Understanding the Cisco IPICS Logs

This chapter describes the information that you can obtain from the Cisco IPICS logs. The log information can aid you in troubleshooting problems that may occur with the Cisco IPICS and the PMC application.

This chapter includes the following sections:

Modifying the PMC Log Levels

The PMC application can generate logs that can be helpful when you analyze user activity and troubleshoot problems you may encounter when using the application. The PMC writes the logs to the hard disk of the PMC client machine, so that the application can continue logging if the communication to the server is disrupted. The logs are transferred to the server during its normal communication with the PMC.

This section has the following topics:

Users can generate PMC logs in the following ways:

- The PMC user can adjust settings within the PMC application. Refer to the *Cisco IPICS PMC Installation and User Guide* for more information.
- From the Administration Console, the Cisco IPICS operator can modify the log settings in the User Details area of the Manage Users window. See the "Setting PMC Log Levels in User Details" section on page 2-10 for more information.

The PMC can generate the following log files:

Table 2-1 PMC Log File Descriptions

PMC Log File Name	PMC Log File Description
Authentication.log	This log file contains a history of all user login and logout attempts per PMC installation. This log appears in XML format.
ChannelStatistics.log	At regular and predefined intervals, this log records each channel's statistics, including data for both sent and received transmissions over the network. This log appears in XML format.
UserInterface.log	This log contains a history of the user interactions with the PMC application. This log appears in XML format.
DebugLog.txt	This log contains debugging information that is relevant to how the PMC operates. You can track several different categories of debugging information and adjust the log levels to three different settings within each category. The DebugLog appears in text format and is rotated each time that the user starts the PMC application. For detailed information about the Debug Log, see the "Understanding Debug Log Information" section on page 2-3.

The default behavior for the DebugLog.txt file is to capture activity for the PMC, such as critical errors, IP changes, and so on. Initially, this log contains the PMC version and system statistics, such as the media devices that are installed on the system (headsets, microphones, and so on). The other PMC logs do not get produced until you set, except Channel Activation which is on by default.

Note You can obtain activity information for PMC users in the Activity Logs window of the Administration Console. This information includes details about user associations to channels and VTGs, channel activation activities, and conference participation. For information about using the Activity Logs window, refer to the *Cisco IPICS Server Administration Guide*.

Cisco IPICS retrieves logs from the PMC when one of the following events occur:

- You request a log in the User Details pane of the Administration Console Manage Users window.
- You set the logs to be uploaded to the Cisco IPICS server automatically when the PMC user logs in, and then out of, a session (this event is called rollover).

Rollover only occurs for the Authentication, Channel Statistics and User Interface logs, but not for the Debug Log. In the case of the Debug Log, the file continues to accumulate data until the server requests the file to be uploaded.

After Cisco IPICS completes the upload, the PMC automatically deletes the file from the hard disk of the client machine.

Understanding Debug Log Information

Cisco IPICS organizes the DebugLog.txt data fields into three categories: User Interface, Signaling, and Media. These data fields are then divided into three logging levels, so that you can capture more precisely the debugging information that you need. The Debug Log categories contain the following information:

- User Interface—These fields provide information about aspects of the user interface for the PMC. The category includes everything that the user can see on the PMC application, such as the buttons and volume controls. The User Interface category also includes information for debugging communications problems with the Cisco IPICS server.

  Table 2-2 describes the type of information you can gather with the User Interface log levels.

Table 2-2 User Interface Log Levels

Logging Level	Purpose
1	Useful for debugging the following types of issues: • The user is not able to log in • The user receives error messages from the server • The PMC goes into offline mode unexpectedly • The user has difficulty activating channels • The user has problems when closing the PMC application
2	This information can assist with translating server XML communications.
3	Issues regarding authentication, the GUI, and the PMC server update function.

- Signaling—The Signaling category includes fields that provide information about the starting and stopping of voice channels. You would turn Signaling on when a user is not able to activate or deactivate a PMC channel.

  Table 2-3 describes the type of information you can gather with the Signaling log levels.

Table 2-3 Signaling Log Levels

Logging Level	Purpose
1	Issues that involve the high level state machines.
2	Issues that involve the high level state machines.
3	Issues that involve SIP messaging.

- Media—These fields involve items related to the voice stream, such as the packets and the codecs that handle the data between end points. You would use Media information to diagnose any voice quality problem.

Table 2-4 describes the type of information you can gather with the Media log levels.

Table 2-4 Media Log Levels

Logging Level	Purpose
1	This information provides RX and TX networking statistics.
2	This information can assist you to diagnose audio mixing issues, such as the combining of audio signals in a channel or VTG.
3	This information can assist in the area of converting audio using audio codecs.

Using the Debugging Log Level

When you choose to begin logging debug information for a PMC user, you select one or more of the information categories, each of which includes a list of debugging fields. You choose the category and logging level as it corresponds to particular fields that you want to capture in the log.

Table 2-5 show the fields that are included in each logging level.

The log levels for each category are cumulative. If you choose Level 2 for a category, the PMC writes Level 1 and Level 2 fields into the DebugLog.txt file. When you set the logging to Level 3, you capture all the fields for that category.

Tip Always start debugging by collecting Level 1 data, which may provide all the data you require. Using Log Level 1 allows you to gather several days of log activity and not fill hard disk of the PMC user. If you cannot locate the cause of the problem, you can set the logging to Level 2 or Level 3.

Use Level 3 only for short durations. You can also closely monitor the hard drive of the user, so that the Level 3 logs do not overwhelm the client hard drive or strain performance of the PMC.

Caution Because of the large amount of information that the system collects and generates when you set all of the debug options, Cisco recommends that you use debug logging only to isolate specific problems. When your debugging tasks have been completed, be sure to turn off debug logging by clearing the debug log.

Table 2-5 lists the fields that are associated with each DebugLog section:

Table 2-5 DebugLog Fields and Log Levels

Category	Field	Log Level
User Interface	channel-activation-debug	1
	error	
	exit-debug	
	sending-source-debug	
	sock-init-cleanup	
	xml-events	2
	xml-post	
	xml-vars	
	Auth	3
	critical-section-tune-debug	
	xml-deck	
	gui-debug	
	server-task-debug	
	server-verbose	

Table 2-5 DebugLog Fields and Log Levels (continued)

Category	Field	Log Level
Signaling	cc	1
	fim	
	fsm	
	gsm	
	lsm	
	multicast-signaling-debug	
	sip-reg-state	
	sip-state	
	vcm	
	sip-task	2
	sip-trx	
	Auth	3
	cc-msg	
	sip-messages	

Table 2-5 DebugLog Fields and Log Levels (continued)

Category	Field	Log Level
Media	AMuteTrans	1
	AudioSink	
	AudioSource	
	MediaStream	
	OpenALAudioSink	
	RTPAudioSink	
	RTPAudioSockets	
	RTPAudioSource	
	RTPAudioStream	
	RTPJitterBuf	
	sock-init-Cleanup	
	WaveAudioSource	
	WaveFileSource	
	RxStats	
	TxStats	

Table 2-5 DebugLog Fields and Log Levels (continued)

Category	Field	Log Level
Media	RxDetailStats	2
	ACMTrans	
	dsp	
	FilePlay	
	PCMMixer	
	PCMVolTrans	
	PCMVolumeMax	
	VAD	
	RTPAudioStreamMgr	
	AudioDump	3
	AudioSamp	
	AudioSampLost	
	AudioSampMgr	
	AudioTrans	
	dtmf	
	FIRTrans	
	FSAudioBuf	
	G7112PCMTrans	
	G7232PCMTrans	
	G729A2PCMTrans	
	Limiter	
	PCM2G711Trans	
	PCM2G723Trans	
	PCM2G729ATrans	
	TimeSample	

Setting PMC Log Levels in User Details

Note You must have operator privileges in Cisco IPICS to access the Manage Users window of the Administration Console.

In the User Details pane of the Manage Users window, you can instruct the Cisco IPICS server to retrieve updated activity logs for a particular PMC user. For the DebugLog.txt file, you can also set a logging level to retrieve specific types of debugging information.

After you obtain the logs that you need, you can easily reset or adjust your log settings by using the following procedure in this section. The log settings that you configured in the User Details pane remain will persist until you change them back to the default (or any other) settings.

Caution The User Details pane displays the new log settings for a user after you change them. Be sure to note the changes you make and the users for whom you made them, so that you can reset the log levels to the default setting after you finish your troubleshooting.

To define log settings and retrieve the file in the User Details pane, follow this procedure:

Procedure

Step 1 From the Operator tab in the Cisco IPICS Administration Console, click the **Manage Users** link.

Step 2 Click a user from the All Users list and then click **Details**.

Step 3 To set the log level for the desired log, use the drop-down lists under the Set PMC Log Level heading. You can set the log levels to the following settings:

- Authentication—Choose 1 to turn the logging on for this log; choose 0 to turn logging off
- User Interface—Choose 1 to turn the logging on for this log; choose 0 to turn logging off

- Channel Statistics—Choose 1 to turn the logging on for this log; choose 0 to turn logging off.
- Debug Log—Choose from one of the following log level options:
  - 1 to capture Level 1 fields
  - 2 to capture Level 1 and Level 2 fields
  - 3 to capture fields for all Log Levels

Step 4 To save the new log levels, click **Save**.

The log level settings display in the User Details pane and Cisco IPICS sends the new log level information to the PMC.

Step 5 Wait for the PMC to collect the log or debugging data.

If you have set the Debug Log to Level 3 in any category, monitor the disk space that the file consumes, so that it does not cause a problem for the user.

Step 6 To retrieve the file, click **Get** in the User Details pane.

Cisco IPICS sends a request (when the PMC next polls the server) to retrieve the specified log. Then, the PMC deletes the file from the hard disk of the PMC client machine.

You can find the retrieved logs in the directory for the PMC user. Cisco IPICS stores the log files in the following directory:

/opt/cisco/ipics/tomcat/current/webapps/ipics_server/pmclogs/<*user_ID*>

where *user_ID* is the user ID for the PMC that you are debugging.

Step 7 When you have completed the debugging for this PMC user, use the drop-down lists under Set PMC Log Levels to reset the log levels to 0 for all logs.

Step 8 Click **Save**.

Viewing Cisco IPICS Logs

Cisco IPICS generates several logs that can be useful in troubleshooting problems that you may encounter. The Cisco IPICS logs are located in the following directory:

/opt/cisco/ipics/tomcat/current/logs

Table 2-6 lists the Cisco IPICS logs that you can use for debugging.

Table 2-6 Cisco IPICS Logs

Log Name	Description
ipics.log	Cisco IPICS writes any known errors to the ipics.log file. When the log reaches approximately 5 MB in size, a new ipics.log is created and the previous logs are closed and archived. The most current entries in the ipics.log display in the System Status window of the Administration Console. For more information about the ipics.log file, see the "Downloading System Logs" section on page 3-6.
catalina.out	If non-typical errors occur in the Cisco IPICS server software or its components, the activity that caused the error may be captured in the catalina.out log.
ipics.rms.log	The ipics.rms.log collects log data for the RMS components that have been added to the Cisco IPICS database. When the log reaches approximately 1 MB in size, a new ipics.rms.log is created and the previous logs are closed and archived.
ipics_audit.log	The ipics_audit.log records, in XML format, every button that any Cisco IPICS user has clicked when using the Cisco IPICS system.
bar_act.log	This log captures information that relates to the Cisco IPICS backup and restore procedures. You can view the log in the Manage Database window of the Administration Console. For more information, refer to the *Cisco IPICS Backup and Restore Guide*.

Checking CSA Logs

If CSA denies a system action, the process generates a message that you can access in several ways. You can open the CSA Utility to view the messages in the Message pane or you can view the Security Events Log, which includes all security events that have occurred on the system.

You can view the latest Security Events Log in the CSA Utility or you can navigate to the /var/logs directory, where you can access the current and archived logs.

The file name of the Security Event Log is csalog. After seven days, CSA creates a new log and renames the previous log with a numbered extension. This process repeats every seven days, so that the logs are named csalog.0, csalog.1, csalog.2, and so on. The oldest log in the directory has the highest numbered extension.

This section includes the following topics:

Viewing the CSA Utility Messages Pane

To view status messages in the CSA utility, click the CSA tray icon (the red flag) to open the CSA Utility. Then, click **Messages**.

Status messages display in the Messages pane.

Opening the Security Events Log from the CSA Utility

To view the Security Events Log in the CSA Utility, perform the following procedure:

Step 1 Click the CSA tray icon (the red flag) to open the CSA Utility.

The CSA Utility displays.

Step 2 To access the Security Logs, click **Messages**.

Step 3 Click **View Log**.

The current Security Events Log displays in a text viewer window.

Opening a Security Events Log with a CLI Command

If you navigate to the **/var/log** directory, you can view the current log or any of the archived logs. You can view them by entering a CLI command.

To view a security event log with a CLI command, perform the following steps:

Step 1 Log in to the Cisco IPICS terminal with root, informix, or system user privileges.

The Cisco Linux desktop displays.

Step 2 To view the contents of the **/var/log** directory, open a Cisco Linux terminal window by clicking the **Red Hat** icon. Then, choose **System Tools > Terminal**.

A terminal window displays.

Step 3 To navigate to the /var/log directory, enter the following command:

Step 4 [root] **#cd /var/log**

Step 5 To view a list of the files in the directory, enter the following command:

Step 6 [root] **#ls -al**

The contents of the directory display. The security event logs are named csalog.*x*, where *x* is the numerical archive extension for the file. The most current log is named csalog and has no numerical extension.

Step 7 To view the contents of a log file, enter the following command:

Step 8 [root] **#cat csalog.*x***

For information about the messages that appear in the CSA logs, see the CSA documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/