



# Troubleshooting

---

- [Use the Reset button, on page 1](#)
- [Troubleshooting the Access Point to Controller Join Process, on page 2](#)
- [Important Information for Controller-based Deployments, on page 3](#)
- [Configuring DHCP Option 43, on page 3](#)

## Use the Reset button

The **Reset** button (see [Connectors and Ports on the Base](#)) is a multi-function button. Using this button, you can reset the AP to factory default or clear the AP's internal storage.

### Reset the AP to Factory Default Settings

#### [Connectors and Ports on the Base](#)

To reset the AP to the default factory-shipped configuration, perform the following steps:

1. Press and continue to press the **Mode** button on the access point during the AP boot cycle.
2. Press until the AP console shows a seconds counter.  
When the counter indicates the number of seconds for which the **Mode** button is pressed, the AP status LED changes to blinking red.
3. Press the **Mode** button for less than 20 seconds to reset the AP to the default factory-shipped configuration.

### Clear the AP Internal Storage

To clear the AP's internal storage, including all the configuration files, perform the following steps:

1. Press and continue to press the **Mode** button on the access point during the AP boot cycle.
2. Press until the AP console shows a seconds counter.  
When the counter indicates the number of seconds for which the **Mode** button is pressed, the AP status LED changes to blinking red.
3. Press the **Mode** button for more than 20 seconds, but less than 60 seconds to clear the AP internal storage, including all the configuration files.

This resets all the configuration settings to factory defaults, including passwords, the IP address, and the SSID.

**Note**

- If the **Mode** button is pressed for more than 30 seconds, but less than 60 seconds, the FIPS mode flag is also cleared during the full factory reset of the AP. If the FIPS flag is set, the console access is disabled.
- The AP status LED changes from blue to red, and all the files in the AP storage directory are cleared.
- If you keep the **Mode** button pressed for more than 60 seconds, the button is assumed as being faulty and no changes are made.

## Troubleshooting the Access Point to Controller Join Process

**Note**

As specified in the [Cisco Wireless Solutions Software Compatibility Matrix](#), ensure that your controller is running Cisco IOS XE Dublin 17.12.3 or a later release to support the Cisco CW9163E AP.

Access points can fail to join a controller for many reasons—a RADIUS authorization is pending, self-signed certificates are not enabled on the controller, the access point and the controller regulatory domains do not match, and so on.

Controller software enables you to configure the access points to send all CAPWAP-related errors to a syslog server. All the CAPWAP error messages can be viewed from the syslog server itself.

When the ordered AP is a CW9163E-MR model, or the AP is in Meraki Management mode, it will not attempt to join the Cisco 9800 Wireless Controller. Contact the Meraki support team to perform the migration procedure on the AP.

The state of the access point is not maintained on the controller. It can be difficult to determine why the discovery request from a certain access point was rejected. In order to troubleshoot such joining problems, we recommend that you run traces commands on the Cisco Catalyst 9800 Wireless Controller.

The controller collects all the join-related information for each access point that sends a CAPWAP discovery request to the controller. Collection begins with the first discovery message received from the access point and ends with the last configuration payload sent from the controller to the access point.

When the controller is maintaining join-related information for the maximum number of access points, it does not collect information for any more access points.

An access point sends all the syslog messages to the IP address 255.255.255.255 by default.

You can also configure a DHCP server to return a syslog server IP address to the access point using Option 7 on the server. The access point then starts sending all the syslog messages to this IP address.

When the access point joins a controller for the first time, the controller sends the global syslog server IP address (the default is 255.255.255.255) to the access point.

The access point sends all the syslog messages to this IP address until it is overridden by the following configuration:

- The access point is still connected to the same controller, and the global syslog server IP address configuration on the controller has been changed using the **syslog host** *<ip address>* command. In this case, the controller sends the new global syslog server IP address to the access point.

To configure the global syslog server IP address, run these commands:

1. **configure terminal**
2. **ap profile** *ap-profile-name*
3. **syslog host** *syslog IP address*
4. **exit**

- The access point is disconnected from the controller and joins another controller. In this case, the new controller sends its global syslog server IP address to the access point.
- Whenever a new syslog server IP address overrides the existing syslog server IP address, the old address is erased from persistent storage, and the new address is stored in its place. The access point also starts sending all the syslog messages to the new IP address, provided the access point can reach the syslog server IP address.



---

**Note** You can configure the syslog server for access points and view the access point join information only from the controller CLI.

---

## Important Information for Controller-based Deployments

Keep these guidelines in mind when you use the AP:

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

## Configuring DHCP Option 43

You can use DHCP Option 43 to provide a list of controller IP addresses to the AP, enabling it to find and join a controller.

The following is a DHCP Option 43 configuration example on a Microsoft Windows 2003 Enterprise DHCP server for Cisco Catalyst lightweight APs. For other DHCP server implementations, consult the product documentation to configure DHCP Option 43. In Option 43, use the IP address of the controller management interface.



**Note** DHCP Option 43 is limited to one AP type per DHCP pool. You must configure a separate DHCP pool for each AP type.

The Cisco Catalyst Wireless 9163E Series Outdoor AP uses the type-length-value (TLV) format for DHCP Option 43. DHCP servers must be programmed to return the option based on the AP DHCP Vendor Class Identifier (VCI) string (DHCP Option 43). The VCI string for the AP:

#### Cisco AP CW9163E

The format of the TLV block is listed below:

- Type—0xf1 (decimal 241)
- Length—Number of controller IP addresses \* 4
- Value—IP addresses of the controller management interfaces are listed sequentially in hexadecimal format.

#### Procedure

- Step 1** Enter configuration mode at the Cisco IOS CLI.
- Step 2** Create the DHCP pool, including the necessary parameters such as default router and name server. A DHCP scope example is as follows:

#### Example:

```
ip dhcp pool <pool name>
network <IP Network> <Netmask>
default-router <Default router>
dns-server <DNS Server>
```

Where:

#### Example:

```
<pool name> is the name of the DHCP pool, such as AP9163E
<IP Network> is the network IP address where the controller resides, such as 10.0.15.1
<Netmask> is the subnet mask, such as 255.255.255.0
<Default router> is the IP address of the default router, such as 10.0.0.1
<DNS Server> is the IP address of the DNS server, such as 10.0.10.2
```

- Step 3** Add the option 43 line using the following syntax:

#### Example:

```
option 43 hex <hex string>
```

The hex string is assembled by concatenating the TLV values shown below:

#### Type + Length + Value

For example, suppose that there are two controllers with management interface IP addresses, 10.126.126.2 and 10.127.127.2. The type is f1(hex). The length is 2 \* 4 = 8 = 08 (hex). The IP addresses translate to 0a7e7e02

and 0a7f7f02. Assembling the string then yields f1080a7e7e020a7f7f02. The resulting Cisco IOS command is added to the DHCP scope is **option 43 hex f1080a7e7e020a7f7f02**.

---

