Understanding the Cisco IPICS Logs

This chapter describes the logs that are available in Cisco IPICS, and how to retrieve and understand the information that is contained in the logs. The logs can help you to troubleshoot problems that may occur with Cisco IPICS and the PMC.

This chapter includes the following sections:

Understanding and Locating the Cisco IPICS Log Files

The Cisco IPICS log files contain information that can be used for auditing or tracking the usage of Cisco IPICS. The log files also can also help you to determine the root cause of an error.

Table 6-1 lists the Cisco IPICS logs.

Table 6-1 Logs That Are Used with Cisco IPICS

Log Name	Description
Cisco IPICS Activity Log	The Cisco IPICS logs store information about activities relating to channels, users, and VTGs. To download and view the information in the activity log in a Microsoft Excel spreadsheet format, log in to the Administration Console as the ipics user, navigate to the **Administration > Activity Log Management > Logs** tab, and click **Download Activity Logs**. You can change the information that Cisco IPICS saves in the activity log by navigating to **Administration > Activity Log Options**. For more information about the activity log, refer to the "Performing Cisco IPICS System Administrator Tasks" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.
csalog	The csalog file contains messages that are related to CSA. The csalog file is located in the **/var/log** directory. For more information about the caslog file, see the "Opening a Security Events Log with CLI Commands" section on page 6-14.
db-maintenance.log	The db-maintenance.log file contains records of any database actions, such as a database backup or restore operation. To download and view the db-maintenance.log file, log in to the Administration Console as the ipics user, navigate to the **Administration > Database Management > Log** tab and click **Download**. The db-maintenance.log file is located in the **/opt/cisco/ipics/database/logs** directory. For more information on the db-maintenance.log file, refer to the "Performing Cisco IPICS Database Backup and Restore Operations" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.
diagnostics.log	The diagnostics.log file contains messages that are related to the database subsystem. The diagnostics.log file is located in the **/opt/cisco/ipics/database/logs** directory.

Table 6-1 Logs That Are Used with Cisco IPICS (continued)

Log Name	Description
install.log	The install.log file shows details of the Cisco IPICS installation, including the packages that were installed and any errors that occurred during the installation. The install.log file is located in the **/root** directory.
ipics.log	The ipics.log file contains information regarding all transactions that occur in the Cisco IPICS server. There are seven severities, from TRACE to FATAL. By default, the ipics.log captures all logging from the INFO to the FATAL level. You can view recent system logs in the **Serviceability > System Logs** window of the Administration Console. To download and view the information in the ipics.log, navigate to the **Serviceability > System Logs** window and click **Download**. For more information on the ipics.log file, refer to the "Understanding Cisco IPICS Serviceability and Diagnostic Information" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*. The ipics.log file is located in the **/root/tomcat/current/logs** directory.
ipics_audit.log	The ipics_audit.log records user activity. This activity includes successful and unsuccessful attempts by users to log in to the server, and actions that Cisco IPICS users perform when they are logged into the Administration Console. The ipics_audit.log file is located in the **/root/tomcat/current/logs** directory.
ipics_rms.log	The ipics_rms.log collects log data for the RMS components that are part of the Cisco IPICS system. The ipics_rms.log file is located in the **/root/tomcat/current/logs** directory. When the log reaches approximately 1 MB in size, Cisco IPICS creates a new ipics_rms.log, and closes and archives the previous logs.

Table 6-1 Logs That Are Used with Cisco IPICS (continued)

Log Name	Description
lmgrd.log	The lmgrd.log file contains information regarding Cisco IPICS licenses and the component that manages the licenses (known as the license manager). Cisco IPICS logs any actions that the license manager performs in the lmgrd.log file. You can download and view the lmgrd.log file by accessing the Administration Console as the ipics user, then navigating to the **Serviceability** > **Diagnostics** window and clicking **Download Diagnostic Results**. You receive a zipped file that contains the lmgrd.log and ipics.log files, along with the information that displays in the Diagnostics window. The lmgrd.log file is located in the **/opt/cisco/ipics/license/versions/2.0/logs** directory.
messages	The messages file logs the following: • Messages that are related to CSA • Users that have logged into the Cisco IPICS server using SSH • Processes that have stopped or started The messages file is located in the **/var/log** directory. After seven days, CSA creates a new log and renames the previous log with a numbered extension so that the logs are named **messages.0**, **messages.1**, **messages.2**, and so on.

Table 6-1 Logs That Are Used with Cisco IPICS (continued)

Log Name	Description
Dial engine log files	The Cisco IPICS dial engine, which controls dial-in and dial-out functionality for the policy engine, produces two sets of log files: • Cisco001MIVR—These log files provide you with information about call signaling and the Session Initiation Protocol (SIP). You configure the size of each Cisco001MIVR file, the total number of files that Cisco IPICS retains, and the information that Cisco IPICS logs in these files, by navigating to **Policy Engine > Control Center > Tracing** in the Administration Console and changing the trace settings. When a log file reaches the configured maximum size, Cisco IPICS closes that log file and creates a new empty log file, and increments the number of the new log file by one. • driverManager—The driverManager logs contain information related to the media that are associated with each call. To configure the level of detail that the driverManager logs capture, navigate to **Policy Engine > Control Center > Tracing** in the Administration Console, and check or uncheck the LIB_MEDIA check boxes. Cisco IPICS sets the size and total number of driverManager files, and you cannot change these settings. The dial engine log files are located in the **/opt/cisco/ippe/log/MIVR** directory. You can also view these files by navigating to **Policy Engine > Control Center > Status > Dial Engine** in the Administration Console. You configure the size of each file, the number of log files that are retained, and the logging levels by navigating to **Policy Engine > Control Center > Tracing** in the Administration Console and changing the trace settings. For more information, refer to the "Configuring and Managing the Cisco IPICS Policy Engine" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

Generating and Modifying the PMC Log Levels

The PMC application generates logs that can help you analyze user activity and troubleshoot problems that you may encounter when you use 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.

Cisco IPICS retrieves logs from the PMC if one of the following conditions are met:

- When you click **Get Logs from PMC** from the **User Management** > **Users** > *Username* > **PMC** tab.

Note You can prevent the server from uploading the logs from the PMC user by navigating to **Settings** > **Channels** in the PMC application and checking the **Optimize for low bandwidth** check box. You should check this box if you are using the PMC in a low bandwidth, high latency network environment. The PMC still generates logs on the hard drive of the PMC client machine.

- When 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 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 that the file be uploaded. For more information about a rollover occurrence, refer to the "Using the PMC Application Logs" chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*.

Users can modify the PMC logs in the following ways:

- The PMC user can adjust settings within the PMC application. For more information about adjusting settings in the PMC application, refer to the "Using the PMC Application Logs" chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*.

- From the Administration Console, the Cisco IPICS operator can modify the log settings in the **User Management** > **Users** > *Username* > **PMC** tab. See the "Performing Cisco IPICS Operator Tasks" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)* for more information about setting and modifying the log settings.

For a list of the log files and their descriptions, refer to the "Using the PMC Application Logs" chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*.

You can download activity logs for PMC users in the **Administration** > **Activity Log Management** > **Logs** tab of the Administration Console. The information that you download includes details about user associations to channels and VTGs, channel activation activities, and conference participation. You configure the activity logs to capture the PMC information in the **Administration** > **Activity Log Options** window. For information about the activity logs, refer to the "Performing Cisco IPICS System Administrator Tasks" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

This section has the following topics:

Understanding PMC 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 communication problems with the Cisco IPICS server.

  Table 6-2 describes the information that Cisco IPICS gathers, by log level:

Table 6-2 User Interface Log Levels

Logging Level	Purpose
Low	Cisco IPICS retrieves information for the following problems at the Low log level: • The user cannot log in • The user has difficulty activating channels • The user cannot close the PMC • The PMC unexpectedly goes into offline mode • The server is reporting errors
Medium	Cisco IPICS reports information that can help translate XML communication from the server.
High	Cisco IPICS gathers information 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 6-3 describes the information that Cisco IPICS reports by signaling levels.

Table 6-3 Signaling Log Levels

Logging Level	Purpose
Low and Medium	Messages at these log levels describe issues with the high level state machines.
High	Messages at this level report issues with 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 6-4 describes the type of information you can gather with the Media log levels.

Table 6-4 Media Log Levels

Logging Level	Purpose
Low	This information provides RX and TX networking statistics.
Medium	This information can help you diagnose audio mixing issues, such as the combining of audio signals in a channel or VTG.
High	This information provides you with information regarding the conversion of 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 the fields that you want to capture in the log.

Table 6-5 shows the fields that are included in each logging level.

The log levels for each category are cumulative. If you choose the Medium level for a category, the PMC writes Low- and Medium-level logs into the DebugLog.txt file. When you set the logging to High, you capture all the fields for that category.

Tip Always start debugging by collecting Low-level log data, which may provide all of the data that you require. Using a log level of Low allows you to gather several days of log activity without filling the hard disk of the PMC user. If you cannot locate the cause of the problem, you can set the logging to Medium or High.

Use the High level only for short durations. If you use the High level, you should closely monitor the hard drive of the user so that the High-level logs do not overwhelm the client hard drive or degrade the 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 you complete your debugging tasks, be sure to turn off debug logging by clearing the debug log.

Table 6-5 lists the debug categories, and the fields and log levels that are associated with each category.

Table 6-5 Debug Log Fields and Log Levels

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

Table 6-5 Debug Log Fields and Log Levels (continued)

Category	Field	Log Level
Signaling	cc	Low
	fim	
	fsm	
	gsm	
	lsm	
	multicast-signaling-debug	
	sip-reg-state	
	sip-state	
	vcm	
	sip-task	Medium
	sip-trx	
	Auth	High
	cc-msg	
	sip-messages	

Table 6-5 Debug Log Fields and Log Levels (continued)

Category	Field	Log Level
Media	AMuteTrans	Low
	AudioSink	
	AudioSource	
	MediaStream	
	OpenALAudioSink	
	RTPAudioSink	
	RTPAudioSockets	
	RTPAudioSource	
	RTPAudioStream	
	RTPJitterBuf	
	sock-init-Cleanup	
	WaveAudioSource	
	WaveFileSource	
	RxStats	
	TxStats	
Media	ACMTrans	Medium
	ASL	
	AudioBufferAndPlayback	
	dsp	
	FilePlay	
	PCMMixer	
	PCMVolTrans	
	PCMVolumeMax	
	RTPAudioStreamMgr	
	RxDetailStats	
	VAD	

Table 6-5 Debug Log Fields and Log Levels (continued)

Category	Field	Log Level
Media	AudioDump	High
	AudioSamp	
	AudioSampLost	
	AudioSampMgr	
	AudioTrans	
	AutomaticGainControl	
	dtmf	
	FIRTrans	
	FSAudioBuf	
	G7112PCMTrans	
	G7232PCMTrans	
	G729A2PCMTrans	
	Limiter	
	PCM2G711Trans	
	PCM2G723Trans	
	PCM2G729ATrans	
	RTCPPacket	
	TimeSample	
	TimeRxSample	
	TimeTxSample	

Checking CSA Logs

If CSA denies a system action, the process generates a message that you can access in one of the following ways:

- You can open the CSA Utility to view the messages in the Message pane
- You can view the Security Events Log, which includes all security events that have occurred on the system
- You can navigate to the **/var/log** directory, and view the current and archived CSA logs

This section includes the following topics:

Viewing the CSA Messages from the CSA Utility

To view status messages in the CSA utility, perform the following procedure:

Procedure

Step 1 Double-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**.

Status messages display in the Messages pane.

Step 3 To view the CSA log, click **View Log**.

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

Opening a Security Events Log with CLI Commands

The **/var/log** directory in the Cisco IPICS server contains the current and archived CSA 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.

To view a security event log by using CLI commands, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server by using the root user ID.

Step 2 To navigate to the **/var/log** directory, enter the following command:

Step 3 [root] #**cd /var/log**

Step 4 To view a list of the files in the directory, enter the following command:

Step 5 [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 6 To view the contents of a log file, enter the following command:

Step 7 [root] #**cat csalog** [**.***x*]

Where:

x is the file extension of the csalog file you would like to view.

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

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