Converting Autonomous Access Points to Lightweight Mode

- 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, on page 5
- Disabling the Reset Button on Converted Access Points (CLI), on page 8
- Monitoring the AP Crash Log Information, on page 9
- How to Configure a Static IP Address on an Access Point, on page 9
- Configuring a Static IP Address on an Access Point (GUI), on page 11
- 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
- AP MAC Authorization, on page 12
- Ethernet VLAN Tagging on Access Points, on page 13

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 devices and cannot communicate with WDS devices. However, the device 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 device, 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 device 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 device and receives a configuration and software image from the device.

Note Autonomous mode is supported only on the following APs:

- Cisco Aironet 1700 Series Access Points
- Cisco Aironet 2700 Series Access Points
- Cisco Aironet 3700 Series Access Points

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 device, you can use the device to load the Cisco IOS release. If the access point is not associated to a device, 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 device IP address that you obtain from the DHCP server is a unicast IP address. Do not configure the device 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 Device

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 device. If the unit rebooted because of a crash, the device pulls up the crash file using existing CAPWAP messages and stores it in the device flash memory. The crash information copy is removed from the access point flash memory when the device 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 device. This section provides instructions to upload access point core dumps using the device GUI or CLI.

Displaying MAC Addresses for Converted Access Points

There are some differences in the way that controllers show the MAC addresses of APs on information pages in the controller GUI:

- On the **AP Summary** window, the controller lists the Ethernet MAC addresses of the APs.
- On the **AP Detail** window, the controller lists the BSS MAC addresses and Ethernet MAC addresses of the APs.
- On the Radio Summary page, the device 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 device 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 device 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)

Procedure

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

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

Procedure

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 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

The following sections describe the various ways in which access points can be authorized:

Authorizing Access Points Using Local Database (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ap auth-list ap-policy authorize-ap** **Example:** `Device(config)# ap auth-list ap-policy authorize-ap`	Configures an access point authorization policy.
Step 4	**username** *user_name* **mac** [**aaa attribute list** *list_name*] **Example:** `Device(config)# username abcdabcdabcd mac aaa attribute list attrlist`	(Optional) Configures the MAC address of an access point locally. **Note** Configure the MAC address for local authentication and AP local authorization using the following command: `username abcdabcdabcd mac`
Step 5	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables new access control commands and functions.

	Command or Action	Purpose
Step 6	**aaa authorization credential-download** {*auth_list* | **default**} **local** **Example:** `Device(config)# aaa authorization credential-download auth_download local`	Downloads EAP credentials from the local server.
Step 7	**aaa attribute list** *list* **Example:** `Device(config)# aaa attribute list alist`	(Optional) Configures AAA attribute list definitions.
Step 8	**aaa session-id common** **Example:** `Device(config)# aaa session-id common`	Configures the AAA common session ID.
Step 9	**aaa local authentication default authorization default** **Example:** `Device(config)# aaa local authentication default authorization default`	(Optional) Configures the local authentication method list.
Step 10	**end**	Saves the configuration and exits the configuration mode and returns to privileged EXEC mode.
Step 11	**show ap name** *Cisco_AP* **config general** **Example:** `Device# show ap name AP01 config general`	Displays the configuration information that corresponds to a specific access point.

Authorizing Access Points Using RADIUS Server (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *server-name* **Example:**	Enters the RADIUS server configuration mode.

	Command or Action	Purpose
	`Device(config)# radius server ise`	
Step 4	**address** {**ipv4** | **ipv6**} *radius-server-ipv4-address-or-name* **auth-port** *udp-port-auth-server* **acct-port** *udp-port-acct-server* **Example:** `Device(config-radius-server)# address ipv4 224.0.0.1 auth-port 1645 acct-port 1646`	Configures the RADIUS server along with other server parameters.
Step 5	**key** *0 cisco* **Example:** `Device(config-radius-server)# key 0 cisco`	Sets a clear text encryption key for the RADIUS authentication server.
Step 6	**exit** **Example:** `Device(config-radius-server)# exit`	Reverts to the Privileged EXEC mode.
Step 7	**aaa group server radius** *server-group* **Example:** `Device(config)# aaa group server radius ise-group`	Configures RADIUS server group definition.
Step 8	**server name** *ise* **Example:** `Device(config-sg-radius)# server name ise`	Configures the RADIUS server name.
Step 9	**ip radius source-interface** *vlan* **Example:** `Device(config-sg-radius)# ip radius source-interface vlan`	(Optional) Configures interface for source address in RADIUS packets.
Step 10	**exit** **Example:** `Device(cconfig-sg-radius)# exit`	Reverts to the Privileged EXEC mode.
Step 11	**aaa authorization network default group** *default-server-group* **local** **Example:** `Device(config)# aaa authorization network default group ise-group local`	Sets the authorization method to local.

	Command or Action	Purpose
Step 12	**aaa authorization credential-download default group** *default-server-group* **local** **Example:** `Device(config)# aaa authorization credential-download default group ise-group local`	Configures local database to download EAP credentials from local, RADIUS, or LDAP server.

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.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**no ap reset-button** **Example:** `Device(config)# no ap reset-button`	Disables the **Reset** buttons on all converted access points that are associated to the device. **Note** To enable the **Reset** buttons on all the converted access points that are associated to the device, enter the **ap reset-button** command.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 5	**ap name** *cisco_ap* **reset-button** **Example:** `Device# ap name AP02 reset-button`	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 device GUI is not currently available.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**show ap crash-file** **Example:** `Device# show ap crash-file`	Verifies whether the crash file is downloaded to the device.

How to Configure a Static IP Address on an Access Point

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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *Cisco_AP* **static-ip ip-address** *static_ap_address* **netmask** *static_ip_netmask* **gateway** *static_ip_gateway* **Example:** `Device# ap name AP03 static-ip ip-address 9.9.9.16 netmask 255.255.0.0 gateway 9.9.9.2`	Configures a static IP address on the access point. This command contains the following keywords and arguments: • **ip-address**— Specifies the Cisco access point static IP address. • *ip-address*— Cisco access point static IP address. • **netmask**—Specifies the Cisco access point static IP netmask. • *netmask*— Cisco access point static IP netmask.

	Command or Action	Purpose
		• **gateway**—Specifies the Cisco access point gateway. • *gateway*— IP address of the Cisco access point gateway. The access point reboots and rejoins the device, 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.
Step 3	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 4	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 5	**ap static-ip name-server** *nameserver_ip_address* **Example:** `Device(config)# ap static-ip name-server 10.10.10.205`	Configures a DNS server so that a specific access point or all access points can discover the device using DNS resolution. **Note** To undo the DNS server configuration, enter the **no ap static-ip name-server** *nameserver_ip_address* command.
Step 6	**ap static-ip domain** *static_ip_domain* **Example:** `Device(config)# ap static-ip domain domain1`	Configures the domain to which a specific access point or all access points belong. **Note** To undo the domain name configuration, enter the **no ap static-ip domain** *static_ip_domain* command.
Step 7	**end** **Example:** `Device(config)# end`	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:** `Device# show ap name AP03 config general`	Displays the IP address configuration for the access point.

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

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 On the **All Access Points** section, click on an **AP Name**.

Step 3 In the **Edit AP** window that is displayed, go to the **IP Config** section.

Step 4 Select the **Static IP (IPv4/IPv6)** check box. This activates the static IP details pane.

Step 5 Enter the **Static IP**, **Netmask**, **Gateway**, and **DNS IP Address**.

Step 6 Click **Update & Apply to Device**.

Recovering the Access Point Using the TFTP Recovery Procedure

Procedure

Step 1 Download the required recovery image from Cisco.com 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 device 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:

```
Device# 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 device.

```
Device# 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.
```

AP MAC Authorization

The AP Authentication Policy feature ensures that only authorized APs can associate with a controller. To authorize an AP, the Ethernet MAC address of the AP must be registered. This can be done locally on the controller or on an external RADIUS server.

Configuring AP MAC Authorization (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**[no] ap auth-list ap-policy authorize-ap** *profile-name* **Example:** `Device(config)# ap auth-list ap-policy authorize-ap`	Configures AP authorization policy.
Step 3	**end** **Example:** `Device(config)# end`	Exits the configuration mode and returns to privileged EXEC mode.
Step 4	**show ap auth-list** *value-in-dBm* **Example:** `Device# show ap auth-list`	Shows the status of AP MAC authorization.

Example

1. Local database configuration:

```
Device(config)# aaa authorization network default local
Device(config)# aaa authorization credential-download default local
```

2. Username configuration:

```
Device(config)# username abcdabcdabcd mac
```

Username is the Ethernet MAC address of the AP, which is to be authorized before the AP associates with the controller. The Ethernet MAC address of the AP must be in the following format:

```
username <abcdabcdabcd> mac
```

Use the **show ap summary** command to get the Ethernet MAC address of the AP.

Ethernet VLAN Tagging on Access Points

Information About Ethernet VLAN Tagging on Access Points

You can configure VLAN tagging on the Ethernet interface either directly on the AP console or through the controller . The configuration is saved in the flash memory and all CAPWAP frames use the VLAN tag as configured, along with all the locally switched traffic, which is not mapped to a VLAN.

Configuring Ethernet VLAN Tagging on Access Points (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points** and expand the **All Access Points** section.

Step 2 To enable VLAN tagging for all access points associated with the controller, select **Set VLAN Tag** from the **Select an Action**drop-down list.

Step 3 In the **Configure VLAN Tag** window enter the VLAN Tag ID to enable VLAN tagging of both CAPWAP control and data packets on the Access Point and click **Apply to Device** for the configuration to take effect. If you do not want all devices to be tagged, select the **Remove Current VLAN Tag** and click **Apply to Device.**

Step 4 Alternatively, if you want to configure VLAN tagging on individual Access Points, click the name of the AP go to **Edit** > **Advanced** and select the **VLAN Tag** to enable the VLAN tagging on the AP.

Step 5 Click **Update & Apply to Device**.

Configuring Ethernet VLAN Tagging on Access Points (CLI)

Follow the procedure given below to configure Ethernet VLAN tagging on APs.

Before you begin

- VLAN tagging is not supported on MAPs that are in bridge mode. The feature is automatically disabled when the APs are set to bridge mode.
- If VLAN tagging is enabled, flex native VLAN ID cannot be configured for an AP.
- APs in flexconnect standalone mode (with VLAN tag enabled) may reload at every 10 minutes, if the APs fail to discover the wireless controller during failover.

Procedure

	Command or Action	Purpose

Step 1	**ap name** *ap-name* **vlan-tag** *vlan-id*
	Example:
	`Device# ap name AP1 vlan-tag 12`
	`Device# ap name AP1 no vlan-tag`
		Configures VLAN tagging for a non-bridge AP. Use the **no** form of this command to disable the configuration.

Step 2	**ap vlan-tag** *vlan-id*
	Example:
	`Device# ap vlan-tag 1000`
	`Device# ap no vlan-tag`
		Configure VLAN tagging for all nonbridge APs. Use the **no** form of this command to disable the configuration.

Step 3	**show ap config general** **Example:** `Device# show ap config general`	(Optional) Shows the common information of all the APs.