Troubleshooting Using the Logs

The following logs may be used to troubleshoot Cisco APIC-EM:

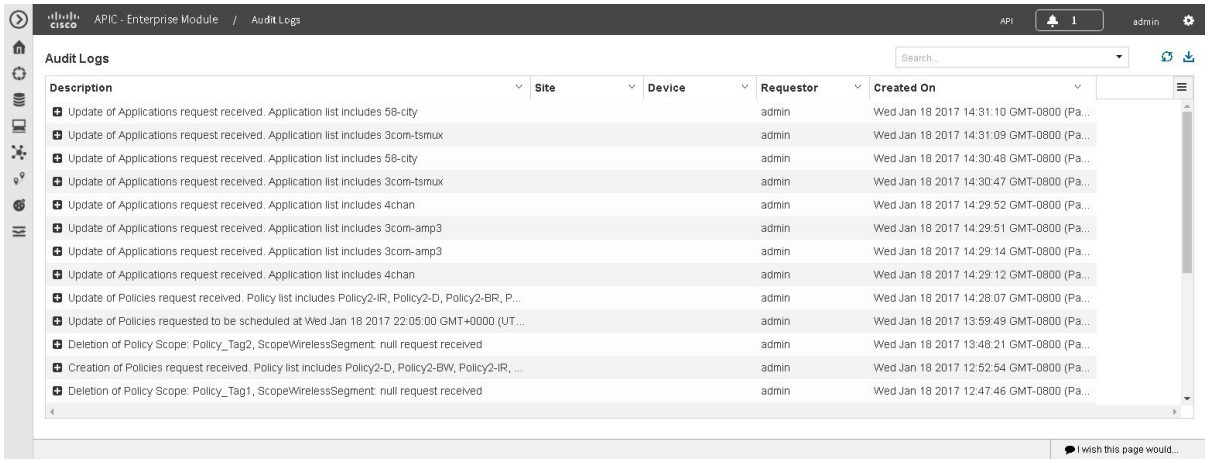
- Audit Logs—Logs used primarily to monitor Cisco APIC-EM policy creation and application.
- Service Logs—Logs used to monitor Cisco APIC-EM services.

Viewing Audit Logs

Audit logs capture information about the various applications (EasyQoS, PnP and IWAN). Additionally, the audit logs also capture information about device PKI notifications. The information in these audit logs can be used to assist in troubleshooting any issues involving the applications or device PKI certificates.

You can view audit logs using the **Audit Logs** window in the Cisco APIC-EM GUI. The Cisco APIC-EM also supports the ability to export the audit logs to a local system.

Figure 1: Audit Logs Window



Before You Begin

You must have successfully installed the Cisco APIC-EM and it must be operational.

You must have either administrator (ROLE_ADMIN), policy administrator (ROLE_POLICY_ADMIN), or Observer (ROLE_OBSERVER) permissions and the appropriate resource scope to perform this procedure.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Audit Logs** link from the drop-down menu.
The **Audit Logs** window appears. In the **Audit Logs** window, you can view logs about the current policies in your network. These policies were applied to network devices by either the IWAN or EasyQoS applications.

The following information is displayed for each policy in the window:

- **Description—**Application or policy audit log description
- **Site—**Name of site for the specific audit log
- **Device—**Device or devices for the audit log
- **Requestor—**User requesting audit log
- **Created On—**Date application or policy audit log was created.

Step 3 Click on the addition icon (+) next to an audit log to view the children audit logs in the **Audit Logs** window.
Each audit log can be a parent to several child audit logs. By clicking on this icon, you can view a series of additional children audit logs.

Note An audit log captures data about a task performed by the controller. Children audit logs are sub-tasks to that one task performed by the controller.

Step 4 Perform a search of the audit logs by clicking on the **Search** field in the **Audit Logs** window, entering a specific parameter, and then clicking the **Submit** button.
You can search for a specific audit log by the following parameters:

- Description
- Requestor
- Device
- Site
- Start Date
- End Date

Step 5 Click on the dual arrow icon to refresh the data displayed in the window.
The data displayed in the window is refreshed with the latest audit log data.

Step 6 Click on the down arrow icon to download a local copy of the audit log in .csv file format.
A .csv file containing audit log data is downloaded locally to your system. You can use the .csv file for additional review of the audit log or archive it as a record of activity on the controller.

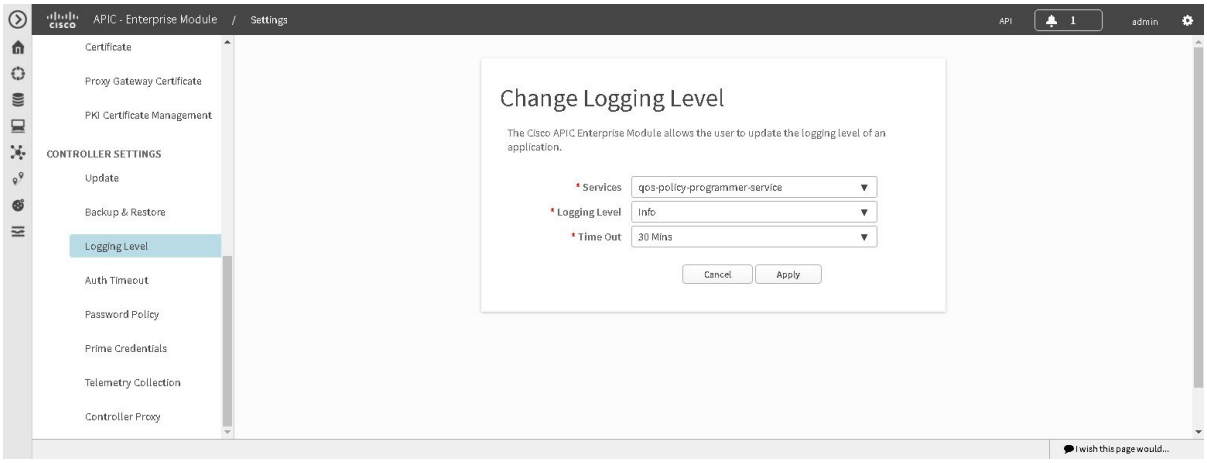
What to Do Next

Proceed to review any additional log files using the controller's GUI, or download individual audit logs as .csv files for further review or archiving purposes.

Changing the Logging Level

To assist in troubleshooting any service issues, you can change the logging level for Cisco APIC-EM services by using the **Changing the Logging Level** window in the Cisco APIC-EM GUI.

Figure 2: Service Logging Level Window



A logging level determines the amount of data that is captured to the controller's log files. Each logging level is cumulative, that is, each level contains all the data generated by the specified level and any higher levels. For example, setting the logging level to **Info** also captures **Warn** and **Error** logs. You may want to adjust the logging level to assist in troubleshooting any issues by capturing more data. For example, by adjusting the logging level you can capture more data to review in a root cause analysis or rca support file.

The default logging level for services in the controller is informational (**Info**). You can change the logging level from informational (**Info**) to a different logging level (**Debug** or **Trace**) to capture more information.

Caution Due to the type of information that may be disclosed, any logs collected at the **Debug** level or higher should be handled with restricted access.

Note The log files are created and stored in a centralized location on your controller. From this location, the controller can query and display them in the GUI. The total compressed size of the log files is 2GB. If log files created are in excess of 2GB, then the pre-existing log files are overwritten with the newer log files.

Before You Begin

You must have successfully installed the Cisco APIC-EM and it must be operational.

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

For information about the user permissions required to perform tasks using the Cisco APIC-EM, see the chapter, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Changing the Logging Level** to view the **Changing Logging Level** window. The **Logging Level** table appears with the following fields:

- **Services**
- **Logging Level**
- **Timeout**

Step 4 In the **Changing Logging Level** window, choose a service from the **Services** field to adjust its logging level.

Note The **Services** field displays any services that are currently configured and running on the controller.

Step 5 In the **Changing Logging Level** window, choose the new logging level for the service from the **Logging Level** field. The following logging levels are supported on the controller:

- **Trace—**Trace messages
- **Debug—**Debugging messages
- **Info—**Normal but significant condition messages
- **Warn—**Warning condition messages
- **Error—**Error condition messages

Step 6 In the **Changing Logging Level** window, choose the time period for the logging level from the **Timeout** field for the logging level adjustment.
You configure logging level time periods in increments of 15 minutes up to an unlimited time period.

Step 7 Review your selection and click the **Apply** button.
To cancel your selection click the **Cancel** button.

The logging level for the specified service is set.