# Configuring Wi-Fi 6



# Wireless Device Overview

Cisco Embedded Wireless Controller on Catalyst Access Points are the next generation of wireless controllers built for the Intent-based networking. The Cisco controllers are IOS XE-based and integrates the RF Excellence from Cisco Catalyst 9105AX Series Access Points with Intent-based Networking capabilities of IOS XE to create the best-in-class wireless experience for your evolving and growing organization.

With a management system based on Cisco IOS XE software, wireless devices are Wi-Fi CERTIFIED™, 802.11a-compliant, 802.11b-compliant, 802.11g-compliant, and 802.11n-compliant wireless LAN transceivers.

By adhering to the 802.11ax Wave 2 standard, the Cisco 1100 Series WLAN offers a data rate of up to 1.488Gbps on the 5-GHz radio. This exceeds the data rates offered by access points that support the 802.11n standard.

The configuration data model is based on design principles of reusability, simplified provisioning, enhanced flexibility and modularization to help manage networks as they scale up and simplify the management of dynamically changing business and IT requirements.

# Wireless Connectivity for Cisco 1100 Series ISR

This module describes how to configure the WiFi card to the internal switch interface on the Cisco C1100 Integrated Services Routers (ISRs).

The WiFi card is connected to the internal switch interface, the *Wlan-GigabitEthernet* interface. The configuration of this interface is identical to the *GigabitEthernet 0/1/0* interface.

For Cisco 1131 and C1131X Series of ISRs, it is always *Wlan-GigabitEthernet 0/1/8*.

```
Router# show run int Wlan-GigabitEthernet 0/1/8
Building configuration...
```

```
Current configuration : 67 bytes
!
interface Wlan-GigabitEthernet0/1/8
switchport mode access

end
```

# Module Managment

The router configures, manages, and controls the supported interfaces and modules using the module management facility built in its architecture. This new centralized module management facility provides a common way to control and monitor all the modules in the system regardless of their type and application.

## Slot and Subslots for WLAN

This section contains information on slots and subslots for WLAN. Slots specify the chassis slot number in your router and subslots specify the slot where the service modules are installed.

The table below describes the slot number for the Cisco 1100 Series ISR models.

***Table 1: Slot Numbers for Cisco 1100 Series ISR Models***

| Cisco 1100 Series SKU | WiFi Slot |
|---|---|
| C1131X-8PLTEPWx | 0/3 |
| C1131-8PLTEPWx | 0/3 |
| C1131X-8PWx | 0/2 |
| C1131-8PWx | 0/2 |

## Supported WiFi Cards

The supported WiFi card Product IDs (PIDs) are as follows:

- ISR-AP1100AX-A
- ISR-AP1100AX-B
- ISR-AP1100AX-E
- ISR-AP1100AX-Q
- ISR-AP1100AX-Z

```
Router#show platform

Chassis type: C1131X-8PLTEPWB

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         C1131X-8PLTEPWB     ok                    3w2d
 0/0      C1131X-2x1GE        ok                    3w2d
```

```
 0/1      C1131X-ES-8         ok                   3w2d
 0/3      ISR-AP1101AX-B      out of service       19:03:2
R0        C1131X-8PLTEPWB     ok, active           3w2d
F0        C1131X-8PLTEPWB     ok, active           3w2d
P0        PWR-12V             ok                   3w2d

Slot      CPLD Version        Firmware Version
--------- ------------------- ---------------------------------------
0         21052400            17.6.0
R0        21052400            17.6.0
F0        21052400            17.6.0
```

# Implementing Modules on Your Router



## Accessing Your Module Through a Console Connection

Before you can access the modules, you must connect to the host router through the router console or through Telnet. After you are connected to the router, you must configure an IP address on the Gigabit Ethernet interface connected to your module. Open a session to your module using the **hw-module session** command in privileged EXEC mode on the router.

To establish a connection to the module, connect to the router console using Telnet or Secure Shell (SSH) and open a session to the switch using the **hw-module session** *slot/subslot* command in privileged EXEC mode on the router.

Use the following configuration examples to establish a connection:

- The following example shows how to open a session from the router using the **hw-module session** command:

```
Router# hw-module session slot/card
Router# hw-module session 0/2 endpoint 0

Establishing session connect to subslot 0/2
```

- The following example shows how to exit a session from the router, by pressing **Ctrl-A** followed by **Ctrl-Q** on your keyboard:

```
type ^a^q
picocom v1.7

port is        : /dev/ttyS3
flowcontrol    : none
baudrate is    : 9600
parity is      : none
databits are   : 8
escape is      : C-a
local echo is  : no
noinit is      : no
noreset is     : no
nolock is      : yes
send_cmd is    : sz -vv
receive_cmd is : rz -vv
imap is        :
omap is        :
emap is        : crcrlf,delbs,
```

```
Terminal ready
```

## Deactivating a Module

A module can be removed from the router without first being deactivated. However, we recommend that you perform a graceful deactivation (or graceful power down) of the module before removing it. To perform a graceful deactivation, use the **hw-module subslot** *slot/subslot* **stop** command in EXEC mode.

**Note** When you are preparing for an OIR of a module, it is not necessary to independently shut down each of the interfaces before deactivating the module. The **hw-module subslot** *slot/subslot* **stop** command in EXEC mode automatically stops traffic on the interfaces and deactivates them along with the module in preparation for OIR. Similarly, you do not have to independently restart any of the interfaces on a module after OIR.

The following example shows how to use the **show facility-alarm status** command to verify if any critical alarm is generated when a module is removed from the system:

```
Device# show facility-alarm status
System Totals  Critical: 8  Major: 0  Minor: 0

Source                          Time                Severity         Description [Index]
------                        --------              --------         -------------------
Power Bay 0                Dec 01 2021 07:21:41       INFO           Power Ethernet Module
 Missing [0]
xcvr container 0/0/1       Dec 01 2021 07:22:28       INFO           Transceiver Missing
[0]
GigabitEthernet0/1/0       Dec 01 2021 07:21:57       CRITICAL       Physical Port Link
Down [1]
GigabitEthernet0/1/1       Dec 01 2021 07:21:57       CRITICAL       Physical Port Link
Down [1]
GigabitEthernet0/1/2       Dec 01 2021 07:21:57       CRITICAL       Physical Port Link
Down [1]
GigabitEthernet0/1/3       Dec 01 2021 07:21:57       CRITICAL       Physical Port Link
Down [1]
GigabitEthernet0/1/4       Dec 01 2021 07:21:57       CRITICAL       Physical Port Link
Down [1]
GigabitEthernet0/1/5       Dec 01 2021 07:21:57       CRITICAL       Physical Port Link
Down [1]
GigabitEthernet0/1/6       Dec 01 2021 07:21:57       CRITICAL       Physical Port Link
Down [1]
GigabitEthernet0/1/7       Dec 01 2021 07:21:57       CRITICAL       Physical Port Link
Down [1]
```

**Note** A critical alarm (Active Card Removed OIR Alarm) is generated even if a module is removed after performing graceful deactivation.

## Deactivating Modules and Interfaces in Different Command Modes

You can deactivate a module and its interfaces using the **hw-module subslot** command in one of the following modes:

- If you choose to use the **hw-module subslot** *slot/subslot* **stop** command in EXEC mode, you cause the module to gracefully shut down. The module is rebooted when the **hw-module subslot** *slot/subslot* **start** command is executed.

To deactivate a module and all of its interfaces before removing the module, use one of the following commands in global configuration mode.

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **hw-module subslot** *slot*/*subslot* [**reload** \| **stop** \| **start**]<br>**Example:**<br>`Router# hw-module subslot 0/2 stop` | Deactivates the module in the specified slot and subslot, where:<br>• *slot*—Specifies the chassis slot number where the module is installed.<br>• *subslot*—Specifies the subslot number of the chassis where the module is installed.<br>• **reload**—Stops and restarts the specified module.<br>• **stop**—Removes all interfaces from the module and the module is powered off.<br>• **start**—Powers on the module similar to a physically inserted module in the specified slot. The module firmware reboots and the entire module initialization sequence is executed in the IOSd and Input/Output Module daemon (IOMd) processes. |

## Reactivating a Module

If, after deactivating a module using the **hw-module subslot** *slot/subslot* **stop** command, you want to reactivate it without performing an OIR, use one of the following commands (in privileged EXEC mode):

- **hw-module subslot** *slot/subslot* **start**
- **hw-module subslot** *slot/subslot* **reload**

# Deploying Cisco Embedded Wireless Controller (EWC)

## Prerequisites for Deploying Embedded Wireless Controller (EWC) Solution

1. It is recommended not to have any other Cisco Wireless LAN Controllers; neither appliance nor virtual in the same network during set up or during daily operation of a Cisco Embedded Wireless Controller (EWC) network.

2. Decide on the first Access Point to be configured as a primary Access Point. This Access Point should be capable of supporting the Wireless LAN Controller function.
3. A DHCP server must be available on the network so that Access Points and clients can obtain an IP Address. Starting from Cisco IOS XE Release 17.7.x or later, one can configure a DHCP server on the primaryAccess Point as well but this is typically used for Site Survey.
4. To configure the EWC and AP integrated into C1100 series router, you must configure a DHCP server, SVI interface, and NAT on the router. For more information on configuring the AP, see **Prerequisites for Configuring the AP on the Router** section.

# Prerequisites for Configuring the AP on the Router

To configure the global parameters for your router, follow these steps:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **ip dhcp pool** *name*<br>**Example:**<br>`Device(config)#ip dhcp pool wireless` | Use this command to create a name for the DHCP server address pool and to enter the DHCP pool configuration mode. |
| **Step 2** | **networkip address subnet mask**<br>**Example:**<br>`Router(dhcp-config)#network 10.10.10.0 255.255.255.0` | Use this command to create a DHCP pool of IP addresses to be used by the Switched Virtual Interface (SVI) (Refer Step 11 and further for SVI). |
| **Step 3** | **default-router ip address**<br>**Example:**<br>`Router(dhcp-config)#default-router 10.10.10.1` | Use this command to assign the default gateway to clients of this DHCP pool. |
| **Step 4** | **dns-serverip address**<br>**Example:**<br>`Router(dhcp-config)#dns-server 192.0.2.1` | Use this command to assign the DNS server IP address to clients in this DHCP pool. |
| **Step 5** | **interface GigabitEthernet** *slot/subslot/port*<br>**Example:**<br>`Router(config)#interface GigabitEthernet 0/0/0` | Use the **interface gigabitEthernet** command to add the interface and set the IP address. **0/0/0** is the slot/subslot/port. |
| **Step 6** | **ip address dhcp**<br>**Example:** | Use this command to configure the ip address using DHCP and static ip. |

| | Command or Action | Purpose |
|---|---|---|
| | `Router(config-if)#ip address dhcp` | |
| **Step 7** | **ip nat outside**<br>**Example:**<br>`Router(config-if)#ip nat outside` | Use this command to connect the interface to the outside network. |
| **Step 8** | **interface Wlan-GigabitEthernet** *slot/subslot/port*<br>**Example:**<br>`Router(config)#interface Wlan-GigabitEthernet 0/1/8` | Use the Wlan-GigabitEthernet command to connect the Wi-Fi card of the internal switch interface. |
| **Step 9** | **switchport accessvlan** *number*<br>**Example:**<br>`Router(config-if)#switchport access vlan 199` | Use the **switchport access vlan** command to assign the port or range of ports into access ports. |
| **Step 10** | **switchport modeaccess**<br>**Example:**<br>`Router(config-if)#switchport mode access` | Use the **switchport modeaccess** command to to configure the VLAN membership mode. |
| **Step 11** | **interface vlan** *number*<br>**Example:**<br>`Router(config)#interface vlan 199` | Use the **interface vlan** *number* command in the configuration mode tocreate a Switched Virtual Interface (SVI) and enter the interface configuration (VLAN) mode for a specific VLAN or a range of VLANs. |
| **Step 12** | **description name**<br>**Example:**<br>`Router(config-if)#description Wireless` | Use this command to add a description for the Switched Virtual Interface (SVI). |
| **Step 13** | **ip address** *ip-address***subnet_mask**<br>**Example:**<br>`Router(config-if)#ip address 10.10.10.1 255.255.255.0` | Use this command to assign an IP address from the DHCP Pool (**Refer Step 2**). |
| **Step 14** | **ip nat inside**<br>**Example:**<br>`Router(config)#ip nat inside` | Connects the interface to the inside network, which is subject to NAT. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 15** | **ip nat inside source list** *number* **interface GigabitEthernet** *slot/subslot/port* overload<br>**Example:**<br>`Router(config)#ip nat inside source list 10 interface GigabitEthernet 0/0/0 overload` | Use this command to establish dynamic source translation, specifying the access list. |
| **Step 16** | **ip route 10.10.10.10 10.10.10.10** *default gateway ip-address*<br>**Example:**<br>`Router(config)#ip route 10.10.10.10 10.10.10.10 192.0.2.1` | Use this command to direct all the traffic to the default gateway of the router. |
| **Step 17** | **ip access-list standard** *number*<br>**Example:**<br>`Router(config)#ip access-list standard 10` | Use the ip access-list standard command to filter the traffic based on a set of rules. |
| **Step 18** | **number permitip address wildcard mask**<br>**Example:**<br>`Router(config)#10 permit 10.10.10.0 0.0.0.255` | Use this command to create ACL entries to permit or deny traffic. |

# Configuring the AP Using Day 0 Provisioning

There are 3 ways to configure the AP using day 0 provisioning:

### Procedure

**Step 1** To connect the SSID to CiscoAirProvision-XXXX, follow the steps added here: https://www.cisco.com/c/en/us/products/collateral/wireless/embedded-wireless-controller-catalyst-access-points/white-paper-c11-743398.html#DeployingtheEWC

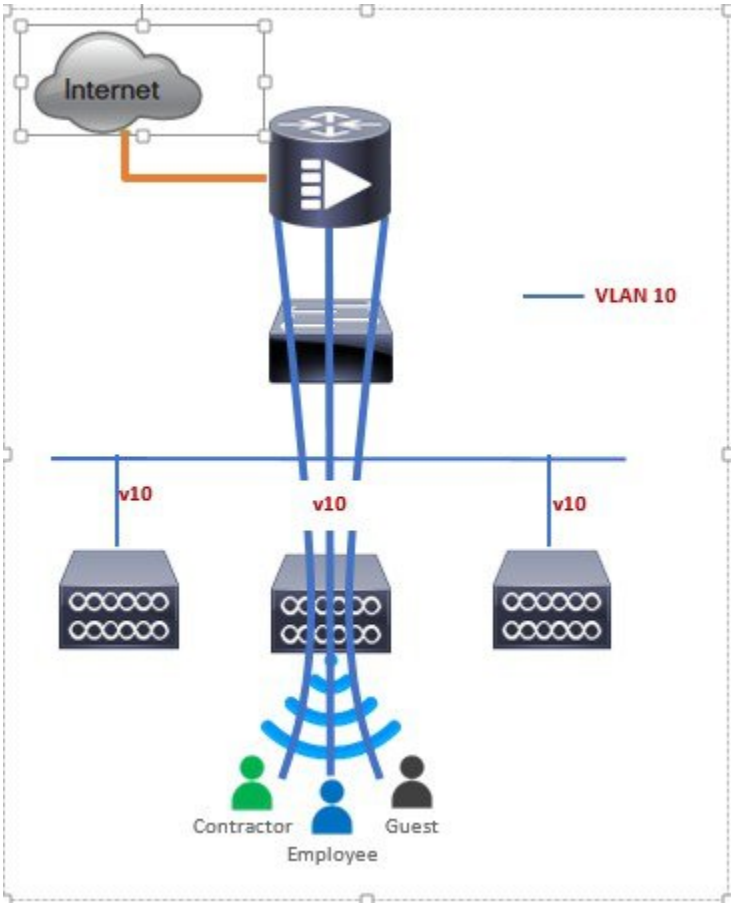
**Step 2** You can also scan the QR Code by using the Catalyst Wireless Application by following the steps added here: https://www.cisco.com/c/en/us/td/docs/wireless/controller/ewc/mob-app/user-guide/cisco_catalyst_wireless_app_user_guide/getting_started.html

**Step 3** You can manually configure the AP using CLI by following the steps added here: https://www.cisco.com/c/en/us/td/docs/wireless/controller/ewc/17-6/config-guide/ewc_cg_17_6/overview_of_the_controller.html#task_gs1_qzh_kpb

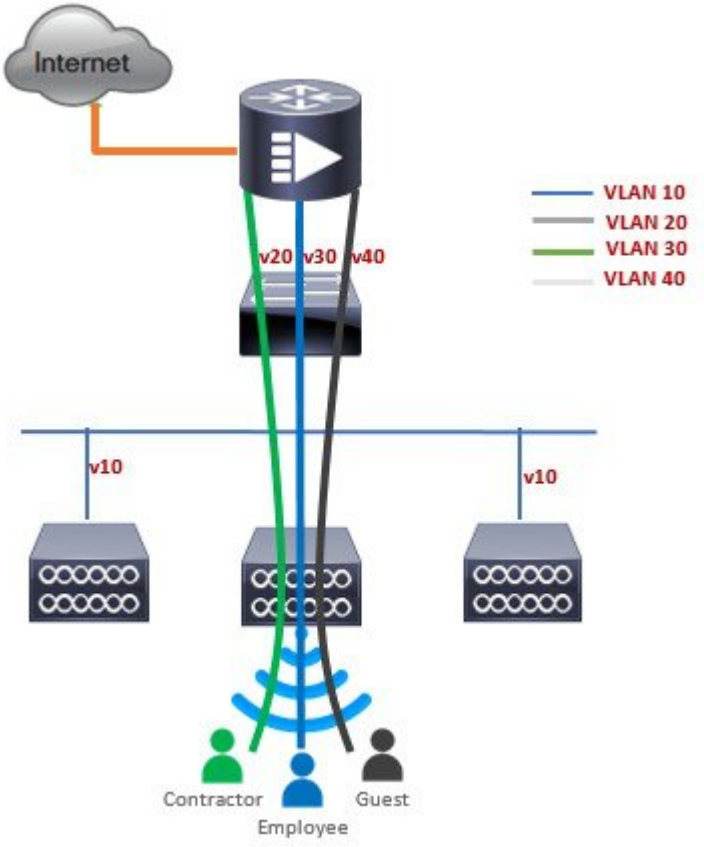
# Connecting Cisco Embedded Wireless Controller (EWC) Capable Access Point to the Network

Depending on the deployment, Embedded Wireless Controller (EWC) Capable Access Point to the Network capable Access Points can be connected to an access port or a trunk port on the switch.

If Access Points and WLANs are all on the same network, Embedded Wireless Controller (EWC) capable Access Points can connect to an access port on the switch as shown below.




On an Embedded Wireless Controller (EWC), management traffic is untagged. If Access Points and WLANs are all on different VLANs, the Embedded Wireless Controller (EWC) capable Access Points will connect to a trunk port on the switch and traffic for individual WLANs will be switched locally on individual VLANs. Shown below is a deployment with Access Points and WLANs on different VLANs.




```
interface Wlan-GigabitEthernet 0/1/8
description » Connected to Master AP «
switchport trunk native vlan 40
switchport trunk allowed vlan 10,20,30,40
switchport mode trunk
```

# Converting Access Point from CAPWAP to Cisco Embedded Wireless Controller (EWC)

One can convert an Access Point running CAPWAP to Embedded Wireless Controller (EWC) and vice versa.

Cisco Embedded Wireless Controller (EWC) support on 802.11ax Access Points is introduced in different IOS XE releases and it is important to note that before an Access Point can be converted to Cisco Embedded Wireless Controller (EWC), it must have the minimum IOS XE CAPWAP image which supports Cisco Embedded Wireless Controller (EWC) capability for that Access Point. Given below is the minimum IOS XE release for an Access Point which will support conversion from CAPWAP to Cisco Embedded Wireless Controller (EWC).

| Access Point | Minimum AireOS Release with CAPWAP image |
|---|---|
| Cisco 1100 Series | Cisco IOS XE Release 17.7.x |

Toperform a conversion on an Access Point running CAPWAP to Embedded Wireless Controller (EWC), follow the procedure below:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Download the conversion imagefor the Access Point from cisco.com to the TFTP server. It is a tar file. Do not untar the file. The following table lists the Cisco Embedded Wireless Controller (EWC) softwarefor Cisco Wireless Release IOS XE 17.7. | |
| **Step 2** | Login to the Access Point | |
| **Step 3** | Execute AP#show version on the Access Point CLI. From the show version output, you can determine the AP Image type and AP Configuration and can then proceed with the conversion | Case 1: If the APis running a CAPWAP image for the conversion, execute the command below:<br>`Router#ap-type ewc-ap tftp://<TFTP Server IP>/<ap image path> tftp://<TFTP Server IP>/<controller image path>`<br>Example:<br>`APC884.A110.0104#ap-type ewc-ap tftp://10.74.9.8/ap1g8-tar_CS00012204433_fix`<br><br>`tftp://10.74.9.8/test/C9800-AP-iosxe-wlc.bin`<br>`Starting download eWLC image tftp://10.74.9.8/userid/C9800-AP-iosxe-wlc.bin ...`<br>`It may take a few minutes. If longer, please abort command, check network and try again.`<br>`##########################################################`<br>`100.0%`<br>`Image download completed.`<br>`Checking ...OK`<br>`Checking image size...OK`<br>`Checking image family...OK`<br>`Verifying ...[*08/25/2021 08:18:20.6120] [*08/25/2021 08:18:20.6120] CAPWAP State: Discovery`<br>`[*08/25/2021 08:18:20.6650] Discovery Request sent to 255.255.255.255, discovery type UNKNOWN(0)`<br>`OK`<br>`Versioning ...ws_management_version: 17.08.01.0.144557`<br>`Successfully downloaded and setup eWLC image.`<br>`Starting download AP image tftp://10.74.9.8/ap1g8-tar_CS00012204433_fix ...`<br>`It may take a few minutes. If longer, please abort command, check network and try again.`<br>`##########################################################`<br>`100.0%`<br>`Image download completed.` |

| | Command or Action | Purpose |
|---|---|---|
| | | Upgrading ...<br>status 'upgrade.sh: Script called with args:[NO_UPGRADE]'<br>do NO_UPGRADE, part1 is active part<br>status 'upgrade.sh: Script called with args:[-c PREDOWNLOAD]'<br>do PREDOWNLOAD, part1 is active part<br>status 'upgrade.sh: Start doing upgrade arg1=PREDOWNLOAD arg2=,from_cli arg3= ...'<br>status 'upgrade.sh: Using image /tmp/cli_part.tar on ax-bcm32 ...'<br>status 'Image signing verify success.'<br>[8/25/2021 8:20:40] : WARNING! Program shadow retry exhausted on flash version 45<br>[8/25/2021 8:20:40] : Shadow is now in-synced with master<br>[8/25/2021 8:20:40] : Verifying against bundle image btldr.img...<br>shared_printenv updated<br>status 'upgrade.sh: ***** part to upgrade is part2 *******'<br>status 'upgrade.sh: AP version1: part2 , img 8.8.1.10'<br>status 'upgrade.sh: BOARD generic case execute'<br>status 'upgrade.sh: Untar /tmp/cli_part.tar to /bootpart/part2...'<br>status 'upgrade.sh: Sync image to disk...'<br>[*08/25/2021 08:19:49.2690]<br>[*08/25/2021 08:19:49.2690] CAPWAP State: Discovery<br>[*08/25/2021 08:19:49.2810] Discovery Request sent to 255.255.255.255, discovery type UNKNOWN(0)<br>status 'upgrade.sh: AP version2: part2 8.8.1.10, img 8.8.1.10'<br>status 'upgrade.sh: AP backup version: 8.8.1.10'<br>status 'upgrade.sh: Finished upgrade task.'<br>status 'upgrade.sh: Cleanup for do_upgrade...'<br>status 'upgrade.sh: /tmp/upgrade_in_progress cleaned'<br>status 'upgrade.sh: Cleanup tmp files ...'<br>status 'upgrade.sh: Script called with args:[ACTIVATE]'<br>do ACTIVATE, part1 is active part<br>status 'upgrade.sh: activate part2, set BOOT to part2'<br>status 'upgrade.sh: AP primary version after reload: 8.8.1.10'<br>status 'upgrade.sh: AP backup version after reload: 17.8.0.4'<br>Successfully setup AP image.<br>Archive done.<br>APC884.A110.0104#[*08/25/2021 |

| | Command or Action | Purpose |
|---|---|---|
| | | `08:20:04.3370] Config Factory Reset triggered: clear saved config files..` |
| **Step 4** | If this is the first Access Point in the network, it will start the controller function and will broadcast the CiscoAirProvison SSID. | |

# Converting Access Point from Cisco Embedded Wireless Controller (EWC) to CAPWAP

There are typically two reasons why one would want to convert an Access Point running Embedded Wireless Controller (EWC) image to CAPWAP. There are as follows:

1. You want to keep the Access Point in a Embedded Wireless Controller (EWC) deploymentbut do not want the Access point to participate in the primary election process upon a failover of the primary AP.
2. You want to migrate one or more Access Points with Embedded Wireless Controller (EWC) to an appliance or vWLC based deployment. (Refer step 1.a in the Prerequisites.

1. If your reason to convert to CAPWAP is 1 above, follow the procedure below:
   a. Login to the Access Point CLI either through console or SSH and go to exec mode. If you are trying to convert the primary AP to CAPWAP, then **hw-module session 0/x** will lead you to the controller CLI. To get to the AP CLI, type **wireless ewc-ap ap shell username [name]** where the default name is "**Cisco**" at the controller prompt and login to the Access Point shell.
   b. Execute **AP#ap-type capwap** CLI. This will change the AP Configuration to NOT Embedded Wireless Controller (EWC) and the Access Point will no longer participate in the primary election process.

# Determining image on the Access Point

TheCisco 1100 Series ISR access points can either have CAPWAP image or the Cisco Embedded Wireless Controller (EWC) image which is capable of running the virtual Wireless LAN controller function on the Access Point. By default, the C1131 AP is shipped with EWC pre-installed. The CCO image consists only of the EWC image. One can manually switch to CAPWAP mode.

To determine the image and capability of an Access Point, follow the procedure below:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Login to the Access Point CLI using a console and type **AP#show version** and check the full output of show version. The default login credentials are Username:**Cisco** and Password:**Cisco**. | |
| **Step 2** | If **show version** output does not display AP Image Type and AP Configuration parameters | `EWC#show version`<br>`Cisco IOS XE Software, Version 17.07.01`<br>`Cisco IOS Software [Cupertino], C9800-AP` |

| | Command or Action | Purpose |
|---|---|---|
| | as highlighted below, it means that the AP is running the CAPWAP image and a conversion to Cisco Embedded Wireless Controller (EWC) is required if you want to run the controller function on the Access Point. To convert from a CAPWAP Access Point to Embedded Wireless Controller (EWC), go to Conversion section. | Software<br>(C9800-AP-K9_IOSXE-UNIVERSALK9-M),<br>Version 17.7.1, RELEASE SOFTWARE (fc5)<br>Technical Support:<br>http://www.cisco.com/techsupport<br>Copyright (c) 1986-2021 by Cisco Systems,<br>Inc.<br>Compiled Sat 04-Dec-21 13:58 by mcpre<br><br>Cisco IOS-XE software, Copyright (c) 2005-2021 by cisco Systems, Inc. All rights reserved. Certain components of Cisco IOS-XE software are licensed under the GNU General Public License ("GPL") Version 2.0. The software code licensed under GPL Version 2.0 is free software that comes with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such GPL code under the terms of GPL Version 2.0. For more details, see the documentation or "License Notice" file accompanying the IOS-XE software, or the applicable URL provided on the flyer accompanying the IOS-XE software.<br><br>ROM: IOS-XE ROMMON<br>WLCC884.A110.045C uptime is 1 week, 3 days, 1 hour, 2 minutes<br>Uptime for this control processor is 1 week, 3 days, 1 hour, 8 minutes<br>System returned to ROM by reload<br>System image file is "/tmp/sw/rp/0/0/rp_wlc/mount/usr/binos/bin/linux_iosd-image"<br>Last reload reason: reload<br><br>This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption.<br><br>Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.<br><br>Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.<br><br>AIR License Level: AIR Network Essentials<br>Next reload AIR license Level: AIR |

| | Command or Action | Purpose |
|---|---|---|
| | | Network Essentials<br>cisco ISR-AP1101AX-K (VXE) processor (revision VXE) with 342303K bytes of memory.<br>Processor board ID 00<br>2048K bytes of non-volatile configuration memory.<br>1989868K bytes of physical memory.<br>100000K bytes of AP Images at ap_images:.<br>513300K bytes of Backup Controller Image at backup_image:.<br>7774207K bytes of virtual hard disk at bootflash:.<br>25000K bytes of Temp trace export at tmp_trace_export:.<br>Installation mode is BUNDLE<br><br>Configuration register is 0x2102 |

# Configuring Cisco Embedded Wireless Controller (EWC)

# Configuring the controller using day 0 wizard

To configure the Web user interface:

### Before you begin

- When the AP has rebooted in the Embedded Wireless Controller (EWC) mode, it broadcasts a provisioning SSID ending with the last digits of the MAC address. You can connect to provisioning SSID using the PSK **password**.
- You can then open a browser and be redirected to mywifi.cisco.com, which takes you to the AP web UI. Enter the username as **webui** and password as **cisco**.

**Note** The web redirection to the Embedded Wireless Controller (EWC) configuration portal only works if you are connected to the provisioning SSID. It does not work if your laptop is connected to another Wi-Fi network or on the wired network. You cannot configure the AP from the wired network even if you enter the EWC IP address when it is in day0 wizard provisioning mode

### Procedure

**Step 1** Log on to the controller and in the **Configuration Setup Wizard**, go to the **General Settings** page.

**Step 2** In the **Configuration Mode** option, select **Non Mesh** and enter the following fields:

a) **Host Name**: Enter the hostname.

b) **Note** As required by the End User License Agreement, please ensure appropriate country code selection so that the unleashed network does not violate local and national regulatory restrictions. Improper country code assignment can disrupt wireless transmissions and may result in government imposed penalties and sanctions on operators of wireless networks utilizing devices set to improper country codes.

**Country**: From the drop-down list, choose the appropriate country code.

c) In the **Management User Settings** section, enter the username and password.

d) In the **Wireless Management Settings** section, check the **DHCP** check box, to display the DHCP server IP address.

e) In the **Wireless Network** section, click **Add** to create at least one WLAN.

**Step 3** Click **Finish**.

# Using internal DHCP server on Cisco Mobility Express

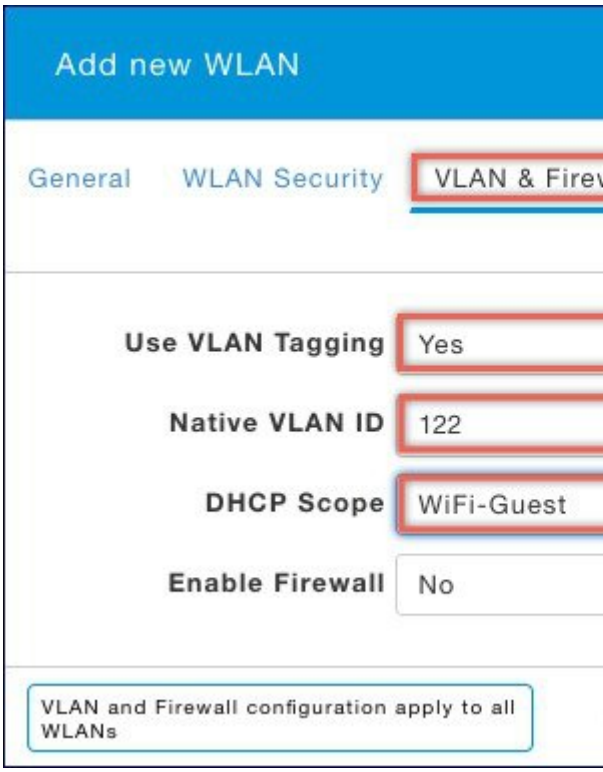
## Creating a DHCP Scope

Internal DHCP server can be enabled and DHCP scope created during Day 0 from Setup Wizard as well as in Day 1 using the controller WebUI. Typically, one would create DHCP scopes in Day 1 if they want to associate the scopes with WLANs.

To create a scope and associate it to a WLAN using the controller WebUI, follow the procedure below:

**Procedure**

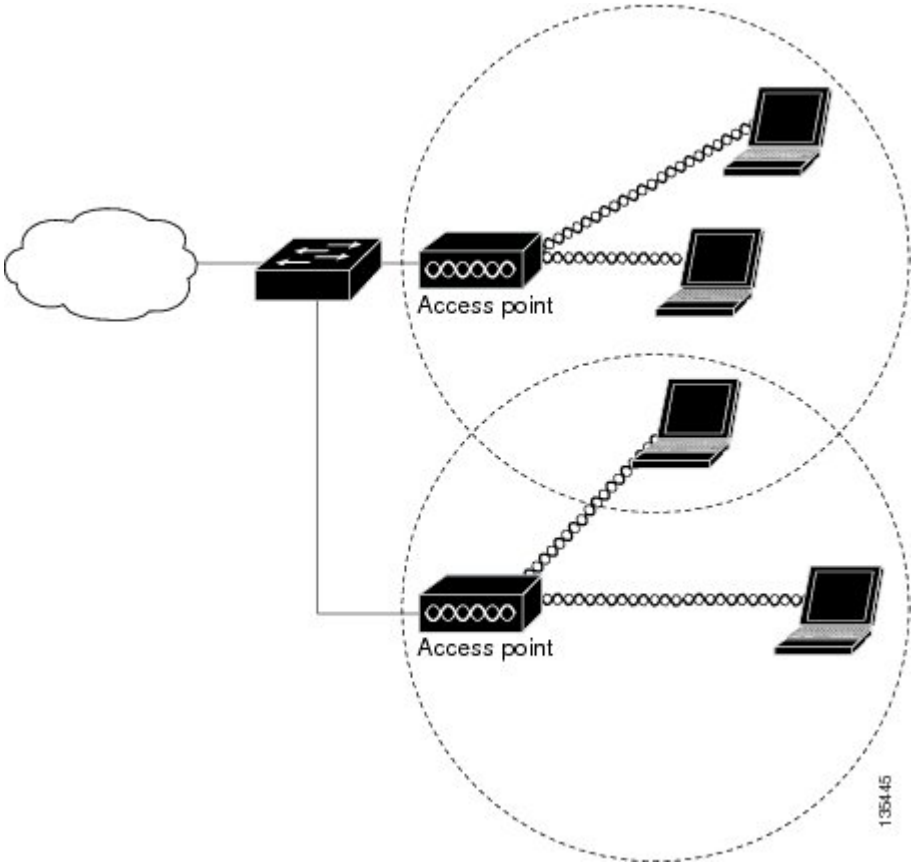
| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Navigate to Wireless Settings > DHCP Server > Add new Pool . The Add DHCP Pool window will pop up. | |
| **Step 2** | On the Add DHCP Pool window. Enter the following fields: | • Enter the Pool Name for the WLAN<br>• Enable the Pool Status<br>• Enter the VLAN ID for the WLAN<br>• Enter the Lease Period for the DHCP clients. Default is 1 Day<br>• Enter the Network/Mask<br>• Enter the Start IP for the DHCP pool<br>• Enter the End IP for the DHCP pool<br>• Enter the Gateway IP for the DHCP pool<br>• Enter the Domain Name (Optional) for the DHCP pool |

| | Command or Action | Purpose |
|---|---|---|
| | | • For Name Servers, select User Defined if one needs to enter IP addresses of Name Servers or select OpenDNS in which case OpenDNS Name Server IP addresses are automatically populated |
| **Step 3** | Click Apply. | |
| **Step 4** | After creating the scope, it is time to assign the VLAN mapped to the DHCP scope to the WLAN. To assign a VLAN to WLAN, navigate to Wireless Settings > WLANs . | |
| **Step 5** | If the WLAN does not exist, create a WLAN or if one does exist, edit the existing WLAN and click on the VLAN and Firewall tab. | |
| **Step 6** | On the VLAN and Firewall tab, configure the following: | • Select Yes for Use VLAN Tagging<br>• Enter the Native VLAN ID<br>• Select the DHCP Scope which was created previously for the WLAN. VLAN ID should be automatically populated after the DHCP scope is selected<br>  |
| **Step 7** | Click Apply. | |

# Access Points

An access point connected directly to a wired LAN provides a connection point for wireless users. If more than one access point is connected to the LAN, users can roam from one area of a facility to another without losing their connection to the network. As users move out of range of one access point, they automatically connect to the network (associate) through another access point. The roaming process is seamless and transparent to the user. The figure below shows access points acting as root units on a wired LAN.

***Figure 1: Access Points as Root Units on a Wired LAN***




In an all-wireless network, an access point acts as a stand-alone root unit. The access point is not attached to a wired LAN; it functions as a hub linking all stations together. The access point serves as the focal point for communications, increasing the communication range of wireless users. Figure below shows an access point in an all-wireless network.

## Configuring and Deploying the Access Point

This section describes how to connect the access point to a wireless LAN controller. The configuration process takes place on the controller. See the Cisco Wireless LAN Controller Configuration Guide for additional information.

## The Controller Discovery Process

The access point uses standard Control and Provisioning of Wireless Access Points Protocol (CAPWAP) to communicate between the controller and other wireless access points on the network. CAPWAP is a standard, inter-operable protocol which enables an access controller to manage a collection of wireless termination points. The discovery process using CAPWAP is identical to the Lightweight Access Point Protocol (LWAPP) used with previous Cisco Aironet access points. LWAPP-enabled access points are compatible with CAPWAP, and conversion to a CAPWAP controller is seamless. Deployments can combine CAPWAP and LWAPP software on the controllers.

The functionality provided by the controller does not change except for customers who have Layer 2 deployments, which CAPWAP does not support.

In a CAPWAP environment, a wireless access point discovers a controller by using CAPWAP discovery mechanisms and then sends it a CAPWAP join request. The controller sends the access point a CAPWAP join response allowing the access point to join the controller. When the access point joins the controller, the controller manages its configuration, firmware, control transactions, and data transactions.

**Note** For additional information about the discovery process and CAPWAP, see the Cisco Wireless LAN Controller Software Configuration Guide. This document is available on Cisco.com.

**Note** CAPWAP support is provided in controller software release 8.5 or later. However, your controller must be running the release that supports Cisco 1100 Series access points.

**Note** You cannot edit or query any access point using the controller CLI if the name of the access point contains a space.

**Note** Make sure that the controller is set to the current time. If the controller is set to a time that has already passed, the access point might not join the controller because its certificate may not be valid for that time.

Access points must be discovered by a controller before they can become an active part of the network. The access point supports these controller discovery processes:

- Layer 3 CAPWAP discovery—Can occur on different subnets than the access point and uses IP addresses and UDP packets.
- Locally stored controller IP address discovery—If the access point was previously joined to a controller, the IP addresses of the primary, secondary, and tertiary controllers are stored in the access point's non-volatile memory. This process of storing controller IP addresses on an access point for later deployment is called priming the access point. For more information about priming, see the "Performing a Pre-Installation Configuration" section.
- DHCP server discovery—This feature uses DHCP option 43 to provide controller IP addresses to the access points. Cisco switches support a DHCP server option that is typically used for this capability. For more information about DHCP option 43, see the "Configuring DHCP Option 43" section.

- DNS discovery—The access point can discover controllers through your domain name server (DNS). For the access point to do so, you must configure your DNS to return controller IP addresses in response to CISCO-CAPWAP-CONTROLLER.localdomain, where localdomain is the access point domain name. Configuring the CISCO-CAPWAP-CONTROLLER provides backwards compatibility in an existing customer deployment. When an access point receives an IP address and DNS information from a DHCP server, it contacts the DNS to resolve CISCO-CAPWAP-CONTROLLER.localdomain. When the DNS sends a list of controller IP addresses, the access point sends discovery requests to the controllers.

## Deploying the Access Point on the Wireless Network

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Connect and power up the router. | |
| **Step 2** | Observe the wireless LAN LED (for LED descriptions, see "Checking the Wireless LAN LED" section ). | |
| **Step 3** | Reconfigure the Cisco wireless LAN controller so that it is not the primary controller. | **Note** A primary Cisco wireless LAN controller should be used only for configuring access points and not in a working network. |

# Checking the Wireless LAN LED

**Note** It is expected that there will be small variations in the LED color intensity and hue from unit to unit. This is within the normal range of the LED manufacturer's specifications and is not a defect.

The wireless LAN status LED indicates various conditions which are described in Table.

LED port: WLAN (1 LED): 3-color LED: Green, Blue, Red

***Table 2: Wireless LAN LED***

| Message Type | LED State | Message Meanings |
|---|---|---|
| Association status | Green | Normal operating condition, but no wireless client associated. |
| | Blue | Normal operating condition, at least one wireless client association. |
| Boot loader status | Green | Executing boot loader |
| Boot loader error | Blinking Green | Boot loader signing verification failure |

| Message Type | LED State | Message Meanings |
|---|---|---|
| Operating status | Blinking Blue | Software upgrade in progress |
| | Alternating between Green and Red | Discovery/join process in progress |
| Access point operating system errors | Cycling through Red-Off-Green-Off-Blue-Off | General warning; insufficient inline power |

# Miscellaneous Usage and Configuration Guidelines

Using the reset command you can reset the AP to the default factory-shipped configuration.

```
hw-module subslot x/y error-recovery password_reset
```

**Note** Since this is an IOS command, you must run this command on the Cisco 1100 router console, instead of the AP console.

The AP configuration files are cleared. This resets all configuration settings to factory defaults, including passwords, encryption keys, the IP address, and the SSID. However, the regulatory domain provisioning is not reset.

**Note** When you run the **hw-module subslot x/y error-recovery password_reset** command, the AP module automatically reloads to restore the configuration settings and enters the maintenance mode. In the maintenance mode, the AP module is on power on mode. When the module configuration reset is confirmed through the console or web UI, the **hw-module subslot x/y reload force** command reloads the AP and then quits the maintenance mode.

# Important Information for Controller-Based Deployments

Keep these guidelines in mind when you use the Cisco 1100 series access points:

- The access point can only communicate with Cisco wireless LAN controllers.
- The access point does not support Wireless Domain Services (WDS) and cannot communicate with WDS devices. However, the controller provides functionality equivalent to WDS when the access point joins it.
- CAPWAP does not support Layer 2. The access point must get an IP address and discover the controller using Layer 3, DHCP, DNS, or IP subnet broadcast.
- The access point console port is enabled for monitoring and debug purposes. All configuration commands are disabled when the access point is connected to a controller.

**Note** To configure the controller using day 0 wizard (GUI), follow the Non Mesh configuration steps only.

**Note** For more information on configuring the Embedded Wireless Networks, see the Cisco Embedded Wireless Controller on Catalyst Access Points Configuration Guide.