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 master 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**.

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 6.
- Clearing controller configuration and resetting the controller to factory-defaults. See Clearing Controller Configuration and Resetting the Controller, on page 6.
- Exporting and importing controller configuration. See Exporting and Importing the Controller Configuration, on page 6.

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 Master AP Election process happens and a Master AP comes online with the new imported controller configuration.

For more information about the Master AP Election Process, see Cisco Mobility Express Controller Failover and Master 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 master 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 master 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**.