Configure 9800 WLC Integration with Aruba ClearPass - Dot1x & FlexConnect for Branches Deployment

Contents

Introduction

This document describes the integration of the Catalyst 9800 Wireless Controller with Aruba ClearPass Policy Manager.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics and that they have been configured and verified:

- Catalyst 9800 Wireless Controller
- Aruba ClearPass Server (Requires Platform License, Access License, Onboard License)
- Operational Windows AD
- Optional Certificate Authority (CA)
- Operational DHCP Server
- Operational DNS Server (required for Certificate CRL validation)
- ESXi
- All pertinent components are synced to NTP and verified to have the correct time (required for certificate validation)
- Knowledge of topics:
  - C9800 deployment and New Config Model
  - FlexConnect operation on C9800
  - Dot1x Authentication

Components Used

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

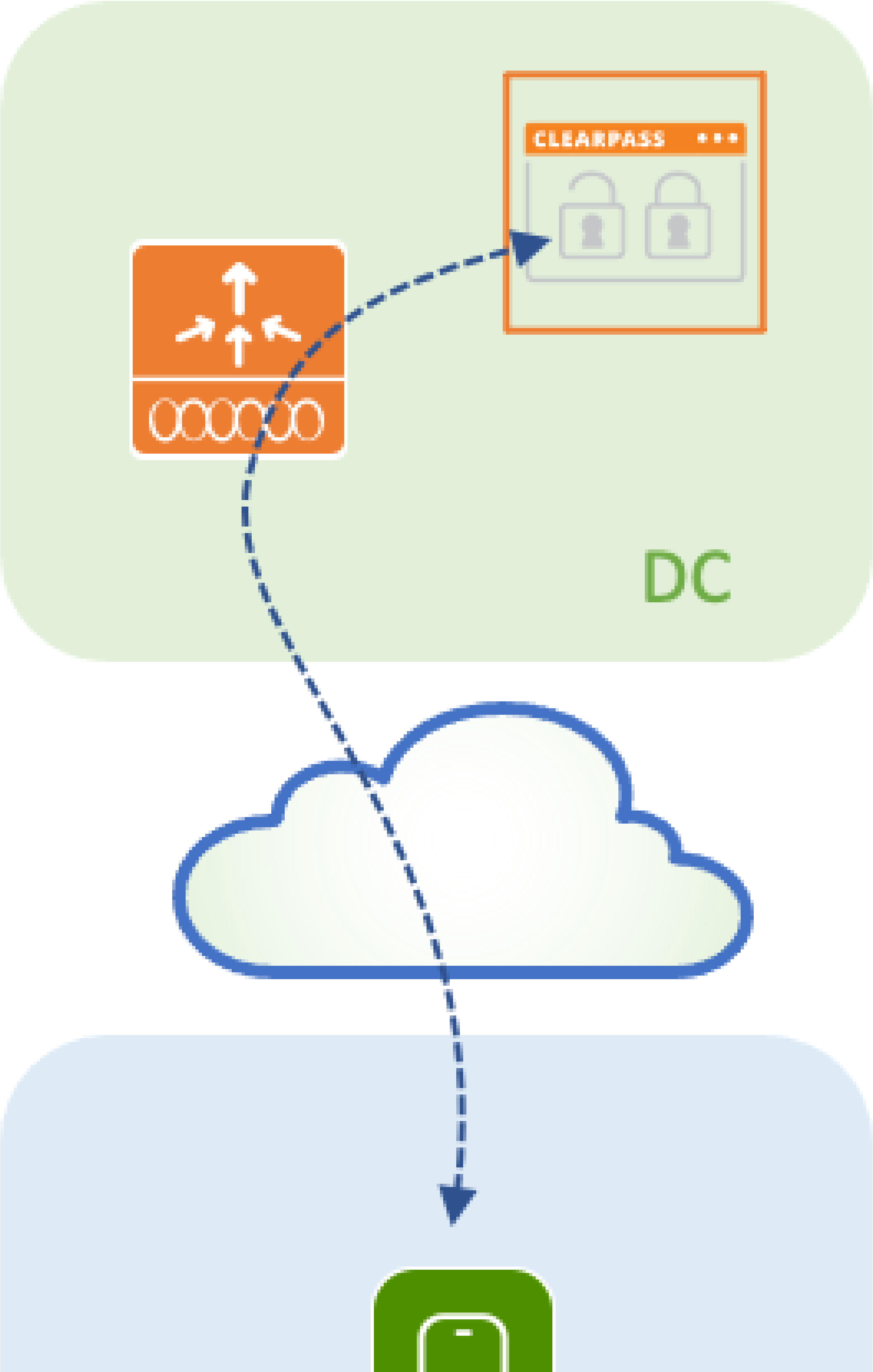
- C9800-L-C Cisco IOS-XE 17.3.3
- C9130AX, 4800 APs
- Aruba ClearPass, 6-8-0-109592 and 6.8-3 patch
- MS Windows Server
  - Active Directory (GP configured for automated machine-based cert issuance to managed endpoints)
  - DHCP Server with option 43 and option 60
  - DNS Server
  - NTP Server to time-sync all the components
  - 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.

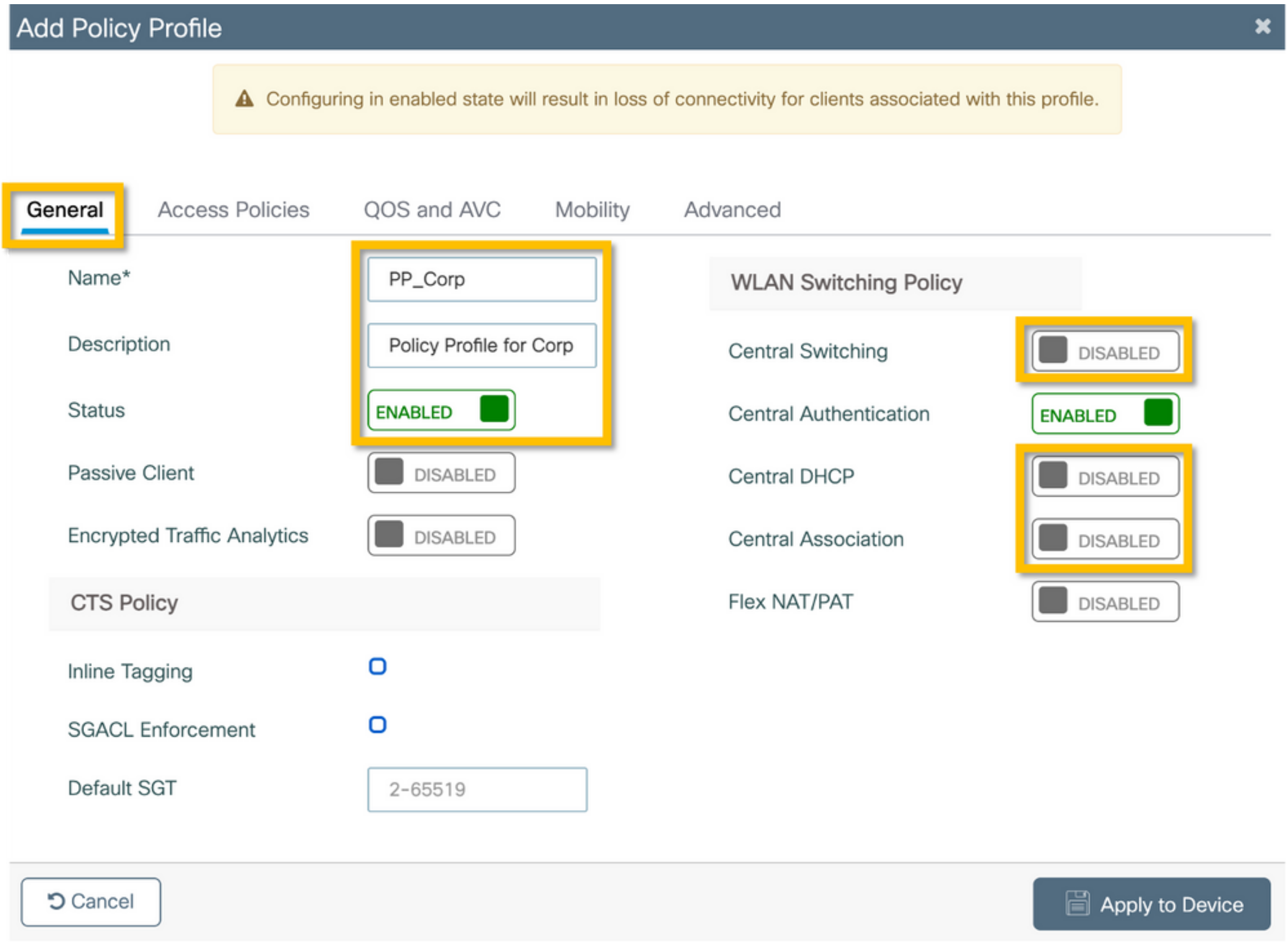
Background Information

Traffic Flow

In a typical enterprise deployment with multiple branch offices, each branch office is set up to provide dot1x access to the corporate employees. In this configuration example, PEAP is used to provide dot1x access to corporate users via a ClearPass instance deployed in the central data center (DC). Machine certificates are used in conjunction with verification of employee credentials against a Microsoft AD server.


CLEARPASS
DC

and enter a policy profile name and description. Enable the policy, and disable central switching, DHCP, and association, as the corporate user traffic is locally switched at the AP as shown in the image.



Add Policy Profile

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

Name* PP_Corp

Description Policy Profile for Corp

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

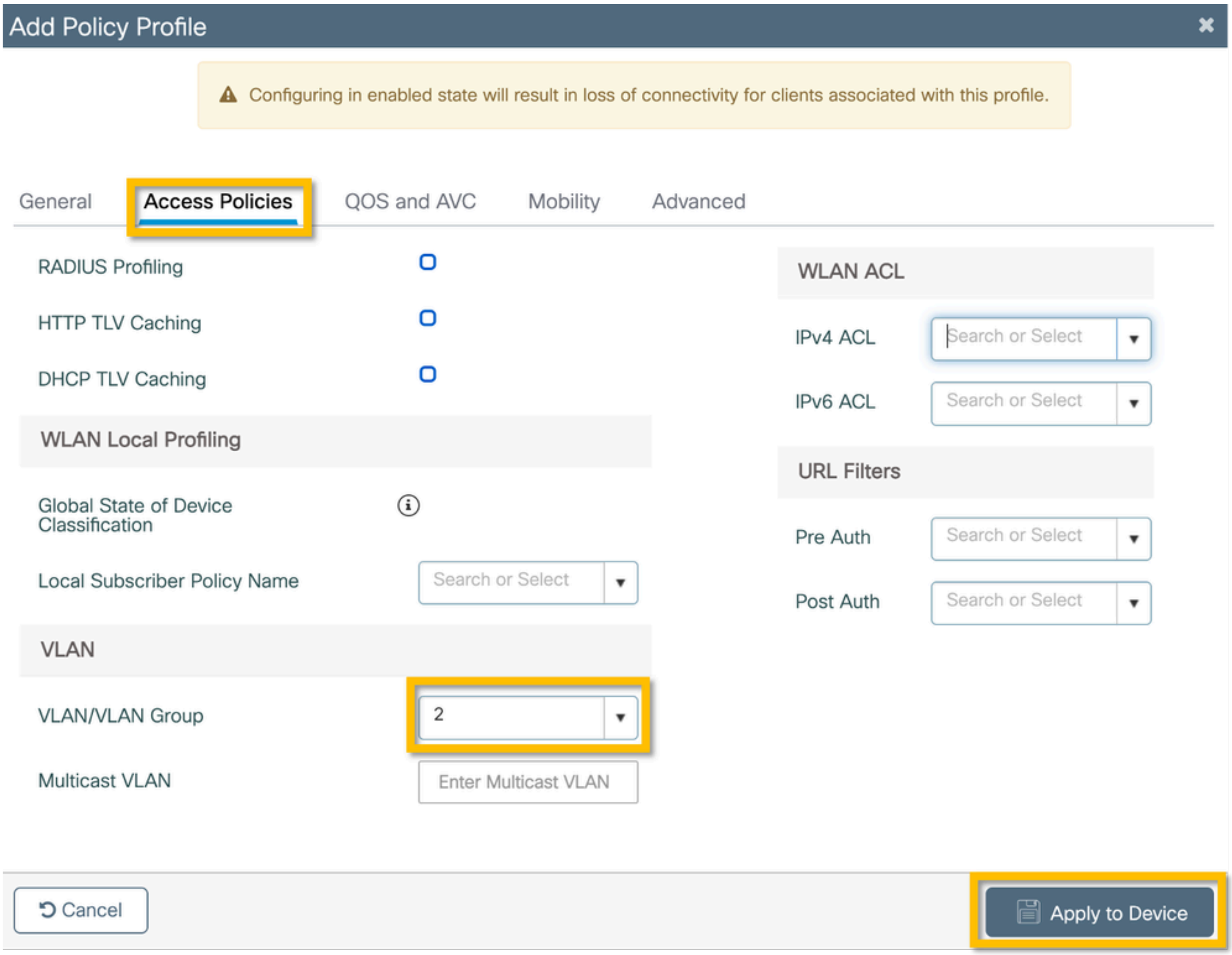
Central Authentication ENABLED

Central DHCP DISABLED

Central Association DISABLED

Flex NAT/PAT DISABLED

Step 2. Navigate to the **Access Policies** tab and manually enter the ID of the VLAN to be used at the branch for the corporate user traffic. This VLAN does not need to be configured on the C9800 itself. It must be configured in the Flex Profile, as detailed further. Do not select a VLAN name from the drop-down list (see Cisco bug ID CSCvn48234 for more information). Click on the **Apply to Device** button as shown in this image.


Add Policy 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: 2

Multicast VLAN: Enter Multicast VLAN

WLAN ACL

IPv4 ACL: Search or Select

IPv6 ACL: Search or Select

URL Filters

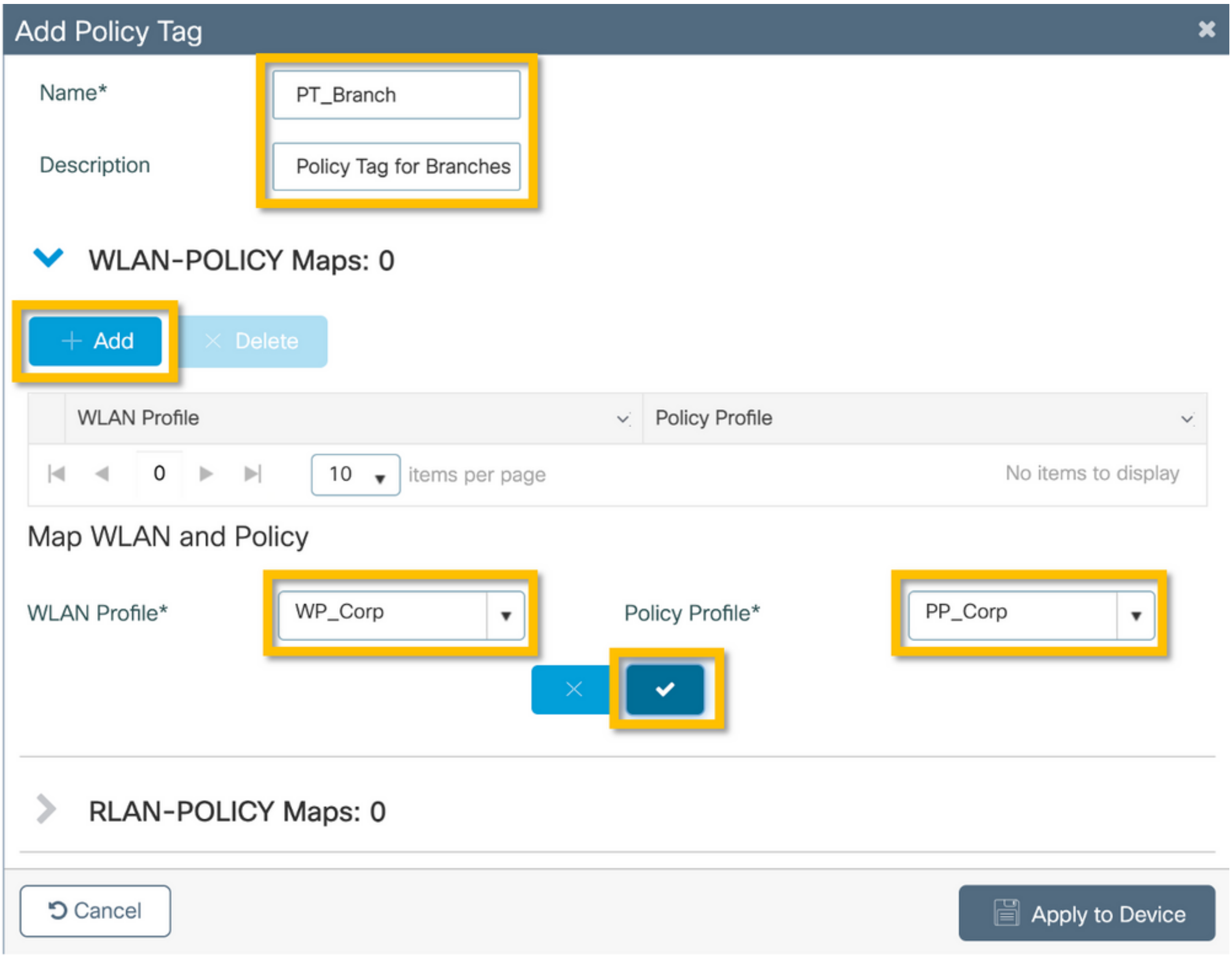
Pre Auth: Search or Select

Post Auth: Search or Select

C9800 - Configure Policy Tag

Once the WLAN Profile (WP_Corp) and Policy Profile (PP_Corp) are created, a Policy Tag must in turn be created to bind these WLAN and Policy Profiles together. This Policy Tag is applied to access points. Assign this Policy Tag to access points to trigger the configuration of these to enable the selected SSIDs on them.

Step 1. Navigate to **Configuration** > **Tags & Profiles** > **Tags**, select the **Policy** tab and click **+Add**. Enter the Policy Tag name and description. Click on **+Add** under **WLAN-POLICY Maps**. Select the WLAN Profile and Policy Profile created earlier, and then click on the checkmark button as shown in this image.



Add Policy Tag

Name* PT_Branch

Description Policy Tag for Branches

WLAN-POLICY Maps: 0

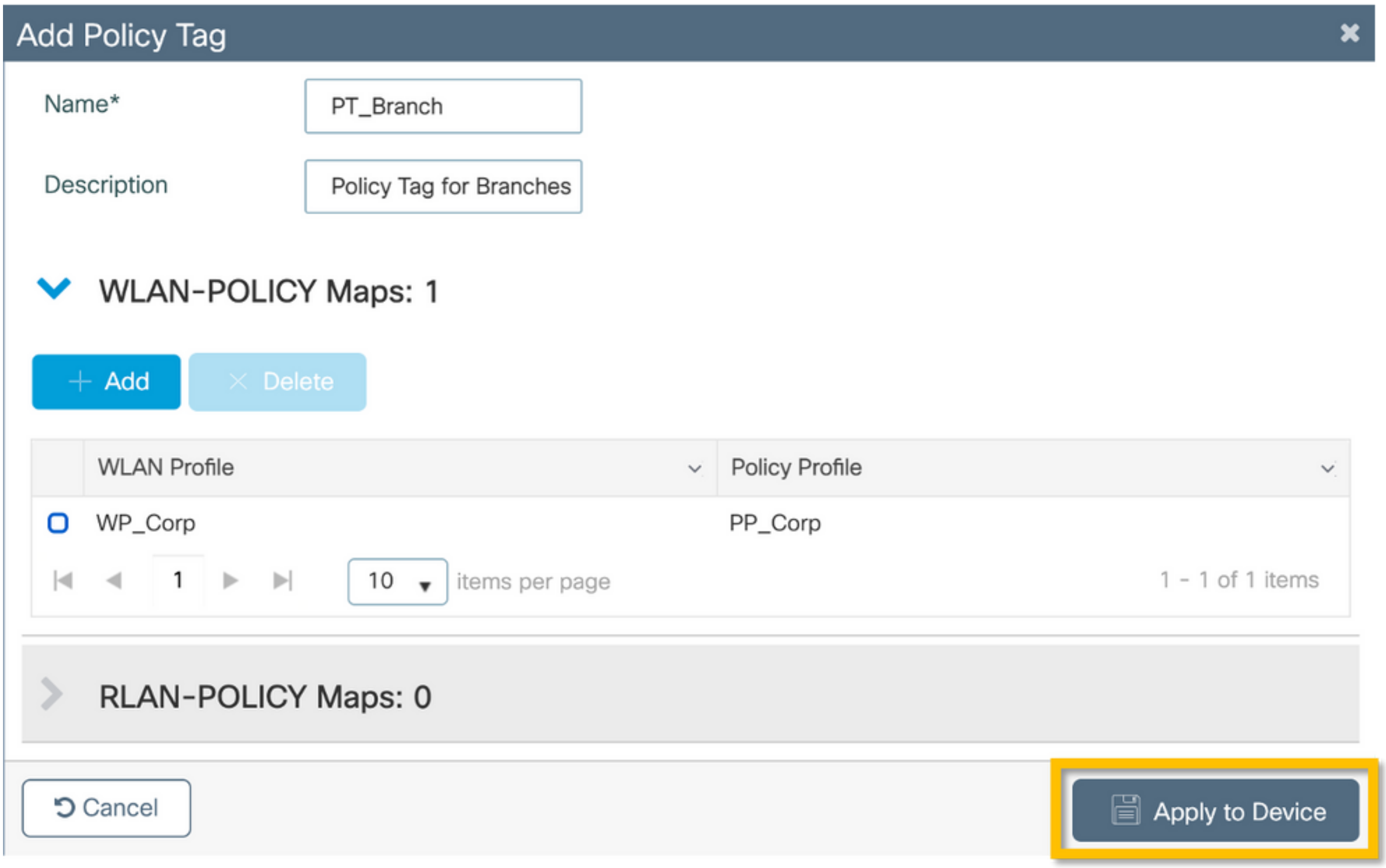
Map WLAN and Policy

WLAN Profile* WP_Corp

Policy Profile* PP_Corp

RLAN-POLICY Maps: 0

Step 2. Verify and click on the **Apply to Device** button as shown in this image.



Add Policy Tag

Name*: PT_Branch

Description: Policy Tag for Branches

WLAN-POLICY Maps: 1

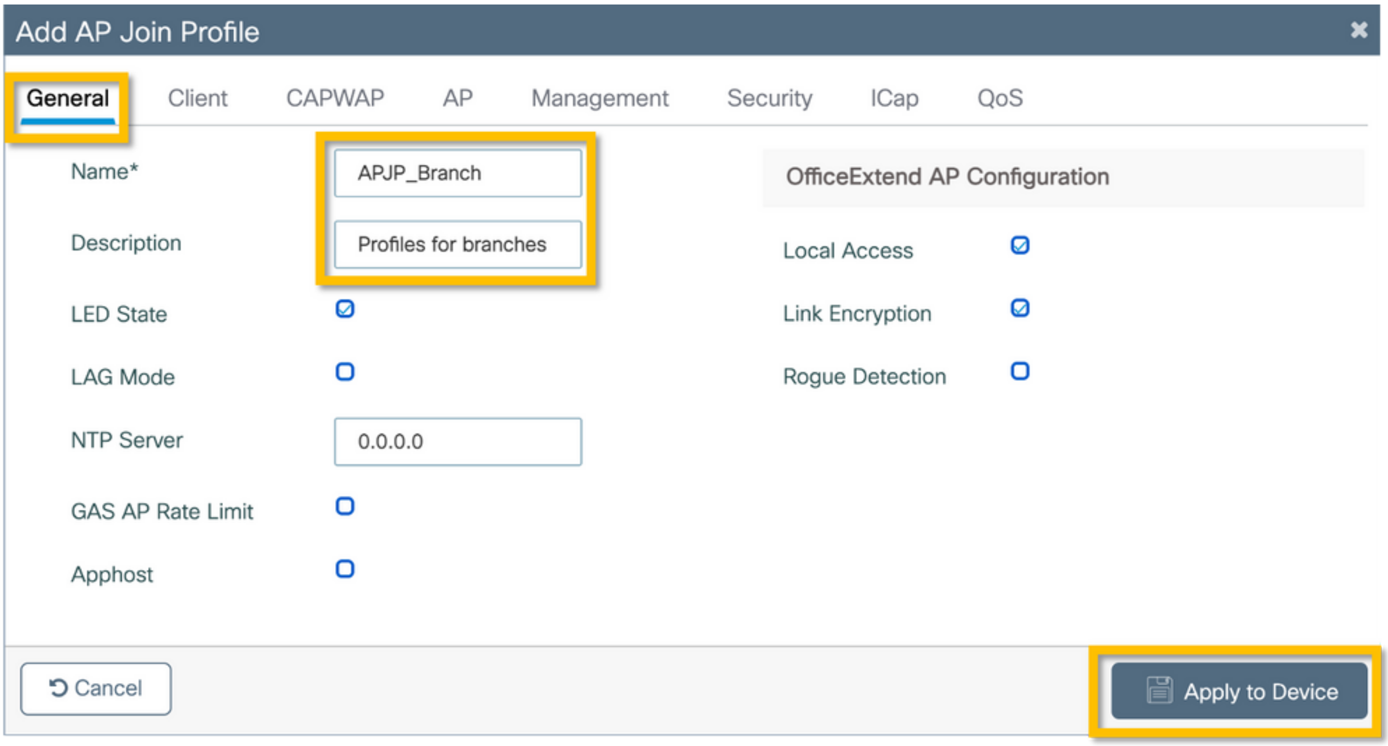
	WLAN Profile	Policy Profile
□	WP_Corp	PP_Corp

RLAN-POLICY Maps: 0

C9800 - AP Join Profile

AP Join Profiles and Flex Profiles need to be configured and assigned to access points with Site Tags. A different Site Tag must be used for each branch in order to support 802.11r Fast Transition (FT) within a branch, yet limit the distribution of the client PMK among the APs of that branch only. It is important not to re-use the same site tag across multiple branches. Configure an AP Join Profile. You can use a single AP Join Profile if all branches are similar, or create multiple profiles if some of the configured parameters must be different.

Step 1. Navigate to **Configuration** > **Tags & Profiles** > **AP Join** and click **+Add**. Enter the AP Join Profile name and description. Click on the **Apply to Device** button as shown in this image.



Name* APJP_Branch

Description Profiles for branches

LED State ☑

LAG Mode □

NTP Server 0.0.0.0

GAS AP Rate Limit □

Apphost □

OfficeExtend AP Configuration

Local Access ☑

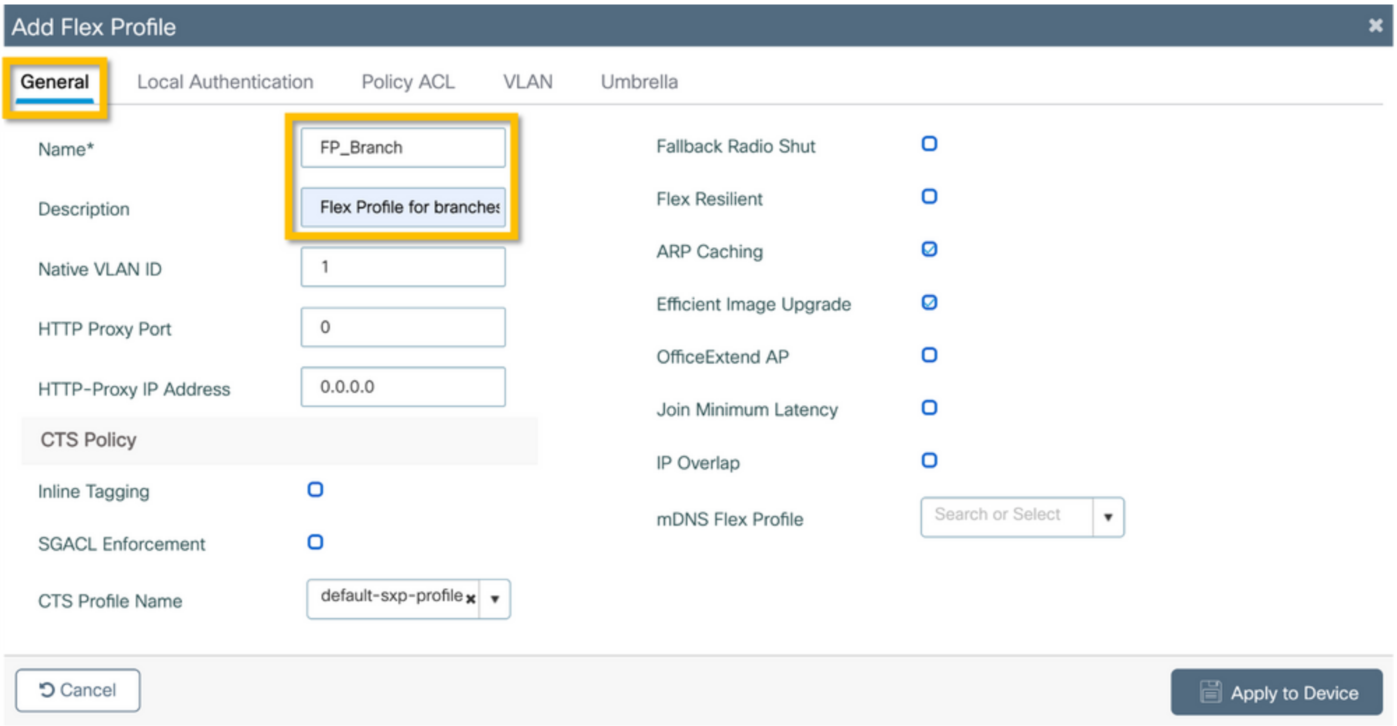
Link Encryption ☑

Rogue Detection □

C9800 - Flex Profile

Now configure a Flex Profile. Again, you can use a single profile for all branches if these are similar, and have the same VLAN/SSID mapping. Or, you can create multiple profiles if some of the configured parameters such as the VLAN assignments are different.

Step 1. Navigate to **Configuration** > **Tags & Profiles** > **Flex** and click **+Add**. Enter the Flex Profile name and description.



Name* FP_Branch

Description Flex Profile for branches

Native VLAN ID 1

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 ☑

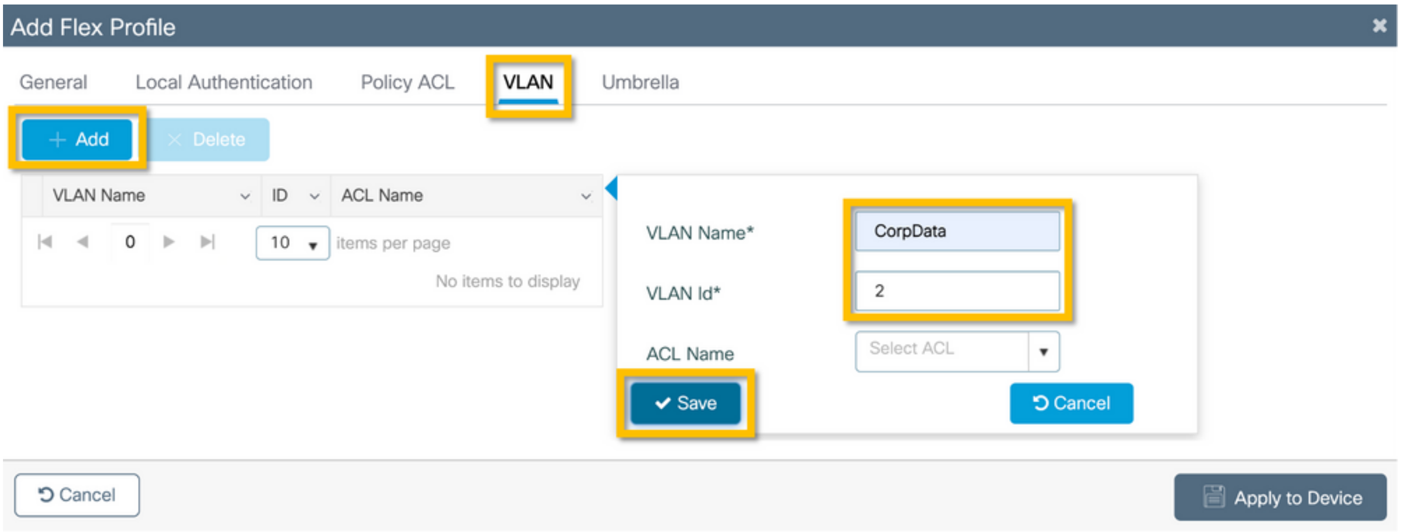
OfficeExtend AP □

Join Minimum Latency □

IP Overlap □

mDNS Flex Profile Search or Select

Step 2. Navigate to the **VLAN** tab and click **+Add**. Enter the VLAN name and ID of the local VLAN at the branch which the AP must use to locally switch the corporate user traffic. Click on the **Save** button as shown in this image.

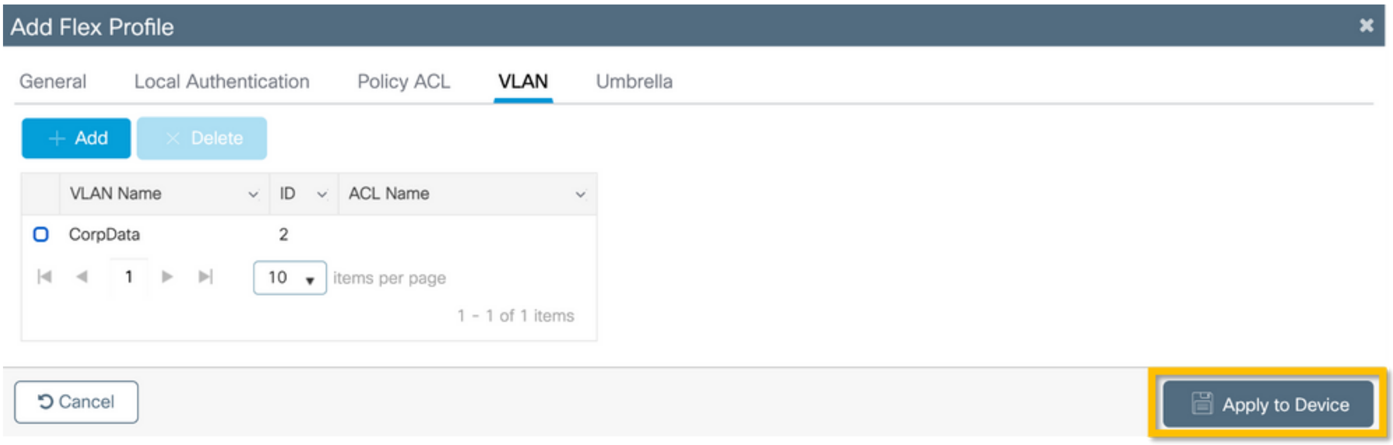


VLAN Name* CorpData

VLAN Id* 2

ACL Name Select ACL

Step 3. Verify and click on the **Apply to Device** button as shown in this image.

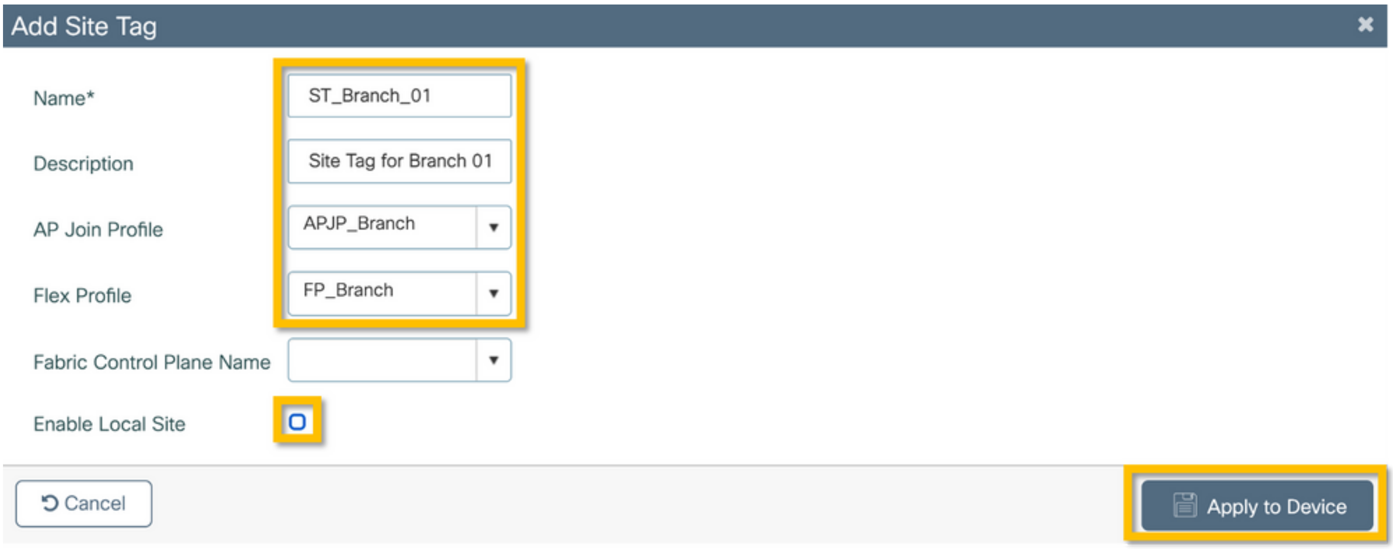


VLAN Name	ID	ACL Name
CorpData	2	

C9800 - Site Tag

Site Tags are used to assign Join Profiles and Flex Profiles to access points. As mentioned before, a different Site Tag must be used for each branch in order to support 802.11r Fast Transition (FT) within a branch, yet limit the distribution of the client PMK among the APs of that branch only. It is important not to re-use the same site tag across multiple branches.

Step 1. Navigate to **Configuration** > **Tags & Profiles** > **Tags**, select the **Site** tab and click **+Add**. Enter a Site Tag name and description, select the AP Join Profile created, uncheck the **Enable Local Site** box, and finally select the Flex Profile created previously. Uncheck the **Enable Local Site** box to change the access point from **Local Mode** to **FlexConnect**. Finally, click on the **Apply to Device** button as shown in this image.



Add Site Tag

Name*: ST_Branch_01

Description: Site Tag for Branch 01

AP Join Profile: APJP_Branch

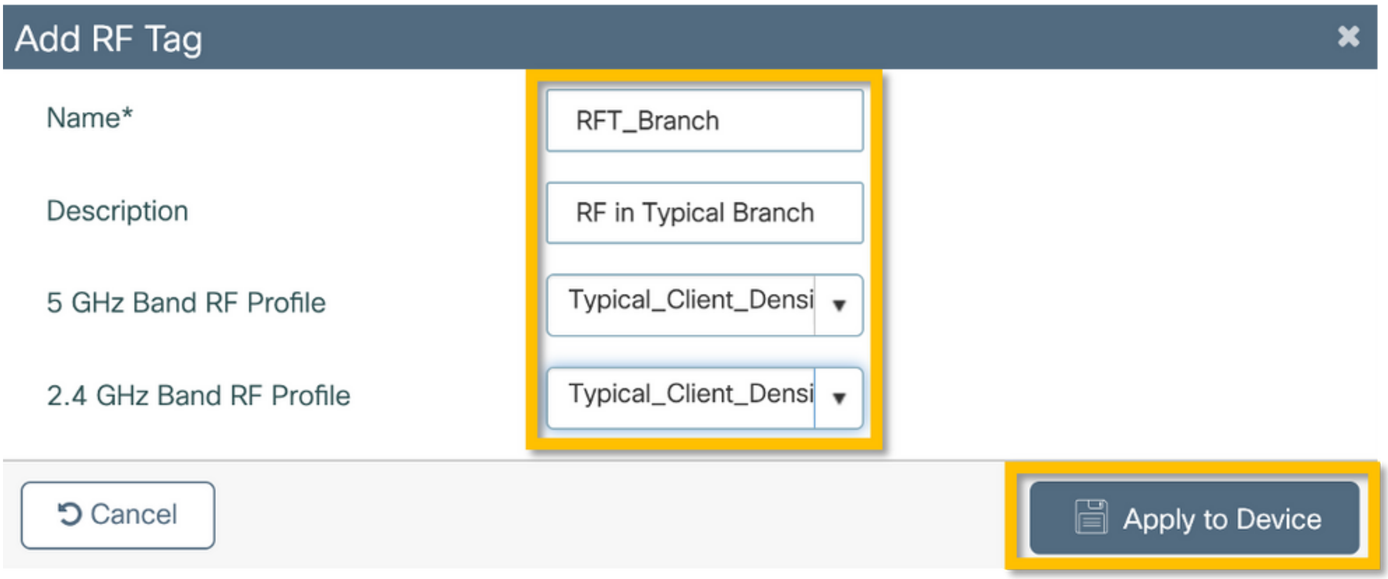
Flex Profile: FP_Branch

Fabric Control Plane Name:

Enable Local Site: ☐

C9800 - RF Tag

Step 1. Navigate to **Configuration** > **Tags & Profiles** > **Tags**, select the **RF** tab and click **+Add.** Enter a name and description for the RF tag.Select the system-defined **RF profiles from the drop-down menu**. Click on the **Apply to Device** button as shown in this image.



Add RF Tag

Name*: RFT_Branch

Description: RF in Typical Branch

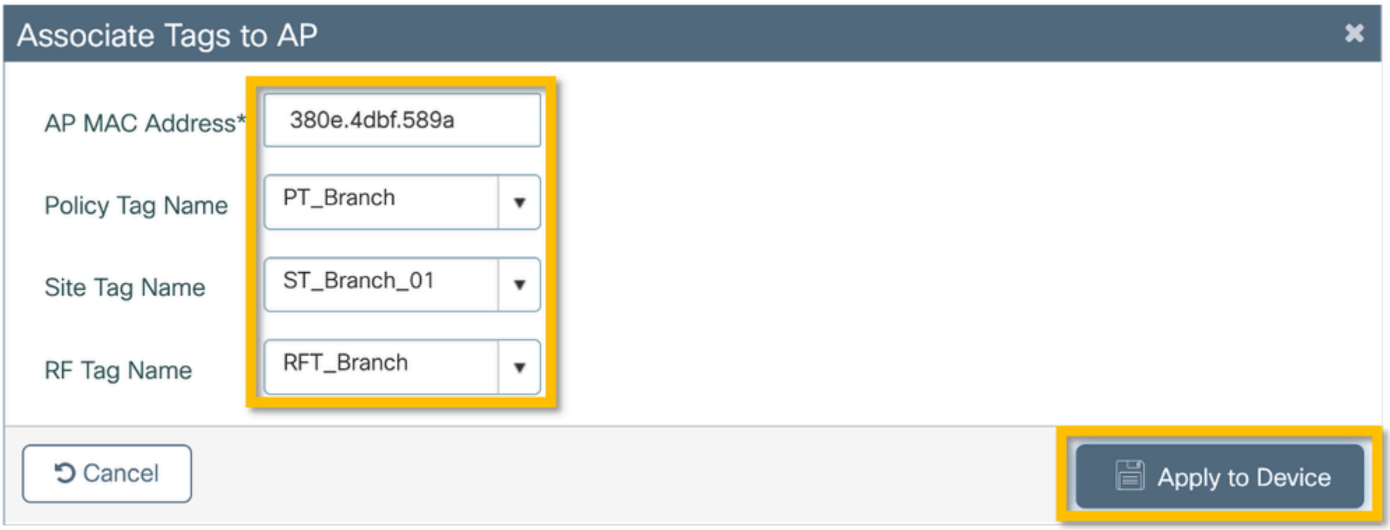
5 GHz Band RF Profile: Typical_Client_Densi

2.4 GHz Band RF Profile: Typical_Client_Densi

C9800 - Assign Tags to AP

Now that the tags are created that include the various policies and profiles required to configure the access points, we must assign them to the access points. This section shows how to perform a static tag assigned to an access point manually, based on its Ethernet MAC Address. For product production environments, it is recommended to use the Cisco DNA Center AP PNP Workflow, or use a static bulk CSV upload method available in 9800.

Step 1. Navigate to **Configure** > **Tags & Profiles** > **Tags**, select the **AP** tab, and then the **Static tab**. Click **+Add** and enter the AP MAC Address, and select the previously defined Policy Tag, Site Tag, and RF Tag. Click on the **Apply to Device** button as shown in this image.



AP MAC Address* 380e.4dbf.589a

Policy Tag Name PT_Branch

Site Tag Name ST_Branch_01

RF Tag Name RFT_Branch

Configure Aruba CPPM

Aruba ClearPass Policy Manager Server Initial Configuration

Aruba clearpass is deployed via OVF template on ESXi server with these resources:

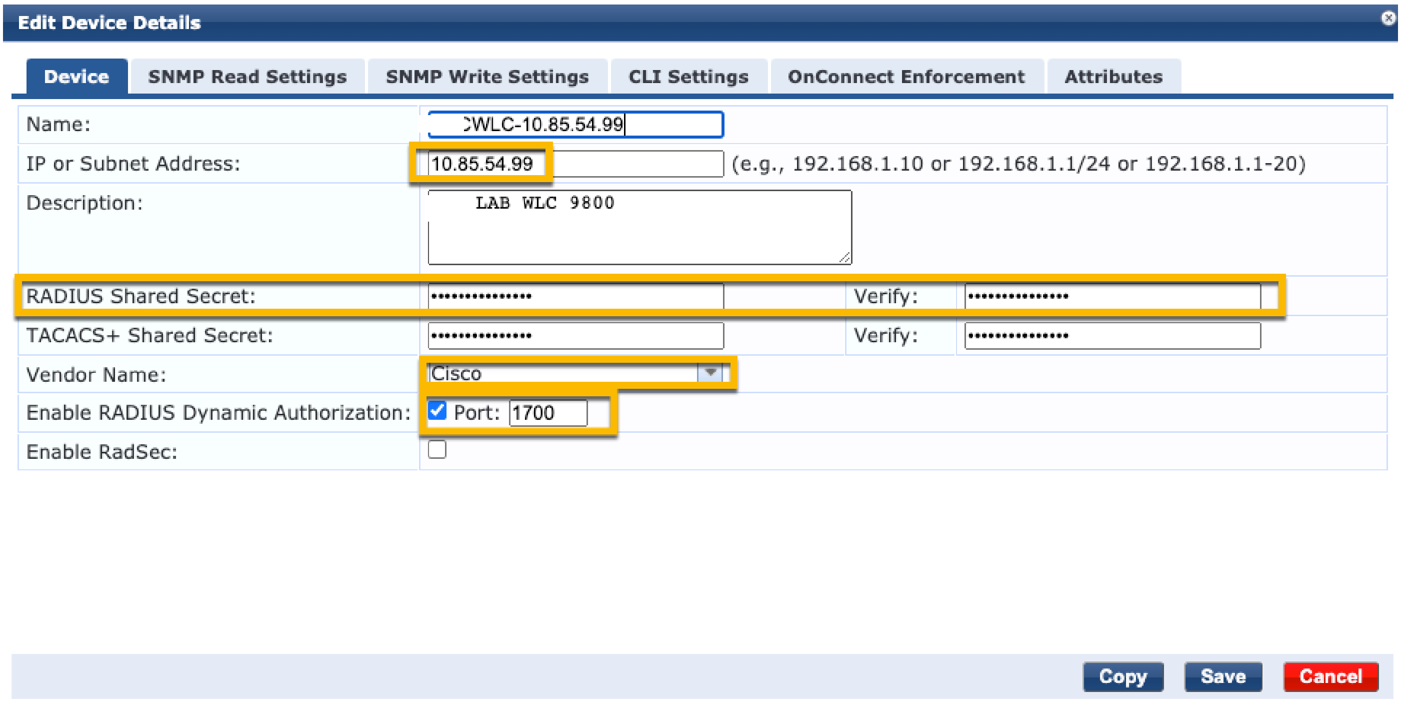
- 2 reserved virtual CPUs
- 6 GB RAM
- 80 GB disk (must be added manually after initial VM deployment before the machine is powered on)

Apply Licenses

Apply platform license via: **Administration** > **Server Manager** > **Licensing**. Add **Access and Onboard**

Add the C9800 Wireless Controller as a Network Device

Navigate to **Configuration** > **Network** > **Devices** > **Add** as shown in this image.



Name: CWLC-10.85.54.99

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: LAB WLC 9800

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

TACACS+ Shared Secret: ••••••••••••••• Verify: •••••••••••••••

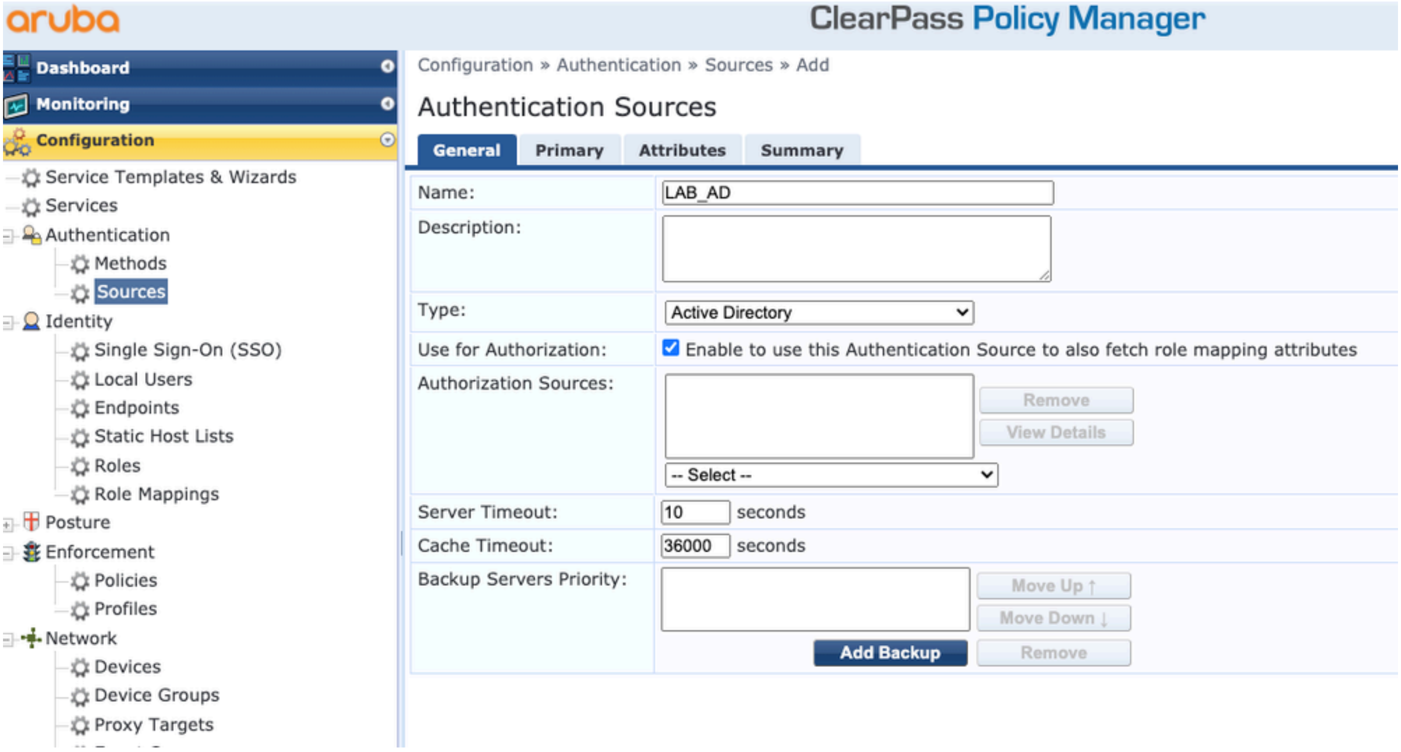
Vendor Name: Cisco

Enable RADIUS Dynamic Authorization: ☑ Port: 1700

Enable RadSec: □

Configure CPPM to Use Windows AD as an Authentication Source

Navigate to **Configuration** > **Authentication** > **Sources** > **Add**. Select **Type: Active Directory** from the drop-down menu as shown in this image.



Configuration » Authentication » Sources » Add

Authentication Sources

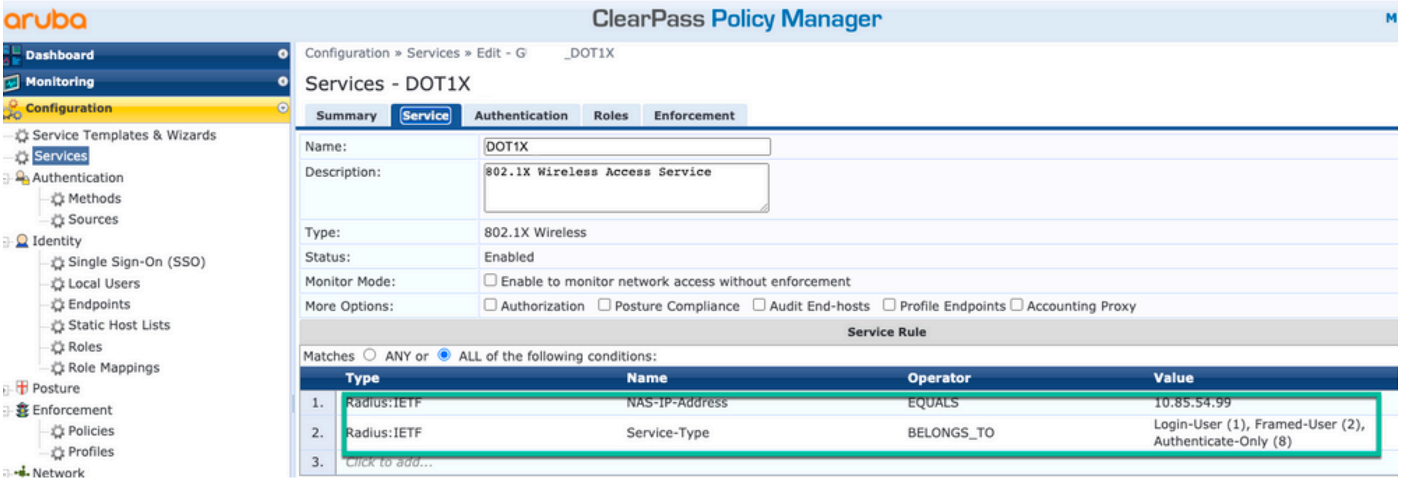
Name:	LAB_AD
Description:	
Type:	Active Directory
Use for Authorization:	☑ Enable to use this Authentication Source to also fetch role mapping attributes
Authorization Sources:	-- Select --
Server Timeout:	10 seconds
Cache Timeout:	36000 seconds
Backup Servers Priority:	

Configure CPPM Dot1X Authentication Service

Step 1. Create a 'service' which matches on several RADIUS Attributes:

- Radius:IETF | Name: NAS-IP-Address | EQUALS | <IP ADDR>
- Radius:IETF | Name: Service-Type | EQUALS | 1,2,8

Step 2. For production, it is recommended to match on SSID name instead of 'NAS-IP-Address' so one condition suffices in a multi-WLC deployment. Radius:Cisco:Cisco-AVPair | cisco-wlan-ssid | Dot1XSSID



Configuration » Services » Edit - G _DOT1X

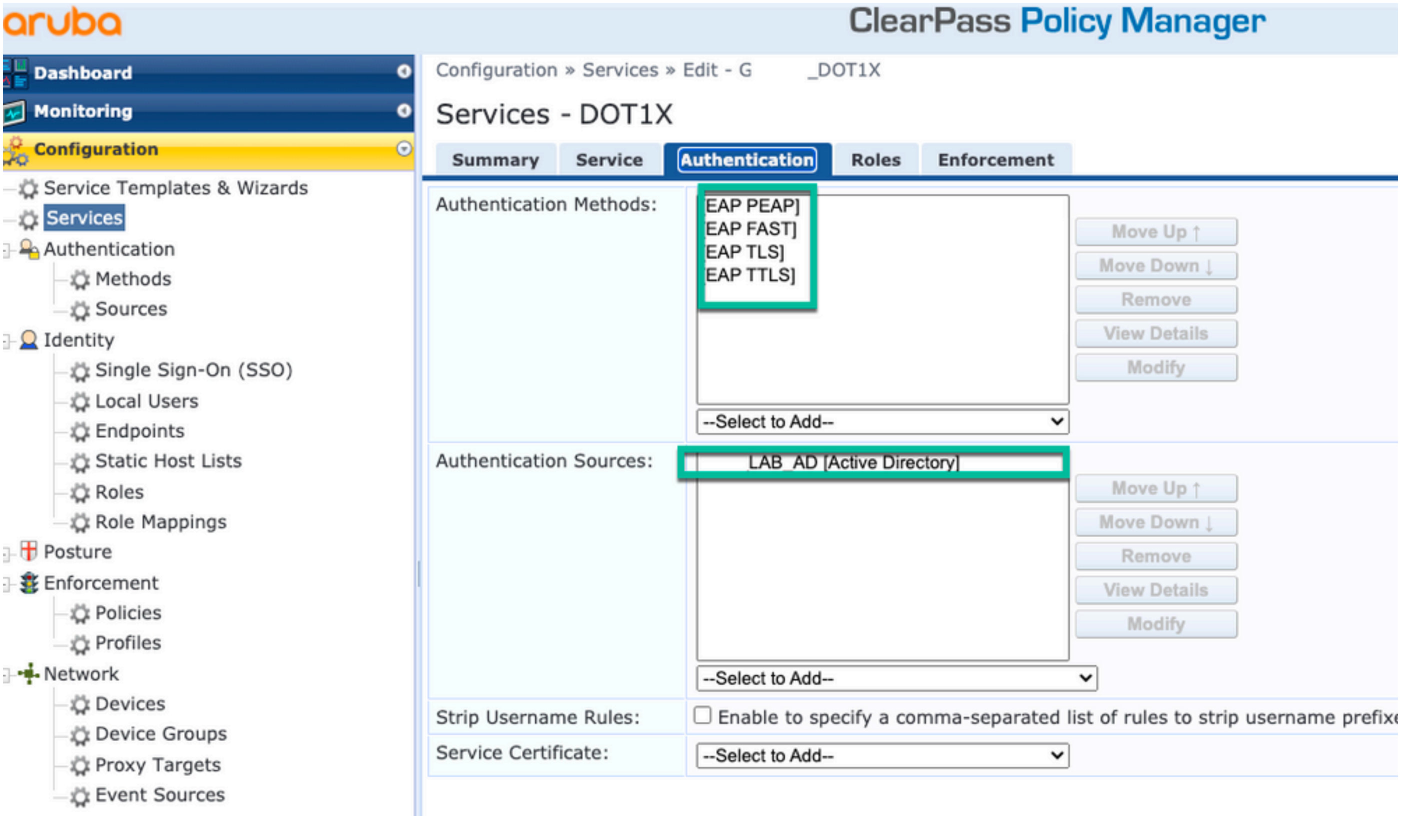
Services - DOT1X

Name:	DOT1X
Description:	802.1X Wireless Access Service
Type:	802.1X Wireless
Status:	Enabled
Monitor Mode:	□ Enable to monitor network access without enforcement
More Options:	□ Authorization □ Posture Compliance □ 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-IP-Address	EQUALS	10.85.54.99
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3.	Click to add...			



Configuration » Services » Edit - G _DOT1X

Services - DOT1X

Authentication Methods: EAP PEAP]
EAP FAST]
EAP TLS]
EAP TTLS]

--Select to Add--

Authentication Sources: LAB AD [Active Directory]

--Select to Add--

Strip Username Rules: □ Enable to specify a comma-separated list of rules to strip username prefixe

Service Certificate: --Select to Add--

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

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.

Related Information

- 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**