Advanced

This chapter contains the following sections:

- Managing SNMP, on page 1
- Setting Up System Message Logs, on page 4
- System Logs, on page 4
- Optimizing RF Parameters, on page 5
- Troubleshooting in Primary AP, on page 10
- Using Primary AP Tools, on page 10
- Saving the Primary AP Configuration, on page 12
- Troubleshooting Files, on page 12
- Configuring Access Control Lists (ACL), on page 16
- Cisco Business Dashboard Settings, on page 18

Managing SNMP

Simple Network Management Protocol (SNMP) is a popular network management protocol used for collecting information from all the devices in the network and configuring and managing these devices. You can configure both SNMPv2c and SNMPv3 access modes using the Primary AP web interface.

Configuring SNMP Access

You can configure the following SNMP access modes for the Primary AP:

- SNMPv2c only
- SNMPv3 only
- Both SNMPv2c and SNMPv3
- Neither SNMPv2c nor SNMPv3

Step 1 Choose **Advanced** > **SNMP**.

Step 2 In the SNMP window, enable **SNMP service** option for querying the configuration using MIB browser. By default, the SNMP service is **disabled**.

Step 3 Select the appropriate check box next to the **SNMP Access** to enable the desired SNMP mode. The SNMP access mode is **disabled** by default.

The selected SNMP access mode is enabled.

Note For information about configuring SNMPv3 users using CBW AP, see topics on SNMPv3 later in this chapter.

Step 4 In the **Read Only Community** field, enter the desired community name.

Step 5 In the **Read-Write Community** field, enter the desired community name.

Step 6 Click **Apply** to save the SNMP access configurations.

Note A community name should be between 8-32 characters and be a combination of lowercase letters, uppercase letters, digits, and special characters.

SNMP Trap Receivers

A Simple Network Management Protocol (SNMP) Trap receiver captures, displays and logs SNMP Traps. Traps are notices of events that are sent immediately to the SNMP client's trap receiver from Primary AP instead of waiting for a poll – a request – to the device by the SNMP client.

To add a SNMP Trap Receiver, do the following:

Step 1 Click **Add New SNMP Trap Receiver**, under **Advanced** > **SNMP**.

Step 2 In the **Add SNMP Trap Receiver** window, configure the following fields:

a) **Receiver Name**—Enter the desired username for the new Trap Receiver.
b) **IP Address**—Specify the IP address of the Trap Receiver to which you wish to connect.
c) **Status**—Enable/Disable the Trap Receiver. By default, it is **enabled**.
d) **SNMPv3**—If you have configured SNMP v3 access and have SNMPv3 User, then enable this option. By default, it is **disabled**.
e) **SNMPv3 User**—Map the SNMPv3 User details for the Trap receiver entry, if SNMPv3 toggle is enabled.

The **SNMP Trap Receiver** table shows the list of SNMP Trap Receivers configured in the network.

Step 3 Click **Apply**.

To Edit/Delete the SNMP Trap Receivers, click the **Edit/Delete** icon in the row containing the SNMP Trap Receiver whose details you wish to modify or delete.

The **SNMP Trap Receivers** table is refreshed and the updated entry appears in the table.

Note Few traps are enabled by default. For a complete list of available traps, refer to SNMP Traps in CBW AP.

Add an SNMPv3 User

Step 1 Choose **Advanced** > **SNMP**.

Step 2 In the **SNMP** window, under the **SNMP v3 Users** section, click the **Add New SNMP v3 User** button.

Step 3 In the **Add SNMP v3 User** window, enter the following details:

Field	Description
User Name	Enter the desired username for the new SNMPv3 user.
Access Mode	From the drop-down list, choose one of the desired modes: **Read Only** or **Read/Write**. The default is **Read Only**.
Authentication protocol	From the **Authentication Protocol** drop-down list, choose one of the options: **HMAC-MD5**, **HMAC-SHA**, or **None**. The default authentication protocol is **HMAC-SHA**.
Authentication Password	Enter the desired authentication password. Use a minimum password length of 12 -31 characters.
Confirm Authentication Password	Confirm the authentication password specified above. You can select the **Show Password** checkbox to display the entries in the **Authentication Password** and the **Confirm Authentication Password** fields and verify if the characters match.
Privacy Protocol	From the drop-down list, select one of the options: **CBC-DES**, **CFB-AES-128**, or **None** The default privacy protocol is **CFB-AES-128**.
Privacy Password	Enter the desired privacy password. Use a minimum password length of 12 -31 characters.
Confirm Privacy Password	Confirm the privacy password specified above. You can select the **Show Password** checkbox to display the entries in the **Privacy Password** and the **Confirm Privacy Password** fields and verify if the characters match.

Step 4 Click **Apply** to create a new SNMPv3 user.

The newly added SNMP v3 User appears in the **SNMP v3 Users** table on the **SNMP** window. You can add up to a maximum of 7 SNMPv3 users.

Delete SNMPv3 User

Step 1 Choose **Advanced** > **SNMP**.

Step 2 In the **SNMP Setup**, click the **X** icon in the row containing the SNMPv3 user you wish to delete.

A warning message appears to confirm the action.

Step 3 Click **Yes** in the pop-up window.

The **SNMP v3 Users** table is refreshed and the deleted entry is removed from the table.

Setting Up System Message Logs

The System Message Log feature logs the system events to a remote server called a Syslog server. Each system event triggers a Syslog message containing the details of that event.

If the System Message Logging feature is enabled, the Primary AP sends a syslog message to the syslog server configured on the Primary AP.

Before you begin

Set up a Syslog server in your network before you start the following procedure.

Step 1 Choose **Advanced** > **Logging**.

The **Logging** window appears.

Step 2 Click **Add Server** to add a new **Syslog Server**.

The System Message Log feature is enabled.

Step 3 In the **Syslog Server IP** field, enter the IPv4 address of the server to which the syslog messages are sent and click **Apply**. The table displays the list of Syslog server configured in the network. You can choose to delete the Syslog server if you wish.

Step 4 Set the severity level for filtering the syslog messages that are sent to the syslog server. From the **Log Syslog Level** drop-down list, you may choose the severity level. It can be one of the following (given in the order of severity):

- **Emergencies (0) (Highest severity)**
- **Alerts (1)**
- **Critical (2)**
- **Errors (3)**
- **Warnings (4)**
- **Notifications (5) (Default)**
- **Informational (6)**
- **Debugging (7) (Lowest severity)**

Messages with a severity equal to or less than the set level are sent to the syslog server.

Step 5 Click **Apply**.

System Logs

This feature is used to analyze the system logs depending upon the log level that the user sets. To view the logs in Primary AP UI, do the following configurations.

Step 1 Navigate to **Advanced** > **Logging**. The Logging window is displayed.

Step 2 From the **Log Buffer level** drop-down list, choose the required log level for the system logs to be redirected to the logging buffer.

Step 3 The System logs will be displayed in the **Logs** section of the same page.

Note The wireless client events such as Assoc, Auth, Success or failure logs will be logged in the Notification level (5)

Step 4 Click **Clear** to clear the logs displayed in the Primary AP UI.

Optimizing RF Parameters

To maximize your network's Wi-Fi performance, you can optimize the radio frequency signals' coverage and quality.

Step 1 Navigate to **Advanced > RF Optimization**.

Step 2 **Enable** the **RF Optimization** option to enhance your Wi-Fi performance by adjusting the APs' radio parameters.

By default, **Medium client density** based RF settings is applied.

Step 3 Select the **Client Density** by moving the slider and choose the **Traffic Type**.

To know the values that are set when low, typical, or high client density type is selected, see RF Parameter Optimization Settings, on page 8.

Step 4 Click **Apply** to save the changes.

Advanced RF Parameters

In addition to changing the client density and traffic type, you can also use the advanced parameters to maximize your network's Wi-Fi performance. The following sections in this chapter, provides details for the same.

Optimized Roaming

Optimized roaming resolves the problem of sticky clients that remain associated to access points that are far away and outbound clients that attempt to connect to a Wi-Fi network without having a stable connection. Optimized roaming allows clients to disassociate based on the RSSI of the client data packets and data rate. The client is disassociated if the RSSI alarm condition is met and the current data rate of the client is lower than the optimized roaming data rate threshold.

Optimized roaming also prevents client association when the client's RSSI is low by checking the RSSI of the incoming client against the RSSI threshold. This check prevents the clients from connecting to a Wi-Fi network unless the client has a viable connection. In many scenarios, even though clients can hear beacons and connect to a Wi-Fi network, the signal might not be strong enough to support a stable connection.

You can also configure the client coverage reporting interval for a radio by using optimized roaming.

Optimized Roaming is useful in the following scenarios:

- To address the sticky client challenge by proactively disconnecting clients.
- To actively monitor data RSSI packets.
- To disassociate a client when the RSSI is lower than the set threshold.

Restrictions for Optimized Roaming

When BSS transition is sent to 802.11v capable clients before the disconnect timer expires, the client is disconnected forcefully. BSS transition is enabled by default for 802.11v capable clients.

Configuring Optimized Roaming

Before you begin

- Ensure you have switched to **Expert View** to be able to configure optimized roaming via Primary AP UI.

Step 1 Choose **Advanced** > **RF Optimization**. The **RF Optimization** page allows you to configure Optimized Roaming parameters, Data Rates, Channels, Global Interferer detection.

Step 2 In the **RF Optimization** page, enable the **2.4 GHz/5 GHz Optimized Roaming** toggle button to set interval and threshold values.

If **2.4 GHz/5 GHz Optimized Roaming** is enabled, the following parameters are displayed.

- 2.4 GHz/ 5 GHz Interval
- 2.4 GHz/ 5 GHz Threshold

Step 3 In the **2.4 GHz Interval** and **5.0 GHz Interval** text boxes, specify the values for the interval at which an access point reports the client coverage statistics to the Primary AP.

- **2. 4 GHz/5 GHz Interval**—Configures the client coverage reporting interval for 2.4 GHz and 5 GHz networks. The interval ranges from 5 seconds to 90 seconds (default). If you configure a low reporting interval, the network can get overloaded with coverage report messages. The client coverage statistics includes data packet RSSIs, Coverage Hole Detection and Mitigation (CHDM) pre-alarm failures, retransmission requests, and current data rates.

  Note
  - By default, the AP sends client statistics to the Primary AP every 90 seconds.
  - If the Interval is set to a value other than the 90 second default, the client statistics will be sent only during failure cases.

- **2.4 GHz / 5 GHz Threshold**—Configures the threshold data rates for 2.4 GHz and 5 GHz. The Threshold values are **disabled** by default.

  For 2.4 GHz threshold value that can be configured are 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps.

  Optimized roaming disassociates clients based on the RSSI of the client data packet and data rate. The client is disassociated if the current data rate of the client is lower than the Optimized Roaming Data Rate Threshold. For 5 GHz threshold value that can be configured are 6, 9, 12, 18, 24, 36, 48, 54 Mbps.

- **Event Driven RRM**—The toggle allows an AP in distress to bypass normal RRM intervals and immediately change channels. This is a global setting and can be enabled or disabled.
- **Interferer detection**—This is global setting which enables the Primary AP to detect the non Wi-Fi sources. By default, it is disabled.
- **5.0 GHz Channel Width**—The dropdown option basically controls how broad the signal is for transferring data as 20MHz/40MHz/80MHz/Best. By increasing the channel width, we can increase the speed and throughput of a wireless broadcast. This Global setting is set to **Best** by default.

Step 4 Set the threshold data rates of the client by manipulating the **2.4 GHz Data Rates** and **5.0 GHz Data Rates** sliders.

The following data rates are available:

- 2.4 GHz—1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
- 5 GHz—6, 9, 12, 18, 24, 36, 48, 54 Mbps

Step 5 Select DCA Channels—One can select or click individual channels to be included in DCA for 2.4 GHz and 5.0 GHz band.

Note A green underline below the channel number indicates that it is selected. Click to unselect the same.

RF Profiles

RF Profiles allows you to tune groups of APs that share a common coverage zone together and selectively change how RRM will operates the APs within that coverage zone. For example, a university might deploy a high density of APs in an area where a high number of users will congregate or meet. This situation requires that you manipulate both data rates and power to address the cell density while managing the co-channel interference. In adjacent areas, normal coverage is provided and such manipulation would result in a loss of coverage. Using RF profiles and AP groups allows you to optimize the RF settings for AP groups that operate in different environments or coverage zones. RF profiles are created for the 802.11 radios. RF profiles are applied to all APs that belong to an AP group, where all APs in that group will have the same profile settings. The RF profile gives you the control over the data rates and power (TPC) values. One can either associate a built in RF Profile with AP Groups or create a new RF Profile and then associate that with the AP Group.

To configure this, do the following:

Step 1 Switch to Expert View in the CBW Web-UI by clicking the bi-directional arrows toggle button on the top-right.

Step 2 Navigate to **Advanced** > **RF Profiles**.

Step 3 Click **Add New RF Profile**.

Step 4 Under the **General** tab, configure the following:

a) **RF Profile Name**—Provide a RF Profile name.
b) **RF Profile description**—Provide an one-line reference for it.
c) **Band**—Select the band 2.4GHz or 5 GHz.
d) **Maximum Clients per radio**—Select the maximum clients per radio. By default, it is 200. The maximum value that is configurable is 200.

e) **Rx SOP Threshold**—Receiver Start of Packet Detection Threshold (RxSOP) determines the Wi-Fi signal level in dBm at which an access point's radio demodulates and decodes a packet. The default value is **Auto**.

As the Wi-Fi level increases, the radio sensitivity decreases and the receiver cell size becomes smaller. Reduction of the cell size affects the distribution of clients in the network. RxSOP is used to address clients with weak RF links, sticky clients, and client load balancing across access points. RxSOP helps to optimize the network performance at high-density deployments (i.e larger number of clients) where access points need to optimize the nearest and strongest clients.

f) **Multicast data rate**—Use the Data rates option to specify the rate at which the multicast traffic can be transmitted between the access points and the client. The default value is **Auto**.

Step 5 In the **802.11** tab, set the data rates and MCS for the RF profile.

a) **Data Rates**—Use the Data rates option to specify the rate at which the data can be transmitted between the access points and the client. The default rate is 11 Mbps.

b) **MCS Settings**—The MCS settings determine the number of spatial streams, the modulation, the coding rate, and the data rate values that are used. Ensure that all of the 0 to 31 MCS data rate indices are enabled (which is the default setting).

Step 6 In the **RRM** tab, set the following parameters:

a) **Channel Width**—By default, 20 MHz and cannot be changed.

b) **Select DCA Channels**—The DCA dynamically manages channel assignment for an AP group. It also evaluates the assignments on a per AP radio basis. The DCA makes decisions during an RSSI based cost metric function which evaluates performance based on interference for each available channel.

It dynamically adjusts the channel plan to maintain performance of individual radios.

Step 7 In the **Client Distribution** tab, set the following parameters:

a) **Window**—In the Window size text box, enter a value between 0 and 20. The default size is 5. The window size becomes part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations:

The access point with the lowest number of clients has the lightest load. The window size and the number of clients on the access point with the lightest load forms the threshold. Access points with more client associations than this threshold is considered busy, and clients can associate only to access points with client counts lower than the threshold.

b) **Denial**—In the Denial Count text box, enter a value between 1 and 10. The denial count sets the maximum number of association denials during load balancing. The default size is 3.

Step 8 Click **Apply**.

RF Parameter Optimization Settings

Use this feature to select the appropriate RF Parameter Optimization settings for your deployment. The following table shows the default values when low, typical, or high client density type is selected.

Note If you do not enable RF Parameter Optimization during the initial configuration wizard, then client density is set to **Typical** (the default value), and RF traffic type is set to **Data** (the default value).

TPC (Tx Power Control) algorithm to determine whether the power of an AP needs to be adjusted down. Reducing the power of an AP helps mitigate co-channel interference with another AP on same channel in close proximity.

Table 1: RF Optimization Table

Parameter	Dependency	Typical (Default Profile)	High Density (Where throughput is most important)	Low Density (For coverage in open spaces)
TX Power	Global per band	Default	Higher	Highest
TPC Threshold, TPC Min, and TPC max (These parameters are equivalent to TX Power)	Specific RF profile per band	TPC Threshold: • -70 dBm for 5 GHz • -70 dBm for 2.4 GHz TPC Min: Default at -10dBm TPC Max: Default at 30 dBm	TPC Threshold: • -65 dB for 5GHz • -70 dB for 2.4 GHz TPC Min: +7 dBm for 2.4 GHz and -10 dBm for 5GHz. TPC Max: Default at 30 dB	TPC Threshold: • -60 dBm for 5GHz • -65 dBm for 2.4 GHz TPC Min: -10 dBm TPC Max: Default at 30 dBm
RX Sensitivity	Global per band (Advanced RX-SOP) RF profiles	Default (Automatic)	Medium (RX-SOP)	Low
CCA Threshold	Global per band 802.11a only (hidden) RF Profiles	Default (0)	Default (0)	Default (0)
Coverage RSSI Threshold	Global per band Data and Voice RSSI RF Profiles	Default (Data: -80dBm, Voice: -80dBm)	Default (Data: -80dBm, Voice: -80dBm)	Default (Data: -90dBm, Voice: -80dBm)
Coverage Client Count	Global per band (Coverage Exception) RF Profiles (Coverage Hole Detection)	Default (3 clients)	Default (3 clients)	Lower (2 clients)

Parameter	Dependency	Typical (Default Profile)	High Density (Where throughput is most important)	Low Density (For coverage in open spaces)
Data Rates	Global per band (network) RF Profiles	12 Mbp mandatory 9Mbp supported 1, 2, 5.5, 6, 11 Mbp disabled	12 Mbp mandatory 9Mbp supported 1, 2, 5.5, 6, 11 Mbp disabled	CCK rates enabled 1, 2, 5.5, 6, 9, 11, 12 Mbp enabled

Troubleshooting in Primary AP

To troubleshoot in the Primary AP, there are features that allow you to check the connectivity, internet access, radio admin state and to analyze the logs depending upon the log level setting. The following sections describe these features.

UI Indicator

Once you login into the Primary AP GUI, navigate to **Monitoring** > **Network Summary**. Check the following indicators:

- **LAN Indicator**—Checks if the default gateway IP of management interface is reachable.
- **Internet Indicator**—Checks if the public DNS (8.8.8.8) is reachable.
- **Wireless Indicator**—Checks the wireless connectivity by looping through all the APs present in Primary AP for both the global networks provided both networks (A and B) are enabled. If any of the network is down in any of the APs, the wireless status is considered to be down. Otherwise, the wireless indicator is operational

Using Primary AP Tools

Note This feature is available only for administrative user accounts with read and write privileges.

You use the **Primary AP Tools** page to manage the following operations:

Restarting the Primary AP

You can reboot (or restart) the Primary AP. Navigate to **Advanced** > **Primary AP Tools**, and then click **Restart Primary AP**.

Clearing the Primary AP Configuration and Resetting to Factory Defaults

This procedure resets your Primary AP to its factory-default configuration.

Step 1 Choose **Advanced > Primary AP Tools**.

Step 2 In the **Primary AP Tools** page, click **Factory Default Primary AP**.

This erases the current Primary AP configuration, resets the configuration to the factory-default values, and reboots the Primary AP.

What to do next

After the Primary AP reboots, proceed to Launching the Setup Wizard.

Clearing Configurations for all APs and Resetting to Factory Defaults

This procedure resets all the CBW APs (including Primary AP) to factory-default configuration.

Step 1 Choose **Advanced > Primary AP Tools**.

Step 2 In the **Primary AP Tools** page, click **Factory Default All APs**.

This erases the current configuration in all the APs simultaneously, resets the configuration to the factory-default values, and reboots all the APs.

Note Primary AP will be rebooted at last.

What to do next

After the Primary AP reboots, proceed to Launching the Setup Wizard.

Export and Import Primary AP Configuration

Exporting / Saving Primary AP Configuration

At any time, you can export the current Primary AP configuration to a .TXT file format.

To export the current configuration, choose **Advanced > Primary AP Tools**, and then under **Configuration management**, click **Export Configuration**. Set the direction as **download** and Transfer Mode as **HTTP**.

The configuration file is saved on the device in which the Primary UI is being viewed. By default the file is saved as *config.txt* in your downloads folder.

Importing / Restoring Primary AP Configuration

You can import configuration from a previously saved configuration file, which is in .TXT file format. Choose **Advanced** > **Primary AP Tools**. Under **Configuration management**, select direction as **Upload**, and choose the **Transfer mode** as HTTP/TFTP/SFTP/FTP.

If HTTP is selected as Transfer mode, then browse the file and click **Apply**.

If FTP/SFTP/TFTP is selected as Transfer mode, configure the IP address, File path, File name, and other mandatory parameters and click **Apply**.

Note You can also do regular import of configuration file, by selecting FTP/SFTP/TFTP transfer mode and by enabling **Scheduled Update** and configuring the Frequency, Time, window.

By default, the option is **disabled**.

The import causes all the Primary Capable APs in the network to reboot. When the APs come back online, the Primary AP Election process happens and a Primary AP comes online with the new imported Primary AP configuration.

For more information about the Primary AP Election Process, see Primary AP Failover and Election Process.

Saving the Primary AP Configuration

Access points have two kinds of memory, the active, but volatile, RAM, and the nonvolatile RAM (NVRAM). During normal operation, the current configuration of the Cisco Business Wireless AP resides on the RAM of the Primary AP. During a reboot, the volatile RAM is completely erased, but the data on the NVRAM is retained.

You can save the Primary AP's configuration from the RAM to the NVRAM of the Primary AP. This ensures that in the event of a reboot, the Primary AP can restart with the last saved configuration.

To save the Primary AP's current configuration from the RAM to the NVRAM, click **Save Configuration** at the top-right of the Primary AP web interface, and then click **Ok**.

Upon successful saving of the configuration, a message conveying the same is displayed.

Troubleshooting Files

This section helps you to download the Support Bundle which includes configuration, logs and crash files for trouble shooting.

Note The Pop-up blocker should be disabled in Browser settings to upload or download the configuration file.

Click **Download Support Bundle** for downloading support bundle to local machine.

The support bundle can also be downloaded via FTP Server if configured. Specify the **IP address**, **File path**, **Username**, **password**, **server port** and select **Apply settings and Export**.

Cisco Business Wireless will attempt to export troubleshooting files as soon as they are generated. If export of troubleshooting files to FTP server is successful, the files are deleted from Cisco Business Wireless.

Troubleshooting Tools

The following tools can be used for troubleshooting:

SSHv2 Access

1. Switch to the Expert View, if you are currently in the Standard View.
2. Enable Secure Shell Version 2 (SSHv2) access mode for Primary AP console, that uses data encryption and a secure channel for data transfer. By default, this is **Disabled**.

Note By default, SSH is disabled for all APs that are connected to the CBW network. SSH can be enabled only by TAC for debugging purposes.

DNS Servers

- Choose **Umbrella** to use Public Open DNS Services
- Choose **User Defined DNS** to configure custom defined DNS Services.

Ping Test

This is similar to the client ping test. You can use this test to check if a particular IP (IP received by sub-ordinate APs or client or open DNS IP) is reachable.

Example: Ping 8.8.8.8

DNS

This feature is used to verify if a particular DNS entered is valid.

Example: Ping google.com

Radius Response

This operates like a simulation tool to verify if the Primary AP is able to reach the RADIUS server. For this, you should have at least one WLAN with WPA2 Enterprise as the access type. It is also used to verify if the username and password details exist in the RADIUS server.

By clicking **Start** all tests will run all the above test.

Uploading Files

This section details the process to upload files to the Primary AP from WebUI using the local file upload such as (HTTP), FTP or TFTP.

To upload a file, do the following:

Step 1 Navigate to **Advanced > Primary AP Tools > Upload File**.

Step 2 Select the **File Type** to upload. It can be one of the following:

- **OUI file**—OUI file contains list of device MAC-IDs and specific owner for the device MAC-ID. The latest file can be downloaded from *http://standards-oui.ieee.org/oui.txt*. Only a **.txt** file format is allowed.

- **EAP Device Certificate**—Certificates that are needed for Extensible Authentication Protocol (EAP) based authentication of the device.

  Note Once the certificate is uploaded successfully, the Primary AP has to be reloaded to apply the new certificate.

- **EAP CA Certificate**—Certificate Authority (CA) Certificates that are needed for Extensible Authentication Protocol (EAP) based authentication. Only a **.pem**, **.crt** file format are allowed.
- **CCO Root CA Certificate**—CloudCenter Orchestrator (CCO) Root CA based certificate for authentication of the device. Only a **.crt** file format is allowed.

  Note A CCO Root CA is a Certificate Authority that owns one or more trusted roots. That means that they have roots in the trust stores of the major browsers.

- **CBD Serv CA Certificate**—The CA certs is used to establish a secure communication from CBW to CBD. If the CBD has updated the self-signed certificate then that certificate file should be uploaded in the CBW.

  If connection between CBW and CBD is based on CBD probe or if the CBD uses certificate signed by a trusted certificate authority, CBD Server CA Certificate upload is not required. The allowed certificate file formats are **.pem**, .**crt**, and **.cert**.

- **WEBAUTH Certificate**—This certificate is used for Captive portal. By default, CBW AP uses self-signed certificate for guest users. You can also upload custom certificate for captive portal using this option. Only **.pem** file format is allowed.
- **WEBADMIN Certificate**—This certificate used for CBW Primary AP UI Access. By default, CBW AP uses self-signed certificate for management access page. You can also upload custom certificate for management access using this option. Only **.pem** file format is allowed. Please ensure that **CommonName** and **SubjectAltName** in the custom certificate is **ciscobusiness.cisco**.

  Note For both Web Auth or Web Admin certificate upload:

  - When the certificate is uploaded successfully, the Primary AP has to be reloaded to apply the new certificate.
  - The root CA certificate has to be installed in the client browser.

Step 3 Select **HTTP**, **FTP** or **TFTP** for the **Transfer Mode** and provide relevant details.

Step 4 If the **Transfer Mode** is **HTTP (Local Machine)**, click **Browse** and upload the file. If the **Transfer Mode** is FTP/TFTP, then please enter the server IP, filename, file path and upload the file.

Step 5 Enter the Certificate password.

This field is available only for EAP Device Certificate or Webauth Certificate or Webadmin Certificate File Type.

The fields **Certificate name** and **Valid up to** show the certificate name and the validity of the certificated that is used by the CBW AP.

Step 6 Click **Apply settings** and **Import** to upload the new certificate.

The status of certificate upload can be viewed in the same page. Once the certificate upload is successful, the **Certificate Name** and **Valid up to** fields will be updated.

Certificates

This section displays the list of all certificates that are installed on CBW Primary AP. For each certificate, the following details will be displayed.

- **Name** - The name of the certificate
- **Common Name** - The fully qualified domain name (FQDN) of the certificate
- **Start Date/End Date** - Displays the start and end date of the certificate during which the certificate would be valid.
- **Status** - Displays whether the certificate is **Active** or **Expired** based on the validity period of the certificate.

Security Settings

This section details on controlling the client traffic using Primary AP UI. You have an option to create ACL rules and apply the rules at per WLAN level. The following topic briefs about the creation of an ACL

Access Control Lists

The Access Control Lists (ACLs) is a set of rules that is usually used to filter network traffic. ACLs contains a list of conditions that categorize packets and help you determine when to allow or deny network traffic.

The Access Control Lists (ACLs) on Cisco Business Wireless APs, supports both IP based and domain based filtering. The ACL rules can be applied either before authentication (pre-Auth ACLs) or after authentication (post-Auth ACLs).

You can selectively allow URLs of your choice without authorizations. With this feature, more than one IP can be learnt for the FQDN configured in the URL rule, for both pre-auth and post-auth.

CBW AP supports the following:

- IPv4 and IPv6
- Wildcard match - Out of the 32 URL rules, a maximum of 20 characters can be wildcard matches.
- Allow/Deny Rules for any post-auth use.
- Configuration of ACL using the FQDN.
- 32 URL rules that can be configured per ACL name.

Note The features that are listed above are also applicable to post-auth.

The Primary AP is configured with the ACL name as per the WLAN, or an AP group, or an AP, or the data returned by the AAA server. The data path of the AP, monitors the DNS requests or responses and learns the IP address of the configured DNS names; and allows traffic for the IP addresses learnt.

If the ACL action is **`Allow`** DNS response, the IP address will be added to the snooped list. For post-auth ACL, if the URL action is **`Deny`**, AP modifies the DNS response and sends the 0.0.0.0 IP address to the client.

The two types of DNS ACL supported on Wave 2 APs are:

- Pre-Auth or Web-Auth DNS ACL: These ACLs have URLs set to **Allow** before the client authentication phase. If the client has the URL rule set to **Allow**, then the client data is switched locally. If the URLs do not match any rule, then all the packets are forwarded to the Primary AP. By default, if the client data does not match any of the configured rules on the AP, the AP sends such traffic to the Primary AP for L3 authorization.
- Post-Auth DNS ACL: These ACLs are applied when the client is running. Post-Auth ACL name can be configured on the WLAN and it can be overridden by the ACL name configured on the AAA server for a given client. If the ACL rule action is set to **Deny** for any URL, these URLs do not get any IP addresses in the DNS response. The APs over-write the DNS response with 0.0.0.0 and sends it to the client.

Configuring Access Control Lists (ACL)

To configure Access Control Lists (ACLs) for pre-auth, do the following:

Note
- Enabling the policy ACL, will make the ACL to be added to default-flex-group and pushed down to APs.
- You can create a maximum of 32 IPv4 and IPv6 ACLs.
- You can also configure both IP and URL rules for the same ACL name.
- ACL rules are applied to the VLAN. Multiple WLANs can use the same VLAN and inherit ACL rules, if any.

Step 1 Choose **Advanced** > **Security Settings**.

Step 2 In the **Security Settings**, click **Add new ACL**.
The **Add ACL Rule** window is displayed.

Step 3 Do the following to add new ACL rules:

a) Choose the **ACL Type**. It can be either **IPV4** or **IPV6**.
b) Enter the **ACL Name**.
c) Use the **Policy ACL** toggle button, to enable or disable the ACL policy.

The device that supports policy-based ACLs allows you to apply access control policies across object groups. An object group is a group of IP addresses or a group of TCP or UDP ports. When you create a rule, you specify the object groups rather than specifying IP addresses or ports.

d) Click the **Add IP Rule** button.
e) In the **Add/Edit IP ACLs** window, enter the following details and click **Apply**:

- **Action**—From the **Action** drop-down list, choose **Deny** for the ACL to **Block** packets or **Permit** for the ACL to allow packets. The default is set to **Deny**. The AP can permit or deny only IP packets in an ACL. Other types of packets, such as ARP packets cannot be specified.
- **Protocol**—Specify the type of protocol. From the **Protocol** drop-down list, choose the protocol ID of the IP packets to be used for this ACL. It can be one of the following or other layer 3 protocols.
  - **Any**—Any protocol (this is the default value)

- **TCP**—Transmission Control Protocol
- **UDP**—User Datagram Protocol
- **ICMP**—Internet Control Message Protocol
- **ESP**—IP Encapsulating Security Payload
- **AH**—Authentication Header
- **GRE**—Generic Routing Encapsulation
- **IP in IP**—Internet Protocol (IP) in IP (permits or denies IP-in-IP packets)
- **Eth Over IP**—Ethernet-over-Internet Protocol
- **OSPF**—Open Shortest Path First
- **Other**—Any other Internet Assigned Numbers Authority (IANA) protocol. If you choose **Other**, enter the number of the desired protocol in the **Protocol** text box. You can find a list of available protocols in the IANA website.

  Note When you specify **Others** as the protocol, you must specify the protocol number in the text box that appears.

- **Source IP/Mask**—You can specify the starting range (here source IP) for applying the IP ACL.
- **Mask**—Masks are used with IP addresses in IP ACLs to specify what should be permitted and denied. Example: 255.255.255.0
- **Source Port**—You can choose a single TCP/UDP source port to which packets are matched.
- **Dest. IP Address/Mask**—You can specify the ending range (destination IP) for applying the IP ACL.
- **Dest. Port**—If you have chosen TCP or UDP, you will need to specify a Destination Port. This destination port can be used by applications that send and receive data to and from the networking stack. Some ports are designated for certain applications such as Telnet, SSH, HTTP, and so on.
- **DSCP**—From the DSCP drop-down list, choose one of these options to specify the differentiated services code point (DSCP) value of this ACL. DSCP is an IP header text box that can be used to define the quality of service across the Internet. You can choose:
  - **Any**—Any DSCP (this is the default value).
  - **Specific**—A specific DSCP ranging from 0 to 63, which you can specify in the DSCP edit box.

After configuring all the above details, click **Apply** to configure IP ACL.

f) Click **Add URL Rules**.

g) In the **Add/Edit URL ACLs** window, enter the **URL** and specify to permit or deny in the **Action** field.

Note You cannot add the same URL in IPv4 and IPv6.

h) Click **Apply**.

On the **Security Settings** page, the ACL Type, ACL Name, and the Policy Name are listed. You can also view if the policy names are mapped.

Applying the ACL to WLAN at Pre-Auth Level

Step 1 Choose **Wireless Settings** > **WLANs**.

Step 2 In the **WLANs** window, click the **Edit** icon adjacent to the Guest WLAN for which you want to add the ACL name.

Step 3 In the **Edit WLAN** window, under the **WLAN Security** tab, from the **ACL Name (IPv4)** and **ACL Name (IPv6)** drop-down lists, choose a value.

Step 4 Click **Apply**.

Applying the ACL to WLAN at Post-Auth Level

Step 1 Choose **Wireless Settings** > **WLANs**.

Step 2 In the **WLANs** window, click the **Edit** icon adjacent to the WLAN for which you want to add ACL rules. The **Edit WLAN** window is displayed.

Step 3 Under the **VLAN & Firewall** tab, in the **Enable Firewall** field, choose **Yes** to enable the firewall.

Step 4 In the **WLAN Post-auth ACL** section, select either **ACL Name(IPv4)** or **ACL Name(IPv6)**, or both.

Step 5 Click **Apply**.

Configuring AAA Override in WLAN

The Allow AAA Override option of a WLAN allows you to configure the WLAN for identity networking. It allows you to apply VLAN tagging, QoS, and ACLs to individual clients based on the returned RADIUS attributes from the AAA server.

Step 1 Switch to the **Expert View**, if you are currently in the Standard View.

Step 2 Choose **Wireless Settings** > **WLANs**.

Step 3 In the **WLANs** window, click the **Edit** icon adjacent to the WLAN you select.

Step 4 In the **Edit WLAN** window, choose the **Advanced** tab and enable the **Allow the AAA Override** toggle button.

Step 5 Click **Apply**.

Cisco Business Dashboard Settings

Cisco Business Dashboard Overview

Cisco Business Dashboard (CBD) is a network management tool for deploying and maintaining Cisco Business Switches, Routers, and Wireless Access Points.

Configuring Cisco Business Dashboard Settings

You can connect CBW Access Points to Cisco Business Dashboard (CBD) by configuring the following parameters under CBD Settings in the Primary AP UI.

Note The below configuration is not applicable if you are using a CBD probe to manage CBW.

When CBW is managed by CBD probe, you are required to configure the SNMP settings on the Primary AP. Refer to Managing SNMP, on page 1 for more details.

1. Navigate to **Advanced** > **CBD settings**. The **Cisco Business Dashboard** window is displayed with the following parameters:
   - **Connection Status**—Indicates if the connectivity status between the CBW and CBD is up or down.
   - **Agent Version**—Specifies the CBD agent version. For example, version 2.4.1

Note To troubleshoot issues with CBD connection, refer to Resolving connection issues between CBW and CBD.

2. In the **CBD settings** page, configure the following fields.

Note Ensure that the data you provide on this page matches with the data configured in the CBD application.

To login and verify the details as configured in the CBD application, refer to Cisco Business Dashboard Administration Guide.

- **Dashboard Connection Enabled**—To enable/disable the CBW connection with CBD application.

Note To update the CBD parameters disable the **Dashboard Connection Enabled** toggle, and then re-enable the toggle to establish the connection with CBD.

- **Dashboard Name or IP**—Specify the IP address or dashboard name to which you wish to connect.

Note The name or IP address specified in this field must be listed in the Subject-Alternative-Name field of the certificate on Cisco Business Dashboard. Refer to the *Managing Certificates* in the Cisco Business Dashboard Administration Guide for more information on configuring the certificate.

- **Dashboard Port**—The default HTTPS port is 443.
- **Organization Name**—Enter the organization name created in the CBD application.
- **Network Name** —Enter the organization name created in the CBD application.
- **Access Key ID**—Enter the access key id created in the CBD application.

- **Access Key Secret**—Enter the access key secret created in the CBD application.

3. Click **Save** to establish a connection between the CBW and CBD.

Note If the CBD is using a self-signed certificate, then download a copy of that certificate from the CBD application. Follow the instructions below to download:

1. In the CBD page, navigate to **System** > **Certificate** and select the **Current Certificate** tab.
2. Click **Download** at the bottom of the page. The certificate will be downloaded in PEM format by your browser.

To upload the certificate, refer to Uploading Files, on page 13.