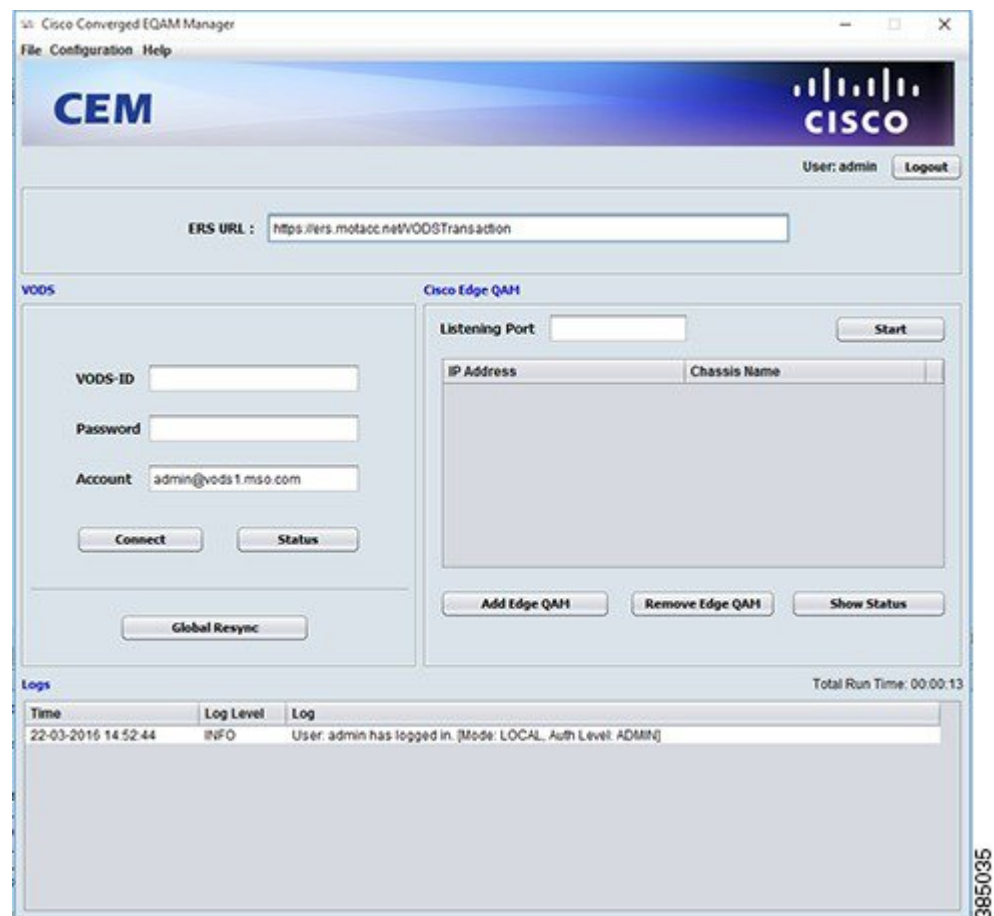




# How to Use Cisco Converged EdgeQAM Manager

This is the main interface of the Cisco CEM application.

**Figure 1: CEM Interface**



- [User Authentication, page 2](#)
- [Communication with the ERS, page 8](#)

- [Communication with Cisco Edge QAM device, page 10](#)
- [General Operation, page 13](#)
- [Configuring SNMP Traps, page 14](#)
- [Feature Information for Converged EdgeQAM Manager, page 17](#)

## User Authentication

The CEM application supports user authentication in two modes: local and TACACS+.

The user authorization level that are supported by the CEM application are:

- **Monitor:** The user can only view the status of the connection with the ERS and Cisco Edge QAM device. The user will not be allowed to close the CEM application.
- **Admin:** The user can access and configure all the settings in the CEM, establish connection with the ERS and Cisco Edge QAM device.

## Local Authentication

When the CEM application is launched for the first time, a local administrator user has to be created. This admin user can then proceed and configure the CEM to connect with the ERS and Cisco Edge QAM device.

**Figure 2: Create Local Admin User**

The validation rules for the passphrase are:

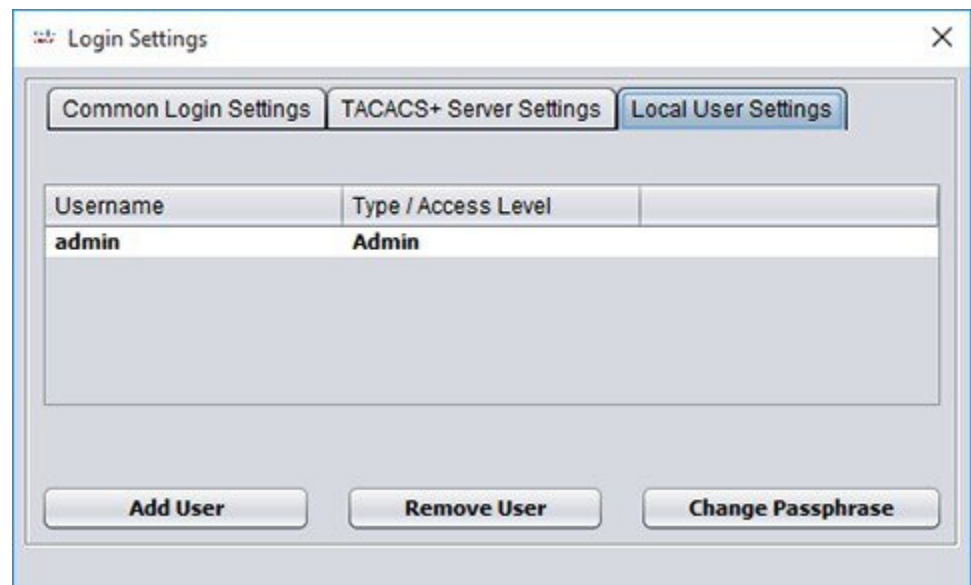
- It must be 6-127 characters in length.
- It must not contain any whitespace.
- Character rules (any 3 of the following 4 rules):

- It must contain at least 1 digit.
  - It must contain at least 1 non alphanumeric character.
  - It must contain at least 1 upper case character.
  - It must contain at least 1 lower case character.
- It must not contain character sequences similar to **qwerty**.

An example of a passphrase that satisfies the aforementioned rules is: V#g0KS7q.

The admin user can create several other users with the Admin/Monitor privilege. The dialog to manage the users can be viewed using the **Configuration > Login Settings** menu item and then choosing the **Local User Settings** tab.

**Figure 3: Local User Setting**

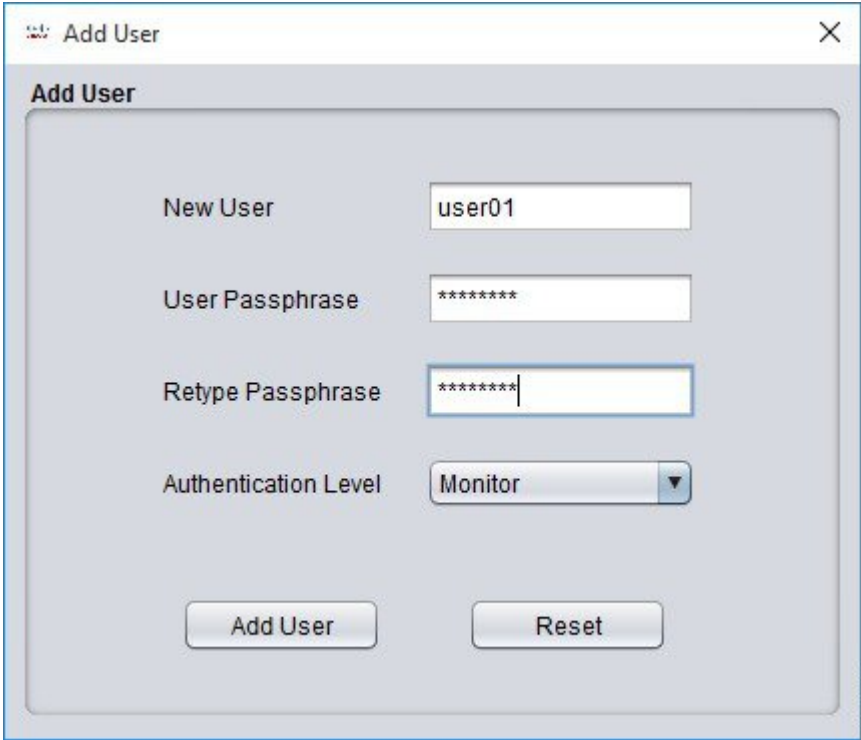


**Note**

If the user forgets the passphrase, it cannot be retrieved by the user. Hence, it is important to know the passphrase of at least one local admin user.

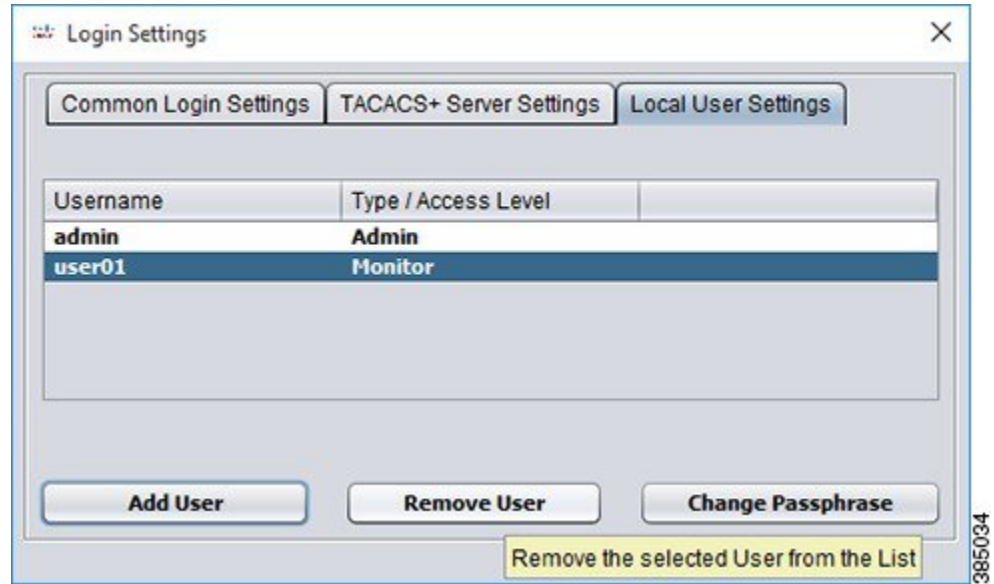
Only a user with the Admin privilege can add/remove users. A new user can be added by clicking the **Add User** button.

**Figure 4: Add User**



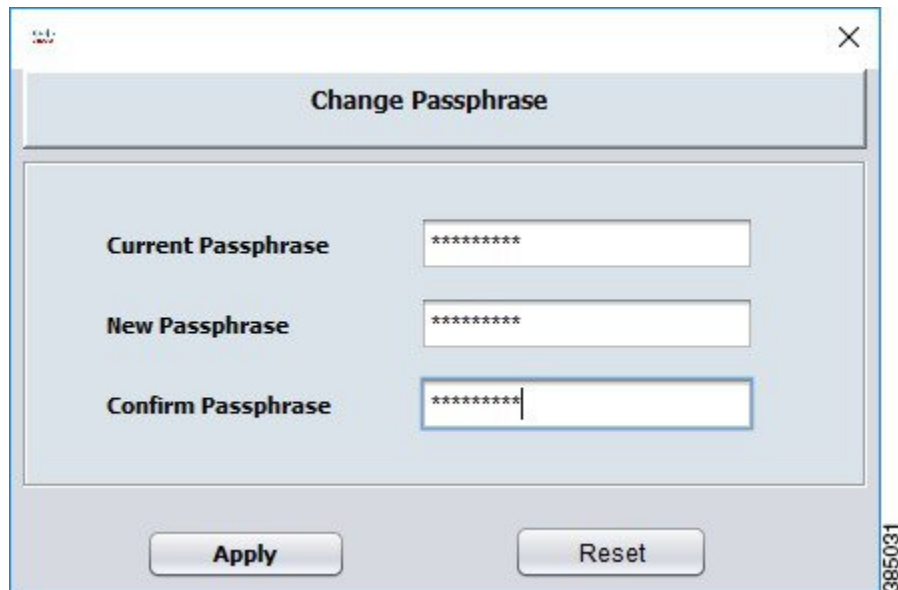
A user can be removed by selecting the user and then clicking the **Remove User** button.

**Figure 5: Remove User**



The passphrase can be updated by clicking the **Change Passphrase** button, and the passphrase rules that mentioned earlier are applicable in this dialog window too.

**Figure 6: Change Passphrase**




## TACACS+ Authentication

The information regarding the TACACS+ server must be specified after logging in the CEM application as the local Admin user.

The dialog to specify the TACACS+ server information can be opened using the **Configuration > Login Settings** menu item then choosing the **TACACS+ Server Settings** tab.

*Figure 7: TACACS+ Server Settings*



The screenshot shows a dialog box titled "Login Settings" with a close button (X) in the top right corner. It has three tabs: "Common Login Settings", "TACACS+ Server Settings" (which is selected), and "Local User Settings". The "TACACS+ Server Settings" tab contains the following fields:

IP	10.78.210.115
Port	49
Key	*****
Accounting	<input checked="" type="checkbox"/>

At the bottom of the dialog are two buttons: "Apply" and "Reset". A vertical ID number "385036" is visible on the right side of the dialog box.

The Shared Secret that is configured on the TACACS+ server as a part of the TACACS+ Authentication Options must be set in the **Key** field of the **Login Settings** Dialog.

If the user intends to enable TACACS+ Accounting, then the checkbox must be selected as shown in the above screenshot.

Please close the **Login Settings** dialog box after clicking the **Apply** button.

Then the user can use the TACACS+ user credentials to login to the CEM application.

**Figure 8: User Login**

The screenshot shows a web-based login interface for the Cisco Converged EQAM Manager. The window has a title bar with the text 'Cisco Converged EQAM Manager' and a close button. The main content area is titled 'User Login'. It contains three input fields: 'User Name' with the text 'tacacs\_admin', 'Passphrase' with masked characters '\*\*\*\*\*', and 'Mode' with a dropdown menu currently showing 'Tacacs'. Below these fields are two buttons: 'Login' and 'Reset'. A vertical ID number '385037' is located on the right side of the window.

## Common Login Settings

The settings that control the user session can be viewed/modified by clicking the **Configuration > Login Settings** menu item then choosing the **Common Login Settings** tab, including:

- **Idle Timeout (minutes)**—Idle session timeout.
- **Maximum Invalid Login Attempt(s)**—Maximum number of attempts a user can try to login with incorrect login credentials.
- **Login Screen Freeze Time (seconds)**—Duration for which the login screen can be frozen after the user has entered invalid credentials for maximum admissible attempts.
- **Local User – Passphrase Expiry Time**—Select the checkbox if you want to configure an expiry time for the passphrase (for the local user).

- **Local User – Passphrase Expiry Time (days)**—Passphrase expiry time in days.

**Figure 9: Common Login Settings**

The screenshot shows a window titled "Login Settings" with three tabs: "Common Login Settings", "TACACS+ Server Settings", and "Local User Settings". The "Common Login Settings" tab is active. It contains the following settings:

Idle Timeout (minutes)	20
Maximum Invalid Login Attempt(s)	5
Login Screen Freeze Time (seconds)	30
Local User – Passphrase Expiry Time	<input checked="" type="checkbox"/>
Local User – Passphrase Expiry Time (days)	180

At the bottom of the dialog are two buttons: "Apply" and "Reset".

367042

### Passphrase Expiry

You can set the passphrase to expire after a period of a maximum of 180 days. By default, the passphrase expiry time is disabled.

Click the **Local User – Passphrase Expiry Time** checkbox to enable and configure the expiry time in the **Common Login Settings** tab. The **Local User – Passphrase Expiry Time (days)** field for specifying the time is enabled only when you select the **Local User – Passphrase Expiry Time** checkbox.

## Communication with the ERS

### Establishing a Connection with the ERS

Complete these steps to establish a connection with the ERS:

**Step 1** Specify the ERS URL and the VODS parameters.

- **ERS URL** - URL of the ERS server.



- **VODS-ID** - Assigned to the MSO by ARRIS.
- **Password** - Assigned to the MSO by ARRIS.
- **Account** - E-mail address of the contact person at the MSO site.

The URL of the licensing ERS is the default URL that is displayed on the GUI. The MSO must use the URL of the production ERS that is provided by ARRIS to establish the connection and get the ECM messages.

The new URL is saved automatically and will be displayed when the application is started the next time.

## Step 2

Click the **Connect** button to establish a connection with the ERS.

After the SSL handshake is complete between the CEM application and the ERS, the CEM will send the ERS sync request to the ERS. If ERS server responds without any error, the CEM will send the ECM request to the ERS to obtain the ECM message.

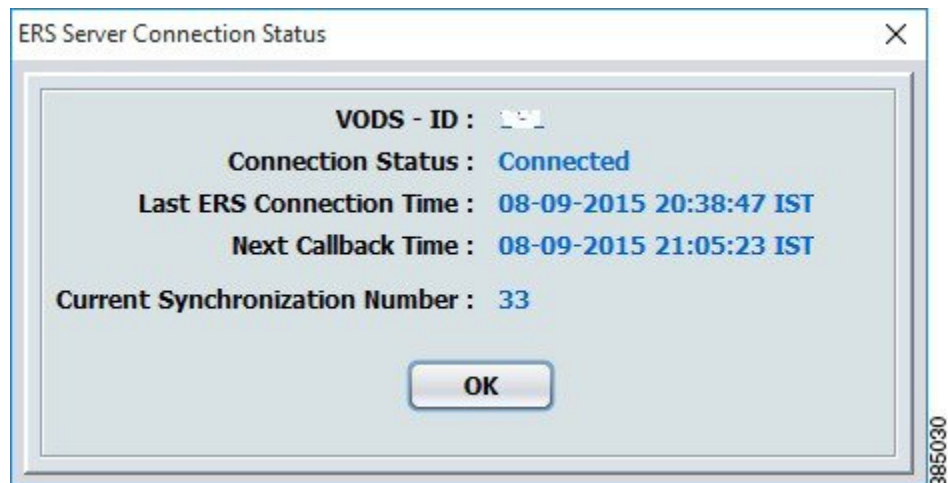
After the connection is established with the ERS, the text boxes corresponding to the ERS server URL and the VODS parameters will be disabled.

The CEM application will send the ERS sync request automatically after the callback time expires and send the ECM request if a new sync number is received from the ERS server.

## Status of the Connection with the ERS

The status of the connection with the ERS server can be ascertained by clicking the **Status** button.

*Figure 10: ERS Connection Status*



## Global Resynchronization

The **Global Resynchronization** Button is used to send the ECM request to the ERS and obtain the new set of ECM messages.

**Note**

---

Global Resynchronization can only be done when ARRIS/CCAD instructs the MSO to request and obtain the new set of ECM messages.

---

## Communication with Cisco Edge QAM device

### Starting the Server Socket

Complete these steps to start the server socket:

---

**Step 1**

Specify the listening port.

- **Listening port** - The port number on which the CEM will listen for connections from Cisco Edge QAM device. It must be in the range of 1024-65534.

**Step 2**

Click the **Start** button to start the server socket and listen for connections from Cisco Edge QAM device.

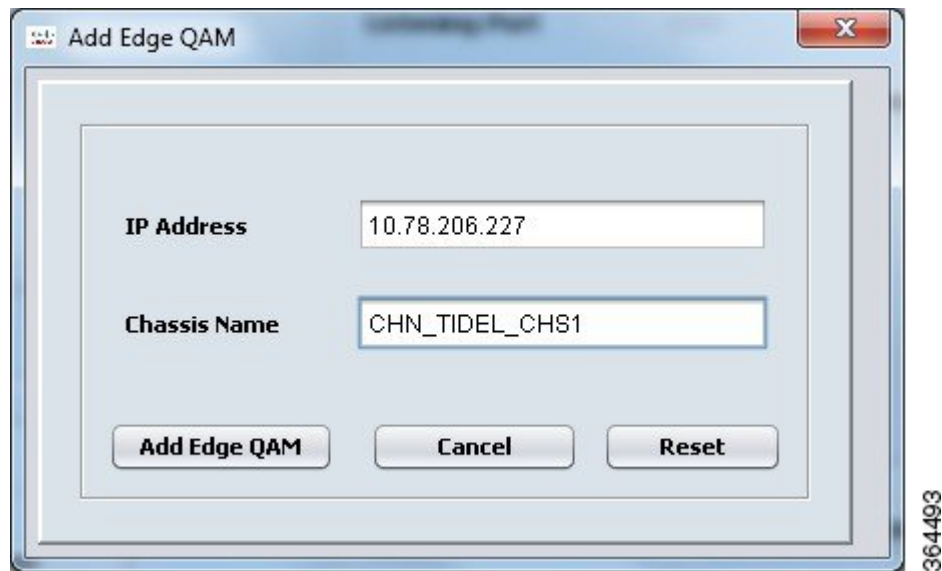
---

## Adding Cisco Edge QAM device

Complete these steps to add Cisco Edge QAM device:

**Step 1** Click the **Add Edge QAM** button to open the **Add Edge QAM** window.

**Figure 11: Add Edge QAM**



**Step 2** Specify the IP address and chassis name of Cisco Edge QAM device to which the CEM application will connect in the above window.

- **IP Address** - The IP address of Cisco Edge QAM device interface from which the connection is established with the CEM.
- **Chassis Name** - The chassis name of Cisco Edge QAM device.

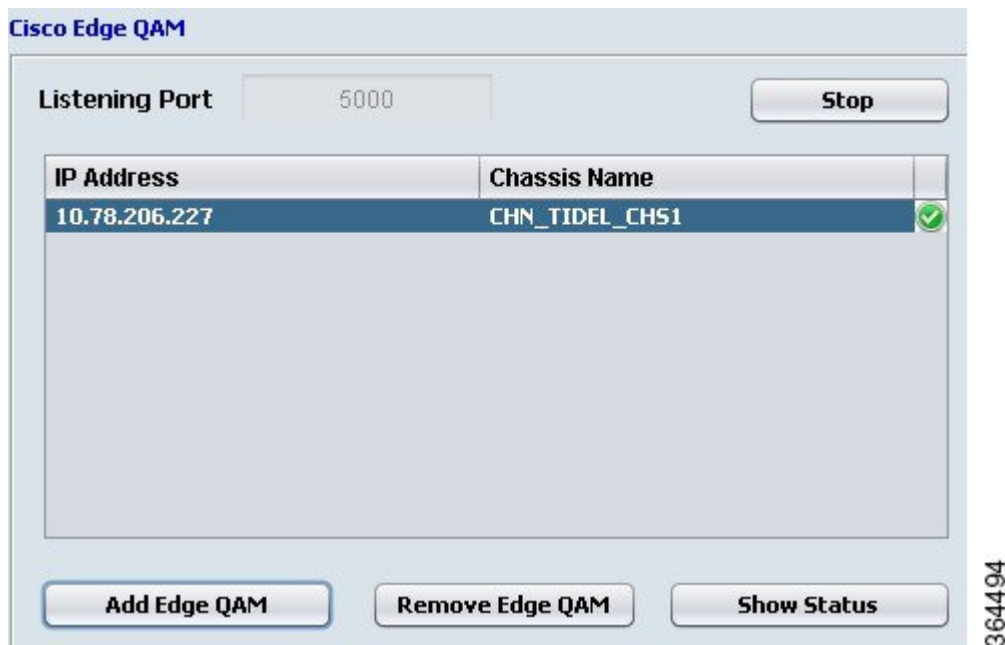
**Step 3** Click the **Add Edge QAM** button in the above window to add Cisco Edge QAM device.

The connection will be established between the CEM application and Cisco Edge QAM device if PME is enabled on Cisco Edge QAM device.

**Note**

The hostname of Cisco Edge QAM device must match the one that is specified on the GUI of the CEM application.

**Figure 12: Connection Established**



The tick symbol in the right-most column of the table indicates that the connection with Cisco Edge QAM device is established. If the cell is blank, it indicates that the connection has not established yet.

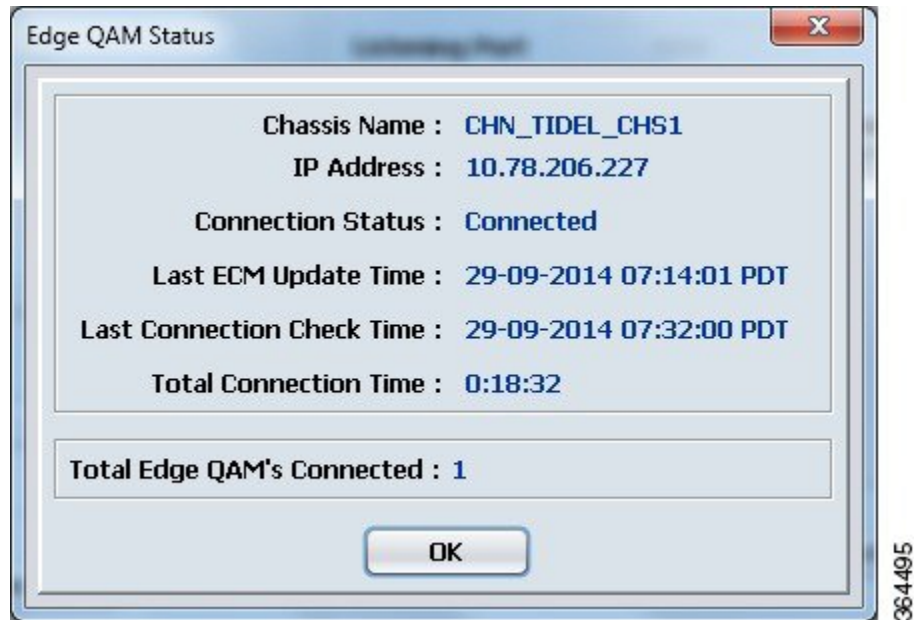
The CEM application will close the connection with Cisco Edge QAM device if:

- no messages are exchanged between the CEM application and Cisco Edge QAM device for 6 minutes.
- Cisco Edge QAM device does not acknowledge the ECM provision message after 3 retries.

## Status of the Connection with the Cisco Edge QAM device

The status of the connection between the CEM application and Cisco Edge QAM device can be ascertained by selecting Cisco Edge QAM device in the Edge QAM List and then clicking the **Show Status** Button.

*Figure 13: Edge QAM Status*



## Removing Cisco Edge QAM device

The connection with Cisco Edge QAM device can be closed and the corresponding entry in the Edge QAM List can be removed by selecting Cisco Edge QAM device in the Edge QAM list and then clicking the **Remove Edge QAM** button.

## General Operation

### Viewing Logs

The logs that are written when the current instance of the CEM application is active will be displayed on the GUI.

Select the **File > View Logs** menu or the **Ctrl+L** shortcut key to view the complete set of logs. The log file will be opened in the default text editor of the operating system.

**Figure 14: Logs**

Time	Log Level	Log
29-09-2014 07:30:38	INFO	ERS Sync Number has not changed.
29-09-2014 07:30:38	INFO	ERS Sync Response from the ERS Server. Sync Number: 20, Callback Time: Mon Sep 29 07:51:10 PDT 2014
29-09-2014 07:30:37	INFO	Sent the Sync Request to the ERS. Waiting for the Response.
29-09-2014 07:30:36	INFO	Sending the Sync Request to the ERS. (Max.Timeout: 240 seconds).
29-09-2014 07:14:02	INFO	Received the ECM Acknowledgement Message from the Edge QAM. Channel ID: 101
29-09-2014 07:14:01	INFO	ECM Messages sent to the Edge QAM. Channel ID: 101
29-09-2014 07:14:01	INFO	Channel Status Message Sent. Channel ID: 101
29-09-2014 07:14:01	INFO	Channel Setup Message Received. VODS-ID: 111, Interface IP Address: 10.78.206.227, Channel ID: 101
29-09-2014 07:14:01	INFO	Accepted the Connection from the Edge QAM with the Interface IP: 10.78.206.227
29-09-2014 07:13:24	INFO	Added the Edge QAM Interface IP-10.78.206.227, Chassis Name: CHN_TIDEL_CHS11 to the List

## Application Settings

The settings that control the communication between the CEM application, the ERS and Cisco Edge QAM device can be viewed/modified using the **File > Application Settings** menu.

The following are the ERS connection settings that can be modified in the application settings dialog:

- timeout for the initial handshake with the ERS server
- timeout for receiving the data from the ERS server
- the time after which the next message should be sent to the ERS server after the server returned an error

Cisco Edge QAM device connection settings including:

- time for which the CEM will wait to receive the acknowledgment message for the ECM provision message from Cisco Edge QAM device before re-sending the ECM provision message
- idle connection timeout

The application settings can be saved by clicking the **File > Save Settings** menu.

## Configuring SNMP Traps

You can configure the CEM application to send SNMP trap messages to the remote SNMP Notification Host/Manager for any connection related errors.

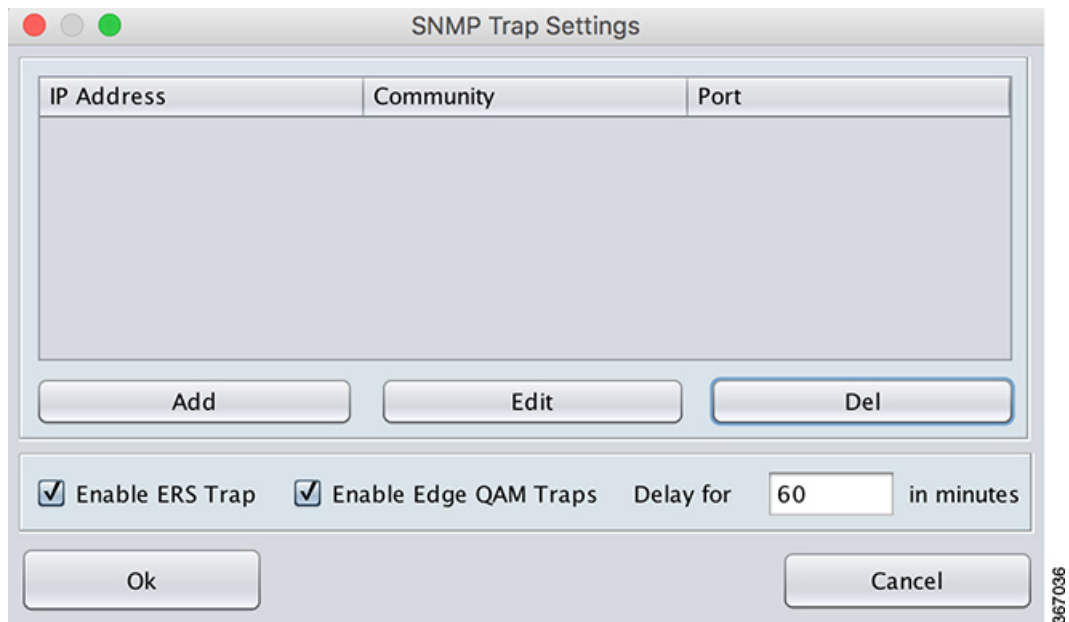
The CEM application sends trap messages only if the connection is not restored before the timeout that is specified on the GUI. By default, trap messages are sent for both ERS connection related errors and Edge QAM connection errors.

## Adding SNMP Notification Host

You can add more than one remote SNMP notification host/manager. Complete these steps to add Cisco Edge QAM device:

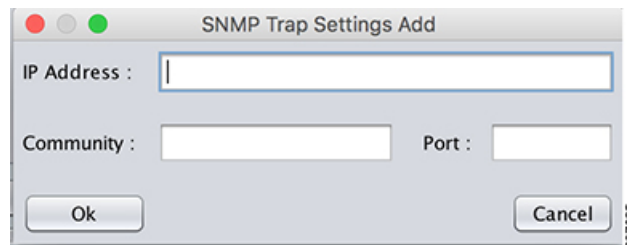
**Step 1** Choose **Configuration > SNMP Trap Settings** menu to open the **SNMP Trap Settings** window.

**Figure 15: SNMP Trap Settings**



**Step 2** Click the **Add** button to open the **SNMP Trap Settings Add** dialog box.

**Figure 16: SNMP Trap Settings Add**



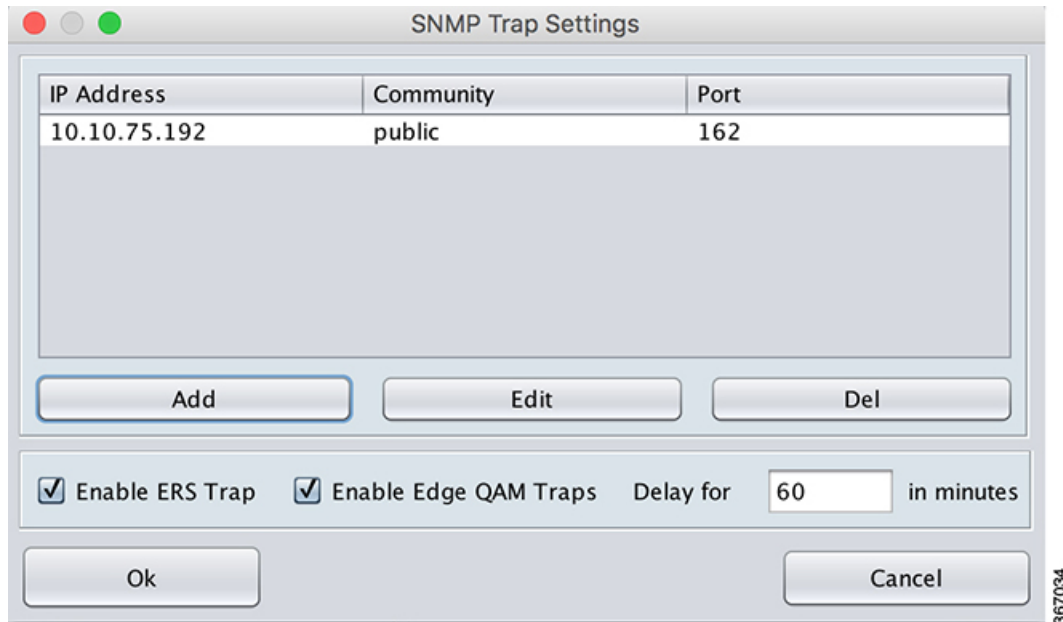
**Step 3** Enter the following details in the **SNMP Trap Settings Add** window:

- IP Address—IP address of the remote SNMP notification host
- Community—SNMP community string

- Port—Port number of the remote SNMP notification host

**Step 4** Click **Ok** to add the host to the list.

*Figure 17: SNMP Trap Settings—Host-list*



**Step 5** Choose the required checkboxes to enable the following:

- **Enable ERS Trap**—ERS connection-related traps
- **Enable Edge QAM Traps**—Cisco Edge QAM connection-related traps

**Step 6** In the **Delay** for text box, specify the time after which the traps should be sent to the configured remote SNMP notification hosts.  
 The traps are sent to the hosts only if the connection is not restored before the timeout that is specified in the UI. By default, the delay is 60 minutes.

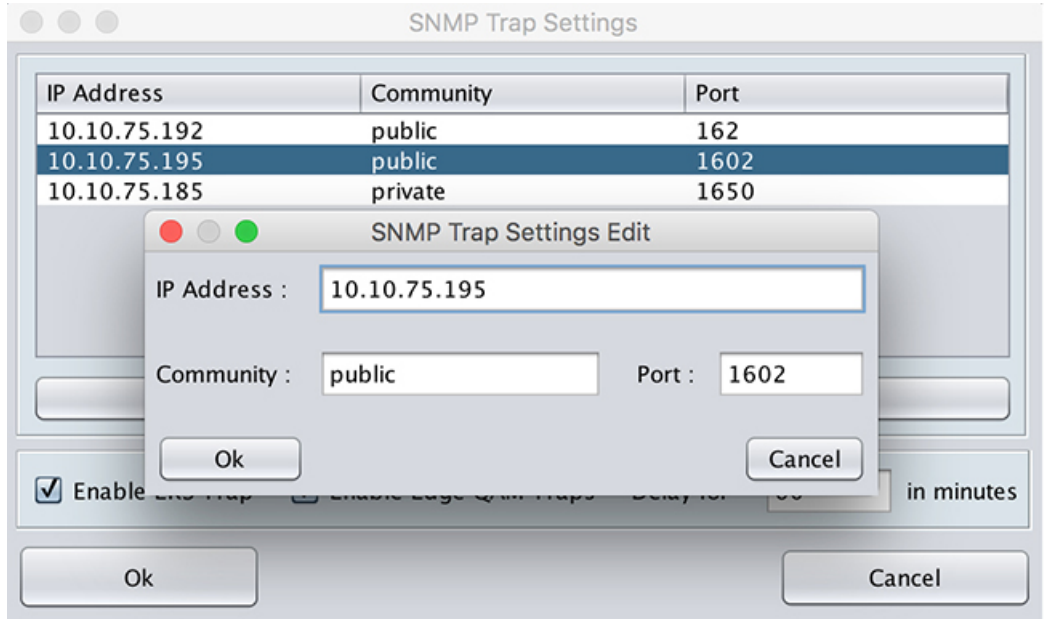
## Modify or Delete SNMP Configuration

You can modify the details of the remote SNMP notification hosts already added in the CEM application.



To edit the details, in the **SNMP Trap Settings** window, select the **IP address** and click the **Edit** button. You can edit the **IP Address**, **Community** (SNMP community string), and the **Port** fields.

**Figure 18: SNMP Trap Settings Edit**



To delete a host configuration, in the **SNMP Trap Settings** window, select the **IP address** and click the **Del** button.

## Feature Information for Converged EdgeQAM Manager

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on [Cisco.com](http://www.cisco.com) is not required.



**Note** The table below lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

**Table 1: Feature Information for Converged EdgeQAM Manager**

Feature Name	Releases	Feature Information
SNMP Trap Configuration	Converged EdgeQAM Manager 2.1	Cisco cBR-8 router is supported in this release.

Feature Name	Releases	Feature Information
Converged EdgeQAM Manager	Version 2.0	Cisco cBR-8 router is supported in this release.
Converged EdgeQAM Manager	Version 1.0	Cisco cBR-8 router is not supported in this release.