Management

This chapter describes how to manage the network and upgrade the software. It contains the following topics:

About Management Access Interface

The Management Access Interface is the default interface for in-band management of the Primary AP and connectivity to enterprise services. It is also used for communication between the Primary AP and connected access points (APs). The management interface has the consistently pingable in-band interface IP address on the Primary AP. You can access the web interface of the Primary AP by entering the management interface IP address of the Primary AP or using *https://ciscobusiness.cisco* in your browser's address bar.

For APs, the Primary AP requires one management interface to control all communications and one AP manager interface to control all Primary AP-to-Access Point communications, regardless of the number of ports.

Setting Up Management Access Interface

To enable or disable the different types of management access to the Primary AP, follow the steps below.

Step 1 Navigate to **Management** > **Access**.

The **Access** window is displayed. The number of enabled management types are displayed at the top of the window.

Step 2 You can enable or disable the following types of management access to the Primary AP, by toggling the switch buttons.

- **HTTP Access**—This enables the HTTP access mode, which allows you to access the Primary AP GUI using `http://<ip-address>` or *http://ciscobusiness.cisco* through a web browser. By default, this is **Enabled**.

  HTTP access mode is not a secure connection.

- **HTTPs Access**—A secure access for Primary AP UI, using `https://<ip-address>` or *https://ciscobusiness.cisco*. By default, this is **Enabled**.
- **HTTP-HTTPS Maximum Session**—To set the maximum number of web sessions (HTTP/HTTPS). It can range between 1-15. By default, you can support up to 15 sessions.
- **WebAuth SecureWeb**—Enable web based authentication for Guest WLAN in order to access or visit the Guest authentication page over HTTPS.

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

You can access the CBW AP UI via HTTP or HTTPS connection. By default, HTTP connection will be redirected to HTTPS connection. If you enter *ciscobusiness.cisco*, you will be redirected to *https://ciscobusiness.cisco* which is a secured connection.

HTTP Access	HTTPS Access	UI Accessibility
On	On	HTTP->HTTPS Redirect
Off	On	HTTPS only
On	Off	HTTP only
Off	Off	UI does not load

Limitation of Web Based Management Sessions

This feature helps to provision the number of sessions supported for the Primary AP UI. It is implemented by limiting the number of UI management sessions based on the number of HTTP/HTTPS sessions configured by the user.

1. Navigate to **Management** > **Access**.
2. In the **HTTP-HTTPS Maximum Sessions** field, set the number of allowed sessions between 1 and 15.
3. Click **Apply** to save the changes. Once configured, try to access the web sessions from the client using management IP.

If the number of users exceeds the configured value, the session access is restricted and you will be prompted for a reload of session.

Managing User Priority Order

When multiple databases are configured, it is important to configure the admin account user priority. To configure the priority, follow the steps below.

Step 1 Enable **Expert View** on the Primary AP UI. To switch to expert view, click the bidirectional arrow icon on the top right of the home screen.

Step 2 Navigate to **Management** > **Admin Accounts**.

Step 3 Click **Management User Priority Order**.

By default, the local database is always queried first. If the username is not found, the Primary AP switches to the RADIUS server if configured for RADIUS or to the TACACS+ server if configured for TACACS+. The default priority setting is in the order of Local Admin Accounts and then RADIUS.

Step 4 To change the priority, between TACACS+ and RADIUS, click the drag icon and it move UP or DOWN.

Note Local Admin Accounts cannot be moved to Priority 3. It can be in the order of either 1 or 2 only.

Step 5 Click **Apply** to save the changes.

Managing Admin Accounts

You can manage the Cisco Business Wireless AP network through the Primary AP UI based on the privileges assigned to your user account. This prevents unauthorized users from accessing or configuring the Primary AP.

You can log in to the Primary AP UI using an admin account having one of the following access types:

Read/Write	This administrative account has complete access to view and modify the Primary AP configuration.
Read Only	This limited access administrative account allows the user to only view the Primary AP configuration. This user is restricted from making any changes to the configuration.
Lobby Ambassador	This restricted administrative account allows the user to only create and manage guest user accounts. The lobby ambassador can also print or email the guest user account credentials.

For information about creating guest user accounts, see Creating a Guest User Account, on page 5.

Adding an Admin Account

Step 1 Navigate to **Management** > **Admin Accounts**.

The total count of admin accounts on the Primary AP is displayed at the top of this window while the table provides a detailed listing of all the available admin accounts.

Step 2 Click **Add New User** to add a new admin user.

Step 3 In the **Add/Edit Local admin account** window, set the following parameters as required:

- **Username**—The login user name used by the administrative user. User name must be unique. You can enter up to 24 ASCII characters.

Note User names are case sensitive.

- **Access**—Set one of the following access privileges for the administrator:
  - **Read Only**
  - **Read/Write**
  - **Lobby Ambassador**
- **Password**—The password is case sensitive and can contain 8-127 ASCII characters. When specifying a password, ensure the following:
  - The password must include a combination of lowercase letters, uppercase letters, digits, and special characters. The special characters can be **~**, **!**, **@**, **#**, **$**, **%**, ^, **&**, *****.
  - No character in the password can be repeated more than three times consecutively.
  - The new password cannot be the same as the associated username or the username reversed.
  - The password cannot be cisco, ocsic, or any variant obtained by changing the capitalization of the letters in the word Cisco. In addition, you cannot substitute 1, I, or ! for i, 0 for o, or $ for s.

Step 4 Re-enter the same password in **Confirm Password**.

Step 5 Enable **Show Password** to view the password entered.

Step 6 **Password Expiry**—This option determines when passwords expire admin accounts. By default, the password expiry is **disabled** and the expiry value is set to 0 (The Admin Account will remain constant until deleted). If the password expiry is enabled, then the value is set to 180 days by default. You can set the value ranging from 1 - 180 days.

Note If the Primary AP UI is logged in with an admin account that has the password expiry enabled, a reminder message will pop-up when you log in. This message will start popping up only when there are 7 days left for password expiry.

When the expiry value is passed, the admin account will be deleted.

Step 7 Click **Update** to save your changes.

Editing an Admin Account

Step 1 Navigate to **Management** > **Admin Accounts**.

The **Admin Accounts** page is displayed, along with the list of all the admin accounts present on the Primary AP. The total count of admin accounts on the Primary AP is displayed at the top of the page.

Step 2 Click the **Edit** icon adjacent to the account you want to edit.

Step 3 Modify the admin account parameters, as required. For descriptions of these parameters, see Adding an Admin Account, on page 3.

Step 4 Click **Update** to modify the parameters.

Deleting an Admin Account

Step 1 Navigate to **Management** > **Admin Accounts**.

The **Admin Accounts** window is displayed, along with the list of all the admin accounts present on the Primary AP. The total count of admin accounts on the Primary AP is displayed at the top of the page.

Step 2 Click the **Delete** icon adjacent to the account you want to delete.

Step 3 Click **Ok** in the confirmation dialog box.

Managing Guest Users using the Lobby Admin account

Guest user accounts are created to allow temporary access to the network. This network access is granted after successful authentication of the guest account credentials.

You can create and manage guest user accounts using the lobby ambassador admin account. To know more about lobby ambassador accounts, see Managing Admin Accounts, on page 3.

Creating a Guest User Account

Before you begin

You will need at least one lobby ambassador user account and one Guest WLAN with **Local User Account** or **RADIUS** Access Type, before you create a guest user account. For information about creating a lobby ambassador account, see Adding an Admin Account, on page 3.

Step 1 In your browser, navigate to the Primary AP UI.

Step 2 Login using valid **Lobby Ambassador** credentials.

Step 3 In the **Lobby Ambassador Guest Management** window, click **Add Guest User**.

Step 4 Enter the following details for the guest user account:

Option	Description
User Name	Specify an user name for the guest user account.
Wireless Network	Select the desired guest WLANs that have already been configured for guest access to the network. To know more about creating a guest WLAN, see Creating a Guest Network.
Permanent User	Select this check box to allow the guest user account access to the network without time restriction.
Expiry Date & Time	Specify the date and time by clicking the calendar and clock icons respectively. The guest user account gets disabled at the specified date and time preventing access to the guest network. If the **Permanent User** check box is selected, then this field disappears from the dialog box.

Option	Description
Generate Password	Click this radio button to automatically generate a password for the guest user account being created. If you prefer to manually specify a password for the guest user account, enter it in the **Password** and **Confirm Password** fields.
Password	Specify a password for the guest user account.
Confirm Password	Ensure that this entry matches what you have typed in the **Password** field.
Description	This field is optional. The user can specify a suitable description for the guest user account.

Step 5 Click **Update**.

You can choose to share the account credentials with the guest user either via email or by printing it out.

The username and password are case sensitive.

To modify or delete the Guest User account, click the **Edit/Delete** icons.

Managing TACACS+ and RADIUS Servers

Primary AP supports up to Six RADIUS and Three TACACS Servers. To configure RADIUS and TACACS+ Servers, click the bidirectional arrow icon on the top right of the home screen to enable **Expert View** on the Primary AP UI.

Adding TACACS+ Servers

Step 1 Navigate to **Management** > **Admin Accounts**.

Step 2 Click the **TACACS+** tab.

Step 3 Click **Add TACACS+ Authentication Server** button and enter the following:

Note To add the TACACS+ Accounting Server, choose **Add TACACS+ Accounting Server** and proceed with the following instructions.

Server Index	Select 1 through 3.
State	Enable the state. By default this is **Enabled**.
Server IP Address	Enter the IPv4 address of the TACACS+ server.
Shared Secret	Enter the shared secret.
Port Number	Enter the port number being used for communicating with the TACACS+ server. By default, the port number is 49.
Server Timeout	Enter the server timeout. By default, the timeout is 5 seconds.

The Table displays the configured TACACS+ (authenticating, authorizing, accounting) servers.

You can also modify or delete TACACS+ servers by using the **Edit/Delete** icons.

Configuring RADIUS Servers

Step 1 Navigate to **Management** > **Admin Accounts**.

Step 2 To add the RADIUS servers, click **RADIUS** and enter data as specified in the following steps:

Step 3 **Authentication Call Station ID Type**—From the drop-down list, choose the option that is sent to the RADIUS server in the Access-Request message. One of the following format types can be chosen as the Authentication Call Station ID Type that is sent to the RADIUS server:

- IP Address
- Primary AP MAC Address
- AP MAC Address
- AP MAC Address:SSID
- AP Name:SSID
- AP Name
- AP Group
- Flex Group
- AP Location
- VLAN ID
- AP Ethernet MAC Address
- AP Ethernet MAC Address: SSID
- AP Label Address
- AP Label Address: SSID
- AP MAC:SSID AP Group
- AP Eth MAC:SSID AP Group

Step 4 **Authentication MAC Delimiter**—From the drop-down list, choose the option that is sent to the RADIUS server in the Access-Request message. The delimiters can be one of the following:

- Colon
- Hyphen
- Single-hyphen
- No Delimiter

Step 5 **Accounting Call Station ID Type**—From the drop-down list, choose the option that is sent to the RADIUS server in the Access-Request message. One of the following format types can be chosen as the Accounting Call Station ID Type that is sent to the RADIUS server:

- IP Address
- Primary AP MAC Address
- AP MAC Address
- AP MAC Address:SSID
- AP Name:SSID

- AP Name
- AP Group
- Flex Group
- AP Location
- VLAN ID
- AP Ethernet MAC Address
- AP Ethernet MAC Address: SSID
- AP Label Address
- AP Label Address: SSID
- AP MAC:SSID AP Group
- AP Eth MAC:SSID AP Group

Step 6 **Accounting MAC Delimiter**—From the drop-down list, choose the option that is sent to the RADIUS server in the Access-Request message. The delimiters can be one of the following:

- Colon
- Hyphen
- Single-hyphen
- No Delimiter

Step 7 **Fallback Mode**—Specify the RADIUS server fallback behavior from the drop-down list. It can be one of the following:

• **Off**	Disables RADIUS server fallback.
Passive	Causes the Primary AP to revert to a server with a lower priority from the available backup servers without using extraneous probe messages. The Primary AP ignores all inactive servers for a time period and retries later when a RADIUS message needs to be sent.
Active	Causes the Primary AP to revert to a server with a lower priority from the available backup servers by using RADIUS probe messages to proactively determine whether a server that has been marked inactive is back online. The Primary AP ignores all inactive servers for all active RADIUS requests. Once the primary server receives a response from the recovered ACS server, the active fallback RADIUS server no longer sends probe messages to the server requesting the active probe authentication.

Step 8 **Username**—If you enabled Active fallback mode, enter the name to be sent in the inactive server probes in the Username field. You can enter up to 16 alphanumeric characters. The default value is **cisco-probe**.

Step 9 **Interval**—If you enabled Active fallback mode, enter the probe interval value (in seconds) in the Interval text box. The interval serves as inactive time in passive mode and probe interval in active mode. The valid range is 180 to 3600 seconds, and the default value is 300 seconds.

Step 10 **AP Events Accounting**—Enable this toggle button to activate sending of accounting requests to RADIUS server. During network issues, the APs join/disjoin from the Primary AP. Enabling this option ensures that these events are monitored and the accounting requests are sent to the RADIUS server to help you detect the network issues.

Step 11 Click **Apply** to save the changes.

Adding RADIUS Servers

Step 1 Navigate to **Management** > **Admin Accounts**.

Step 2 Click **RADIUS**.

This page lists any RADIUS servers that have already been added. Choose to add one of the following:

- **Add RADIUS Authentication Server**
- **Add RADIUS Accounting Server**

Note The pages used to add authentication and accounting servers contain similar fields. The following instructions are detailed for both the **Add RADIUS Authentication Server** and **Add RADIUS Accounting Server** pages. The steps are the same for both pages.

- You can also modify or delete the Radius servers by using the **Edit/Delete** icons.

Step 3 Click **Add RADIUS Authentication Server** and enter the following:

Server Index	Select 1 through 6.
State	Enable the state. By default this is **Enabled**.
Server IP Address	Enter the IPv4 address of the RADIUS server
Shared Secret	Enter the shared secret
Port Number	Enter the port number used for communicating with the RADIUS server. By default, the port number of Authentication server is 1812, and the Accounting server is 1813.
Server Timeout	Enter the server timeout. By default, the timeout is 5 seconds.

Viewing Auth Cached Users

Before you begin

To view the client entries which are connected to WLANs with **Authentication Caching** enabled follow the steps below.

Step 1 Switch to **Expert View** and navigate to **Management** > **Admin Accounts**.

Step 2 In the **Admin Accounts** page, choose the **Auth Cached Users** tab.

Step 3 The client entries stored in the local cache of Primary AP are displayed in the table with the following details:

- **MAC Address**—Displays the MAC address of the client.
- **Username**—Displays the username of the client. The MAC address is shown by default.
- **SSID**—Displays the WLAN in use by the client.

- **Timeout (Minutes)**—Displays the **User Cache Timeout Value** configured in the WLAN under **Authentication Caching**. By default, the timeout interval is 1440 minutes.
- **Remaining Time (Minutes)**—Displays the amount of time the local cache client entry is valid.

Step 4 Double-click the listed auth cached user to view the details.

You can also delete the client entry from CBW Primary AP local cache by selecting the client and click **Delete Selected**. If the client entry is removed from local cache, the authentication of the client will be done by Radius Server. For more details see Authentication Server information in Configuring the WLAN Security.

Setting Date and Time

The date and time on the Cisco Business Wireless Primary AP is first set when running the initial configuration setup wizard. You can enter the date and time manually or you can specify a Network Time Protocol (NTP) server that sets the time and date.

Using NTP Servers to Automatically Set the Date and Time

You can have up to three Network Time Protocol (NTP) servers that the Primary AP can automatically sync to and set the date and time.

By default three NTP servers are automatically created. The default fully qualified domain names (FQDN) of the NTP servers are:

- 0.ciscome.pool.ntp.org, with NTP Index value 1.
- 1.ciscome.pool.ntp.org, with NTP Index value 2.
- 2.ciscome.pool.ntp.org, with NTP Index value 3.

For adding and editing NTP server details, go to **Management** > **Time**. This opens the Time Settings page.

Adding and Editing NTP Servers

You can have up to three Network Time Protocol (NTP) servers that the Primary AP can automatically sync to and set the date and time.

Step 1 Navigate to **Management** > **Time**.

The **Time Settings** window is displayed, with the set time zone shown at the top of the page. The current date and time are displayed in the **Set Time Manually** field. If there are any existing NTP servers, they are listed in the order of their **NTP Index** values.

Step 2 In the **NTP Polling Interval** field, specify the polling interval, in seconds.

Step 3 To edit an existing NTP server, click its **Edit** icon. To add a new NTP server, click **Add NTP Server**.

Step 4 You can add or edit the following values for an NTP server:

Option	Description
NTP Index	Specify an NTP Index value to set the priority of the NTP server. NTP Index values can be set from 1 to 3, in the order of decreasing priority. The Primary AP will try and sync with the NTP server with the highest priority first, until the specified polling interval time runs out. If the sync is successful, the Primary AP will not try to sync with any of the remaining NTP servers. If the sync is unsuccessful, then the Primary AP will try to sync with the next NTP server.
NTP Server	Specify the IPv4 address or the fully qualified domain name (FQDN) for the NTP server. When you specify an FQDN, a DNS lookup is done. If the lookup fails, an error will be logged in the Syslog server. The Primary AP will continue to resolve this FQDN and errors will be logged until you change the NTP configuration or specify a valid FQDN.

Step 5 Click **Apply**.

Refreshing NTP Server Status

The NTP server table on the **Time Settings** page, displays the status of the connection to each NTP server in the **NTP Status** column. The status may be one of the following:

- **Not Tried**—A sync has not been attempted yet.
- **In Sync**—The Primary AP time is in sync with the NTP server.
- **Not Synched**—The Primary AP time is not in sync with the NTP server.
- **In Progress**—A sync is being attempted.

The NTP status is automatically updated every minute.

Deleting and Disabling NTP Servers

To delete an NTP server:

1. Navigate to **Management** > **Time**.
2. In the **Time Settings** page, click the **Delete** icon of the NTP server you want to delete.
3. Click **OK** in the confirmation dialog box.
4. Click **Apply**.

To disable the option of setting up the date and time using NTP servers, you will need to delete all configured NTP servers following the same process shown above.

Configuring Date and Time Manually

Step 1 Navigate to **Management** > **Time**.

The **Time Settings** window is displayed, with the set time zone shown at the top of the page. The current date and time are displayed in the **Set Time Manually** field.

Step 2 From the **Time Zone** drop-down list, choose your local time zone.

When you choose a time zone that uses Daylight Saving Time (DST), the automatically sets its system clock to reflect the time change when DST occurs. DST starts on the second Sunday in March, and ends on the first Sunday in November in the U.S.

Step 3 Select the **Set Time Automatically from Current Location** check box to set the time based on the time zone specified.

Step 4 In the **Set Time Manually** field:

- Click the calendar icon and choose the month, day, and year.
- Click the clock icon and specify the time, in hours and minutes.

Step 5 Click **Apply**.

Updating the CBW AP Software

Note Refer to Image Update Prerequisite, on page 13 for updating a device later in this section.

To view the current software version of your Primary AP, you can choose the one of the following methods:

- Click the gear icon at the top-right corner of the web interface, and then click **Primary AP Information**.
- Choose **Management** > **Software Update**. The **Software Update** window is displayed with the current software version number listed on the top.

You can update the CBW AP software using the Primary AP's web interface. Current configurations on the Primary AP will not be deleted.

The following are the software update methods:

- Updating the Software using HTTP, on page 14
- Updating the Software using TFTP, on page 16
- Updating the Software using SFTP, on page 17
- Updating the Software through Cisco Business Dashboard, on page 18

A software update ensures that both the Primary AP software and the software on all the associated Subordinate APs are updated. Newly joining APs will be upgraded to the current version of the software running on the Primary AP.

The software download happens in the background, without impacting the network. The upgrades are automatically sequenced to ensure that the network performance is not impacted by software update.

Note The software of up to three access points can be concurrently updated.

Image Update Prerequisite

Before updating the CBW APs, you are required to obtain the Primary AP firmware image and the Mesh Extender (if your network has any Mesh Extenders) firmware image using the following steps:

- Navigate to the **Cisco Download Software** page: *http://software.cisco.com/download/navigator.html*
- From the **Download Software** window, browse to **Wireless** > **Access Points**. Navigate to **Business 100 Series Access Points**. Choose the model (CBW150AX), to view a list of currently available software, with the latest displayed on the top.
- Choose a software release number.
- Click **Download** corresponding to the **CBW-Bundle-10-x-2-0.zip** file.
- Read the **Cisco's End User Software License Agreement** and then click **Agree** to proceed.
- Save the ZIP file to the hard drive on your computer, and then extract the contents to a directory on your computer.

CBW AP Series	Software File to Select	Image Size
CBW150AX (Primary Capable APs)	ap1g8	~100MB
CBW151AXM (Mesh Extenders)	ap1g8-capwap	~70MB

Pre-download Image Status

You can monitor the status and progress of the update via HTTP/TFTP/SFTP/ on the Software Update page. The following data is displayed as the update progresses:

- Total number of APs in the network.
- Number of APs that are currently being updated, waiting to be updated, being rebooted and those that failed to update.

In addition to the summary above, each AP update progress is also shown with the following data:

- **AP Name**—The AP name.
- **AP Type** —Displays if the AP is a Primary AP or Primary Capable AP or Mesh Extender.
- **AP Role**— The operating role of the AP. It can be **Root** or **Mesh**. This field is available only in Mesh deployments.
- **AP Location**—The AP location.
- **Download Percentage**— By default, it displays as **NA**. While pre-downloading the software, the percentage of download is displayed.
- **Last Update Error**—In case of any error, during pre-download, the error is displayed here.

- **State**—Status of the pre-image download to the Mesh Extenders in the network. It can be one of the following:
  - **None**
  - **Initiated**
  - **Pre-downloading**
  - **Completed**
- **Retry Attempts**—Number of Attempts re-tried.

Updating the Software using HTTP

Step 1 Obtain the ZIP file and extract the Primary AP software image and Mesh Extender (if your network has any Mesh Extenders) firmware image.

Step 2 From the Primary AP web interface, navigate to **Management** > **Software Update**.

The **Software Update** window with the current software version number is displayed.

Step 3 In the **Transfer Mode** drop-down list, choose **HTTP**.

Note For Mesh deployments, you must upgrade the Mesh Extender image prior to the Primary AP image upgrade.

Important Proceed with Step 4-7 if you have Mesh Extenders in the CBW AP network.

Step 4 Enable **Mesh Extender Image** option to load the Mesh Extender image **ap1g8-capwap**. By default, this option will be **disabled**.

Step 5 Click the **Browse** button adjacent to the **Mesh Image File** field, navigate to the folder having the unpacked ZIP file contents, and choose **ap1g8-capwap** software file.

Note The file explorer that opens here is an operating system-specific explorer depending on the OS of your computer.

Step 6 Click **Update**, and then click **Ok** in the confirmation dialog.

Caution The top section of the page indicates the status of the download. Do not manually power down or reset the Primary AP or any AP during this process.

The **Pre-Download Image Status** section displays the status of the pre-image download to the Mesh Extenders in the network.

You can abort a software update that is in progress, at any time before the Primary AP completes rebooting, by clicking **Abort.**

Step 7 One Mesh Extender in the network obtains the image first and then shares the image to other Mesh Extenders. Once all the Mesh Extenders in the network are pre-downloaded or moved to **Complete** status, **Disable** the **Mesh Extender Image** option.

Step 8 Now, update the Primary AP and other Primary Capable APs in the network. To do so, click **Browse** adjacent to the **File** field. Navigate to the folder having the unpacked ZIP file contents, and choose the **ap1g8** software file.

Step 9 Check the **Auto Restart** check box for the Primary AP and Mesh Extender to reboot automatically after the image pre-download is complete for all the APs. By default, this option is **Enabled**.

Step 10 Click **Update** and then click **Ok** in the confirmation dialog.

The status of the download is displayed on top of the page.

Step 11 One Primary AP in the network obtains the image and shares the image to all other Primary capable APs.

Step 12 After all the APs' state is moved to **Complete**, the Primary AP restarts (or reboots) to complete the software upgrade. If you have not checked the **Auto Restart** check box, you can manually reboot the Primary AP, after the upgrade, by choosing **Advanced > Primary AP Tools**, and clicking **Restart Primary AP**.

Step 13 Log in to the Primary AP UI (after clearing the cache) and verify the Primary AP software version in the **Software Update** window.

Note
- While adding the Mesh Extender to the existing Mesh deployment, the new Mesh Extender will obtain the image from the existing connected Mesh Extender. This ensures efficient upgrade.
- The newly joining Mesh Extender can obtain the image from Cisco.com, TFTP/SFTP server, or via CBD. Configure the **Transfer Type** accordingly to enable the new Mesh Extender obtain the image and join the CBW network. You can also upgrade software through HTTP. For more information see Upgrading the Software for First Mesh Extender using HTTP, on page 15

Upgrading the Software for First Mesh Extender using HTTP

You will be required to upgrade the software of first Mesh Extender that joins the CBW Primary AP. To add a new Mesh Extender to the Primary AP, refer to Adding Mesh Extenders.

Once you have added the MAC Address of the Mesh Extender in **Local MAC Addresses** list, check the predownload status of the Mesh Extender by navigating to **Network Summary > Management > Software Update** page.

If the Mesh Extender has not joined, the predownload status shows as `ImageReq to AP failed`. This requires that you upgrade the software of the Mesh Extender to enable it join the network. Do the following to upgrade the software using HTTP:

Step 1 Obtain the ZIP file and extract the Primary AP software image and Mesh Extender firmware image.

Step 2 From the Primary AP web interface, choose **Management > Software Update**. The **Software Update** window with the current software version number is displayed.

Step 3 In the **Transfer Mode** drop-down list, choose **HTTP**.

Step 4 Enable the **Mesh Extender Image** option to load the Mesh Extender image **ap1g8-capwap**. By default, this option will be **Disabled**.

Step 5 Click **Browse** adjacent to the **Mesh Image File** field, navigate to the folder containing the unpacked ZIP file contents, and choose **ap1g8-capwap** software file.

Caution The top section of the page indicates the status of the image upload to Primary AP. Do not manually power down or reset the Primary AP or any AP during this process.

Note The uploaded **ap1g8-capwap** image will be stored in temporary location of the Primary AP. So do not upgrade or reload the Primary AP until the first Mesh Extender joins the network.

Step 6 Click **Update**, and then click **Ok** in the confirmation dialog.

Step 7 When the first Mesh Extenders attempts to joins the network, the Primary AP shares the **ap1g8-capwap** image to the Mesh Extender.

The **Pre-Download Image Status** section displays the status of the image download to the Mesh Extenders in the network.

Once the image is transferred, the Mesh Extender reloads and joins the CBW network.

Updating the Software using TFTP

Before you begin

- Prepare a TFTP server to host the CBW AP software file using the following guidelines:
  - Ensure that the TFTP server supports extended TFTP for file sizes greater than 32 MB. Some TFTP servers that support files of this size are tftpd32.
  - If you attempt to download the Primary AP software and your TFTP server does not support the file size, an error message is displayed: `TFTP failure while storing in flash`.
- A computer that can access *Cisco.com* and the TFTP server will be required.

Note Ensure that the TFTP server has the latest software bundle on *Cisco.com*.

Step 1 Obtain the ZIP file and extract the Primary AP software image and Mesh Extender (if your network has any Mesh Extenders) firmware image. Copy the folder to the default directory on your TFTP server.

Step 2 From the Primary AP UI, navigate to **Management** > **Software Update**.

The **Software Update** window with the current software version number is displayed.

Step 3 In the **Transfer Mode** drop-down list, choose **TFTP**.

Step 4 In the **IP Address (IPv4)** field, enter the IP address of the TFTP server.

Step 5 In the **File Path** field, enter the TFTP server directory path of the software file.

Step 6 To set the Primary AP to automatically reboot after the image pre-download is complete, check the **Auto Restart** check box. By default, this option is **Enabled**.

You can also manually reboot the Primary AP after the upgrade. Navigate to **Advanced** > **Primary AP Tools** and click **Restart Primary AP**.

Step 7 Click **Save** to save the parameters that you have specified.

These parameters (IP address and File Path of the TFTP server) will remain saved unless you specifically change them in future. You do not have to re-enter these parameters during the next software update.

Step 8 You can perform the update right away or schedule it for a later time.

- To proceed with the update right away, click **Update**, and then click **Ok** in the confirmation dialog.

- To perform the update later, up to a maximum of 5 days from the current date, enable **Schedule Update** and specify the later date & time in the **Set Update Time** field.

The top section of the page indicates the status of the download. Do not manually power down or reset the Primary AP or any AP during this process.

The **Pre-Download Image Status** section of the page displays the status of the pre-image download to the APs in the network.

You can abort a software update that is in progress, at anytime before the Primary AP completes rebooting, by clicking **Abort**.

Step 9 After you click **Update**, one Primary Capable AP and one Mesh Extender will obtain the image from the configured TFTP server and share the images to other Primary Capable APs and Mesh Extenders correspondingly.

Step 10 After the image pre-download is **Complete**, the Primary AP must restarts (or reboots) to complete the software upgrade. If you have not checked the **Auto Restart** check box, you can manually reboot the Primary AP, after the upgrade. Navigate to **Advanced** > **Primary AP Tools**, and click **Restart Primary AP**.

Step 11 Clear the cache and log in to the Primary AP UI and verify the Primary AP software version in the **Software Update** window.

Updating the Software using SFTP

Software update through SFTP Transfer Mode works for all Access Points supported in a CBW AP Deployment. You would need a SFTP server which can communicate with the Primary Access Point to use this upgrade method.

Step 1 Obtain the ZIP file and extract the Primary AP software image and Mesh Extender (if your network has any Mesh Extenders) firmware image. Copy the folder to the default directory on your SFTP server.

Step 2 From the Primary AP web interface, navigate to **Management** > **Software Update**.

The **Software Update** window with the current software version number is displayed.

Step 3 In the **Transfer Mode** drop-down list, choose **SFTP**.

Step 4 In the **IP Address (IPv4)/Name** field, enter the IP address or the domain name of the SFTP server.

Step 5 In the **Port Number** field, enter the port number. The default is 22.

Step 6 In the **File Path** field, enter the SFTP server directory path of the software file.

Step 7 Enter the **username** and **password** to log in to the SFTP server.

Step 8 To set the Primary AP to automatically reboot after the image pre-download is complete, check the **Auto Restart** check box. By default, this option is **Enabled**. You can also manually reboot the Primary AP, after the upgrade. Navigate to **Advanced** > **Primary AP Tools**, and click **Restart Primary AP**.

Step 9 Click **Save** to save the parameters (IP address, file path, port number, username and password) that you have specified. These parameters will remain saved until you change them in future. You do not have to re-enter these parameters for the next software update.

Step 10 You can perform the update right away or schedule it for a later time.

- To proceed with the update right away, click **Update**, and then click **Ok** in the confirmation dialog.
- To perform the update at a later time, up to a maximum of 5 days from the current date, click the **Schedule Update** and specify the later date & time in the **Set Update Time** field.

Note The top of the page indicates the status of the download. Do not manually power down or reset the Primary AP or any AP during this process.

The **Predownload Image Status** section of the page shows the status of image predownloaded to the APs in the network.

You can abort a software update that is in progress, at anytime before the Primary AP completes rebooting, by clicking **Abort**.

Step 11 After you click **Update**, one Primary Capable AP and one Mesh Extender will obtain the image from the configured SFTP server, and share the images to other Primary capable APs and Mesh Extenders correspondingly.

Step 12 After all the APs' state are moved to **Complete** state, the Primary AP restarts (or reboots) to complete the software upgrade. If you have not checked the **Auto Restart** check box, you can manually reboot the Primary AP, after the upgrade Navigate to**Advanced** > **Primary AP Tools** and click **Restart Primary AP.**

Step 13 Clear the cache and log in to the Primary AP. Verify the Primary AP software version in the **Software Update** window.

Updating the Software through Cisco Business Dashboard

When you add a Mesh Extender(S) to your Access Point network for the first time, you may choose to upgrade the firmware for the Mesh AP(s) through the Cisco Business Dashboard (CBD).

Updating the Software through Cisco Business Dashboard is possible, only if CBW is currently managed by CBD.

Before you start the image upgrade for the Mesh AP in Cisco Business Dashboard, configure the **Transfer Mode** in CBW interface.

Note

1. When the CBW is connected to CBD through direct management, then you can check the **Connection Status** in CBW GUI under **Advanced** > **CBD Settings** and confirm if the connection is up/down.
2. If the CBW is managed by CBD Probe, then check the status of the device online/offline in CBD inventory using the device's serial number. Device serial number can be found in CBW GUI under **Monitoring** > **Access Points**. Click on the AP name to view the information.

Step 1 From the Primary AP UI, navigate to **Management > Software Update**.

The **Software Update** window indicating the current software version number is displayed.

Step 2 From the **Transfer Mode** drop-down list, choose **CBD-HTTPS** to update the software through CBD.

Step 3 Click **Save**.

Step 4 Refer to *Performing Device Actions*, in the Cisco Business Dashboard Administration Guide and follow the instructions to update the software.

Step 5 Click the **Predownload Image Status** arrows to display the status of the software update.