



Converting Autonomous Access Points to Lightweight Mode

- [Finding Feature Information, on page 1](#)
- [Guidelines for Converting Autonomous Access Points to Lightweight Mode, on page 1](#)
- [Information About Autonomous Access Points Converted to Lightweight Mode, on page 2](#)
- [How to Convert a Lightweight Access Point Back to an Autonomous Access Point, on page 4](#)
- [Authorizing Access Points \(CLI\), on page 5](#)
- [Authorizing Access Points \(GUI\), on page 6](#)
- [Disabling the Reset Button on Converted Access Points \(CLI\), on page 7](#)
- [Monitoring the AP Crash Log Information, on page 8](#)
- [How to Configure a Static IP Address on an Access Point, on page 8](#)
- [Recovering the Access Point Using the TFTP Recovery Procedure, on page 11](#)
- [Configuration Examples for Converting Autonomous Access Points to Lightweight Mode, on page 11](#)

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Guidelines for Converting Autonomous Access Points to Lightweight Mode

- Access points that are converted to lightweight mode do not support Wireless Domain Services (WDS). Converted access points communicate only with Cisco wireless LAN controllers and cannot communicate with WDS devices. However, the controller provides functionality that is equivalent to WDS when an access point is associated to it.

- All Cisco lightweight access points support 16 Basic Service Set Identifiers (BSSIDs) per radio and a total of 16 wireless LANs per access point. When a converted access point is associated to a controller, only wireless LANs with IDs 1 through 16 are pushed to the access point, unless the access point is a member of an access point group.
- Access points that are converted to lightweight mode must get an IP address and discover the controller using DHCP, DNS, or IP subnet broadcast.

Information About Autonomous Access Points Converted to Lightweight Mode

You can convert autonomous Cisco Aironet access points to lightweight mode. When you upgrade the access points to lightweight mode, the access point communicates with the controller and receives a configuration and software image from the controller.

Reverting from Lightweight Mode to Autonomous Mode

After you convert an autonomous access point to lightweight mode, you can convert the access point from a lightweight unit back to an autonomous unit by loading a Cisco IOS release that supports autonomous mode (Cisco IOS Release 12.3(7)JA or earlier releases). If the access point is associated with a controller, you can use the controller to load the Cisco IOS release. If the access point is not associated to a controller, you can load the Cisco IOS release using TFTP. In either method, the access point must be able to access a TFTP server that contains the Cisco IOS release to be loaded.

Using DHCP Option 43 and DHCP Option 60

Cisco Aironet Access Points use the type-length-value (TLV) format for DHCP option 43. You must program the DHCP servers to return the option based on the access point's DHCP Vendor Class Identifier (VCI) string (DHCP option 60).

See the product documentation for your DHCP server for instructions on configuring DHCP option 43. The [Converting Autonomous Access Points to Lightweight Mode](#) document contains example steps for configuring option 43 on a DHCP server.

If the access point is ordered with the Service Provider Option - AIR-OPT60-DHCP selected, the VCI string for that access point will be different than those strings listed in the previous table. The VCI string has the following suffix: ServiceProvider, for example, a 1260 with this option returns the VCI string Cisco AP c1260-ServiceProvider.



Note Ensure that the controller IP address that you obtain from the DHCP server is a unicast IP address. Do not configure the controller IP address as a multicast address when configuring DHCP option 43.

Restrictions for DHCP Option 60

- Cisco Wave2 APs support strings with length up to 256 characters only.



Note When the string length exceeds the limit, the default value is sent during the DHCP discover process.

How Converted Access Points Send Crash Information to the Controller

When a converted access point unexpectedly reboots, the access point stores a crash file on its local flash memory at the time of the crash. After the unit reboots, it sends the reason for the reboot to the controller. If the unit rebooted because of a crash, the controller pulls up the crash file using existing CAPWAP messages and stores it in the controller flash memory. The crash information copy is removed from the access point flash memory when the controller pulls it from the access point.

Uploading Memory Core Dumps from Converted Access Points

By default, access points converted to lightweight mode do not send memory core dumps to the controller. This section provides instructions to upload access point core dumps using the controller GUI or CLI.

Displaying MAC Addresses for Converted Access Points

There are some differences in the way that controllers display the MAC addresses of converted access points on information pages in the controller GUI:

- On the **AP Summary** window, the controller lists the Ethernet MAC addresses of the converted access points.
- On the **AP Detail** window, the controller lists the BSS MAC addresses and Ethernet MAC addresses of the converted access points.
- On the Radio Summary page, the controller lists converted access points by the radio MAC address.

Configuring a Static IP Address for a Lightweight Access Point

If you want to specify an IP address for an access point rather than having one assigned automatically by a DHCP server, you can use the controller GUI or CLI to configure a static IP address for the access point. Static IP addresses are generally used only for deployments with a limited number of APs.

An access point cannot discover the controller using domain name system (DNS) resolution if a static IP address is configured for the access point, unless you specify a DNS server and the domain to which the access point belongs. You can configure these parameters using either the controller CLI or the GUI.



Note If you configure an access point to use a static IP address that is not on the same subnet on which the access point's previous DHCP address was, the access point falls back to a DHCP address after the access point reboots. If the access point falls back to a DHCP address, enter the **show ap config general Cisco_AP** CLI command to show that the access point is using a fallback IP address. However, the GUI shows both the static IP address and the DHCP address, but it does not identify the DHCP address as a fallback address.

How to Convert a Lightweight Access Point Back to an Autonomous Access Point

Converting a Lightweight Access Point Back to an Autonomous Access Point (CLI)

SUMMARY STEPS

1. enable
2. ap name *Cisco_AP* tftp-downgrade *tftp_server_ip_address* *tftp_server_image_filename*

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>Controller# enable</pre>	Enters privileged EXEC mode.
Step 2	<p>ap name <i>Cisco_AP</i> tftp-downgrade <i>tftp_server_ip_address</i> <i>tftp_server_image_filename</i></p> <p>Example:</p> <pre>Controller# ap name AP02 tftp-downgrade 10.0.0.1 tsrvname</pre>	<p>Converts the lightweight access point back to autonomous mode.</p> <p>Note After entering this command, you must wait until the access point reboots and then reconfigure the access point using the CLI or GUI.</p>

Converting a Lightweight Access Point Back to an Autonomous Access Point (Using the Mode Button and a TFTP Server)

- Step 1** Configure the PC on which your TFTP server software runs with a static IP address in the range of 10.0.0.2 to 10.0.0.30.
- Step 2** Make sure that the PC contains the access point image file (such as *c1140-k9w7-tar.123-7.JA.tar* for a 1140 series access point) in the TFTP server folder and that the TFTP server is activated.
- Step 3** Rename the access point image file in the TFTP server folder to *c1140-k9w7-tar.default* for a 1140 series access point.
- Step 4** Connect the PC to the access point using a Category 5 (CAT5) Ethernet cable.
- Step 5** Disconnect power from the access point.
- Step 6** Press and hold the **MODE** button while you reconnect power to the access point.

Note The **MODE** button on the access point must be enabled.
- Step 7** Hold the **MODE** button until the status LED turns red (approximately 20 to 30 seconds), and release the **MODE** button.
- Step 8** Wait until the access point reboots as indicated by all the LEDs turning green followed by the Status LED blinking green.

Step 9 After the access point reboots, reconfigure the access point using the GUI or the CLI.

Authorizing Access Points (CLI)

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ap auth-list ap-policy authorize-ap`
4. `username user_name mac aaa attribute list list_name`
5. `aaa new-model`
6. `aaa authorization credential-download auth_list local`
7. `aaa attribute list list`
8. `aaa session-id common`
9. `aaa local authentication default authorization default`
10. `show ap name Cisco_AP config general`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Controller# <code>enable</code>	Enters privileged EXEC mode.
Step 2	<code>configure terminal</code> Example: Controller# <code>configure terminal</code>	Enters global configuration mode.
Step 3	<code>ap auth-list ap-policy authorize-ap</code> Example: Controller(config)# <code>ap auth-list ap-policy authorize-ap</code>	Configures an access point authorization policy.
Step 4	<code>username user_name mac aaa attribute list list_name</code> Example: Controller(config)# <code>username aaa.bbb.ccc mac aaa attribute list attrlist</code>	Configures the MAC address of an access point locally.
Step 5	<code>aaa new-model</code> Example: Controller(config)# <code>aaa new-model</code>	Enables new access control commands and functions.

	Command or Action	Purpose
Step 6	aaa authorization credential-download <i>auth_list</i> local Example: Controller(config)# aaa authorization credential-download auth_download local	Downloads EAP credentials from the local server.
Step 7	aaa attribute list <i>list</i> Example: Controller(config)# aaa attribute list alist	Configures AAA attribute list definitions.
Step 8	aaa session-id common Example: Controller(config)# aaa session-id common	Configures the AAA common session ID.
Step 9	aaa local authentication default authorization default Example: Controller(config)# aaa local authentication default authorization default	Configures the local authentication method list.
Step 10	show ap name <i>Cisco_AP</i> config general Example: Controller(config)# show ap name AP01 config general	Displays the configuration information that corresponds to a specific access point.

Authorizing Access Points (GUI)

Step 1 Choose **Configuration > Security > AAA > AP Policy**.

The **AP Policy** page is displayed.

Step 2 In the Policy Configuration area, enable or disable the following parameters:

- **Authorize LSC APs against Auth-List**
- **AP with Self-Signed Certificate**
- **Authorize MIC APs against AAA**
- **AP with Manufacturing Installed Certificate**

Step 3 Click **Apply**.

Step 4 Click **Save Configuration**.

Disabling the Reset Button on Converted Access Points (CLI)

You can enable or disable the **Reset** button on access points that are converted to lightweight mode. The **Reset** button is labeled **MODE** on the outside of the access point.



Note The procedure to perform this task using the controller GUI is not currently available.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no ap reset-button**
4. **end**
5. **ap name *cisco_ap* reset-button**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Controller# <code>enable</code>	Enters privileged EXEC mode.
Step 2	configure terminal Example: Controller# <code>configure terminal</code>	Enters global configuration mode.
Step 3	no ap reset-button Example: Controller(config)# <code>no ap reset-button</code>	Disables the Reset buttons on all converted access points that are associated to the controller. Note To enable the Reset buttons on all the converted access points that are associated to the controller, enter the ap reset-button command.
Step 4	end Example: Controller(config)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.
Step 5	ap name <i>cisco_ap</i> reset-button Example: Controller# <code>ap name AP02 reset-button</code>	Enables the Reset button on the converted access point that you specify.

Monitoring the AP Crash Log Information



Note The procedure to perform this task using the controller GUI is not currently available.

SUMMARY STEPS

1. `enable`
2. `show ap crash-file`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Controller# <code>enable</code>	Enters privileged EXEC mode.
Step 2	show ap crash-file Example: Controller# <code>show ap crash-file</code>	Verifies whether the crash file is downloaded to the controller.

How to Configure a Static IP Address on an Access Point

Configuring a Static IP Address on an Access Point (CLI)

SUMMARY STEPS

1. `enable`
2. `ap name Cisco_AP static-ip ip-address static_ap_address netmask static_ip_netmask gateway static_ip_gateway`
3. `enable`
4. `configure terminal`
5. `ap static-ip name-server nameserver_ip_address`
6. `ap static-ip domain static_ip_domain`
7. `end`
8. `show ap name Cisco_AP config general`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>Controller# enable</pre>	Enters privileged EXEC mode.
Step 2	<p>ap name <i>Cisco_AP</i> static-ip ip-address <i>static_ap_address</i> netmask static_ip_netmask gateway <i>static_ip_gateway</i></p> <p>Example:</p> <pre>Controller# ap name AP03 static-ip ip-address 9.9.9.16 netmask 255.255.0.0 gateway 9.9.9.2</pre>	<p>Configures a static IP address on the access point. This command contains the following keywords and arguments:</p> <ul style="list-style-type: none"> • ip-address— Specifies the Cisco access point static IP address. • <i>ip-address</i>— Cisco access point static IP address. • netmask— Specifies the Cisco access point static IP netmask. • <i>netmask</i>— Cisco access point static IP netmask. • gateway— Specifies the Cisco access point gateway. • <i>gateway</i>— IP address of the Cisco access point gateway. <p>The access point reboots and rejoins the controller, and the static IP address that you specify is pushed to the access point. After the static IP address has been sent to the access point, you can configure the DNS server IP address and domain name. You must perform Steps 3 and Step 4 after the access points reboot.</p>
Step 3	<p>enable</p> <p>Example:</p> <pre>Controller# enable</pre>	Enters privileged EXEC mode.
Step 4	<p>configure terminal</p> <p>Example:</p> <pre>Controller# configure terminal</pre>	Enters global configuration mode.
Step 5	<p>ap static-ip name-server <i>nameserver_ip_address</i></p> <p>Example:</p> <pre>Controller(config)# ap static-ip name-server 10.10.10.205</pre>	<p>Configures a DNS server so that a specific access point or all access points can discover the controller using DNS resolution.</p> <p>Note To undo the DNS server configuration, enter the no ap static-ip name-server <i>nameserver_ip_address</i> command.</p>
Step 6	<p>ap static-ip domain <i>static_ip_domain</i></p> <p>Example:</p>	Configures the domain to which a specific access point or all access points belong.

	Command or Action	Purpose
	<pre>Controller(config)# ap static-ip domain domain1</pre>	Note To undo the domain name configuration, enter the no ap static-ip domain static_ip_domain command.
Step 7	end Example: <pre>Controller(config)# end</pre>	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.
Step 8	show ap name Cisco_AP config general Example: <pre>Controller# show ap name AP03 config general</pre>	Displays the IP address configuration for the access point.

Configuring a Static IP Address on an Access Point (GUI)

-
- Step 1** Choose **Configuration > Wireless > Access Points > All APs**.
The **All APs** page is displayed.
- Step 2** Click the name of the access point.
The **AP > Edit** page is displayed.
- Step 3** In the **General** tab, in the **IP Config** area, select the **Static IP** check box if you want to assign a static IP address to the access point.
- Step 4** Enter the following details:
- **Static IP**
 - **Netmask**
 - **Gateway**
- Step 5** Click **Apply**.
The access point reboots and rejoins the controller, and the static IP address that you specified is sent to the access point.
- Step 6** After the static IP address has been sent to the access point, configure the **DNS IP Address** and **Domain Name**.
- Step 7** Click **Apply**.
- Step 8** Click **Save Configuration**.
-

Recovering the Access Point Using the TFTP Recovery Procedure

-
- Step 1** Download the required recovery image from Cisco.com (ap3g2-k9w8-tar.152-2.JA.tar) and install it in the root directory of your TFTP server.
- Step 2** Connect the TFTP server to the same subnet as the target access point and power-cycle the access point. The access point boots from the TFTP image and then joins the controller to download the oversized access point image and complete the upgrade procedure.
- Step 3** After the access point has been recovered, you can remove the TFTP server.
-

Configuration Examples for Converting Autonomous Access Points to Lightweight Mode

Example: Displaying the IP Address Configuration for Access Points

This example shows how to display the IP address configuration for an access point:

```
Controller# show ap name AP03 dot11 24ghz config general
Cisco AP Identifier..... 4
Cisco AP Name..... AP6
IP Address Configuration..... Static IP assigned
IP Address..... 10.10.10.118
IP NetMask..... 255.255.255.0
Gateway IP Addr..... 10.10.10.1
Domain..... Domain1
Name Server..... 10.10.10.205
...
```

Example: Displaying Access Point Crash File Information

This example shows how to display access point crash file information. Using this command, you can verify whether the file is downloaded to the controller.

```
Controller# show ap crash-file
Local Core Files:
lrad_AP1130.rdump0 (156)
```

The number in parentheses indicates the size of the file. The size should be greater than zero if a core dump file is available.

