# Converting Autonomous Access Points to Lightweight Mode

## Converting Autonomous Access Points to Lightweight Mode

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

See the Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode document for instructions to upgrade an autonomous access point to lightweight mode:

http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/configuration-guide/b_cg80/b_cg80_chapter_01101010.html

The following are some guidelines for converting autonomous APs to lightweight mode APs:

- All Cisco lightweight access points support 16 BSSIDs per radio and a total of 16 wireless LANs per access point. When a converted access point associates with a controller, wireless LANs with IDs 1 through 16 are pushed to the access point if the AP is part of the default AP group on the controller. You can use other AP group configurations to push other wireless LANs to the new AP.

When a 802.11ac module (the RM3000AC) is added to a 3600 AP, you can have only 8 wireless LANs on the 802.11a/n/ac radio.

- Access points converted to lightweight mode must get an IP address and discover the controller using DHCP, DNS, or IP subnet broadcast.
- It is not possible to perform archive download while CAPWAP image download is in progress or CAPWAP DTLS is flipping. (CSCvn74377)

This section contains the following subsections:

# Restrictions for Converting Autonomous Access Points to Lightweight Mode

- Access points 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 the access point associates to it.
- After you convert an access point to lightweight mode, the console port provides read-only access to the unit.

# Converting Autonomous Access Points to Lightweight Mode

1. Download the CAPWAP file matching your access point model from Cisco.com. Two types of CAPWAP files are available:
    - Fully functional CAPWAP files, identified by the *k9w8* string in their name. When booting this image, the AP is fully functional and can join a controller to obtain its configuration.
    - Recovery mode CAPWAP files, identified by the *rcvk9w8* string in their name. These files are smaller than the fully functional *k9w8* CAPWAP files. When booting *rcvk9w8* files, the AP can join a controller to download a fully functional image. The AP will then reboot, use the fully functional image and rejoin a controller to obtain its configuration.
2. position the image on an FTP server
3. Configure the AP to connect to the FTP server as a FTP client. This is done under global configuration mode, with the command **ip ftp** *username*, and **ip ftp** *password*. For example:

```
Ap#configure terminal
ap(config)#ip ftp username cisco
ap(config)#ip ftp password Cisco123
ap(config)#exit
```

4. Once the parameters are configured, you can start the download process on the AP. Use the **archive download-sw** command, with the **/force-reload** argument to have the AP reboot at the end of the cycle, and **/overwrite** to replace the autonomous code with the CAPWAP code. See the following example:

```
ap#archive download-sw /force-reload /overwrite
ftp://10.100.1.31/ap3g2-rcvk9w8-tar.152-4.JB6.tar
examining image...
Loading ap3g2-rcvk9w8-tar.152-4.JB6.tar
extracting info (273 bytes)!
Image info:
    Version Suffix: rcvk9w8-
    Image Name: ap3g2-rcvk9w8-mx
    Version Directory: ap3g2-rcvk9w8-mx
    Ios Image Size: 2335232
    Total Image Size: 2335232
    Image Feature: WIRELESS LAN|CAPWAP|RECOVERY
    Image Family: ap3g2
    Wireless Switch Management Version: 3.0.51.0
Extracting files...
ap3g2-rcvk9w8-mx/ (directory) 0 (bytes)
extracting ap3g2-rcvk9w8-mx/ap3g2-rcvk9w8-mx (2327653 bytes)!!!!!!!!!
extracting ap3g2-rcvk9w8-mx/info (273 bytes)
```

The AP reboots into lightweight mode and looks for a 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. If the access point is associated to 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.

## Reverting to a Previous Release (CLI)

**Step 1** Log on to the CLI on the controller to which the access point is associated.

**Step 2** Revert from lightweight mode, by entering this command:

**config ap tftp-downgrade** *tftp-server-ip-address filename access-point-name*

**Step 3** Wait until the access point reboots and reconfigure the access point using the CLI or GUI.

## Reverting to a Previous Release 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 *ap3g2-k9w7-tar.152-4.JB4.tar* for a 2700 or 3700 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 **ap3g2-k9w7-tar.default** for a 2700 or a 3700 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

In controller software releases prior to 5.2, the controller may either use self-signed certificates (SSCs) to authenticate access points or send the authorization information to a RADIUS server (if access points have manufactured-installed certificates [MICs]). In controller software release 5.2 or later releases, you can configure the controller to use a local significant certificate (LSC).

Access points manufactured after July 18, 2005 contain a manufactured-installed certificate (MIC). The controller can use this certificate to authenticate the access points. Alternatively, you can use an authentication list on the controller or an external RADIUS server.

## Authorizing Access Points Using SSCs

Cisco APs manufactured prior to 2005 did not have MICs. Tools were provided to generate SSCs on older APs without MICs. Those tools and APs are no longer supported. All such SSCs expired on January 1, 2020. To allow the APs with the expired SSCs to join the controller, use the following command:

**config ap cert-expiry-ignore ssc enable**

This section contains the following subsections:

## Authorizing Access Points for Virtual Controllers Using SSC

Virtual controllers use SSC certificates instead of Manufacturing Installed Certificates (MIC) used by physical controllers. You can configure the controller to allow an AP to validate the SSC of the virtual controller. When an AP validates the SSC, the AP checks if the hash key of the virtual controller matches the hash key stored in its flash. If a match is found, the AP associates with the controller. If a match is not found, the validation fails and the AP disconnects from the controller and restarts the discovery process. By default, hash validation is enabled. An AP must have the virtual controller hash key in its flash before associating with the virtual controller. If you disable hash validation of the SSC, the AP bypasses the hash validation and directly moves to the Run state. APs can associate with a physical controller, download the hash keys and then associate with a virtual controller. If the AP is associated with a physical controller and hash validation is disabled, the AP associates with any virtual controller without hash validation. The hash key of the virtual controller can be configured for a mobility group member. This hash key gets pushed to the APs, so that the APs can validate the hash key of the controller.

### Configuring SSC (GUI)

**Step 1** Choose **Security** > **Certificate** > **SSC** to open the Self Significant Certificates (SSC) page.

The SSC device certification details are displayed.

**Step 2** Select the **Enable SSC Hash Validation** check box to enable the validation of the hash key.

**Step 3** Click **Apply** to commit your changes.

## Configuring SSC (CLI)

**Step 1** To configure hash validation of SSC, enter this command:

**config certificate ssc hash validation** {**enable** | **disable**}

**Step 2** To see the hash key details, enter this command:

**show certificate ssc**

# Authorizing Access Points Using MICs

You can configure controllers to use RADIUS servers to authorize access points using MICs. The controller uses an access point's MAC address as both the username and password when sending the information to a RADIUS server. For example, if the MAC address of the access point is 000b85229a70, both the username and password used by the controller to authorize the access point are 000b85229a70.

# Authorizing Access Points Using LSCs

You can use an LSC if you want your own public key infrastructure (PKI) to provide better security, to have control of your certificate authority (CA), and to define policies, restrictions, and usages on the generated certificates.

The LSC CA certificate is installed on access points and controllers. You need to provision the device certificate on the access point. The access point gets a signed X.509 certificate by sending a certRequest to the controller. The controller acts as a CA proxy and receives the certRequest signed by the CA for the access point.

### Guidelines and Restrictions

- Starting in Release 8.3.112.0, device certification is required to enable LSC. Due to this requirement, we recommend that you follow these guidelines:
  - Ensure that APs are provisioned with LSC for them to associate with LSC-enabled controllers.
  - Ensure that there is no mixed environment where some APs use MIC and some use LSC.
  - You do not have to specify the **Number of attempts to LSC** and **AP Ethernet MAC addresses**.

    For more information about this, see CSCve63755.
- When the CA server is in manual mode and if there is an AP entry in the LSC SCEP table that is pending enrollment, the controller waits for the CA server to send a pending response. If there is no response from the CA server, the controller retries a total of three times to get a response, after which the fallback

mode comes into effect where the AP provisioning times out and the AP reboots and comes up with MIC.

- LSC on controller does not take password challenge. Therefore, for LSC to work, you must disable password challenge on the CA server.

## Configuring Locally Significant Certificates (GUI)

**Step 1** Choose **Security** > **Certificate** > **LSC** to open the Local Significant Certificates (LSC) - General page.

**Step 2** In the CA Server URL text box, enter the URL to the CA server. You can enter either a domain name or an IP address.

**Step 3** In the Params text boxes, enter the parameters for the device certificate. [Optional] The key size is a value from 2048 to 4096 (in bits), and the default value is 2048.

**Step 4** Click **Apply** to commit your changes.

**Step 5** To add the CA certificate into the controller’s certificate database, hover your cursor over the blue drop-down arrow for the certificate type and choose **Add**.

**Step 6** To add the device certificate into the controller's certificate database, hover your cursor over the blue drop-down arrow for the certificate type and choose **Add**.

**Step 7** Select the **Enable LSC on Controller** check box to enable the LSC on the system.

**Step 8** Click **Apply** to commit your changes.

**Step 9** Choose the **AP Provisioning** tab to open the Local Significant Certificates (LSC) - AP Provisioning page.

**Step 10** Select the **Enable** check box and click **Update** to provision the LSC on the access point.

**Step 11** Click **Apply** to commit your changes.

**Step 12** When a message appears indicating that the access points will be rebooted, click **OK**.

**Step 13** In the **Number of Attempts to LSC** field, enter the number of times that the access point attempts to join the controller using an LSC before the access point reverts to the default certificate (MIC or SSC). The range is 0 to 255 (inclusive), and the default value is 3.

**Note** If you are using Release 8.3.112.0 or a later release, due to the requirement per CSCve63755, you do not have to perform this task. You must ensure that APs are provisioned with LSC prior to associating with LSC-enabled controllers.

**Note** If you set the number of retries to a nonzero value and the access point fails to join the controller using an LSC after the configured number of retries, the access point reverts to the default certificate. If you set the number of retries to 0 and the access point fails to join the controller using an LSC, the access point does not attempt to join the controller using the default certificate.

**Note** If you are configuring LSC for the first time, we recommend that you configure a nonzero value.

**Step 14** Enter the access point MAC address in the **AP Ethernet MAC Addresses** field and click **Add** to add access points to the provision list.

**Note** If you are using Release 8.3.112.0 or a later release, due to the requirement per CSCve63755, you do not have to perform this task. You must ensure that APs are provisioned with LSC prior to associating with LSC-enabled controllers.

**Note** To remove an access point from the provision list, hover your cursor over the blue drop-down arrow for the access point and choose **Remove**.

**Note** If you configure an access point provision list, only the access points in the provision list are provisioned when you enable AP provisioning. If you do not configure an access point provision list, all access points with a MIC or SSC certificate that join the controller are LSC provisioned.

**Step 15** Click **Apply** to commit your changes.

**Step 16** Click **Save Configuration** to save your changes.

## Configuring Locally Significant Certificates (CLI)

**Step 1** Configure the URL to the CA server by entering this command:

**config certificate lsc ca-server** *http://url:port/path*

where *url* can be either a domain name or IP address.

**Note** You can configure only one CA server. To configure a different CA server, delete the configured CA server using the **config certificate lsc ca-server delete** command, and then configure a different CA server.

**Step 2** Configure the parameters for the device certificate by entering this command:

**config certificate lsc subject-params** *country state city orgn dept e-mail*

**Note** The common name (CN) is generated automatically on the access point using the current MIC/SSC format C*xxxx-MacAddr*, where *xxxx* is the product number.

**Step 3** [Optional] Configure a key size by entering this command:

**config certificate lsc other-params** *keysize*

The *keysize* is a value from 2048 to 4096 (in bits), and the default value is 2048.

**Step 4** Add the LSC CA certificate into the controller's certificate database by entering this command:

**config certificate lsc ca-cert** {**add** | **delete**}

**Step 5** Add the LSC device certificate into the controller's certificate database by entering this command:

**config certificate lsc device-cert** {**add** | **delete**}

**Step 6** Enable LSC on the system by entering this command:

**config certificate lsc** {**enable** | **disable**}

**Step 7** Provision the LSC on the access point by entering this command:

**config certificate lsc ap-provision** {**enable** | **disable** }

**Step 8** Configure the number of times that the access point attempts to join the controller using an LSC before the access point reverts to the default certificate (MIC or SSC) by entering this command:

**config certificate lsc ap-provision revert-cert** *retries*

where *retries* is a value from 0 to 255, and the default value is 3.

**Note** If you are using Release 8.3.112.0 or a later release, due to the requirement per CSCve63755, you do not have to perform this task. You must ensure that APs are provisioned with LSC prior to associating with LSC-enabled controllers.

**Note** If you set the number of retries to a nonzero value and the access point fails to join the controller using an LSC after the configured number of retries, the access point reverts to the default certificate. If you set the number of retries to 0 and the access point fails to join the controller using an LSC, the access point does not attempt to join the controller using the default certificate.

**Note** If you are configuring LSC for the first time, Cisco recommends that you configure a nonzero value.

**Step 9** Add access points to the provision list by entering this command:

**config certificate lsc ap-provision auth-list add** *AP_mac_addr*

**Note** If you are using Release 8.3.112.0 or a later release, due to the requirement per CSCve63755, you do not have to perform this task. You must ensure that APs are provisioned with LSC prior to associating with LSC-enabled controllers.

**Note** To remove access points from the provision list, enter the **config certificate lsc ap-provision auth-list delete** *AP_mac_addr command.*

**Note** If you configure an access point provision list, only the access points in the provision list are provisioned when you enable AP provisioning (in *Step 8*). If you do not configure an access point provision list, all access points with a MIC or SSC certificate that join the controller are LSC provisioned.

**Step 10** See the LSC summary by entering this command:

**show certificate lsc summary**

Information similar to the following appears:

```
LSC Enabled.......................................... Yes
LSC CA-Server........................................ http://10.0.0.1:8080/caserver

LSC AP-Provisioning.................................. Yes
 Provision-List.................................. Not Configured
 LSC Revert Count in AP reboots.................. 3

LSC Params:
 Country......................................... US
 State........................................... ca
 City............................................ ss
 Orgn............................................ org
 Dept............................................ dep
 Email........................................... dep@co.com
 KeySize......................................... 2048

LSC Certs:
 CA Cert......................................... Not Configured
 RA Cert....................................... Not Configured
```

**Step 11** See details about the access points that are provisioned using LSC by entering this command:

**show certificate lsc ap-provision**

Information similar to the following appears:

```
LSC AP-Provisioning.......................... Yes
Provision-List............................... Present

Idx  Mac Address
---  ------------
1  00:18:74:c7:c0:90
```

# Authorizing Access Points (GUI)

**Step 1** Choose **Security** > **AAA** > **AP Policies** to open the **AP Policies** page.

**Step 2** If you want the access point to accept self-signed certificates (SSCs), manufactured-installed certificates (MICs), or local significant certificates (LSCs), select the appropriate check box.

**Step 3** If you want the access points to be authorized using a AAA RADIUS server, check the **Authorize MIC APs against auth-list or AAA** check box.

**Step 4** If you want the access points to be authorized using an LSC, check the **Authorize LSC APs against auth-list** check box.

Enter the Ethernet MAC address for all APs except when in bridge mode (where you need to enter the radio MAC address).

**Step 5** Click **Apply** to commit your changes.

**Step 6** Follow these steps to add an access point to the controller's authorization list:

a) Click **Add** to access the **Add AP to Authorization List** area.
b) In the **MAC Address** field, enter the MAC address of the access point.
c) From the **Certificate Type** drop-down list, choose **MIC**, **SSC**, or **LSC**.
d) Click **Add**. The access point appears in the access point authorization list.

**Note** To remove an access point from the authorization list, hover your cursor over the blue drop-down arrow for the access point and choose **Remove**.

**Note** To search for a specific access point in the authorization list, enter the MAC address of the access point in the Search by MAC text box and click **Search**.

# Authorizing Access Points (CLI)

### Procedure

- Configure an access point authorization policy by entering this command:

  **config auth-list ap-policy** {**authorize-ap** {**enable** | **disable**} | **authorize-lsc-ap** {**enable** | **disable**}}

- Configure an access point to accept manufactured-installed certificates (MICs), self-signed certificates (SSCs), or local significant certificates (LSCs) by entering this command:

  **config auth-list ap-policy** {**mic** | **ssc** | **lsc** {**enable** | **disable**}}

- Configure the user name to be used in access point authorization requests.

**config auth-list ap-policy** {**authorize-ap username** {**ap_name** | **ap_mac** | **both**}}

- Add an access point to the authorization list by entering this command:

  **config auth-list add** {**mic** | **ssc** | **lsc**} *ap_mac* [*ap_key*]

  where *ap_key* is an optional key hash value equal to 20 bytes or 40 digits.

**Note** To delete an access point from the authorization list, enter this command: **config auth-list delete ap_mac**.

- See the access point authorization list by entering this command:

  **show auth-list**

# Configuring VLAN Tagging for CAPWAP Frames from Access Points

## VLAN Tagging for CAPWAP Frames from 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.

For more information about which APs support CAPWAP VLAN Tagging, see Feature Matrix for Wave 2 and 802.11ax (Wi-Fi 6) Access Points.

This section contains the following subsections:

## Configuring VLAN Tagging for CAPWAP Frames from Access Points (GUI)

**Step 1** Choose **Wireless** > **Access Points** > **All APs** to open the **All APs** page.

**Step 2** Click the AP name from the list of AP names to open the Details page for the AP.

**Step 3** Click the **Advanced** tab.

**Step 4** In the **VLAN Tagging** area, check the **VLAN Tagging** check box.

**Step 5** In the **Trunk VLAN ID** field, enter an ID.

If the AP is unable to route traffic through the specified trunk VLAN after about 10 minutes, the AP performs a recovery procedure by rebooting and sending CAPWAP frames in untagged mode to try and reassociate with the controller. The controller sends a trap to a trap server such as the Cisco Prime Infrastructure, which indicates the failure of the trunk VLAN.

If the AP is unable to route traffic through the specified trunk VLAN, it untags the packets and reassociates with the controller. The controller sends a trap to a trap server such as the Cisco Prime Infrastructure, which indicates the failure of the trunk VLAN.

If the trunk VLAN ID is 0, the AP untags the CAPWAP frames.

The VLAN Tag status is displayed showing whether the AP tags or untags the CAPWAP frames.

**Step 6** Click **Apply**.

**Step 7** You are prompted with a warning message saying that the configuration will result in a reboot of the AP. Click **OK** to continue.

**Step 8** Click **Save Configuration**.

### What to do next

After the configuration, the switch or other equipment connected to the Ethernet interface of the AP must also be configured to support tagged Ethernet frames.

## Configuring VLAN Tagging for CAPWAP Frames from Access Points (CLI)

**Step 1** Configure VLAN tagging for CAPWAP frames from APs by entering this command:

**config ap ethernet tag** {**disable** | **id** *vlan-id*} {*ap-name* | **all**}

**Step 2** You can see VLAN tagging information for an AP or all APs by entering this command:

**show ap ethernet tag** {**summary** | *ap-name*}

### What to do next

After the configuration, the switch or other equipment connected to the Ethernet interface of the AP must also be configured to support tagged Ethernet frames.

# Using DHCP Option 43 and DHCP Option 60

Cisco access points use the type-length-value (TLV) format for DHCP option 43. DHCP servers must may be programmed to return the option based on the access point’s DHCP Vendor Class Identifier (VCI) string (DHCP option 60).

The format of the TLV block is as follows:

- Type: 0xf1 (decimal 241)
- Length: Number of controller IP addresses * 4
- Value: List of the IP addresses of controller management interfaces

See the product documentation for your DHCP server for instructions on configuring DHCP option 43. For more information about DHCP option 43, see https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/97066-dhcp-option-43-00.html.

If the AP is ordered with the Service Provider Option - AIR-OPT60-DHCP selected, the VCI string for that AP will be different than those listed above. The VCI string will have the “ServiceProvider”. For example, a 3600 with this option will return this VCI string: "Cisco AP c3600-ServiceProvider".

**Note** The controller IP address that you obtain from the DHCP server should be a unicast IP address. Do not configure the controller IP address as a multicast address when configuring DHCP Option 43.

# Troubleshooting the Access Point Join Process

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

Controller software release 5.2 or later releases enable you to configure the access points to send all CAPWAP-related errors to a syslog server. You do not need to enable any debug commands on the controller because all of the CAPWAP error messages can be viewed from the syslog server itself.

The state of the access point is not maintained on the controller until it receives a CAPWAP join request from the access point, so it can be difficult to determine why the CAPWAP discovery request from a certain access point was rejected. In order to troubleshoot such joining issues without enabling CAPWAP debug commands on the controller, the controller collects information for all access points that send a discovery message to this controller and maintains information for any access points that have successfully joined this controller.

The controller collects all 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.

You can view join-related information for the following numbers of access points:

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.

If any of these conditions are met and the access point has not yet joined a controller, 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 syslog messages to this IP address.

**Note** The access point joins the controller with a DHCP address from an internal DHCP pool configured on WLC. When the DHCP lease address is deleted in WLC, the access point reloads with the following message:

AP Rebooting: Reset Reason - Admin Reload. This is a common behavior in Cisco Wave 1 and Wave 2 APs.

You can also configure the syslog server IP address through the access point CLI, provided the access point is currently not connected to the controller by entering the **capwap ap log-server** *syslog_server_IP_address command.*

When the access point joins a controller for the first time, the controller pushes the global syslog server IP address (the default is 255.255.255.255) to the access point. After that, the access point sends all syslog messages to this IP address, until it is overridden by one of the following scenarios:

- 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 **config ap syslog host global** *syslog_server_IP_address* command. In this case, the controller pushes the new global syslog server IP address to the access point.

- The access point is still connected to the same controller, and a specific syslog server IP address has been configured for the access point on the controller using the **config ap syslog host specific** *Cisco_AP syslog_server_IP_address* command. In this case, the controller pushes the new specific syslog server IP address to the access point.
- The access point gets disconnected from the controller, and the syslog server IP address has been configured from the access point CLI using the **lwapp ap log-server** *syslog_server_IP_address* command. This command works only if the access point is not connected to any controller.
- The access point gets disconnected from the controller and joins another controller. In this case, the new controller pushes 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 syslog messages to the new IP address, provided the access point can reach the syslog server IP address.

You can configure the syslog server for access points using the controller GUI and view the access point join information using the controller GUI or CLI.

When the name of the access point is modified using the **config ap name** *new_name old_name* command, then the new AP name is updated. You can view the new AP name updated in both the **show ap join stats summary all** as well as the **show ap summary** commands.

**Note** When an AP in a Release 8.0 image tries to join Cisco WLC, Release 8.3 (having Release 8.2 as the primary image and Release 8.2.1 as the secondary image on Flash), the AP goes into a perpetual loop. (Note that the release numbers are used only as an example to illustrate the scenario of three different images and does not apply to the releases mentioned.) This loop occurs due to version mismatch. After the download, when the AP compares its image with the Cisco WLC image, there will be a version mismatch. The AP will start the entire process again, resulting in a loop.

## Configuring the Syslog Server for Access Points (CLI)

**Step 1** Perform one of the following:

- To configure a global syslog server for all access points that join this controller, enter this command:

  **config ap syslog host global** *syslog_server_IP_address*

  **Note** By default, the global syslog server IPv4/IPv6 address for all access points is 255.255.255.255. Make sure that the access points can reach the subnet on which the syslog server resides before configuring the syslog server on the controller. If the access points cannot reach this subnet, the access points are unable to send out syslog messages.

  **Note** Only one Syslog Server is used for both IPv4 and IPv6.

- To configure a syslog server for a specific access point, enter this command:

  **config ap syslog host specific** *Cisco_AP syslog_server_IP_address*

  **Note** By default, the syslog server IPv4/IPv6 address for each access point is 0.0.0.0, which indicates that the access point is not yet set. When the default value is used, the global access point syslog server IP address is pushed to the access point.

**Step 2** Enter the **save config** command to save your changes.

**Step 3** See the global syslog server settings for all access points that join the controller by entering this command:

**show ap config global**

Information similar to the following appears:

```
AP global system logging host.................... 255.255.255.255
```

**Step 4** See the syslog server settings for a specific access point by entering this command:

**show ap config general** *Cisco_AP*

# Viewing Access Point Join Information

Join statistics for an access point that sends a CAPWAP discovery request to the controller at least once are maintained on the controller even if the access point is rebooted or disconnected. These statistics are removed only when the controller is rebooted or when you choose to clear the statistics.

## Viewing Access Point Join Information (GUI)

**Step 1** Choose **Monitor** > **Statistics** > **AP Join** to open the AP Join Stats page.

This page lists all of the access points that are joined to the controller or that have tried to join. It shows the radio MAC address, access point name, current join status, Ethernet MAC address, IP address, and last join time for each access point.

The total number of access points appears in the upper right-hand corner of the page. If the list of access points spans multiple pages, you can view these pages by clicking the page number links. Each page shows the join statistics for up to 25 access points.

**Note** If you want to remove an access point from the list, hover your cursor over the blue drop-down arrow for that access point and click **Remove**.

**Note** If you want to clear the statistics for all access points and start over, click **Clear Stats on All APs**.

**Step 2** If you want to search for specific access points in the list of access points on the AP Join Stats page, follow these steps to create a filter to display only access points that meet certain criteria (such as MAC address or access point name).

**Note** This feature is especially useful if your list of access points spans multiple pages, preventing you from viewing them all at once.

a) Click **Change Filter** to open the Search AP dialog box.

b) Select one of the following check boxes to specify the criteria used when displaying access points:

- **MAC Address**—Enter the base radio MAC address of an access point.
- **AP Name**—Enter the name of an access point.

**Note** When you enable one of these filters, the other filter is disabled automatically.

c) Click **Find** to commit your changes. Only the access points that match your search criteria appear on the AP Join Stats page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC Address:00:1e:f7:75:0a:a0 or AP Name:pmsk-ap).

**Note** If you want to remove the filter and display the entire access point list, click **Clear Filter**.

**Step 3** To see detailed join statistics for a specific access point, click the radio MAC address of the access point. The AP Join Stats Detail page appears.

This page provides information from the controller's perspective on each phase of the join process and shows any errors that have occurred.

## Viewing Access Point Join Information (CLI)

Use these CLI commands to see access point join information:

- See the MAC addresses of all the access points that are joined to the controller or that have tried to join by entering this command:

  **show ap join stats summary all**

- See the last join error detail for a specific access point by entering this command:

  **show ap join stats summary** *ap_mac*

  where *ap_mac* is the MAC address of the 802.11 radio interface.

  **Note** To obtain the MAC address of the 802.11 radio interface, enter the **show interfaces Dot11Radio 0** command on the access point.

  Information similar to the following appears:

```
Is the AP currently connected to controller................ Yes
Time at which the AP joined this controller last time...... Aug 21
 12:50:36.061
Type of error that occurred last.......................... AP got
 or has been disconnected
Reason for error that occurred last....................... The AP
 has been reset by the controller
Time at which the last join error occurred............. Aug 21
12:50:34.374
```

- See all join-related statistics collected for a specific access point by entering this command:

  **show ap join stats detailed** *ap_mac*

  Information similar to the following appears:

```
Discovery phase statistics
- Discovery requests received............................. 2
- Successful discovery responses sent..................... 2
- Unsuccessful discovery request processing............... 0
- Reason for last unsuccessful discovery attempt.......... Not applicable
- Time at last successful discovery attempt................ Aug 21 12:50:23.335
- Time at last unsuccessful discovery attempt.............. Not applicable

Join phase statistics
- Join requests received.................................. 1
- Successful join responses sent.......................... 1
- Unsuccessful join request processing.................... 1
- Reason for last unsuccessful join attempt................ RADIUS authorization
 is pending for the AP
- Time at last successful join attempt..................... Aug 21 12:50:34.481
- Time at last unsuccessful join attempt................... Aug 21 12:50:34.374

Configuration phase statistics
- Configuration requests received......................... 1
- Successful configuration responses sent................. 1
- Unsuccessful configuration request processing........... 0
- Reason for last unsuccessful configuration attempt....... Not applicable
- Time at last successful configuration attempt........... Aug 21 12:50:34.374
- Time at last unsuccessful configuration attempt.......... Not applicable

Last AP message decryption failure details
- Reason for last message decryption failure............... Not applicable

Last AP disconnect details
- Reason for last AP connection failure.................... The AP has been reset by
the controller

Last join error summary
- Type of error that occurred last......................... AP got or has been
disconnected
- Reason for error that occurred last...................... The AP has been reset by
the controller
- Time at which the last join error occurred.............. Aug 21 12:50:34.374
```

- Clear the join statistics for all access points or for a specific access point by entering this command:

  **clear ap join stats** {**all** | *ap_mac*}

# Sending Commands to Access Points

You can enable the controller to send commands to an AP by entering this command:

**debug ap** {**enable** | **disable** | **command** *cmd*} *Cisco_AP*

When this feature is enabled, the controller sends commands to the AP as character strings. You can send any command supported by Cisco APs. The immediate output from the AP command is sent to the controller terminal session after pressing **`Enter`**; however, the output from AP debugging is not sent to the controller terminal.

### Example

```
<Cisco Controller> debug ap enable AP3802i

<Cisco Controller>debug ap command "show clock" ap-name AP3802i

<Cisco Controller>*spamApTask7: May 05 16:52:05.406: a0:e0:af:f9:37:e0
AP3802i: *16:52:05 UTC Wed May 5 2021
```

```
<Cisco Controller> debug ap disable AP3802i
```

# Understanding How Access Points Send Crash Information to the Controller

When an AP unexpectedly reboots, the AP 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 info copy is removed from the AP flash memory when the controller pulls it from the AP.

# Understanding How Access Points Send Radio Core Dumps to the Controller

When a radio module in an AP generates a core dump, the AP stores the core dump file of the radio on its local flash memory at the time of the radio crash. It sends a notification message to the controller indicating which radio generated a core dump file. The controller sends a trap that alerts you so that you can retrieve the radio core file from the AP.

The retrieved core file is stored in the controller flash and can be uploaded through TFTP or FTP to an external server for analysis. The core file is removed from the AP flash memory when the controller pulls it from the AP.

### Restrictions

This feature is supported only on Cisco Wave 1 (IOS-based) and 802.11n APs.

## Retrieving Radio Core Dumps (CLI)

**Step 1** Transfer the radio core dump file from the access point to the controller by entering this command:

**config ap crash-file get-radio-core-dump** *slot Cisco_AP*

For the *slot* parameter, enter the slot ID of the radio that crashed.

**Step 2** Verify that the file was downloaded to the controller by entering this command:

**show ap crash-file**

Information similar to the following appears:

```
Local Core Files:
lrad_APxxxx.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.
```

## Uploading Radio Core Dumps (GUI)

**Step 1** Choose **Commands** > **Upload File** to open the Upload File from Controller page.

**Step 2** From the File Type drop-down list, choose **Radio Core Dump**.

**Step 3** From the Transfer Mode drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP**

**Step 4** In the IP Address text box, enter the IP address of the server.

**Step 5** In the File Path text box, enter the directory path of the file.

**Step 6** In the File Name text box, enter the name of the radio core dump file.

**Note** The *filename* that you enter should match the filename generated on the controller. You can determine the *filename* on the controller by entering the **show ap crash-file** command.

**Step 7** If you chose FTP as the Transfer Mode, follow these steps:

a) In the Server Login Username text box, enter the FTP server login name.
b) In the Server Login Password text box, enter the FTP server login password.
c) In the Server Port Number text box, enter the port number of the FTP server. The default value for the server port is 21.

**Step 8** Click **Upload** to upload the radio core dump file from the controller. A message appears indicating the status of the upload.

## Uploading Radio Core Dumps (CLI)

**Step 1** Transfer the file from the controller to a server by entering these commands:

- **transfer upload mode** {**tftp** | **ftp** | **sftp**}
- **transfer upload datatype radio-core-dump**
- **transfer upload serverip** *server_ip_address*
- **transfer upload path** *server_path_to_file*
- **transfer upload filename** *filename*

**Note** The *filename* that you enter should match the filename generated on the controller. You can determine the *filename* on the controller by entering the **show ap crash-file** command.

**Note** Ensure that the *filename* and *server_path_to_file* do not contain these special characters: \, :, *, ?, ", <, >, and |. You can use only / (forward slash) as the path separator. If you use the disallowed special characters in the filename, then the special characters are replaced with _ (underscores); and if you use the disallowed special characters in the *server_path_to_file*, then the path is set to the root path.

**Step 2** If you are using an FTP server, also enter these commands:

- **transfer upload username** *username*
- **transfer upload password** *password*
- **transfer upload port** *port*

**Note** The default value for the *port* parameter is 21.

**Step 3** View the updated settings by entering this command:

**transfer upload start**

**Step 4** When prompted to confirm the current settings and start the software upload, answer **y**.

# 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.

## Uploading Access Point Core Dumps (GUI)

**Step 1** Choose **Wireless** > **Access Points** > **All APs** > *access point name* > and choose the **Advanced** tab to open the All APs > Details for (Advanced) page.

**Step 2** Select the **AP Core Dump** check box to upload a core dump of the access point.

**Step 3** In the TFTP Server IP text box, enter the IP address of the TFTP server.

**Step 4** In the File Name text box, enter a name of the access point core dump file (such as *dump.log*).

**Step 5** Select the **File Compression** check box to compress the access point core dump file. When you enable this option, the file is saved with a .gz extension (such as *dump.log.gz*). This file can be opened with WinZip.

**Step 6** Click **Apply** to commit your changes.

**Step 7** Click **Save Configuration** to save your changes.

## Uploading Access Point Core Dumps (CLI)

**Step 1** Upload a core dump of the access point by entering this command on the controller:

**config ap core-dump enable** *tftp_server_ip_address filename* {**compress** | **uncompress**} {*ap_name* | **all**} where

- *tftp_server_ip_address* is the IP address of the TFTP server to which the access point sends core dump files.

  **Note** The access point must be able to reach the TFTP server.

- *filename* is the name that the access points uses to label the core file.

- **compress** configures the access point to send compressed core files whereas **uncompress** configures the access point to send uncompressed core files.

  **Note** When you choose **compress**, the file is saved with a .gz extension (for example, dump.log.gz). This file can be opened with WinZip.

- *ap_name* is the name of a specific access point for which core dumps are uploaded and **all** is all access points converted to lightweight mode.

**Step 2** Enter the **save config** command to save your changes.

# Viewing the AP Crash Log Information

Whenever the controller reboots or upgrades, the AP crash log information gets deleted from the controller. We recommend that you make a backup of AP crash log information before rebooting or upgrading the controller.

### Restrictions

This feature is supported only on Cisco Wave 1 (IOS-based) and 802.11n APs.

## Viewing the AP Crash Log information (GUI)

### Procedure

- Choose **Management** > **Tech Support** > **AP Crash Log** to open the AP Crash Logs page.

## Viewing the AP Crash Log information (CLI)

**Step 1** Verify that the crash file was downloaded to the controller by entering this command:

**show ap crash-file**

Information similar to the following appears:

```
Local Core Files:
lrad_APxxxx.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.
```

**Step 2** See the contents of the AP crash log file by entering this command:

**show ap crash-file** *Cisoc_AP*

# Viewing MAC Addresses of 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** window, the controller lists APs by radio MAC address.

# Disabling the Reset Button on Access Points to Lightweight Mode

You can disable the reset button on APs to lightweight mode. The reset button is labeled MODE on the outside of the AP.

Use this command to disable or enable the reset button on one or all APs joined to a controller:

**config ap rst-button** {**enable** | **disable**} {*ap-name*}

The reset button on APs is enabled by default.

### Restrictions

This feature is supported only on Cisco Wave 1 (IOS-based) and 802.11n APs.

# Configuring a Static IP Address on 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.

**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.

## Configuring a Static IP Address (GUI)

**Step 1** Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.

**Step 2** Click the name of the access point for which you want to configure a static IP address. The All APs > Details for (General) page appears.

**Step 3** Under IP Config, select the **Static IP (IPv4/IPv6)** check box if you want to assign a static IP address to this access point. The default value is unselected.

**Note** The static IP configured on the AP will take precedence over the preferred mode configured on the AP. For example: If AP has static IPV6 address and prefer-mode is set to IPV4, then the AP will join over IPv6.

**Step 4** Enter the static IPv4/IPv6 address of the access point, subnet mask/ prefix length assigned to the access point IPv4/IPv6 address, and the IPv4/IPv6 gateway of the access point in the corresponding text boxes.

**Step 5** Click **Apply** to commit your changes. The access point reboots and rejoins the controller, and the static IPv4/IPv6 address that you specified in Step 4 is sent to the access point.

**Step 6** After the static IPv4/IPv6 address has been sent to the access point, you can configure the DNS server IP address and domain name as follows:

a) In the DNS IP Address text box, enter the IPv4/IPv6 address of the DNS server.
b) In the Domain Name text box, enter the name of the domain to which the access point belongs.
c) Click **Apply** to commit your changes.
d) Click **Save Configuration** to save your changes.

## Configuring a Static IP Address (CLI)

**Step 1** Configure a static IP address on the access point by entering this command:

For IPv4—**config ap static-ip enable** *Cisco_AP ip_address mask gateway*

For IPv6—**config ap static-ip enable** *Cisco_AP ip_address prefix_length gateway*

**Note** To disable static IP for the access point, enter the **config ap static-ip disable** *Cisco_AP* command.

**Note** The static IP configured on the AP takes precedence over the preferred mode that is configured on the AP. For example: If AP has static IPv6 address and prefer-mode is set to IPv4, then the AP will join over IPv6.

**Step 2** Enter the **save config** command to save your changes.

The access point reboots and rejoins the controller, and the static IP address that you specified in Step 1 is pushed to the access point.

**Step 3** After the static IPv4/IPv6 address has been sent to the access point, you can configure the DNSv4/DNSv6 server IP address and domain name as follows:

a) To specify a DNSv4/DNSv6 server so that a specific access point or all access points can discover the controller using DNS resolution, enter this command:

**config ap static-ip add nameserver** {*Cisco_AP* | **all**} *ip_address*

**Note** To delete a DNSv4/DNSv6 server for a specific access point or all access points, enter the **config ap static-ip delete nameserver** {*Cisco_AP* | **all**} command.

b) To specify the domain to which a specific access point or all access points belong, enter this command:

**config ap static-ip add domain** {*Cisco_AP* | **all**} *domain_name*

**Note** To delete a domain for a specific access point or all access points, enter this command: **config ap static-ip delete domain** {*Cisco_AP* | **all**}.

c) Enter the **save config** command to save your changes.

**Step 4** See the IPv4/IPv6 address configuration for the access point by entering this command:

- For IPv4:

  **show ap config general** *Cisco_AP*

  Information similar to the following appears:

```
show ap config general <Cisco_AP>

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
...
```

- For IPv6:

  **show ap config general** *Cisco_AP*

  Information similar to the following appears:

```
show ap config general <Cisco_AP>

Cisco AP Identifier.............................. 16
Cisco AP Name.................................... AP2602I-A-K9-1
...
IPv6 Address Configuration....................... DHCPv6
IPv6 Address..................................... 2001:9:2:16:1ae:a1da:c2c7:44b
IPv6 Prefix Length............................... 128
Gateway IPv6 Addr................................ fe80::c60a:cbff:fe79:53c4
NAT External IP Address.......................... None

...
```

```
IPv6 Capwap UDP Lite............................ Enabled
Capwap Prefer Mode.............................. Ipv6 (ApGroup Config)
Hotspot Venue Group............................. Unspecified
Hotspot Venue Type.............................. Unspecified
DNS server IP ............................ Not Available
```

# Supporting Oversized Access Point Images

Controller software release 5.0 or later releases allow you to upgrade to an oversized access point image by automatically deleting the recovery image to create sufficient space.

The recovery image provides a backup image that can be used if an access point power-cycles during an image upgrade. The best way to avoid the need for access point recovery is to prevent an access point from power-cycling during a system upgrade. If a power-cycle occurs during an upgrade to an oversized access point image, you can recover the access point using the TFTP recovery procedure.

## Recovering the Access Point—Using the TFTP Recovery Procedure

**Step 1** Download the required recovery image from Cisco.com (for example, ap3g2-rcvk9w8-tar.152-4.JB6.tar for 2700 or 3700 APs) 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 may remove the TFTP server.