Using Advanced Settings and Operations

Managing SNMP

Simple Network Management Protocol is a popular network management protocol used for collecting information from all the devices in the network and configuring and managing these devices.

Starting Cisco Wireless Release 8.3, you can configure both SNMPv2c and SNMPv3 using the Cisco Mobility Express web interface.

Configuring SNMP Access

You can configure the following SNMP access modes for the Cisco Mobility Express primary AP:

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

Note You can configure SNMPv1, SNMPv2c, and SNMPv3 using the Cisco Mobility Express CLI too.

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

The **SNMP Setup** window appears.

Step 2 Next to **SNMP Access**, select the appropriate check box to enable the desired SNMP mode.

The default mode is v2c (or by default both or neither SNMP access mode is selected).

The selected SNMP access mode is enabled.

Note For information about configuring SNMPv3 users using Cisco Mobility Express, see the Configuring SNMPv3 users section.

Step 3 In the **Read Only Community** field, enter the desired community name.

The default name is *public*.

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

The default name is *private*.

Step 5 From the **SNMP Trap** drop-down list, choose **Enabled** or **Disabled** to configure the SNMP Trap Receiver. This tool receives, logs, and displays SNMP traps sent from network devices.

The default setting is **Disabled**.

Step 6 In the **SNMP Server IP** field, specify the IP address of the server you wish to connect to.

Add an SNMPv3 User

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

The **SNMP Setup** window appears.

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

The **Add SNMP v3 User** window appears.

Step 3 In the **User Name** field, enter the desired username for the new SNMPv3 user.

The username must meet the following conditions:

-
-

Step 4 From the **Access Mode** drop-down list, choose the desired mode among **Read Only** and **Read/Write**.

The default is **Read Only**.

Step 5 From the **Authentication Protocol** drop-down list, select one of **HMAC-MD5**, **HMAC-SHA**, or **None**.

The default authentication protocol is **HMAC-SHA**.

Step 6 In the **Authentication Password** and **Confirm Authentication Password** fields, enter the desired authentication password as per the following password policy:

Note You can select the **Show Password** checkbox to display the entries in the **Authentication Password** and the **Confirm Authentication Password** fields and verify that they match.

Step 7 In the **Privacy Protocol** drop-down list, select one of **CBC-DES**, **CFB-AES-128**, or **None**.

The default privacy protocol is **CFB-AES-128**.

Step 8 In the **Privacy Password** and **Confirm Privacy Password** fields, enter the desired privacy password as per the following password policy:

Note You can select the **Show Password** checkbox to display the entries in the **Privacy Password** and the **Confirm Privacy Password** fields and verify that they match.

Step 9 Click **Apply** to create a new SNMPv3 user.

The newly added SNMP v3 User appears in the **SNMP v3 Users** table on the **SNMP Setup** window.

Note You can add up to a maximum of 7 SNMPv3 users.

Edit SNMPv3 User

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

The **SNMP Setup** window appears.

Step 2 Click the <edit_icon.gif> icon in the row containing the SNMPv3 user whose details you wish to modify.

The desired row in the **SNMPv3 Users** table becomes editable (or the **Edit SNMPv3 User** window appears.)

Step 3 In the **SNMPv3 Users** table, make the desired modifications inline (or in the **Edit SNMPv3 User** window).

Step 4 Click **Apply**.

The **SNMP v3 Users** table is refreshed and the updated entry appears in this table.

Delete SNMPv3 User

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

The **SNMP Setup** window appears.

Step 2 Click the **X** icon in the row containing the SNMPv3 user you wish to delete.

A warning message appears.

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

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

Setting Up System Message Logging

The System Message Logging 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 controller sends a syslog message to the syslog server configured on the controller.

Before you begin

Set up a Syslog server in your network before starting with the following procedure.

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

The **Logging Setup** window appears.

Step 2 From the **Syslog Logging** drop-down list, choose **Enabled**. The default is Disabled.

The System Message Logging feature is enabled.

Step 3 In the **Syslog Server IP** field, enter the IPv4 address of the server to which the syslog messages are to be sent.

Step 4 Set the severity level for filtering syslog messages to the syslog server. From the **Logging Level** drop-down list, set the severity level by choosing one of the following (given in the order of severity):

- **Emergencies (Highest severity)**
- **Alerts**
- **Critical**
- **Errors (Default)**
- **Warnings**
- **Notifications**
- **Informational**
- **Debugging (Lowest severity)**

After a syslog level is set, only messages with a severity equal to or more than the set level are sent to the syslog server.

Step 5 To set the facility for outgoing syslog messages to the syslog servers, choose one of the following options from the **Syslog Facility** drop-down list:

- Kernel = Facility level 0
- User Process = Facility level 1
- Mail = Facility level 2
- System Daemons = Facility level 3
- Authorization System = Facility level 4
- Syslog = Facility level 5 (default value)
- Line Printer = Facility level 6
- USENET = Facility level 7
- Unix-to-Unix Copy = Facility level 8
- Cron = Facility level 9
- FTP Daemon = Facility level 11
- System Use 12 = Facility level 12

- System Use 13 = Facility level 13
- System Use 14 = Facility level 14
- System Use 15 = Facility level 15
- Local Use 0 = Facility level 16
- Local Use 1 = Facility level 17
- Local Use 2 = Facility level 18
- Local Use 3 = Facility level 19
- Local Use 4 = Facility level 20
- Local Use 5 = Facility level 21
- Local Use 6 = Facility level 22
- Local Use 7 = Facility level 23
- Authorization System (Private) = Facility level 24

Step 6 Click **Apply**.

Optimizing RF Parameters

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

Step 1 Choose **Enabled** from the **RF Optimization** drop-down list.

Step 2 Indicate the expected **Client Density** and **Traffic Type** in your network.

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

Step 3 Click **Apply**.

Optimized Roaming

Information About 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. You can disable the data rate option so that only RSSI is used for disassociating clients.

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

- You cannot configure the optimized roaming interval until you disable the 802.11a/b network.
- When BSS transition is sent 802.11v capable clients and if the clients are not transitioned to other BSS 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 GUI.
- You cannot configure the optimized roaming interval until you disable the 802.11a/b network.

Step 1 Choose **Advanced** > **RF Optimization**.

The **RF Optimization** page is displayed.

Step 2 Enable the **Optimized Roaming** knob.

You are presented with various options to configure for optimized roaming. data rate checks and default RSSI threshold values taken from Coverage Hole Detection and Mitigation (CHDM).

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.

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 The access point sends client statistics to the primary AP based on the following conditions:

- When the interval is set to 90 seconds by default.
- When the interval is configured (for instance to 10 secs) only during optimized roaming failure due to Coverage Hole Detection (CHD) RED ALARM.

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

• 5 GHz—6, 9, 12, 18, 24, 36, 48, 54

Information About RSSI Low Check

The Received Signal Strength Indicator (RSSI) low check feature causes the controller to deny a client's association if the signal from the client is below the configured RSSI threshold. In most deployments, this feature is not required and may lead to client connectivity issues

Restrictions for RSSI Low Check

• This feature is not supported if you have enabled optimized roaming.

Using Controller Tools

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

The **Controller Tools** page provides the following operations on the controller:

• Restarting the controller.

See Restarting the Controller, on page 7.

• Clearing controller configuration and resetting the controller to factory-defaults. See Clearing Controller Configuration and Resetting the Controller, on page 7.

• Exporting and importing controller configuration. See Exporting and Importing the Controller Configuration, on page 8.

Restarting the Controller

At any time, you can restart (or reboot) the controller by choosing **Advanced** > **Controller Tools**, and then clicking **Restart Controller**.

Clearing Controller Configuration and Resetting the Controller

This procedure resets your Cisco Mobility Express wireless LAN controller to its factory-default configuration.

Step 1 Choose **Advanced** > **Controller Tools**.

This opens the **Controller Tools** page.

Step 2 Click **Clear Controller Configuration**.

This erases the current Cisco Mobility Express controller configuration , resets the configuration to the factory-default values, and reboots the Cisco Mobility Express wireless LAN controller.

What to do next

After the Cisco Mobility Express Controller reboots, proceed to Starting the Initial Configuration Wizard.

Exporting and Importing the Controller Configuration

Exporting Controller Configuration

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

To export the current configuration, choose **Advanced > Controller Tools**, and then under **Configuration File**, click **Export Configuration**.

The configuration file is saved, though HTTPS, onto the device on which the Mobility Express UI is being viewed. By default the file is saved as *configuration.txt* in your downloads folder.

Importing Controller Configuration

You can import configuration from a previously saved configuration file, which is in .TXT file format. For this, choose **Advanced > Controller Tools**, and then under **Configuration File**, click **Import Configuration**, and then browse to and choose the required file.

The import causes all controller-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 controller configuration.

For more information about the primary AP Election Process, see Cisco Mobility Express Controller Failover and Primary AP Election Process.

Saving Controller 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 Mobility Express controller 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.

At any time, you can save the Cisco Mobility Express controller's configuration from the RAM to the NVRAM of the primary AP. This ensures that in the event of a reboot, the controller can restart with the last saved configuration.

To save the controller's current configuration from the RAM to the NVRAM, click **Save Configuration** at the top-right corner of the Cisco Mobility Express web interface, and then click **Ok**.

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

Using CMX Cloud Presence Analytics

Cisco Connected Mobile Experiences Cloud (Cisco CMX Cloud) is a Software-as-a-Service (SaaS) product that provides in-venue analytics. You can configure the Cisco CMX Cloud solution using the Cisco Mobility Express web interface.

The Cisco CMX Cloud solution integrated with Cisco Mobility Express provides the following capabilities:

- Enables configuration of secure guest-access solutions for visitors through a custom portal.

  Note CMX Connect configuration is done at the WLAN level for guest access.

- Facilitates detection of all Wi-Fi devices.
- Provides analytics on the Wi-Fi device's presence, such as dwell times, new vs. repeat visitors, and peak times.
- Engages visitors directly on the guest portal page or mobile app with location-based content.

Prerequisites for CMX Presence Analytics

- You should have a valid CMX server URL and the corresponding CMX server token. To register for a CMX Cloud account, go to www.cmxcisco.com. For more information, see http://support.cmxcisco.com/hc/en-us.

  Note In the server URL field, ensure that the URL is appended with /visitor/login.

- A WLAN is created for CMX Cloud. For more information, see the **Adding a WLAN** section in the **Specifying Wireless Settings** chapter.

Enabling CMX Presence Analytics

Before you begin

You will need a valid CMX server URL and a corresponding token.

Step 1 Choose **Advanced** > **CMX**.

The **CMX** window appears.

Step 2 In the **CMX Status** drop-down box, select **Enabled**.

Step 3 In the **CMX Server URL** field, enter a valid CMX server URL.

Step 4 In the **CMX Server Token** field, enter a valid CMX server token.

Step 5 Click **Apply**.

DNS Access Control Lists

The DNS Access Control Lists (ACLs) feature is now supported on Cisco Mobility Express, which allows domain based filtering for Flex Mode. Now, you can selectively allow URLs of your choice without authorizations. With this feature, more than one IPs can be learnt for the FQDN configured in the URL rule, for both pre-auth and post-auth.

This feature supports:

- 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 With this enhancement, the features that are listed above are applicable to post-auth also.

The controller is configured with the ACL name as per the WLAN, or an AP group, or an AP, or that what is 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 these 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 controller. By default, if the client data does not match any of the configured rules on the AP, the AP sends such traffic to the controller 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 DNS Access Control Lists (ACL)

The steps to configure DNS ACLs for pre-auth have been modified. Follow the procedure given below to configure DNS ACLs:

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

The **Security Settings** page is displayed.

Step 2 Click **Add new ACL**.
The Add ACL Rule window is displayed.

Step 3 Follow the procedure given below to add new ACL rules:

a) Choose the **ACL Type**, either **`IPv4`** or **`IPv6`**.
b) Enter the **ACL Name**.
c) Use the **Policy ACL** toggle button, to enable or disable policy ACL.
d) Click the **Add IP Rule** button.
The **Add/Edit IP ACLs** window is displayed.
e) In the Add/Edit IP ACLs window, enter details such as **Action**, **Protocol**, **Source IP/Mask**, **Source Port**, **Dest. IP Address/Mask**, **Dest. Port**, **DSCP**, and click **Apply**.
f) Click the **Add URL Rules** button.
The **Add/Edit URL ACLs** window is displayed.
g) In the Add/Edit URL ACLs window, enter the **URL** and **Action**.

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 Policy Name are listed. You can also view if the policy names are mapped or not.

Applying the ACL to WLAN at Pre-Auth Level

Step 1 Choose **Wireless Settings** > **WLANs**.
The **WLAN Configuration** window is displayed.

Step 2 Click the **Edit** icon adjacent to the WLAN you want to enable or disable.
The **Edit WLAN** window is displayed.

Step 3 Under the **WLAN Security** tab, enable **Guest Network**.

Step 4 From the **Rule Name(IPv4)** and **Rule Name (IPv6)** drop-down lists choose a value.

Step 5 Click **Apply**.

Applying the ACL to WLAN at Post-Auth Level

Step 1 Choose **Wireless Settings** > **WLANs**.
The **WLAN Configuration** window is displayed.

Step 2 Click the **Edit** icon adjacent to the WLAN you want to enable or disable.
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

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

Step 2 Choose **Wireless Settings** > **WLANs**.
The **WLAN Configuration** window is displayed.

Step 3 Click the **Edit** icon adjacent to the WLAN you want to enable or disable.
The **Edit WLAN** window is displayed.

Step 4 Choose the **Advanced** tab and enable the **Allow the AAA Override** toggle button.

Step 5 Click **Apply**.