



The bridge to possible

[Ordering guide](#)

Cisco public

# Embedded Wireless on Catalyst 9000 series Switch (non-SDA) using WebUI

---

# Contents

Technology use case	3
Platform scale	4
Requirements	8
Design models	9
Installing the wireless sub-package	13
Prerequisite configurations	17
Enable the embedded wireless setup	28
Onboard and provision wireless access points	41

---

As part of mode consolidation **Embedded Wireless on Catalyst 9000 Series Switch (non-SDA) using WebUI** will be **End of Support (Q3FY21)** with no additional feature development or code changes and 17.3.x is the last supported release.

The supported workflow is shown in this deployment guide.

This mode has limited ability to customize configuration or assist deployments for Brownfield migration. Also, it does not provide a centralized management orchestrator to manage the infrastructure.

For customers looking for flexible architecture to suit their needs, we recommend the following options:

- Option 1 : Embedded Wireless on an Access Point (up to 100 APs)
- Option 2 : Embedded Wireless on Catalyst 9000 Series switches using DNAC (SD-Access) (up to 200 APs)
- Option 3 : 9800-L (or 9800-CL) locally on branches or in FlexConnect mode (up to 500 APs)

**Please note:** There are no changes to the support for Embedded Wireless on Catalyst 9k (SD-Access) using DNAC.

For any further questions regarding this mode, please reach out to: [ask-ewc-nonsda-pm-tm@cisco.com](mailto:ask-ewc-nonsda-pm-tm@cisco.com)

## Technology use case

Among small to medium-sized customers, many are looking to deploy a wireless network in their branch or single-site offices while optimizing their operational expenses. Many of these customers are heavily invested in the Cisco® Catalyst® 9000 switching platform and want to maximize the value of the platform, leveraging the reliability and programmability of the Cisco IOS® XE software. They are looking for a solution that enables them to easily deploy access points in their network without having to manage another device at their sites. In addition, the solution must provide secure and resilient access for all employees and guests at the site while also giving the customer an option to expand their wireless capabilities as they grow.

The Cisco Embedded Wireless Controller (EWC) on Catalyst 9000 Switches (non-SD-Access) using WebUI combines the best-in-class performance of the Catalyst 9000 switching family and the Catalyst 9800 Series wireless controllers in a single box. Through the switch's WebUI, customers can easily deploy their corporate and guest WLAN for their site. Additionally, the EWC provides a great migration strategy for customers that have already purchased Catalyst 9000 family switches, allowing them to enable wireless capabilities without the need for an additional standalone controller.



This solution helps customers reduce complexity, optimize IT, and lower operational costs by leveraging the existing expertise of their network administrators on Cisco IOS XE switches to deploy wireless solutions, regardless of where they are in the intent-based networking journey.

**This guide covers the deployment of the following network capabilities:**

- Enabling the EWC on Catalyst 9000 Switches
- Examples of WLAN configurations for both corporate and guest networks
- Common Quality-of-Service (QoS) and security policies
- Onboarding and provisioning of Access Points (APs)

Platform scale

Supported scale per switch

The supported number of access points and clients per switch or switch stack is shown in Table 1. For a single site, there can be two separate, active embedded controller instances on separate Catalyst 9000 switches. In such cases, the scale of APs and clients will double.

**Table 1.** AP and client scale for the EWC on Catalyst 9000 switches (non-SD-Access)

Switch model	AP scale	Client scale
9300L models	50	1000
9300 Series	200	4000
9400 Series		
9500 and 9500H Series		

## Scale in comparison to other models

The scale in comparison to some of the other WLC models, specifically the Cisco Software-Defined Access (SD-Access) enabled models and the EWC on Catalyst APs, is shown in Table 2 below. For a more comprehensive comparison, please see:

[https://www.cisco.com/c/dam/en/us/products/se/2020/4/Business\\_Unit/WLC\\_Comparison.pdf](https://www.cisco.com/c/dam/en/us/products/se/2020/4/Business_Unit/WLC_Comparison.pdf)

**Table 2.** Scale comparison of the EWC on Catalyst 9000 Switches (non-SD-Access) using WebUI to the EWC on Catalyst APs and SD-Access enabled WLCs

	Catalyst 9800-40	Catalyst 9800-L	EWC on Catalyst 9000 Switches (SD-Access)	EWC on Catalyst APs	EWC on Catalyst 9000 Switches (non-SD-Access)
<b>Scale</b>					
<b>Access points</b>	2000	500 <sup>1</sup>	200 <sup>2</sup>	100 <sup>3</sup>	200 <sup>2</sup>
<b>Clients</b>	32,000	10,000 <sup>1</sup>	4000 <sup>2</sup>	2000 <sup>3</sup>	4000 <sup>2</sup>
<b>WLANs</b>	4096	4096	64	16	64
<b>Management</b>					
<b>AP deployment modes</b>	Local, Flex, Fabric	Local, Flex, Fabric	Fabric	Flex with local switching	Fabric <sup>4</sup>
<b>Multisite deployments</b>	X	X	X <sup>5</sup>	X	
<b>SD-Access fabric deployments</b>	X	X	X		
<b>Integrated WebUI</b>	X	X	X	X	X
<b>Cisco DNA Center</b>	X	X	X	X	
<b>Cisco DNA Center Cloud</b>				X	
<b>Supported access points</b>					
<b>Catalyst 9100 802.11ax</b>	X	X	X	X	X
<b>Aironet® 802.11ac Wave 2</b>	X	X	X	X	X
<b>Aironet 802.11ac Wave 1</b>	X	X	X		

<sup>1</sup>Based on the Performance license.

<sup>2</sup>Based on scale for the Catalyst 9300, 9400, 9500, and 9500H Series.

<sup>3</sup>Based on scale for the Catalyst 9120AX and 9130AX Series AP models.

<sup>4</sup>Cisco FlexConnect® configuration appears in WebUI but is not supported.

<sup>5</sup>Each fabric site will require its own EWC on Catalyst 9000 Switches (SD-Access).

## Supported matrix

The features that are supported on the EWC on Catalyst 9000 Switches (non-SD-Access) using WebUI is shown in Table 3.

**Table 3.** Supported features on the EWC on Catalyst 9000 switches (non-SD-Access) using WebUI.

	Features
Full stack health visibility	WebUI Programmability (NETCONF+ YANG)
AP modes	WGB mode Monitor mode
Infrastructure	Pre-image download Client IPv6 DHCP Option 82
Security and authentication	WPA-PSK 802.1X (WPA2/AES) 802.1X (WPA2/TKIP) WPA3 Identity PSK Multi-PSK on single SSID Internal Webauth External Webauth Central Webauth DNS pre-auth ACL WEP 802.11r 802.11k 802.11v BSS transition 802.11v DMS PMF (802.11w) TACACS Radius server per WLAN Backup RADIUS servers Cisco Centralized Key Management User idle timeout per WLAN

	Features
Services	AVC-mark, drop, RL AAA override-VNID AAA override: ACL, QoS AAA override – session timeout AAA override of AVC profile AAA override BW contract QoS Local profiling RADIUS profiling Per-user bandwidth contract Per-SSID bandwidth contract Multicast CAC, WMM policy Adaptive 11r Fastlane MAB MAC authentication Rogue detection Passive clients BYOD, NAC RADIUS, CWA, LWA
RF and radio	RRM-DCA, TPC, CHDM FRA Band Select Load balancing RF profiles XOR Optimized roaming RX-SOP DFS DBS Off-channel scanning Off-channel scan defer ClientLink A-MSDU/A-MPDU aggregation config per priority ATF UL OFDMA DL OFDMA

	Features
	UL MU MIMO DL MU MIMO TWT BSS coloring
<b>Resiliency</b>	High availability: SSO <sup>1</sup> High availability: N+1 Hot/cold patching AP service pack (APSP) AP device pack (APDP)
<b>Segmentation</b>	Up to 4 segments No SGT-based segmentation

<sup>1</sup> HA SSO is supported only on the 9300 and 9300L as well as the 9400 with Dual Supervisor. HA SSO is not supported with StackWise Virtual.

## Requirements

To use the EWC on the switch, the following components are needed:

### Cisco Catalyst 9000 switch family

9300, 9300L, 9400, 9500, or 9500H Series

Software requirements:

- Release 17.3 with the wireless sub-package installed
- Management IP address to access the WebUI
- Loopback0 IP address

**Note:** EWC configuration is supported only via the WebUI.

### Cisco Catalyst access points

All Catalyst 9100 APs

### Cisco Aironet access points

Indoor Wave 2: Aironet 1800, 2800, 3800, or 4800 Series APs

Outdoor Wave 2 (local mode only): 1540 or 1560 Series

## Licensing

Both the switches and APs require Cisco DNA Advantage licenses.

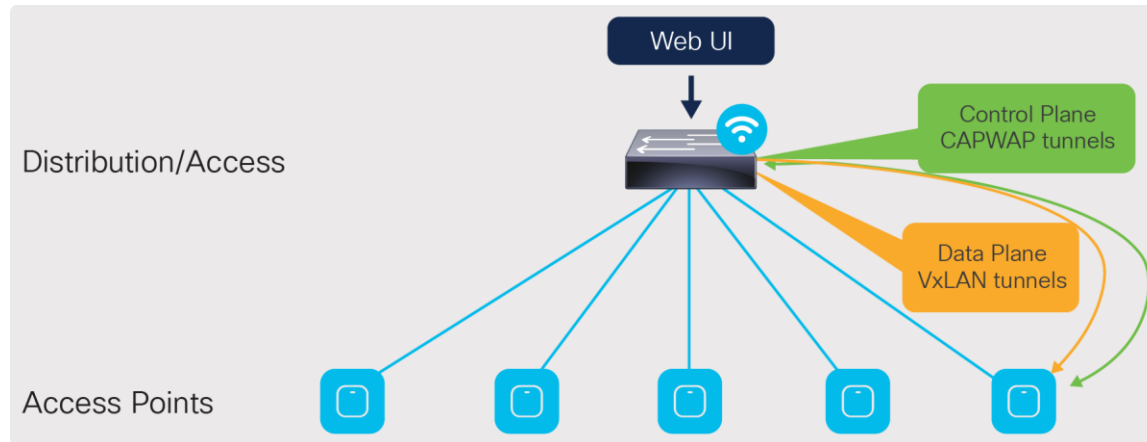


## Design models

The EWC can be deployed in the following ways:

- Single switch
- High Availability Stateful Switchover (HA SSO)
- N+1 redundancy

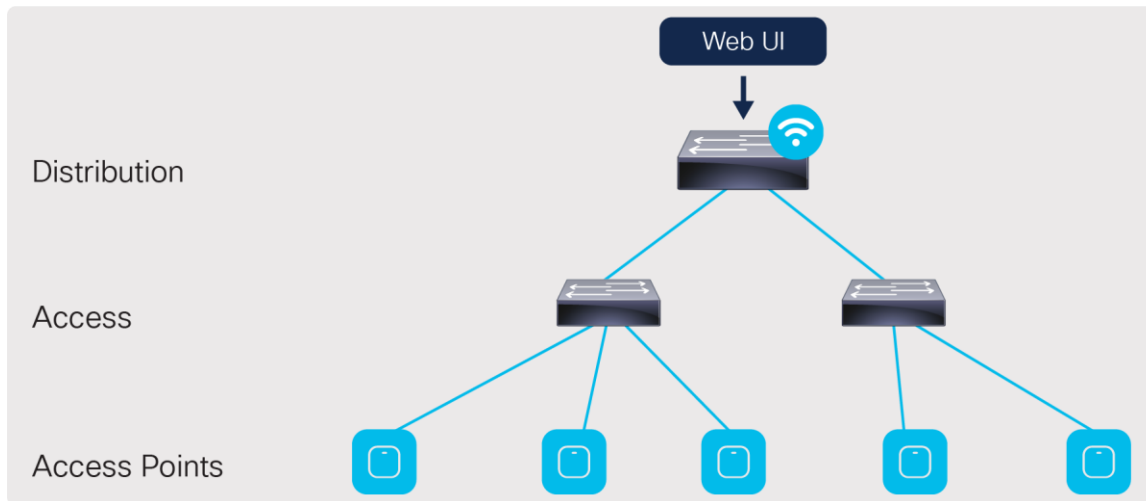
### Single switch deployment



**Figure 1.**  
Single switch design

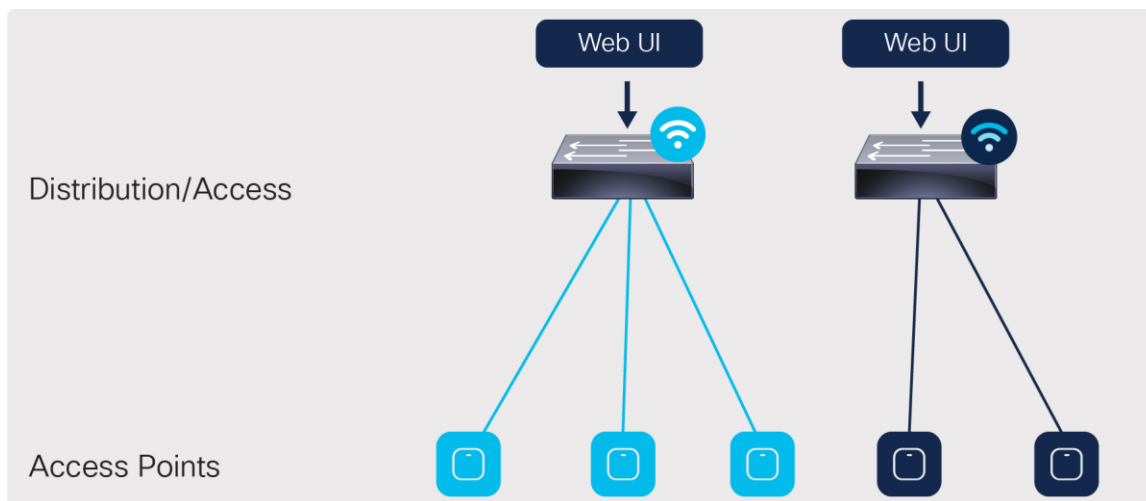
At a minimum, the EWC can be deployed on a single switch with all the APs connected directly into it. However, this is not recommended, as in the event of a switch failure, the entire wireless network will go down until the switch is recovered or replaced.

The APs can also be connected to an external edge node, which is then connected to the EWC. The connections between the EWC and the external edge nodes as well as between any intermediate switches need to be Layer 2 connections with the appropriate VLAN trunking between them. As discussed later in the “Onboard and provision wireless access points - Setting up network topology” section, the APs discover and join the EWC via the AP onboarding VLAN. The VLAN tagging between the AP and EWC needs to be preserved across the multiple switches. Otherwise, the AP will fail to join the EWC.



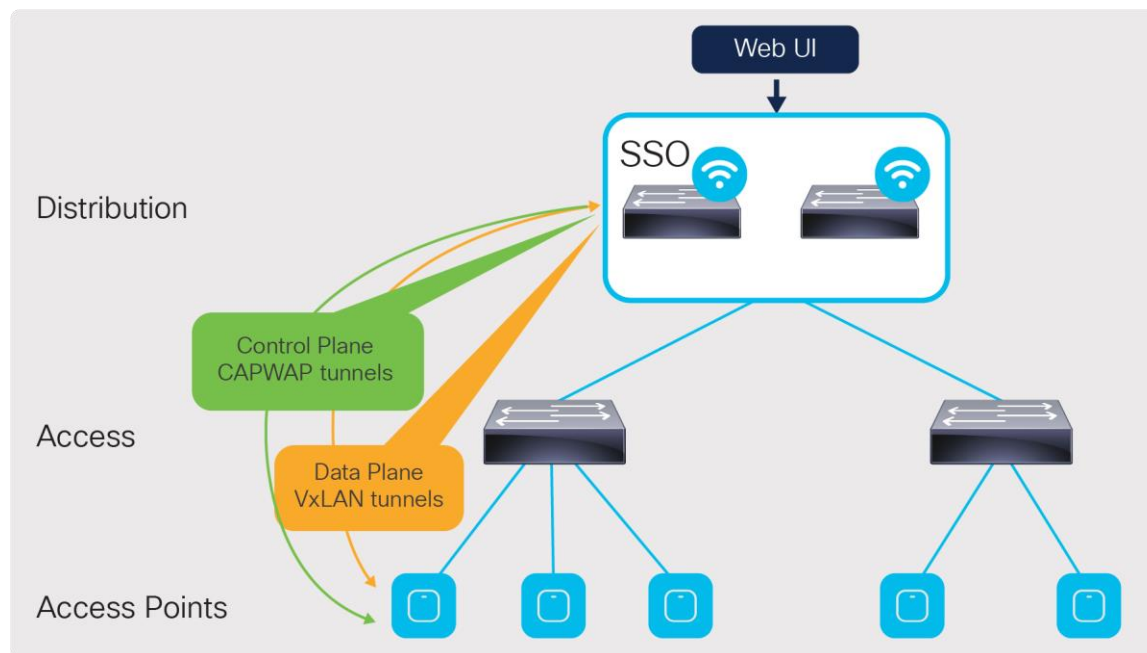
**Figure 2.**  
Connection via an external edge node

For a single site, there can be two separate embedded controller instances on separate Catalyst 9000 switches. In such cases, the scale for both the APs and the clients will double.



**Figure 3.**  
A single site with two controller instances

## High Availability Stateful Switchover (HA SSO)



**Figure 4.**  
HA SSO design

This is the recommended deployment model for the embedded wireless controller.

In this deployment, all the control plane-related information is synchronized between the active and standby units.

For the switches, HA SSO will be implemented by:

- Catalyst 9300L Models: StackWise®-320
- Catalyst 9300 Series: StackWise-480
- Catalyst 9400 Series: Dual supervisor

To the APs and network, the stack of switches for the EWC will appear logically as a single controller. The active controller centrally manages all the control and management communication. The control plane data is synchronized between the two switches through the StackWise ports.

The APs connected to the stack also have their Control and Provisioning of Wireless Access Points (CAPWAP) states synced between the active and hot-standby controllers on the switches. In the event that the active controller or switch fails, all the APs will switch over to the hot-standby rather than go into discovery mode to join the standby controller. This enables little to no downtime in the event of a failure.

APs can be directly connected to an individual switch in the stack, but this is not recommended. They should be aggregated through an intermediate switch, and the intermediate switch will connect to both switches in the stack. This prevents the APs from going down in the event that one of the switches in the stack fails.

**Note:** HA SSO is not supported with the Catalyst 9400 Series StackWise Virtual setups, nor with the Catalyst 9500 or 9500H Series

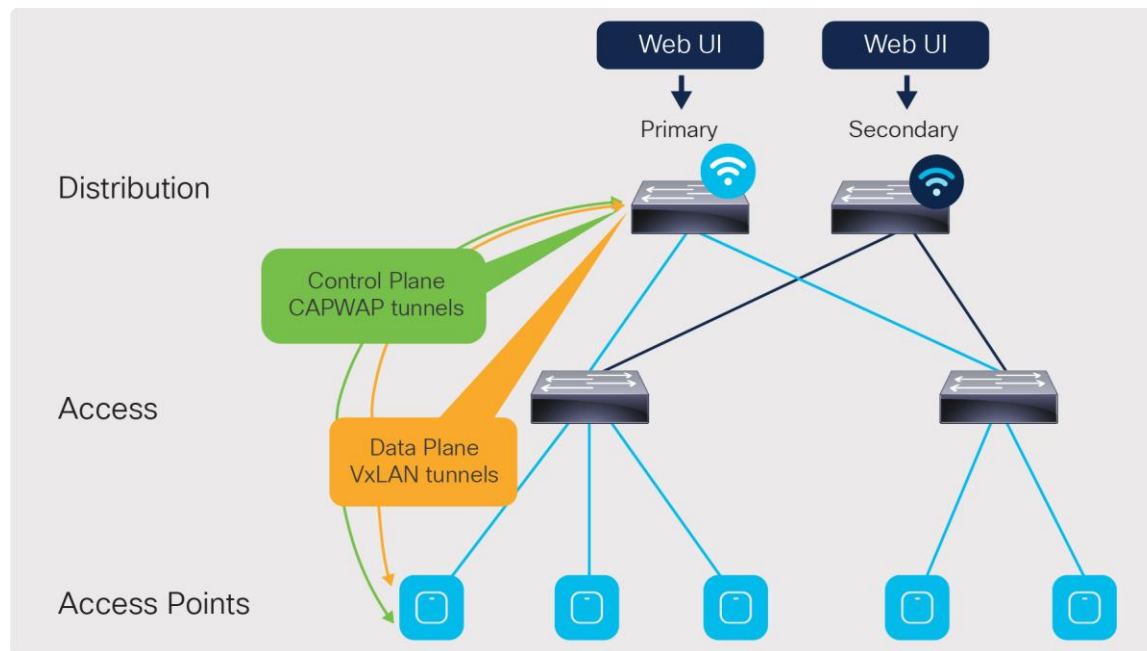
Catalyst 9300 Series StackWise configuration:

[https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-3/configuration\\_guide/stck\\_mgr\\_ha/b\\_173\\_stck\\_mgr\\_ha\\_9300\\_cg/managing\\_switch\\_stacks.html#concept\\_i2w\\_shc\\_31b](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-3/configuration_guide/stck_mgr_ha/b_173_stck_mgr_ha_9300_cg/managing_switch_stacks.html#concept_i2w_shc_31b)

Catalyst 9400 Series dual supervisor installation:

[https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9400/hardware/sup\\_install/b-c9400-sup-note.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9400/hardware/sup_install/b-c9400-sup-note.html)

## N+1 redundancy



**Figure 5.**  
N+1 redundancy design

In the N+1 deployment model, the two embedded controllers are independent of each other and do not sync configuration data across any interface. Each of the EWCs will need to be managed individually. Because of this, the redundancy method is not stateful, and so the CAPWAP state of the APs will restart in the event of a failure. The APs will go into discovery mode to join the backup controller, resulting in longer failover times.

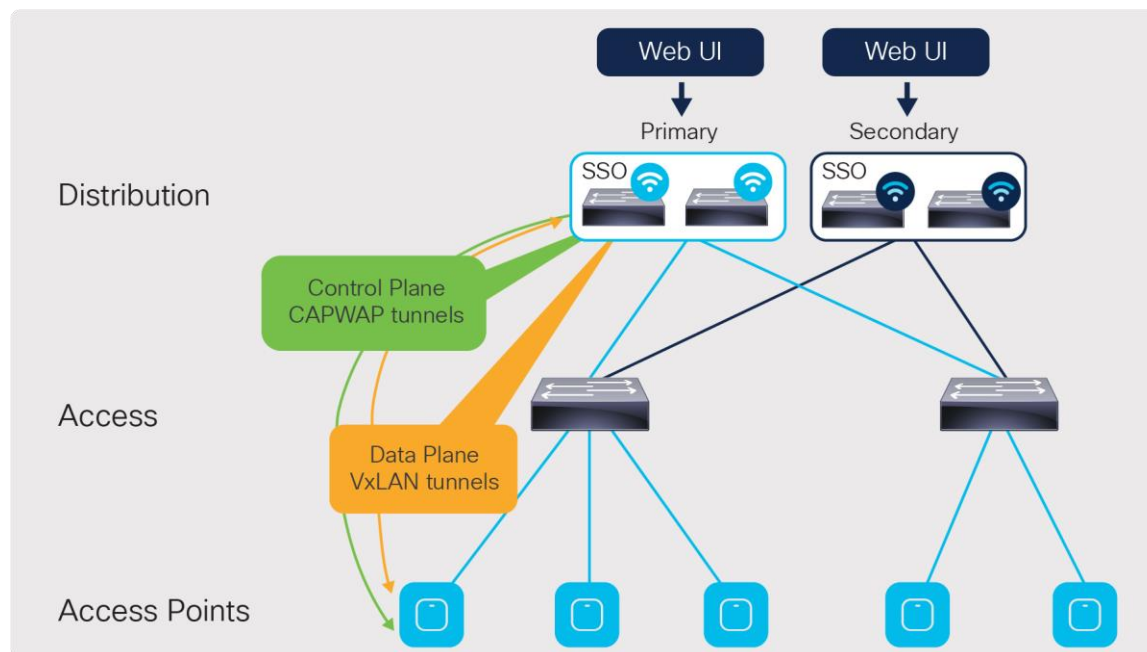
To minimize the failover time, we recommend having the same configuration, in terms of WLANs, profiles, mobility group, policy, RF, and site tags, as well as AP-to-tag mappings, on the primary and secondary controllers.

The EWCs can be deployed in two N+1 configurations:

- One controller will be the primary for all the access points, and the other is the secondary.
- One controller will be the primary for some of the APs, and the other controller will be the primary for the remaining APs. The controllers will be the secondary for each other.

In either case, the scale for the number of APs and clients stays the same as shown earlier in Table 1. The only change is in which controller will be the primary for the APs.

The N+1 design can also be configured alongside the HA SSO redundancy method. The same two deployment configurations apply to this type of design. Figure 6 shows an example topology in which one SSO pair will be the primary controller while another SSO pair will be the secondary.



**Figure 6.**  
N+1 redundancy with HA SSO design

For more information, please see the Catalyst 9800 Series N+1 configuration guide:  
[https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-3/config-guide/b\\_wl\\_17\\_3\\_cg/m\\_vewlc\\_high\\_availability.html#task\\_k2c\\_nps\\_xfb](https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-3/config-guide/b_wl_17_3_cg/m_vewlc_high_availability.html#task_k2c_nps_xfb)

## Installing the wireless sub-package

To enable the non-SD-Access EWC on a Catalyst 9000 switch, the switch needs to have at least the Cisco IOS XE Release 17.3.1 image installed, along with the corresponding wireless sub-package. Please note that the base Cisco IOS XE image and wireless sub-package always need to be the same exact release.

The latest wireless sub-package can be found at [software.cisco.com](https://software.cisco.com).

Once on the webpage, go to **Software Download**.

Cisco Software Central

InternalTestDemoAccount20.cisco.com

### Download & Upgrade

[Software Download](#)  
Download new software or updates to your current software

[eDelivery](#)  
Get fast electronic fulfillment of software, licenses, and documentation

[Version Upgrade using MCE](#) New  
Order major upgrades to software such as Unified Communications

[Product Upgrade Tool \(PUT\)](#)

[Upgradeable Products](#)  
Browse a list of all available software updates.

### Network Plug and Play

[Plug and Play Connect](#)  
Device management through Plug and Play Connect portal

[Learn about Network Plug and Play](#)  
Training, documentation and videos

### License

[Traditional Licensing](#)  
Generate and manage PAK-based and other device licenses, including demo licenses

[Smart Software Licensing](#)  
Track and manage Smart Software Licenses.

[Enterprise Agreements](#)  
Generate and manage licenses from Enterprise Agreements.

[View My Consumption](#)  
View all my customers based on smart accounts

Enter the **switch model** into the search bar and click **Enter**.

- **Note:** The switch model can be found in the top bar of the WebUI for the switch.

Cisco C9300-48UXM  
17.3.1

Search Menu Items

Dashboard

Overview

## Software Download

### My Previous Downloads

Product	Software Type	Latest Release	Last Downloaded
Catalyst 9300-48UXM-A Switch	IOS XE Wireless Controller Software Package	--	17.3.1
Catalyst 9300-48UXM-A Switch	IOS XE Software	Fuji-16.9.6	Amsterdam-17.3.1
Catalyst 9120AXI Access Point	Lightweight AP Software	15.3.3-JPJ4	15.3.3-JPJ3a

[View all 25 Downloads >](#)

### Most Popular

- [AnyConnect Secure Mobility Client v4.x](#)
- [Jabber for Windows](#)
- [Small Business RV Series Routers](#)
- [ASA 5515-X IPS Security Services Pro...](#)
- [Identity Services Engine Software](#)
- [CLI Analyzer](#)

Select a Product

9300-48UXM-A

Browse all

For the Software Type, select **IOS XE Wireless Controller Software Package**.

# Software Download

[Downloads Home](#) / [Switches](#) / [Campus LAN Switches - Access](#) / [Catalyst 9300 Series Switches](#) / [Catalyst 9300-48UXM-A Switch](#)

## Select a Software Type

[IOS XE Hardware Programmable Devices](#)  
[IOS XE Software](#)  
[IOS XE Software Maintenance Upgrades \(SMU\)](#)  
[IOS XE Wireless Controller Software Package](#)  
[NBAR2 Protocol Packs](#)

Select and download the sub-package version that matches the Cisco IOS XE image installed on the switch.

[Downloads Home](#) / [Switches](#) / [Campus LAN Switches - Access](#) / [Catalyst 9300 Series Switches](#) / [Catalyst 9300-48UXM-A Switch](#) / [IOS XE Wireless Controller Software Package- 17.3.1](#)

[Expand All](#) [Collapse All](#)

Latest Release

17.3.1

16.12.4a

All Release

17

### Catalyst 9300-48UXM-A Switch

Release 17.3.1  
[My Notifications](#)

Related Links and Documentation  
[Release Notes for 17.3.1](#)

File Information	Release Date	Size	
Cisco Catalyst 9800 Wireless Controller for Switch C9800-SW-iosxe-wlc.17.03.01.SPA.bin	09-Aug-2020	570.42 MB	<a href="#">Download</a> <a href="#">Add to Cart</a> <a href="#">Share</a>

Go to the switch's WebUI and navigate to **Administration** → **Software Management**.

Dashboard

Monitoring

Configuration

Administration

Licensing

Troubleshooting

Command Line Interface

Device

DHCP Pools

DNS

Management

Backup & Restore

File Manager

HTTP/HTTPS/Netconf

SDM-Template

SNMP

Power Management

Reload

Smart Call Home

Software Management

Time

User Administration

In the Software Upgrade section, choose the preferred method to upload the wireless sub-package to the switch and click **Download and Install**.

Administration > Software Management

Software Upgrade

Software Maintenance Upgrade (SMU)

Upgrade Mode INSTALL  
Current Mode (until next reload): INSTALL

Transport Type My Desktop

File System Flash Free Space: 7897.05 MB

Source File Path\* Select File  
C9800-SW-iosxe-wlc.17.03.01.S...

Download & Install Save Configuration & Reload

[Manage](#)  
[Remove Inactive Files](#)  
[Rollback](#)

Once the sub-package is finished installing, the switch will need to be reloaded for the sub-package to be applied. Click **Save Configuration & Reload**.

Upgrade Mode INSTALL  
Current Mode (until next reload): INSTALL

Transport Type My Desktop

File System Flash Free Space: 7897.05 MB

Source File Path\* Select File  
C9800-SW-iosxe-wlc.17.03.01.S... ✓

Download & Install Save Configuration & Reload

[Manage](#)  
[Remove Inactive Files](#)  
[Rollback](#)

**Status**

- ✓ Download Image/Package  
C9800-SW-iosxe-wlc.17.03.01.SPA.bin
- > Copying to stack members
- Install Image/Package
- ✓ Set Boot Params

[Show Logs](#)

Once the switch is reloaded, log back into the WebUI and click the **wireless icon** in the dashboard.

Cisco C9300-48UXM 17.3.1

Welcome admin

Dashboard

Overview Switch View

CPU & Memory Pressure Graph  
Last Updated: 9/9/2020, 9:31:35 AM

Slot: 1-RP0

CPU Utilization

CPU: 0

Process	CPU (%)
User	3.10

CPU (%) vs Device Time

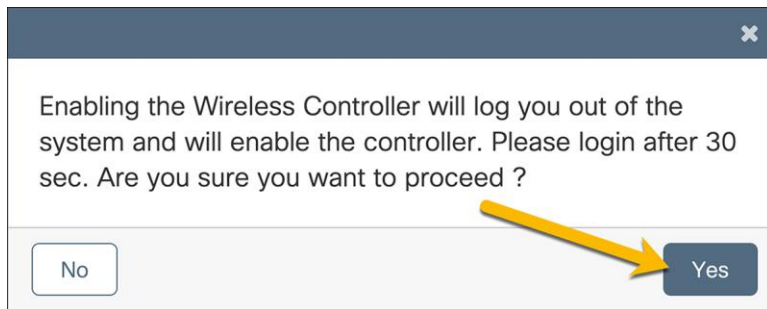
Memory Utilization

Memory Details	Size (KB)
Total	7757632
Used	3064044
Free	4693588

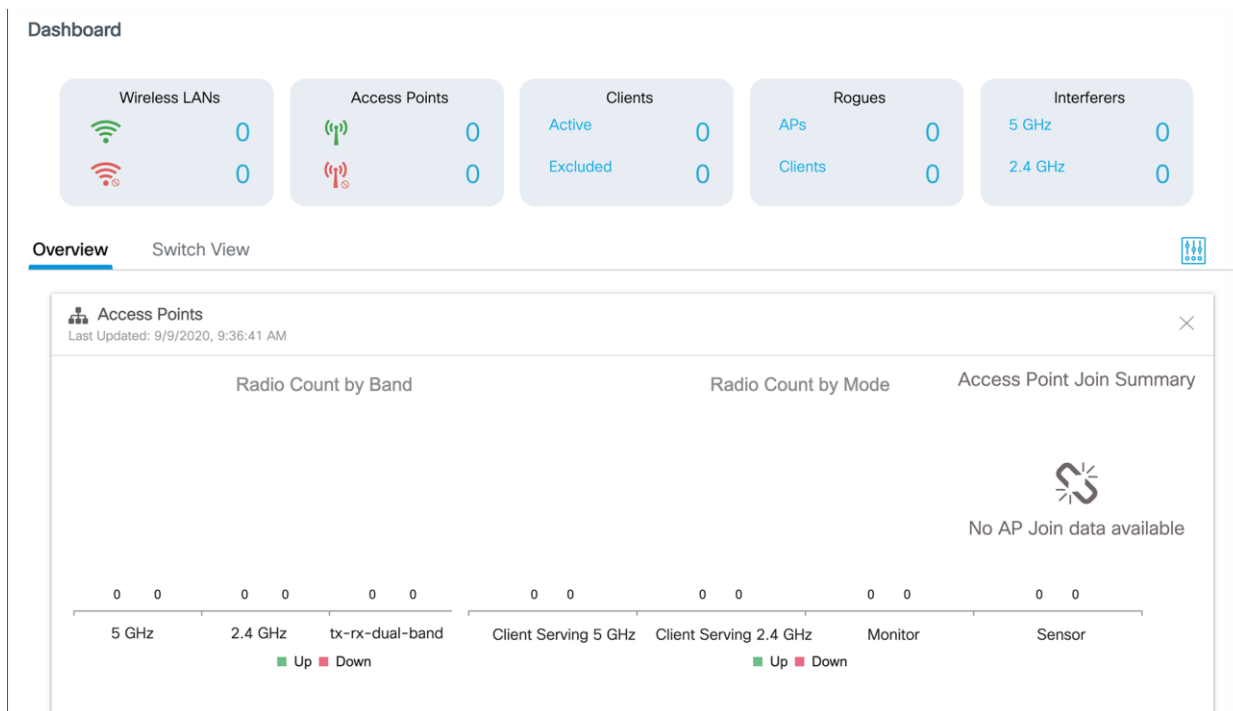
Memory Used (%) vs Device Time

In the resulting window, choose **Yes** to enable the wireless controller.





After 30 seconds, log back in to the WebUI. Notice that the homepage dashboard now shows readouts for a wireless LAN controller. The switch is now ready to be configured for all the necessary WLANs in the network.



## Prerequisite configurations

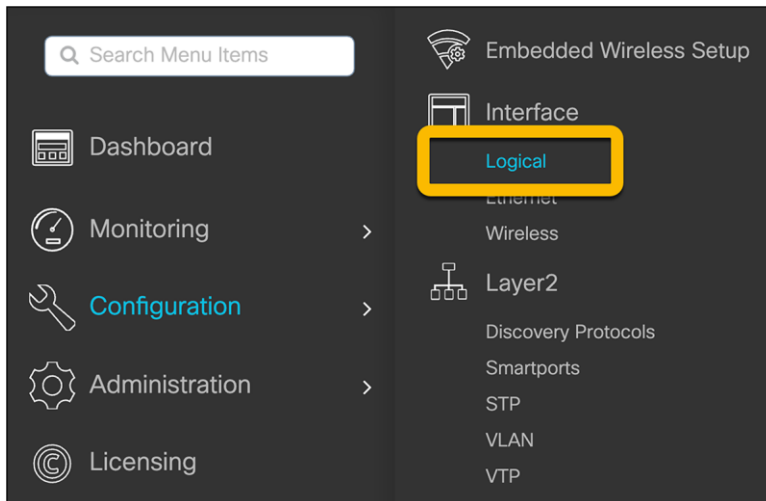
When deploying the EWC, ensure that the following options have been configured. This will allow for a smoother process when creating the WLANs for the site.

### Verify loopback interface

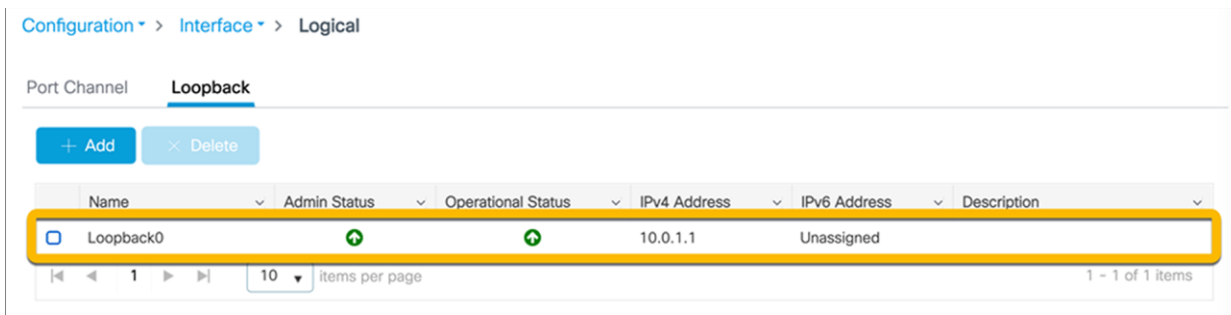
Interface Loopback0 is required to enable the EWC. Since the EWC operates in Fabric Mode, the Loopback0 address serves as the routing locator of the device. If it is not configured, you will be prompted to create it.

**Note:** The Loopback interface must be Loopback0. If a different Loopback interface is used, there will be errors in deploying the EWC.

Navigate to **Configuration** → **Interface** → **Logical** and go to the **Loopback** tab.



Verify that the Loopback0 address has been configured.



If it is not configured, click the **Add** button and configure the Loopback0 interface. The Loopback0 IP address can be any IP address that is reachable within the network.

Click **Apply to Device**.

The screenshot shows the 'Add Loopback Interface' dialog box. It contains the following fields and options:

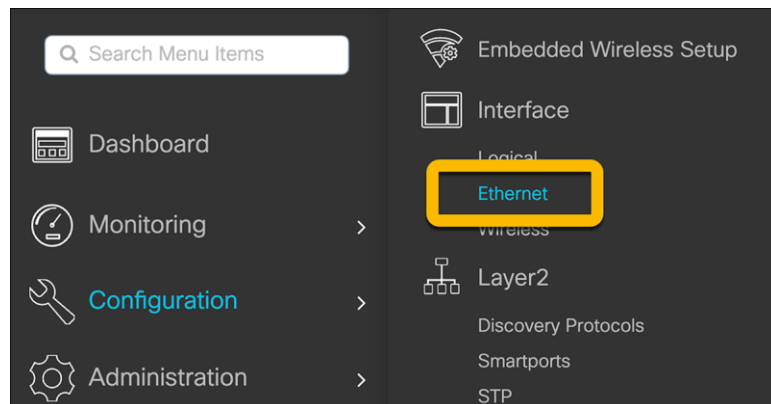
- Loopback Number\***: 0
- Description**: (empty text box)
- Admin Status**: UP (with a green up arrow icon)
- VRF**: None (dropdown menu)
- Relay Information Option**: DISABLED (checkbox)
- IP Options**:
  - ☒ **IPv4** ☐ **IPv6**
  - IPv4 Type**: Static (dropdown menu)
  - IP Address\***: 10.0.1.1
  - Subnet Mask\***: 255.255.255.255

At the bottom, there are 'Cancel' and 'Apply to Device' buttons.

## Configure Virtual Route Forwarding (VRF)

To segment the network, the EWC supports up to four VRFs. This allows the IP networks in separate VRFs to be isolated from each other, as the routing table for each VRF is separate from that of every other VRF. Putting the corporate network and guest network traffic in their own separate VRFs prevents communication between devices in the different networks, ensuring that guest network traffic will be completely isolated from corporate network traffic. Furthermore, both the corporate and guest networks will be isolated from the AP management network, preventing devices from either network from accessing the AP and EWC, accidentally or intentionally.

To create the VRFs, navigate to **Configuration → Interface → Ethernet**.



Click **Create VRF-Lite**.

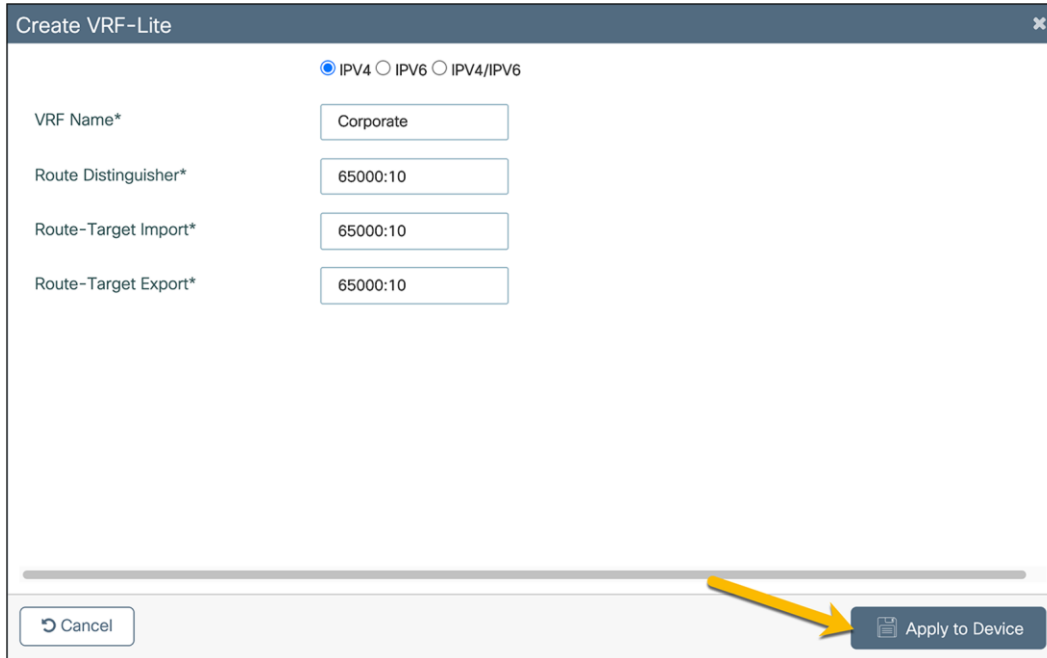
Configuration > Interface > Ethernet

Multi Port Configuration [Create VRF-Lite](#)

	Name	Admin Status	Operational Status	IPv4 Address	IPv6 Address	Layer	Description
<input type="checkbox"/>	GigabitEthernet0/0	↑	↑	172.20.229.194	Unassigned	L3	
<input type="checkbox"/>	TwoGigabitEthernet1/0/1	↑	↓	unassigned	Unassigned	L2/L3	AP1
<input type="checkbox"/>	TwoGigabitEthernet1/0/2	↑	↑	unassigned	Unassigned	L2/L3	Aggregation AP Switch to ...
<input type="checkbox"/>	TwoGigabitEthernet1/0/3	↑	↓	unassigned	Unassigned	L2/L3	
<input type="checkbox"/>	TwoGigabitEthernet1/0/4	↑	↓	unassigned	Unassigned	L2/L3	
<input type="checkbox"/>	TwoGigabitEthernet1/0/5	↑	↓	unassigned	Unassigned	L2/L3	
<input type="checkbox"/>	TwoGigabitEthernet1/0/6	↑	↓	unassigned	Unassigned	L2/L3	
<input type="checkbox"/>	TwoGigabitEthernet1/0/7	↑	↓	unassigned	Unassigned	L2/L3	
<input type="checkbox"/>	TwoGigabitEthernet1/0/8	↑	↓	unassigned	Unassigned	L2/L3	
<input type="checkbox"/>	TwoGigabitEthernet1/0/9	↑	↓	unassigned	Unassigned	L2/L3	

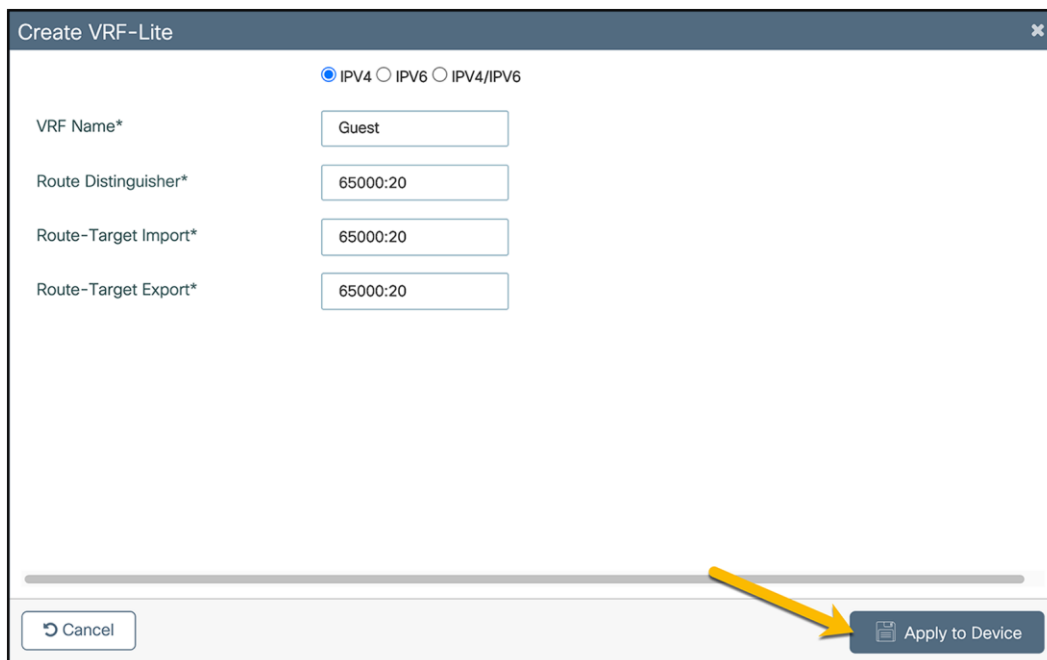
10 items per page 1 - 10 of 131 items

In the Create VRF-Lite window, configure the corporate VRF with the requisite settings.  
Click **Apply to Device**.



The screenshot shows the 'Create VRF-Lite' dialog box. At the top, there are radio buttons for 'IPV4' (selected), 'IPV6', and 'IPV4/IPV6'. Below this, there are four labeled input fields: 'VRF Name\*' with the value 'Corporate', 'Route Distinguisher\*' with '65000:10', 'Route-Target Import\*' with '65000:10', and 'Route-Target Export\*' with '65000:10'. At the bottom left is a 'Cancel' button, and at the bottom right is an 'Apply to Device' button with a disk icon. A yellow arrow points from the center of the dialog towards the 'Apply to Device' button.

Repeat the steps to create the guest VRF.



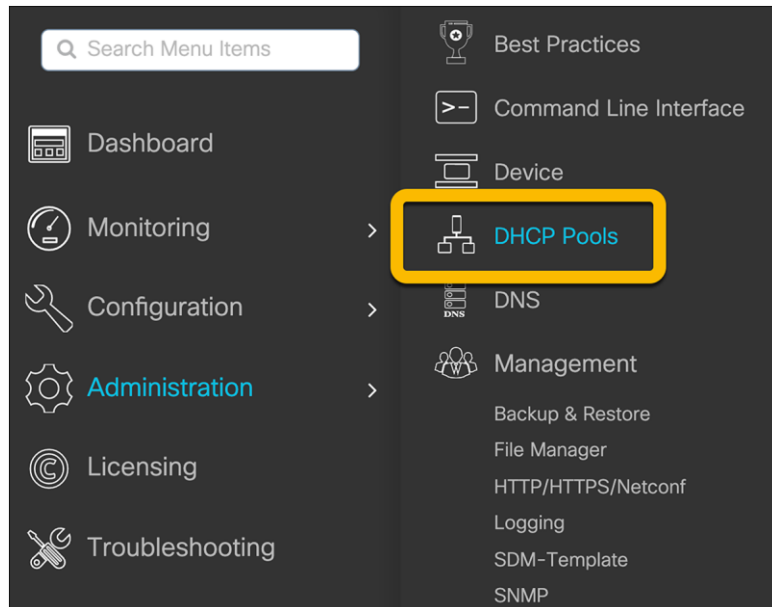
The screenshot shows the 'Create VRF-Lite' dialog box for the 'Guest' VRF. The radio buttons at the top are 'IPV4' (selected), 'IPV6', and 'IPV4/IPV6'. The input fields are: 'VRF Name\*' with the value 'Guest', 'Route Distinguisher\*' with '65000:20', 'Route-Target Import\*' with '65000:20', and 'Route-Target Export\*' with '65000:20'. At the bottom left is a 'Cancel' button, and at the bottom right is an 'Apply to Device' button with a disk icon. A yellow arrow points from the center of the dialog towards the 'Apply to Device' button.

If route leaking between VRFs and the Global Routing Table (GRT) is required, this can be done on the EWC without a next-hop. Please see the “BGP Support for IP Prefix Import” or “Policy Based Routing (PBR)” sections here: <https://www.cisco.com/c/en/us/support/docs/ip/ip-routing/200158-Configure-Route-Leaking-between-Global-a.html>

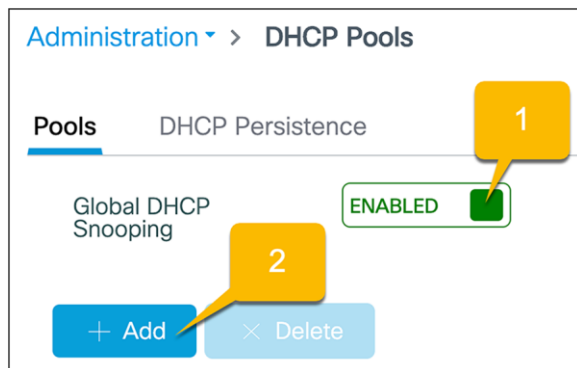
## Create corporate and guest DHCP pools

The corporate and guest Dynamic Host Configuration Protocol (DHCP) pools can be located anywhere in the network, but for the purposes of this guide, the DHCP pools will be located on a 9300 Series switch.

Navigate to **Administration** → **DHCP Pools**.



Ensure that Global DHCP Snooping is **Enabled** and click **Add** to create the corporate DHCP pool.



Configure the corporate DHCP pool with the required settings for the corporate network and click **Apply to Device**. Repeat these steps to create the guest DHCP pool.

Create DHCP Pool

Basic Advanced

DHCP Pool Name\* VLAN100\_Corporate (1-236 Characters)

IP Type IPv4

Network\* 192.168.100.1

Subnet Mask\* 255.255.255.0

Starting ip\* 192.168.100.1

Ending ip\* 192.168.100.254

Reserved Only DISABLED

Lease\* Never Expires

(0-365 days) (0-23 hours) (0-59 minutes)

Enable DNS Proxy ☐

Default Router(s)

IP Address	Remove
192.168.100.1	X

DNS Server(s)

IP Address	Remove
8.8.8.8	X

NetBios Name Server(s)

IP Address	Remove
No items to display	

Domain cisco.com

Cancel Apply to Device

If either or both of the corporate and guest networks are put into VRFs other than the default VRF, ensure that the DHCP server as well as other shared services, such as DNS, are reachable from the VRF. In the case where the DHCP server is located on the EWC switch, the DHCP pool for the required VLAN will need to be associated with the VRF. Additionally, DHCP snooping for the required VLAN will need to be configured (see the note below).

- **Note:** In Release 17.3, the DHCP pool and VRF association is done via CLI. Below is an example of the DHCP configuration for the corporate network on VLAN 100 in the corporate VRF.

```
configure terminal
ip dhcp snooping vlan 100
ip dhcp pool Corporate_100
vrf Corporate
```

Route leaking will need to be configured in order for the DHCP server as well as other shared services, such as DNS, to be reached by the devices in the VRFs.

---

## Configure 802.1X security

If the deployment requires 802.1X security, the EWC supports authentication done locally on the switch as well as through an external Authentication, Authorization, and Accounting (AAA) server.

### Local EAP authentication

For deployments without an external AAA server, 802.1X security can be done locally on the switch by configuring local Extensible Authentication Protocol (EAP) authentication.

To configure this option on the EWC, please follow the guide here:

<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/215026-local-eap-authentication-on-catalyst-980.html>

### Authentication with external AAA server

Using an external AAA server, such as Cisco Identity Services Engine (ISE), will allow for dynamic VLAN assignments as well as Access Control Lists (ACL) and QoS policies based on the user's role. This is one of the few ways to allow for role segmentation, as the EWC on Catalyst switches does not support Scalable Group Tag (SGT) segmentation.

For instructions on how to configure ISE users and policies, see:

<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213919-configure-802-1x-authentication-on-catal.html>

## Create a guest access captive portal (optional)

Before guests can access the network, you can have them be redirected to a webpage where they can be authenticated. The authentication methods are:

- WebAuth: This is a basic web authentication. The controller presents a policy page with the username and password. You need to enter the correct credentials to access the network.
- Consent or web-passthrough: The controller presents a policy page with the Accept or Deny buttons. Users need to click the Accept button to access the network.
- Webconsent: This is a combination of the WebAuth and consent web authentication types. The controller presents a policy page with Accept or Deny buttons along with username or password. Users need to enter the correct credentials and click the Accept button to access the network.

Follow the steps in the link below to configure this option:

[https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-3/config-guide/b\\_wl\\_17\\_3\\_cg/m\\_vewlc\\_sec\\_webauth\\_cg.html](https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-3/config-guide/b_wl_17_3_cg/m_vewlc_sec_webauth_cg.html)

## Create Access Control Lists (ACLs)

For more information on configuring ACLs, see the following link:

[https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-3/config-guide/b\\_wl\\_17\\_3\\_cg/m\\_conf\\_ipv4\\_acl\\_ewlc.html](https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-3/config-guide/b_wl_17_3_cg/m_conf_ipv4_acl_ewlc.html)

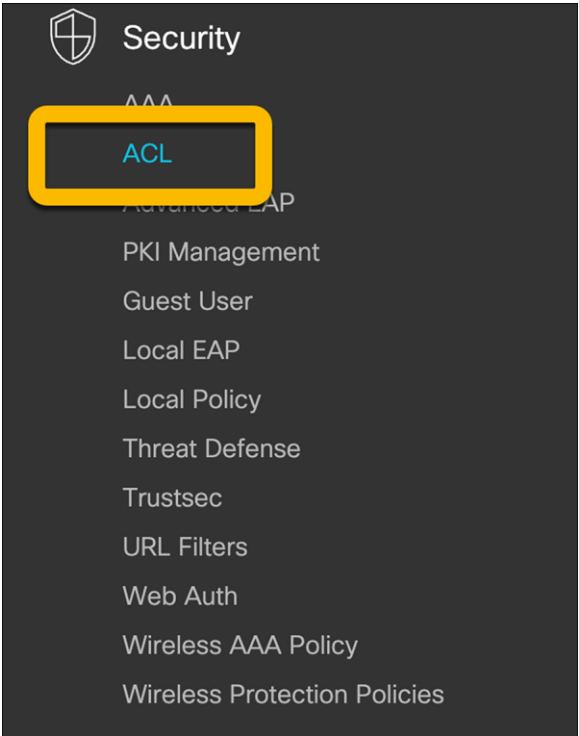
For cases in which separate VRFs will not be configured for the different networks, ACLs can be configured to keep the networks from communicating.

Additionally, these can be used to prevent networks or devices within the same VRF from communicating.

Below is an example of ACLs used to prevent the AP management, corporate, and guest networks from communicating when they are all within the same VRF.

**ACL to prevent communication between the AP management, corporate, and guest networks**

Navigate to **Configuration → Security → ACL**.



On the ACL page, click **Add**.

Configuration > Security > ACL

+ Add

✖ Delete

✎ Associate Interfaces

	ACL Name	ACL Type	ACE Count	Downloaded ACL
<input type="checkbox"/>	meraki-fqdn-dns	IPv4 Extended	0	No
<input type="checkbox"/>	implicit_deny	IPv4 Extended	1	No
<input type="checkbox"/>	implicit_permit	IPv4 Extended	1	No
<input type="checkbox"/>	implicit_deny_v6	IPv6	1	No



Configure the corporate ACL to meet the requirements of the network. Click **Apply to Device** when done.  
An example of a corporate ACL is shown below.

**Add ACL Setup**

ACL Name\*  ACL Type

Rules

Sequence\*  Action

Source Type

Destination Type

Protocol

Log ☐ DSCP

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
<input type="checkbox"/> 10	deny	192.168.100.0	0.0.0.255	192.168.101.0	0.0.0.255	ip	None	None	None	Disable
<input type="checkbox"/> 15	deny	192.168.101.0	0.0.0.255	192.168.100.0	0.0.0.255	ip	None	None	None	Disable
<input type="checkbox"/> 20	deny	192.168.100.0	0.0.0.255	10.10.10.0	0.0.0.255	ip	None	None	None	Disable
<input type="checkbox"/> 25	deny	10.10.10.0	0.0.0.255	192.168.100.0	0.0.0.255	ip	None	None	None	Disable
<input type="checkbox"/> 30	permit	192.168.100.0	0.0.0.255	any		ip	None	None	None	Disable
<input type="checkbox"/> 40	deny	any		any		ip	None	None	None	Disable

1 - 6 of 6 items

Block Corporate Network and Guest Network communication.

Block Corporate Network and AP Mgmt Network communication.

Repeat the steps to configure the guest ACL to meet the requirements of the network.  
Click **Apply to Device** when done.  
An example of a guest ACL is shown below.

Add ACL Setup

ACL Name\*
Guest\_ACL

ACL Type
IPv4 Extended

Rules

Sequence\*

Source Type
any

Destination Type
any

Protocol
ahp

Log
☐

Action
permit

DSCP
None

Add
Delete

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
<input type="checkbox"/> 10	deny	192.168.101.0	0.0.0.255	192.168.100.0	0.0.0.255	ip			None	Disable
<input type="checkbox"/> 15	deny	192.168.100.0	0.0.0.255	192.168.101.0	0.0.0.255	ip			None	Disable
<input type="checkbox"/> 20	deny	192.168.101.0	0.0.0.255	10.10.10.0	0.0.0.255	ip			None	Disable
<input type="checkbox"/> 25	deny	10.10.10.0	0.0.0.255	192.168.101.0	0.0.0.255	ip			None	Disable
<input type="checkbox"/> 30	permit	192.168.101.0	0.0.0.255	any		ip			None	Disable
<input type="checkbox"/> 40	deny	any		any		ip			None	Disable

1
10 items per page
1 - 6 of 6 items

Cancel
Apply to Device

Block Corporate Network and Guest Network communication.

Block Guest Network and AP Mgmt Network communication.

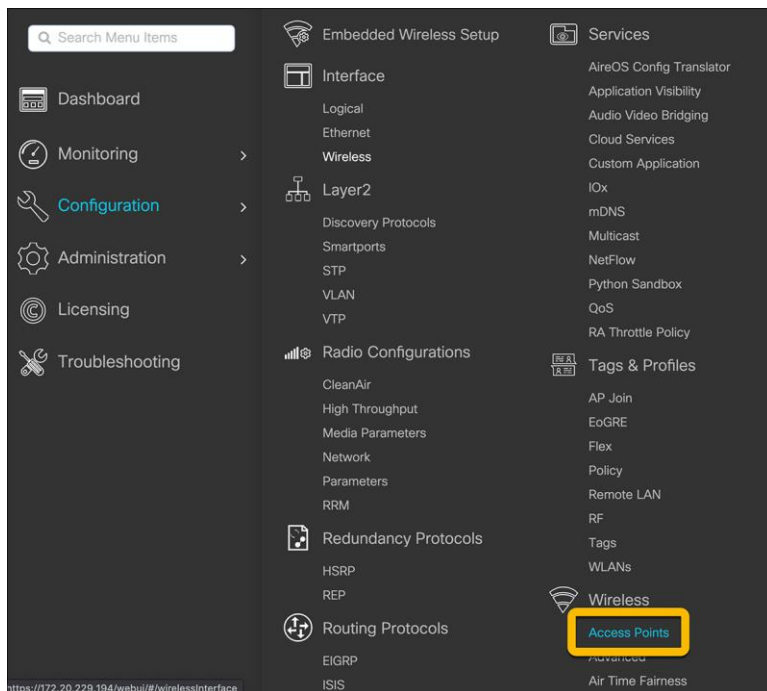
## Set country codes for APs

To ensure that each radio's broadcast frequency bands, interfaces, channels, and transmit power levels are compliant with country-specific regulations, the country that the EWC will be used in must be set.

- Note:** For Release 17.3, set the country code through the Command-Line Interface (CLI) with the following commands:

```
configure terminal
wireless country <Country-Code>
```

Navigate to **Configuration → Wireless → Access Points**.



In the Country section, select the applicable country from the table and click **Apply**. This ensures that the APs that join the EWC will be in compliance with the selected country.

Country

Click [here](#) for list of access point models and protocols supported per country and regulatory domain.

Selected Country

Regulatory Domain 802.11a/n/ac: [ Indoor: , Outdoor: ]

802.11b/g/n: [ Indoor: , Outdoor: ]

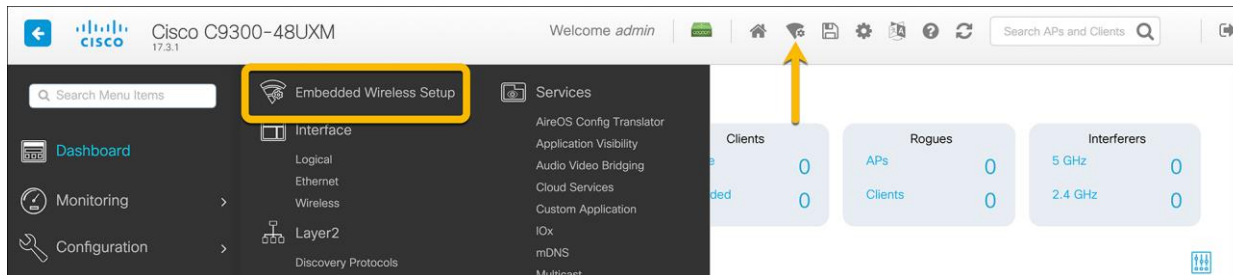
	Country Code	Name
<input type="checkbox"/>	SA	Saudi Arabia
<input type="checkbox"/>	SE	Sweden
<input type="checkbox"/>	SG	Singapore
<input type="checkbox"/>	SI	Slovenia
<input type="checkbox"/>	SK	Slovak Republic
<input type="checkbox"/>	TH	Thailand
<input type="checkbox"/>	TI	Trinidad
<input type="checkbox"/>	TN	Tunisia
<input type="checkbox"/>	TR	Turkey
<input checked="" type="checkbox"/>	US	United States
<input type="checkbox"/>	UY	Uruguay
<input type="checkbox"/>	VE	Venezuela
<input type="checkbox"/>	VN	Vietnam
<input type="checkbox"/>	ZA	South Africa

2

Apply

## Enable the embedded wireless setup

The EWC supports only the location-based workflow to configure the wireless networks. This is similar to the Basic Setup workflow on the Catalyst 9800 appliances. To access the workflow, navigate to the EWC configuration page by going to **Configuration → Embedded Wireless Setup** or clicking the **wireless icon** in the dashboard.

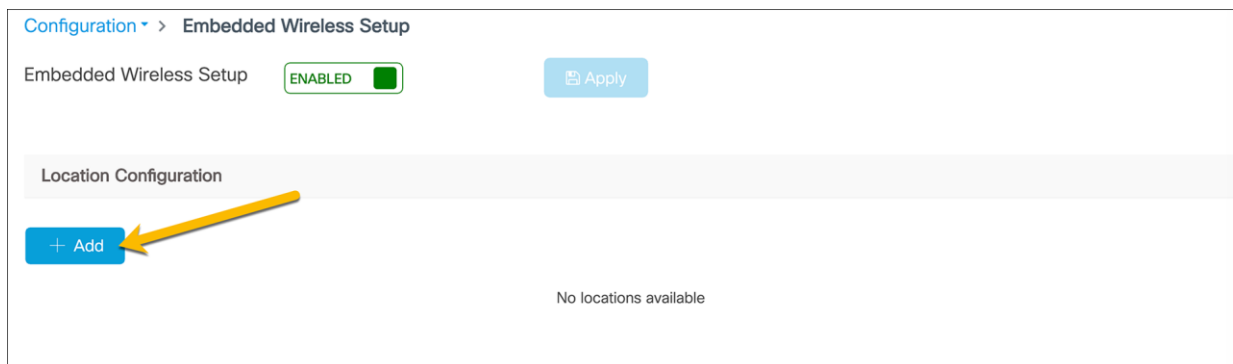


If the loopback address is configured, there will be a toggle for enabling and disabling the EWC. Set the toggle to **Enabled** and click **Apply**.



Click the **Add** button to create a new location.

- **Note:** The EWC supports only a single location. When clicking the **Add** button after a location has been configured, the WebUI will redirect to the settings page for the existing location.



Enter the **Location Name**, **Client Density**, and **AP Onboarding** details. Click **Apply**.

- **Note:** The AP Onboarding VLAN ID is required to be between 2045 and 4094 to be consistent with the INFRA VLAN requirements. The VLAN chosen for the APs should be different than the VLANs used for clients.

Configuration > Embedded Wireless Setup

Location Configuration

Back Delete Location

General Wireless Networks AP Provisioning

Location Name\* SanJose

Description Enter Description

Client Density 
◀
▶
Low
Typical
High

AP Onboarding

VLAN\* 2045

IP Address\* 10.10.10.1

Subnet Mask\* 255.255.255.0

DHCP Server\* 10.0.1.1

Apply

## Create a corporate wireless network

Go to the **Wireless Networks** tab and click **Add**.

Configuration > Embedded Wireless Setup

Location Configuration

Back Delete Location

General **Wireless Networks** AP Provisioning

+ Add Delete

WLANs on this Location

WLAN Name	VRF
<span>◀ ▶ 0 ▶▶</span> <span style="margin-left: 10px;">10 items per page</span> <span style="float: right;">No items to display</span>	

In the Add Location Setup window, click **Define new** to create the corporate WLAN.

Add Location Setup

Wireless Network Details Policy Details

WLAN\* Search or Select ▼ or Define new

VRF\* DEFAULT\_VN ▼  
[Click here to add VRF](#)

VLAN\* Add or Select ▼

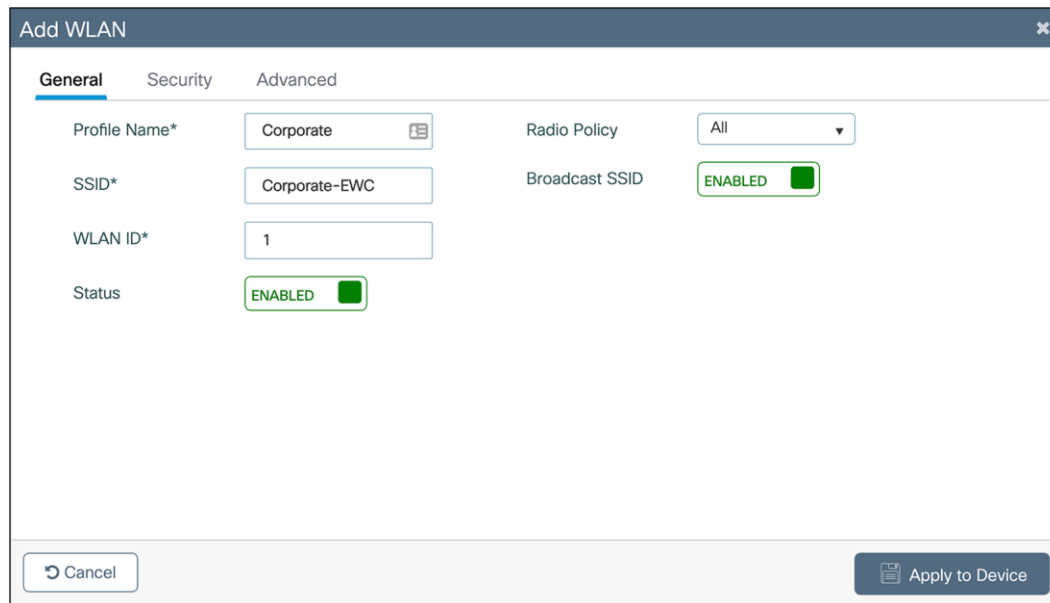
QoS Search or Select ▼

Close Add

## Corporate WLAN configuration

### General tab configuration

In the **Add WLAN** window, set the **Profile Name**, **SSID**, and **WLAN ID** as well as toggling the Status to **Enabled**.



The screenshot shows the 'Add WLAN' configuration window with the 'General' tab selected. The window has three tabs: 'General', 'Security', and 'Advanced'. The 'General' tab contains the following fields and controls:

- Profile Name\***: A text field containing 'Corporate' with a dropdown arrow icon.
- Radio Policy**: A dropdown menu set to 'All'.
- SSID\***: A text field containing 'Corporate-EWC'.
- Broadcast SSID**: A toggle switch labeled 'ENABLED' with a green indicator.
- WLAN ID\***: A text field containing '1'.
- Status**: A toggle switch labeled 'ENABLED' with a green indicator.

At the bottom of the window, there are two buttons: 'Cancel' on the left and 'Apply to Device' on the right.

### WLAN security configuration

#### Pre-shared key

Go to the **Security** → **Layer2** tab and configure the Layer 2 security.

1. Set the Layer 2 Security Mode to WPA2 + WPA3.
2. Set Fast Transition to Enabled.
3. Set the Auth Key Management to SAE and FT + PSK.
4. Set the corporate WLAN password.
5. Click Apply to Device.

Add WLAN

General

Security

Advanced

Layer2

Layer3

AAA

Layer 2 Security Mode

WPA2 + WPA3

Lobby Admin Access

☐

MAC Filtering

☐

Fast Transition

Enabled

Protected Management Frame

Over the DS

☐

PMF

Optional

Reassociation Timeout

20

Association Comeback Timer\*

1

MPSK Configuration

SA Query Time\*

200

MPSK

☐

WPA Parameters

WPA Policy

☐

WPA2 Policy

☒

GTK Randomize

☐

WPA3 Policy

☒

WPA2/WPA3 Encryption

☒ AES(CCMP128)

☐ CCMP256

☐ GCMP128

☐ GCMP256

Auth Key Mgmt

☐ 802.1x

☐ PSK

☐ CCKM

☒ SAE

☐ OWE

☐ FT + 802.1x

☒ FT + PSK

☐ 802.1x-SHA256

☐ PSK-SHA256

Anti Clogging Threshold\*

1500

Max Retries\*

5

Retransmit Timeout\*

40

PSK Format

ASCII

PSK Type

Unencrypted

Pre-Shared Key\*

corporate-psk

Cancel

Apply to Device

## 802.1X security

Go to the **Security** → **Layer2** tab and configure the Layer 2 security.

1. Set the Layer 2 Security Mode to **WPA2 + WPA3**.
2. Set Fast Transition to **Adaptive Enabled**.
3. Set the Auth Key Management to **802.1x**.
4. Click Apply to Device.

**Add WLAN**

General **Security** Advanced

**Layer2** Layer3 AAA

Layer 2 Security Mode: WPA2 + WPA3

MAC Filtering: ☐

Protected Management Frame

PMF: Optional

Association Comeback Timer\*: 1

SA Query Time\*: 200

WPA Parameters

WPA Policy: ☐

WPA2 Policy: ☒

GTK Randomize: ☐

WPA3 Policy: ☒

WPA2/WPA3 Encryption: ☒ AES(CCMP128)  
☐ CCMP256  
☐ GCMP128  
☐ GCMP256

Auth Key Mgmt: ☒ 802.1x  
☐ PSK  
☐ CCKM  
☐ SAE  
☐ OWE  
☐ FT + 802.1x  
☐ FT + PSK  
☐ 802.1x-SHA256  
☐ PSK-SHA256

Lobby Admin Access: ☐

Fast Transition: Adaptive Enabled

Over the DS: ☐

Reassociation Timeout: 20

MPSK Configuration

MPSK: ☐

Cancel Apply to Device



## Local EAP authentication

Go to the **Security** → **AAA** tab.

1. Set the Authentication List to the configured local AAA authentication method.
2. Check Local EAP Authentication.
3. Select the configured EAP Profile Name.
4. Click Apply to Device.

The screenshot shows the 'Add WLAN' configuration window with the 'Security' tab selected. Under the 'AAA' sub-tab, the 'Authentication List' is set to 'default' (callout 1), 'Local EAP Authentication' is checked (callout 2), and the 'EAP Profile Name' is set to 'Local-EAP' (callout 3). At the bottom right, the 'Apply to Device' button is highlighted with callout 4. A 'Cancel' button is located at the bottom left.

## Authentication with an external AAA server

Go to the **Security** → **AAA** tab.

1. Set the Authentication List to the ISE AAA authentication method that was configured in the “Configure 802.1X security – Authentication with external AAA server” section.
2. Click Apply to Device.

The screenshot shows the 'Add WLAN' configuration window with the 'Security' tab selected. Under the 'AAA' section, the 'Authentication List' dropdown menu is set to 'ISE-Authentication'. A callout labeled '1' points to this dropdown. Below it, 'Local EAP Authentication' is unchecked. At the bottom right, the 'Apply to Device' button is highlighted with a callout labeled '2'. A 'Cancel' button is located at the bottom left.

### Corporate wireless policy details

In the Add Location window, set the required **VRF**, **VLAN**, and **QoS** details. Click **Add**.

- **Note:** The VLAN for the corporate clients should be different than the VLAN for AP onboarding. Also, ensure that the corporate VLAN has IP connectivity from the EWC to the rest of the network. If the corporate network is placed in a VRF other than the default VRF, the Switch Virtual Interface (SVI) for the corporate VLAN will need to be manually added to the corporate VRF.

Enter a VLAN that does not exist on the switch and does not have an SVI configured. If the corporate VLAN and SVI have not yet been configured, the details can be added in this window. Otherwise, if both the VLAN and SVI are configured, select the VLAN from the drop-down menu.

- **Note:** The switch comes preconfigured with four different QoS policies that will prioritize different traffic types.
  - Platinum: Used for VoIP clients
  - Gold: Used for video clients
  - Silver: Used for traffic that can be considered best effort
  - Bronze: Used for Non-Real-Time (NRT) traffic

To create custom QoS and AVC polices, please see:

[https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-3/config-guide/b\\_wl\\_17\\_3\\_cg/m\\_wireless\\_qos\\_cg\\_vewlc.html](https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-3/config-guide/b_wl_17_3_cg/m_wireless_qos_cg_vewlc.html)

×

Add Location Setup

Wireless Network Details

Policy Details

WLAN\*

Corporate

▼

or [Define new](#)

VRF\*

Corporate

▼

[Click here to add VRF](#)

VLAN\*

100

⌵

IP Address\*

192.168.100.1

Subnet Mask\*

255.255.255.0

DHCP Server\*

10.0.1.1

QoS

platinum

▼

×

Close

✓ Add

## Create a guest wireless network

The EWC on Catalyst switches does not support being used as a guest anchor nor as a guest foreign controller. All guest network configurations will be done on the EWC on the switch.

While still in the **Wireless Networks** tab, create the guest WLAN by clicking **Add**.

General

**Wireless Networks**

AP Provisioning

+ Add

× Delete

WLANs on this Location

WLAN Name

☐ Corporate

⏪

⏩

1

⏪

⏩

10

▼

items per page

In the Add Location Setup window, click **Define new** to create the guest WLAN.

×

Add Location Setup

Wireless Network Details

Policy Details

WLAN\*

Search or Select

▼

or [Define new](#)

VRF\*

DEFAULT\_VN

▼

[Click here to add VRF](#)

VLAN\*

Add or Select

⌵

QoS

Search or Select

▼

×

Close

✓ Add

## Guest WLAN configuration

### General tab configuration

In the **Add WLAN** window, set the **Profile Name**, **SSID**, and **WLAN ID** as well as toggling the Status to **Enabled**.

The screenshot shows the 'Add WLAN' configuration window with the 'General' tab selected. The window has a title bar 'Add WLAN' with a close button. Below the title bar are three tabs: 'General', 'Security', and 'Advanced'. The 'General' tab contains the following fields and controls:

- Profile Name\***: A text input field containing 'Guest' and a small icon to its right.
- SSID\***: A text input field containing 'Guest-EWC'.
- WLAN ID\***: A text input field containing '2'.
- Status**: A toggle switch labeled 'ENABLED' with a green square indicator.
- Radio Policy**: A dropdown menu showing 'All'.
- Broadcast SSID**: A toggle switch labeled 'ENABLED' with a green square indicator.

At the bottom of the window, there are two buttons: 'Cancel' on the left and 'Apply to Device' on the right.

### WLAN security configuration

#### Pre-shared key

Go to the **Security** → **Layer2** tab and configure the Layer 2 security.

1. Set the Layer 2 Security Mode to **WPA2 + WPA3**.
2. Set Fast Transition to **Enabled**.
3. Set the Auth Key Management to **SAE** and **FT + PSK**.
4. Set the Guest WLAN password.

Add WLAN

General

Security

Advanced

Layer2

Layer3

AAA

Layer 2 Security Mode

WPA2 + WPA3

1

Lobby Admin Access

☐

MAC Filtering

☐

Fast Transition

2

Enabled

Protected Management Frame

Over the DS

☐

Reassociation Timeout

20

PMF

Optional

MPSK Configuration

MPSK

☐

Association Comeback Timer\*

1

SA Query Time\*

200

WPA Parameters

WPA Policy

☐

WPA2 Policy

☒

GTK Randomize

☐

WPA3 Policy

☒

WPA2/WPA3 Encryption

☒ AES(CCMP128)

☐ CCMP256

☐ GCMP128

☐ GCMP256

Auth Key Mgmt

☐ 802.1x

☐ PSK

☐ CCKM

☒ SAE

☐ OWE

☐ FT + 802.1x

☒ FT + PSK

☐ 802.1x-SHA256

☐ PSK-SHA256

Anti Clogging Threshold\*

1500

Max Retries\*

5

Retransmit Timeout\*

40

PSK Format

ASCII

PSK Type

Unencrypted

Pre-Shared Key\*

guest-psk

4

Cancel

Apply to Device

## WebAuth captive portal

Go to the **Security** → **Layer2** tab.

1. Set the Layer 2 Security Mode to **None**.
2. Set Fast Transition to **Adaptive Enabled**.
3. Uncheck OWE Transition Mode.

**Add WLAN**

General **Security** Advanced

Layer2 **Layer3** AAA

Layer 2 Security Mode: None (1)

MAC Filtering: ☐

OWE Transition Mode: ☐ (3)

Lobby Admin Access: ☐

Fast Transition: Adaptive Enabled (2)

Over the DS: ☐

Reassociation Timeout: 20

Cancel Apply to Device

Go to the **Security** → **Layer3** tab.

1. Check the **Web Policy** option.
2. Choose the Web Auth Parameter Map that was configured.
3. If you will be having users log in using the captive portal, select the configured, local Authentication List.

**Add WLAN**

General **Security** Advanced

Layer2 **Layer3** AAA

Web Policy: ☒ (1)

Web Auth Parameter Map: global (2)

Authentication List: default (3)

Show Advanced Settings >>>

*For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device*

Cancel Apply to Device

## Prevent guest hosts from communicating with each other

Go to the **Advanced** tab.

1. Set P2P Blocking Action to **Drop**.
2. Click Apply to Device.

The screenshot shows the 'Add WLAN' configuration window with the 'Advanced' tab selected. The 'P2P Blocking Action' is set to 'Drop'. The 'Apply to Device' button is highlighted with a yellow callout '2'.

### Guest wireless policy details

In the Add Location window, set the required **VRF**, **VLAN**, and **QoS** details. Click **Add**.

- **Note:** The VLAN for the guest clients should be different than the VLAN for AP onboarding. Also, ensure that the guest VLAN has IP connectivity from the EWC to the rest of the network. If the guest network is placed in a VRF other than the default VRF, the SVI for the guest VLAN will need to be manually added to the guest VRF.

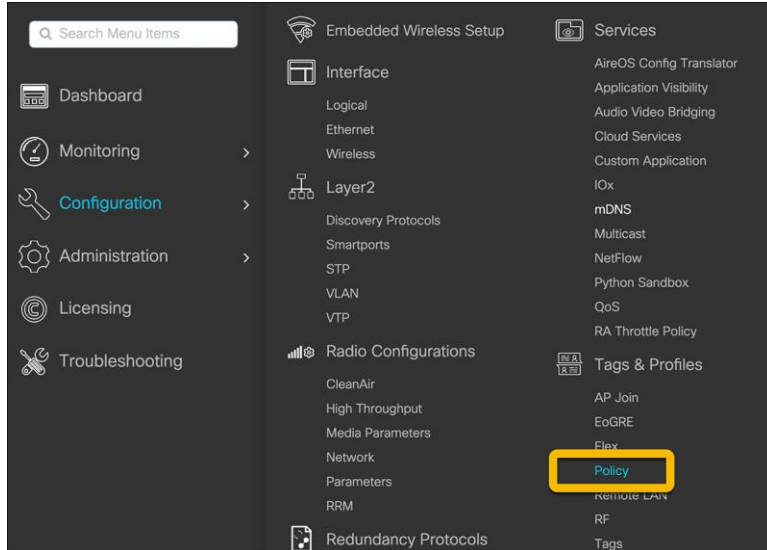
Enter a VLAN that does not exist on the switch and does not have an SVI configured. If the guest VLAN and SVI have not yet been configured, the details can be added in this window. Otherwise, if both the VLAN and SVI are configured, select the VLAN from the drop-down menu.

The screenshot shows the 'Add Location Setup' configuration window. The 'Wireless Network Details' section shows 'WLAN\*' set to 'Guest'. The 'Policy Details' section shows 'VRF\*' set to 'Guest', 'VLAN\*' set to '101', 'IP Address\*' set to '192.168.101.1', 'Subnet Mask\*' set to '255.255.255.0', 'DHCP Server\*' set to '10.0.1.1', and 'QoS' set to 'platinum'. The 'Add' button is highlighted.

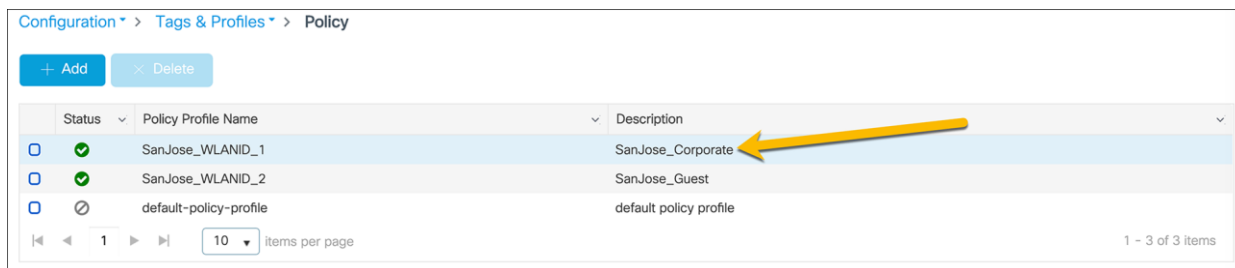
## Apply ACLs to WLANs

For cases in which networks for WLANs are in the same VRF and are not allowed to communicate, apply the created ACLs to the respective WLANs.

Navigate to **Configuration → Tags and Profiles → Policy**.



Select the policy name that matches the WLAN that requires an ACL.





Go to the **Access Policies** tab in the Edit Profiles window.

1. Set the **IPv4 ACL** to the ACL for the network.
2. Click Update and **Apply to Device**.

The screenshot shows the 'Edit Policy Profile' window with the 'Access Policies' tab selected. The window has a header bar with tabs: General, Access Policies, QOS and AVC, Mobility, and Advanced. The 'Access Policies' tab is active. On the left, there are sections for 'RADIUS Profiling' (with checkboxes for HTTP TLV Caching and DHCP TLV Caching), 'WLAN Local Profiling' (with 'Global State of Device Classification' set to 'Disabled'), and 'VLAN' (with 'VLAN/VLAN Group' set to '1' and a 'Multicast VLAN' field). On the right, there are sections for 'WLAN ACL' (with 'IPv4 ACL' set to 'Corporate\_ACL' and 'IPv6 ACL' set to 'Search or Select'), and 'URL Filters' (with 'Pre Auth' and 'Post Auth' both set to 'Search or Select'). At the bottom, there is a 'Cancel' button and an 'Update & Apply to Device' button. Two yellow callouts are present: callout '1' points to the 'IPv4 ACL' dropdown, and callout '2' points to the 'Update & Apply to Device' button.

Repeat the steps for all the other required networks.

## Onboard and provision wireless access points

### Setting up network topology

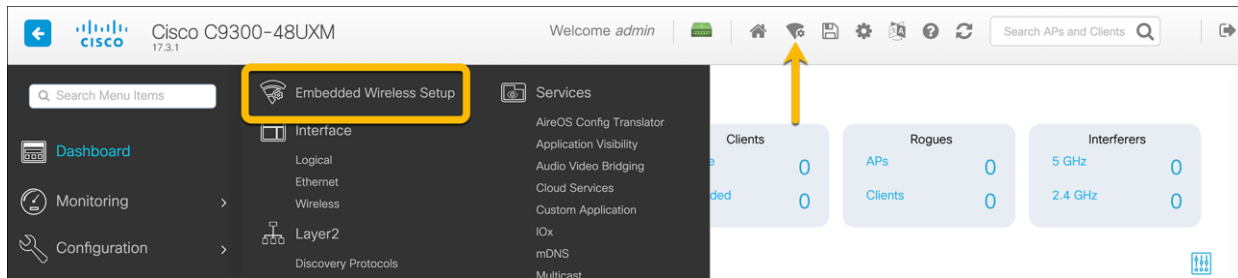
In order for the access points to discover and join the EWC, they need to be assigned to the same VLAN that was configured for the AP onboarding. The AP onboarding VLAN should be in the GRT of the EWC even when multiple VRFs are configured. Additionally, if the DHCP server for the AP onboarding is located on a device other than the EWC, ensure that it is reachable by the access points during the DHCP request.

If the APs are directly connected to the EWC switch, the switch ports where the APs are connected can be assigned to correct VLAN.

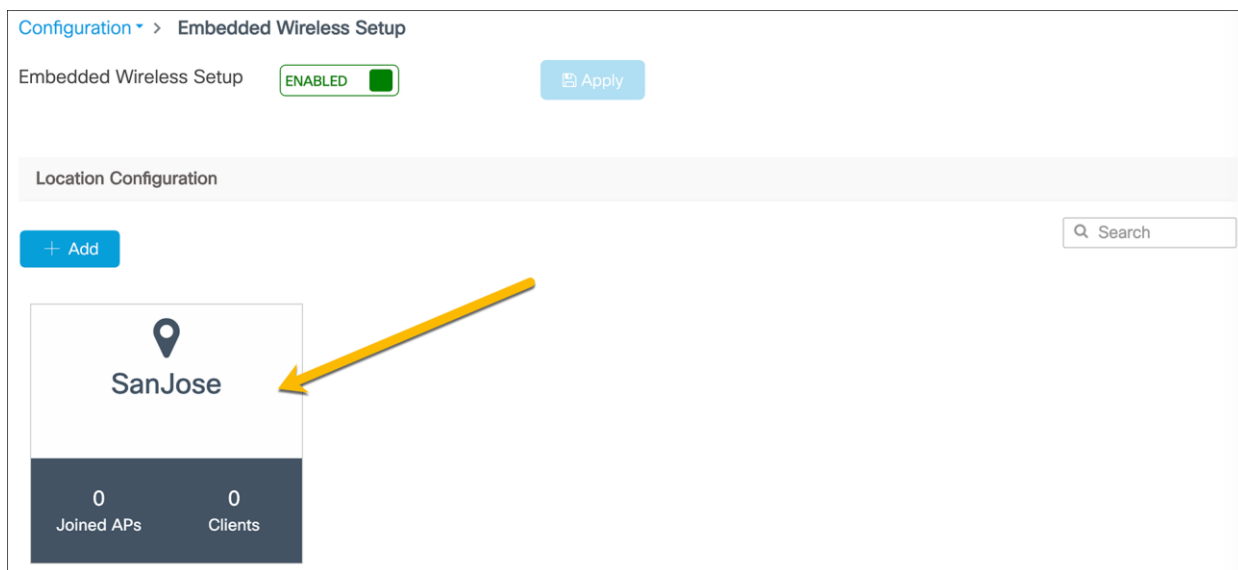
Otherwise, if there are intermediate switches between the EWC and the access points, the connections between the EWC switch and intermediate switches need to be Layer 2 connections with the appropriate VLAN trunking configured. Since the APs are required to be on the AP onboarding VLAN, the VLAN ID for all traffic sent between the AP and EWC needs to be preserved. If there are any Layer 3 hops between the AP and EWC, the AP onboarding VLAN ID of the traffic is lost, preventing the AP from joining the APs.

## Tagging the access points

Navigate to the EWC configuration page by going to **Configuration → Embedded Wireless Setup** or clicking the **wireless icon** in the dashboard.



Select the created site.



Go to the **AP Provisioning** tab.

1. Select the APs from the list to add to the site.
  - **Note:** If the access points are not appearing in the **Available AP List**, this means they have not successfully joined the EWC by creating the CAPWAP tunnels. Once the APs have successfully joined, they will appear in the **Available AP List**. If the APs do not automatically populate the list, refresh the page. If the APs have joined, they will now appear.
2. Click the blue arrow icon to add them to the associated AP list.

General Wireless Networks **AP Provisioning**

Add/Select APs

Import AP MAC

Select File
Select CSV File

AP MAC Address

Available AP list

Search

Number of selected APs : 1

☒

AP MAC	AP Name
<input checked="" type="checkbox"/> 2cf8.9b5f.a26c	AP-EWC-Switch-1

1
5... items per page
1 - 1 of 1 items

The AP status should say **Joined**, indicating the AP has formed the CAPWAP tunnel with the AP. To tag the AP and add it to the configured location, click **Apply**.

- **Note:** The APs that are added may need to have the correct software version installed and will be reloaded.

APs on this Location

Apply

Associated AP list

Search

Number of selected APs : 0

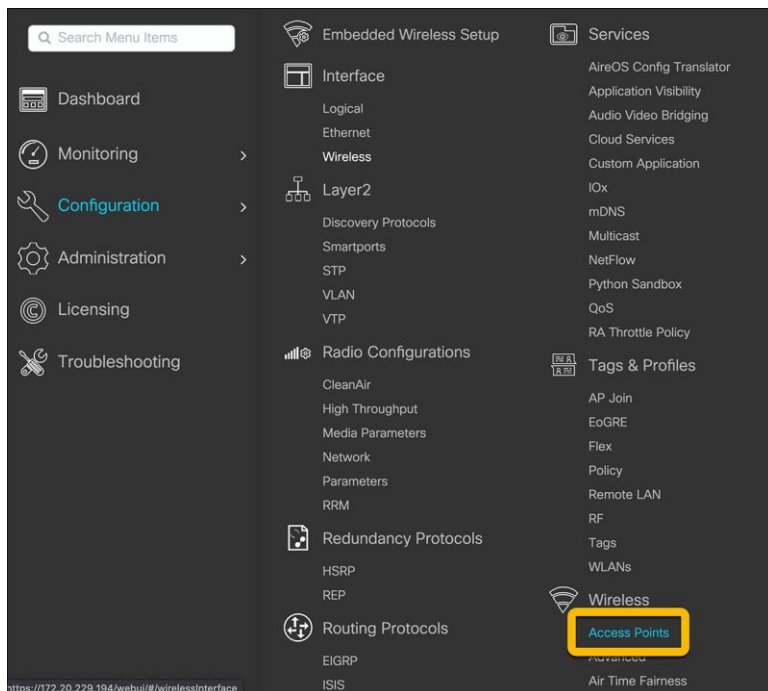
☐

AP MAC	AP Name	Status
<input type="checkbox"/> 2cf8.9b5f.a26c	AP-EWC-Switch-1	Joined

1
5... items per page
1 - 1 of 1 items

The APs will then be tagged with the necessary policy, site, and RF tags for the location. Through the location-based workflow, these are automatically created.

To verify that the APs have been successfully added, go to **Configuration → Wireless → Access Points**.



For the APs that were added, check that the tags match those of the site.

▼ All Access Points

Number of AP(s): 1

AP Name	AP Model	Slots	Admin Status	IP Address	Base Radio MAC	AP Mode	Operation Status	Configuration Status	Policy Tag	Site Tag	RF Tag
AP-EWC-Switch-1	C9120AXI-B	2	✓	10.10.10.4	084f.f982.e500	Local	Registered	Healthy	SanJose	default-site-tag	SanJose

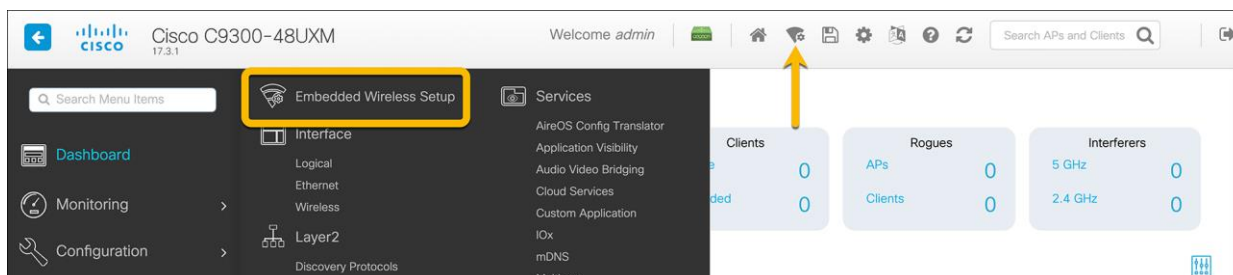
1 - 1 of 1 access points

## Other methods of adding APs

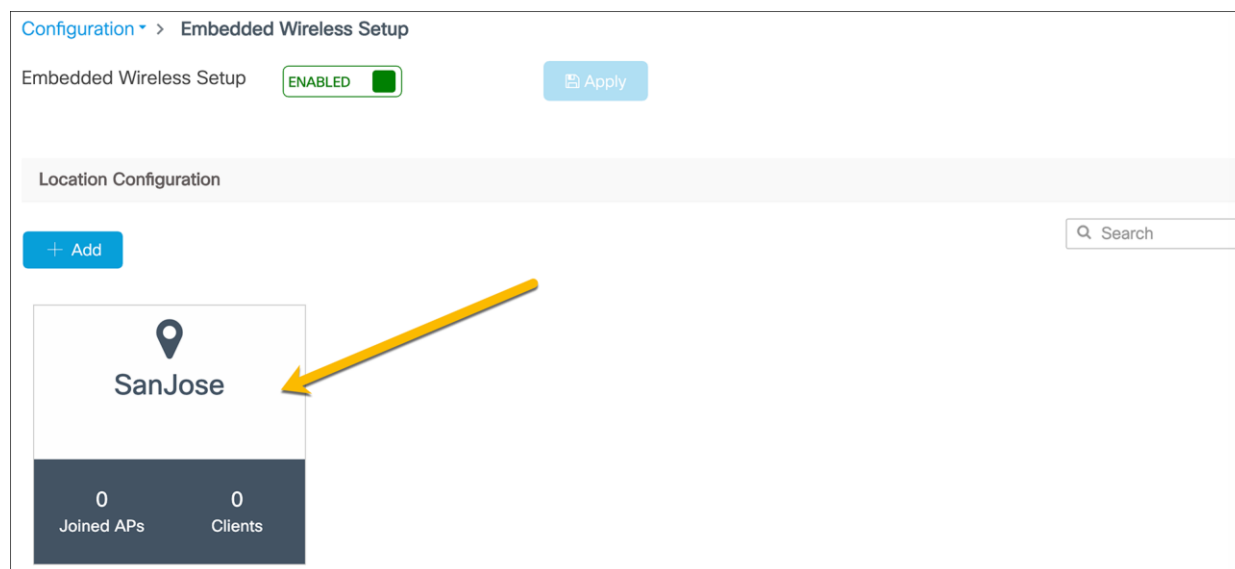
### CSV file upload for AP tagging

If multiple APs need to be added to the site at one time, they can be added using a CSV file of all the APs' MAC addresses. With this method, the AP does not need to be joined with the EWC to be tagged and added to the site. Upon joining the EWC, the AP will automatically be tagged.

Navigate to the EWC configuration page by going to **Configuration → Embedded Wireless Setup** or clicking the **wireless icon** in the dashboard.

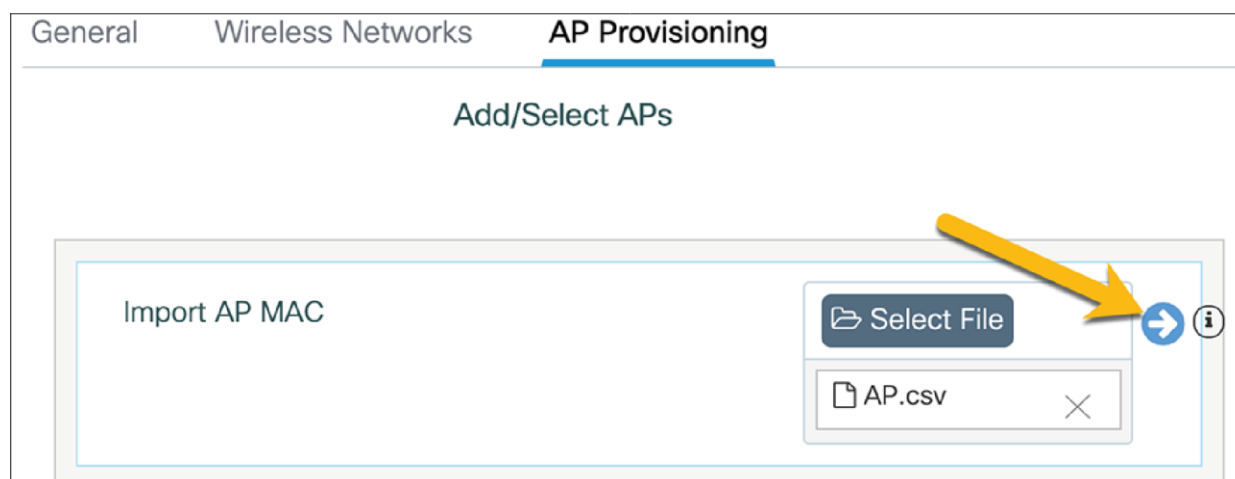


Select the created site.



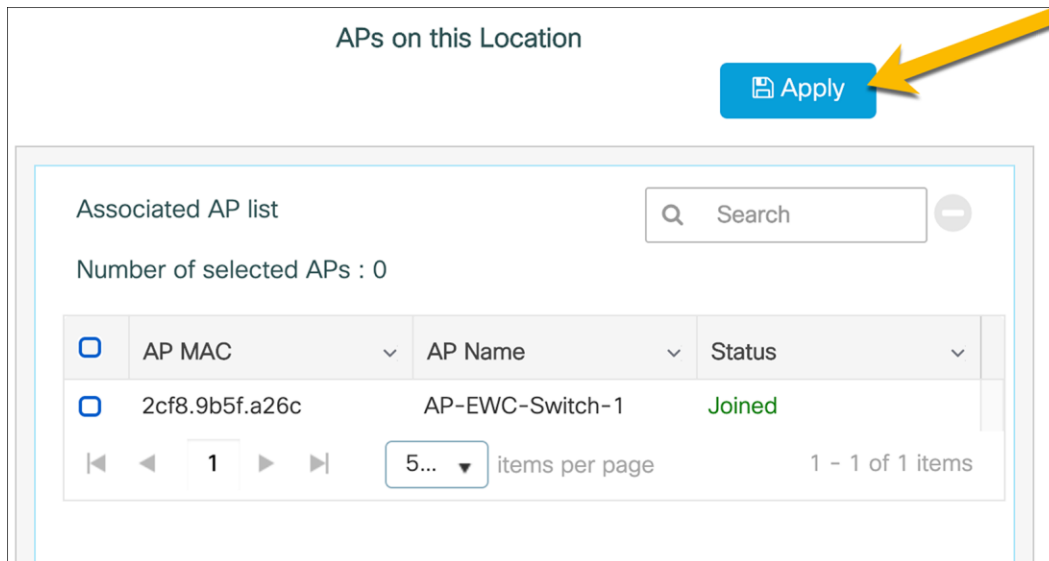
Go to the **AP Provisioning** tab.

Upload the CSV file and click the **blue arrow** to add the APs to the location.

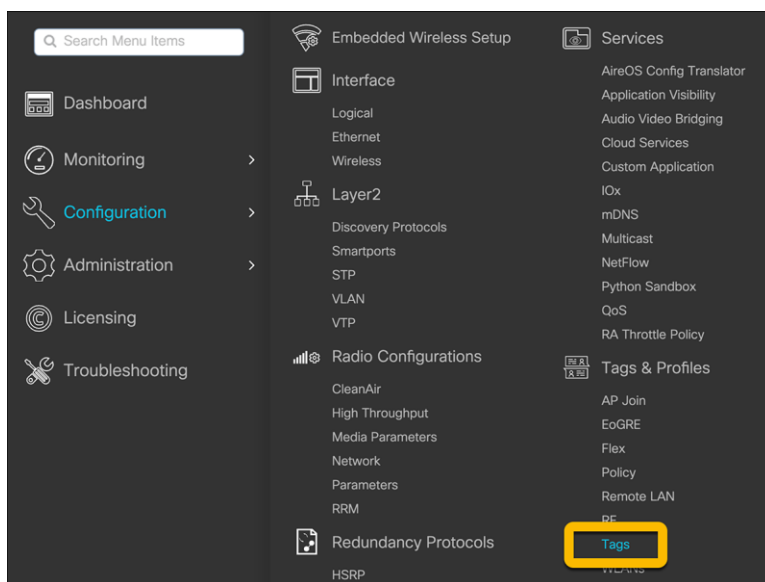


Click **Apply** to add the APs to the site.

- **Note:** The APs that are added may need to have the correct software version installed and will be reloaded.



CSV files can also be uploaded by going to **Configuration → Tags and Profiles → Tags**. This will allow for multiple APs to be added to different locations.



Go to the **AP** tab and the **Static** subtab. Upload a CSV file. The file can have the following columns: AP MAC address, Policy Tag name, Site Tag name, and RF Tag name. The only mandatory column is the AP MAC address. If the policy, site, and RF tags are included in the file, the APs will be automatically mapped with those tags, and once the APs join the EWC they will be correctly tagged. If they are not included, the AP will be mapped to the default policy, site, and RF tags.

The steps to change the AP tag mappings from the default tags to the required tags are shown below.

Configuration > Tags & Profiles > Tags

Policy Site RF **AP**

Tag Source **Static** Filter

[+ Add](#) [- Delete](#)

[Select File](#) [Upload File](#)

AP.csv

Number of AP Tag mappings selected : 0

<input type="checkbox"/>	AP MAC Address	Policy Tag Name	Site Tag Name	RF Tag Name
No items to display				

10 items per page

Select each of the APs and assign the required **policy**, **site**, and **RF** tags.

Tag Source **Static** Filter

[+ Add](#) [- Delete](#)

[Select File](#) [Upload File](#)

Select CSV File

Number of AP Tag mappings selected : 0

<input type="checkbox"/>	AP MAC Address	Policy Tag Name	Site Tag Name	RF Tag Name
<input checked="" type="checkbox"/>	2cf8.9b5f.a24f	default-policy-tag	default-site-tag	default-rf-tag

10 items per page 1 - 1 of 1 items

Edit Tags

AP MAC Address\* 2cf8.9b5f.a24f

Policy Tag Name SanJose

Site Tag Name default-site-tag

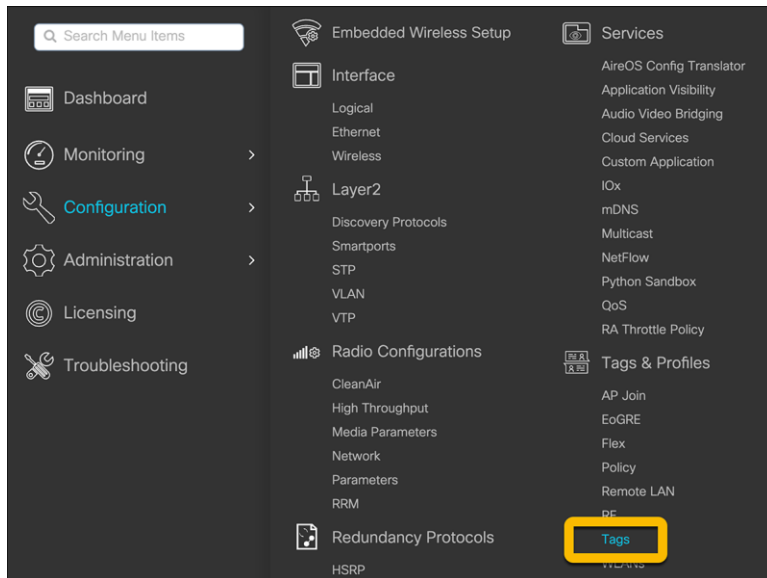
RF Tag Name SanJose

[Cancel](#) [Update & Apply to Device](#)

## Regular expressions (regex) rules for AP tagging

APs can also be added to the site by using regex rules based on the AP name. Depending on the AP name, it will be tagged with the necessary tags upon joining the EWC. As with the CSV file upload method, the AP does not need to be joined with the EWC to tag and assign it to the location.

Navigate to **Configuration** → **Tags and Profile** → **Tags**.



Go to the **AP** tab and the Filter subtab. Click **Add**.

Policy Site RF **AP**

Tag Source Static **Filter**

**+ Add** **Delete**

Priority	Rule Name	AP name regex	Policy Tag Name	Site Tag Name	RF Tag Name
0					

10 items per page No items to display

In the Associate Tags to AP window, fill out the requisite **AP name regex\*** rules to match the AP name and associate the appropriate **Policy**, **Site**, and **RF** tags for the APs. Click **Apply to Device**.

**Associate Tags to AP**

Rule Name\* San Jose Rules Policy Tag Name SanJose

AP name regex\* AP-SanJose-\* Site Tag Name default-site-tag

Active YES RF Tag Name SanJose

Priority\* 1

Cancel Apply to Device



## Note: WLAN VLANs

Due to the EWC being deployed in fabric mode and the data plane using VXLAN, when the VLAN is viewed in the WLAN policy, the VLAN group does not match what was previously configured.

Edit Policy Profile

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

RADIUS Profiling ☐

HTTP TLV Caching ☒

DHCP TLV Caching ☒

**WLAN Local Profiling**

Global State of Device Classification Disabled ⓘ

Local Subscriber Policy Name Search or Select ▼

**VLAN**

VLAN/VLAN Group 1 ▼

Multicast VLAN Enter Multicast VLAN

**WLAN ACL**

IPv4 ACL Guest\_ACL ▼

IPv6 ACL Search or Select ▼

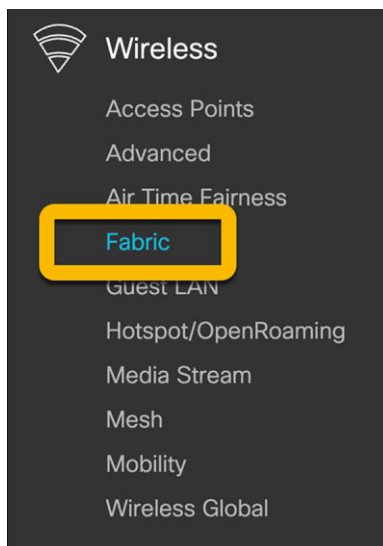
**URL Filters**

Pre Auth Search or Select ▼

Post Auth Search or Select ▼

Cancel Update & Apply to Device

To verify that the VLAN matches what was previously configured, go to **Configuration → Wireless → Fabric**.



In the **General** tab, there is a list of the fabric VNID mappings. The naming convention is <location>\_<WLAN\_ID>\_<VLAN>\_<L3\_VNID>\_<L2\_VNID>. The names below will show the correct VLAN associated with WLANs configured.

- **Note:** The Layer 3 VNID will match what was configured for the VRF.

**General** Control Plane Profiles

Fabric Status ENABLED Apply

Fabric VNID Mapping

+ Add × Delete

Name	L2 VNID	L3 VNID	IP Address	Netmask
<input type="checkbox"/> SanJose_1_100_10_8190	8190	0		
<input type="checkbox"/> SanJose_2_101_20_8191	8191	0		
<input type="checkbox"/> APONBOARDING_0_2045_4097_8188	8188	4097	10.10.10.0	255.255.255.0

1 10 items per page 1 - 3 of 3 items

**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)