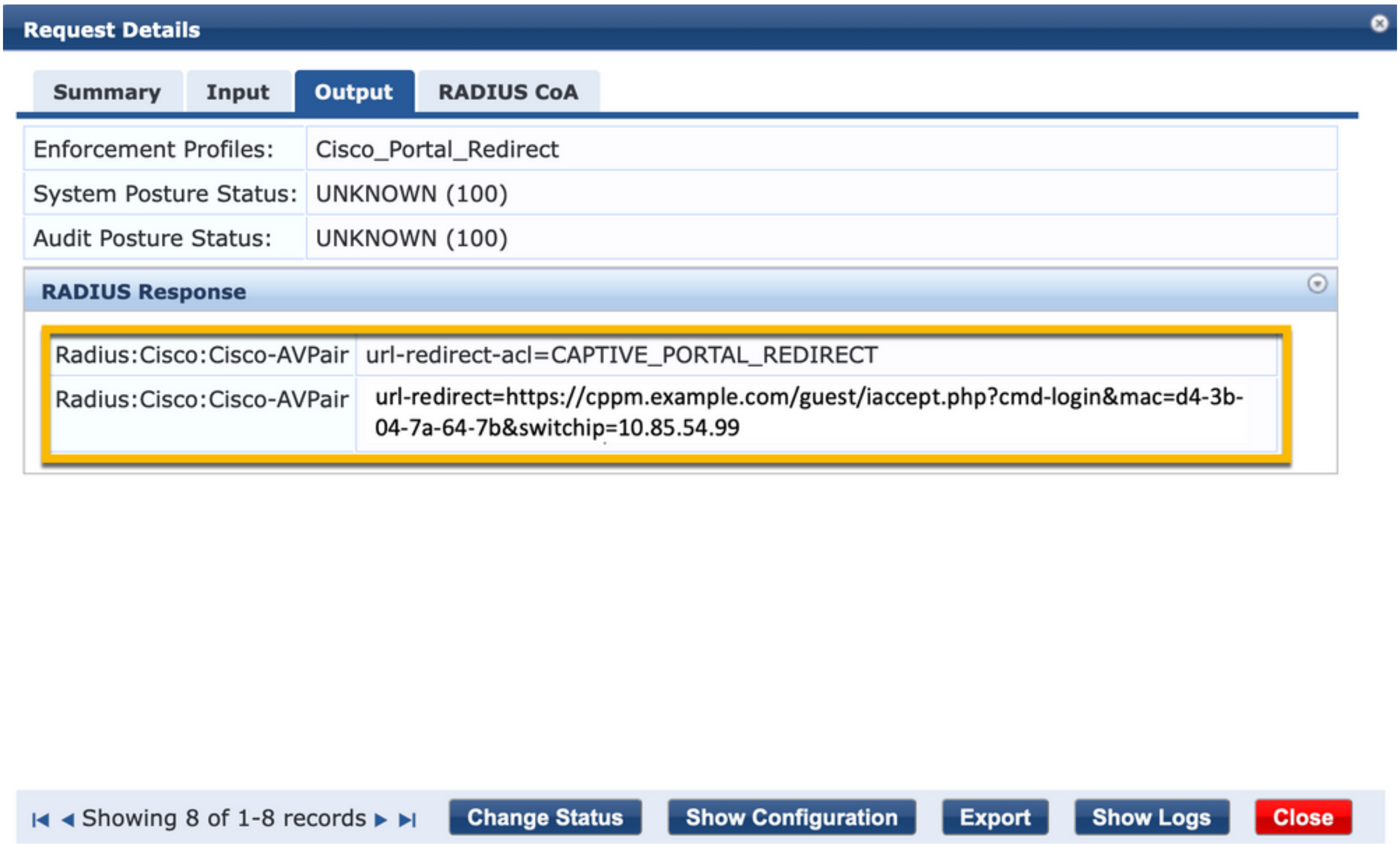


Username:	d43b047a647b
End-Host Identifier:	d4-3b-04-7a-64-7b (Computer / Windows / Windows)
Access Device IP/Port:	10.85.54.99:73120 (WLC_9800_Branch / Cisco)

RADIUS Request

Radius:Airespace:Airespace-Wlan-Id	4
Radius:Cisco:Cisco-AVPair	audit-session-id=6336550A00006227CE452457
Radius:Cisco:Cisco-AVPair	cisco-wlan-ssid=Guest
Radius:Cisco:Cisco-AVPair	client-iif-id=1728058392
Radius:Cisco:Cisco-AVPair	method=mab
Radius:Cisco:Cisco-AVPair	service-type=Call Check
Radius:Cisco:Cisco-AVPair	vlan-id=21
Radius:Cisco:Cisco-AVPair	wlan-profile-name=WP_Guest
Radius:IETF:Called-Station-Id	14-16-9d-df-16-20:Guest
Radius:IETF:Calling-Station-Id	d4-3b-04-7a-64-7b

In the same dialogue, navigate to the Output Tab.



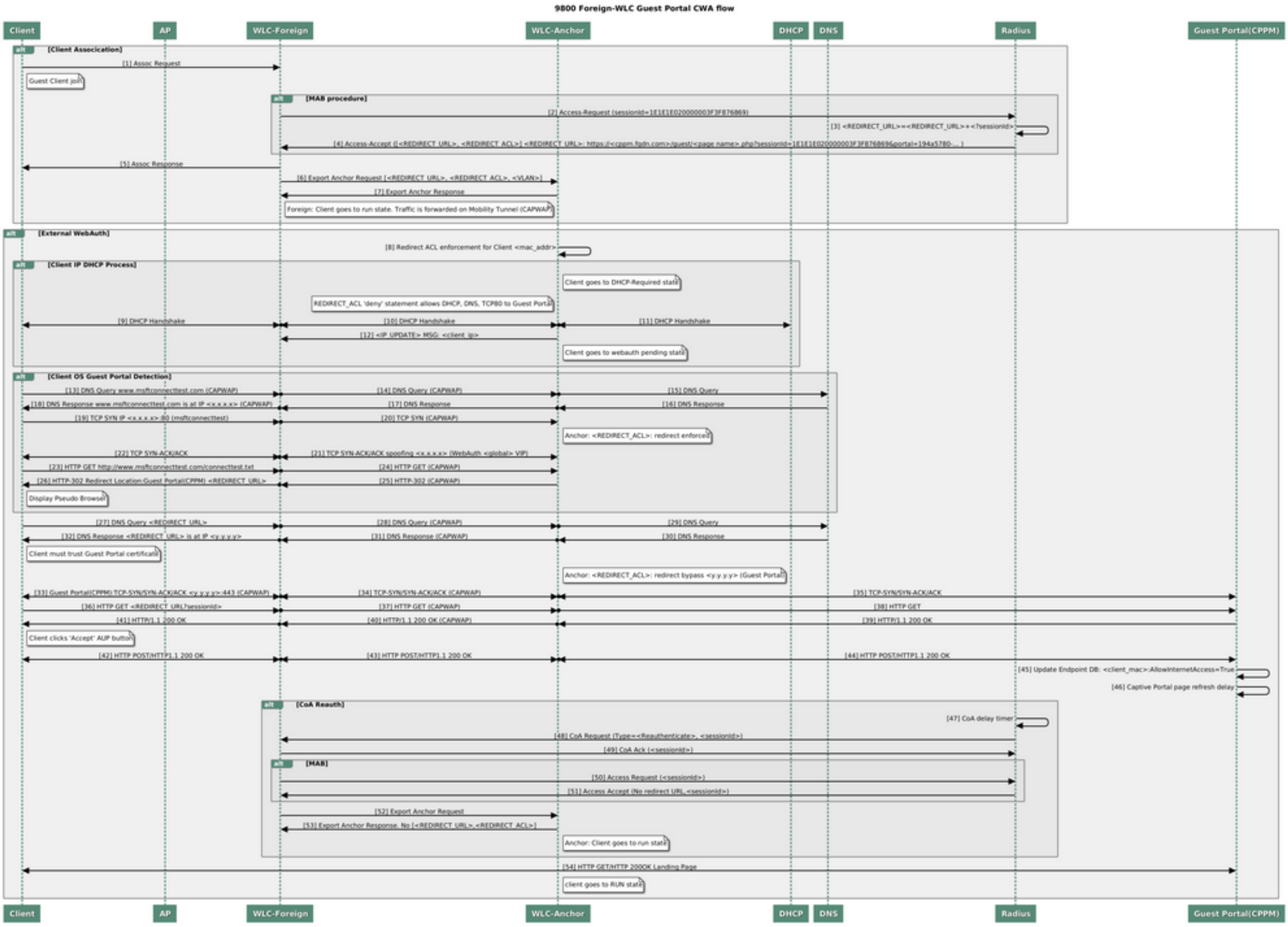
Enforcement Profiles:	Cisco_Portal_Redirect
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:Cisco:Cisco-AVPair	url-redirect-acl=CAPTIVE_PORTAL_REDIRECT
Radius:Cisco:Cisco-AVPair	url-redirect=https://cppm.example.com/guest/iaccept.php?cmd-login&mac=d4-3b-04-7a-64-7b&switchip=10.85.54.99

Appendix

For reference purposes, a state flow diagram is presented here for Cisco 9800 Foreign, Anchor controller interactions with RADIUS Server and externally hosted Guest Portal.


9800 Foreign-WLC Guest Portal CWA flow
Client
AP
WLC-Foreign
WLC-Anchor
DHCP
DNS
Radius
Guest Portal(CPPM)
alt [Client Assocication]
[1] Assoc Request
Guest Client join
alt [MAB procedure]
[2] Access-Request (sessionId=1E1E1E020000003F3F876869)
[3] <REDIRECT_URL>=<REDIRECT_URL>+<?sessionId>
[4] Access-Accept ([<REDIRECT_URL>, <REDIRECT_ACL>] <REDIRECT_URL>: https://<cppm.fqdn.com>/guest/<page name>.php?sessionId=1E1E1E020000003F3F876869&portal=194a5780-...)
[5] Assoc Response
[6] Export Anchor Request [<REDIRECT_URL>, <REDIRECT_ACL>, <VLAN>]
[7] Export Anchor Response
Foreign: Client goes to run state. Traffic is forwarded on Mobility Tunnel (CAPWAP)
alt [External WebAuth]
[8] Redirect ACL enforcement for Client <mac_addr>
alt [Client IP DHCP Process]
Client goes to DHCP-Required state
REDIRECT_ACL 'deny' statement allows DHCP, DNS, TCP80 to Guest Portal
[9] DHCP Handshake
[10] DHCP Handshake
[11] DHCP Handshake
[12] <IP_UPDATE> MSG: <client_ip>
Client goes to webauth pending state
alt [Client OS Guest Portal Detection]
[13] DNS Query www.msftconnecttest.com (CAPWAP)
[14] DNS Query (CAPWAP)
[15] DNS Query
[16] DNS Response
[17] DNS Response
[18] DNS Response www.msftconnecttest.com is at IP <x.x.x.x> (CAPWAP)
[19] TCP SYN IP <x.x.x.x>:80 (msftconnecttest)
[20] TCP SYN (CAPWAP)
Anchor: <REDIRECT_ACL>: redirect enforced
[21] TCP SYN-ACK/ACK spoofing <x.x.x.x> (WebAuth <global> VIP)
[22] TCP SYN-ACK/ACK
[23] HTTP GET http://www.msftconnecttest.com/connecttest.txt
[24] HTTP GET (CAPWAP)
[25] HTTP-302 (CAPWAP)
[26] HTTP-302 Redirect Location:Guest Portal(CPPM) <REDIRECT_URL>
Display Pseudo Browser
[27] DNS Query <REDIRECT_URL>
[28] DNS Query (CAPWAP)
[29] DNS Query
[30] DNS Response
[31] DNS Response (CAPWAP)
[32] DNS Response <REDIRECT_URL> is at IP <y.y.y.y>
Client must trust Guest Portal certificate
Anchor: <REDIRECT_ACL>: redirect bypass <y.y.y.y> (Guest Portal)
[33] Guest Portal(CPPM):TCP-SYN/SYN-ACK/ACK <y.y.y.y>:443 (CAPWAP)
[34] TCP-SYN/SYN-ACK/ACK (CAPWAP)
[35] TCP-SYN/SYN-ACK/ACK
[36] HTTP GET <REDIRECT_URL?sessionId>
[37] HTTP GET (CAPWAP)
[38] HTTP GET
[39] HTTP/1.1 200 OK
[40] HTTP/1.1 200 OK (CAPWAP)
[41] HTTP/1.1 200 OK
Client clicks 'Accept' AUP button
[42] HTTP POST/HTTP1.1 200 OK
[43] HTTP POST/HTTP1.1 200 OK
[44] HTTP POST/HTTP1.1 200 OK
[45] Update Endpoint DB: <client_mac>:AllowInternetAccess=True
[46] Captive Portal page refresh delay
alt [CoA Reauth]
[47] CoA delay timer
[48] CoA Request (Type=<Reauthenticate>, <sessionId>)
[49] CoA Ack (<sessionId>)
alt [MAB]
[50] Access Request (<sessionId>)
[51] Access Accept (No redirect URL, <sessionId>)
[52] Export Anchor Request
[53] Export Anchor Response, No [<REDIRECT_URL>,<REDIRECT_ACL>]
Anchor: Client goes to run state
[54] HTTP GET/HTTP 200OK Landing Page
client goes to RUN state
Client
AP
WLC-Foreign
WLC-Anchor
DHCP
DNS
Radius
Guest Portal(CPPM)

Guest Central Web Authentication State Diagram with Anchor WLC

Related Information

It is important to note that the 9800 WLC does not reliably use the same UDP source port for a given wireless client RADIUS transaction. This is something ClearPass can be sensitive to. It is also important to base any RADIUS load balancing on the client calling-station-id and not try to rely on UDP source port from the WLC side.

- Cisco 9800 Deployment Best Practices Guide
- Understand Catalyst 9800 Wireless Controllers Configuration Model
- Understand FlexConnect on Catalyst 9800 Wireless Controller

- Technical Support & Documentation - Cisco Systems