CHAPTER 10

Log Configuration

The Log windows let you set up and view the IP camera log file, which captures information about the IP camera and its activities.

The IP camera stores the log file in its internal SDRAM. If the SDRAM becomes full, the IP camera begins to overwrite existing information. To avoid losing log information, you can configure the IP camera to send log information to a Syslog server.

Caution Because the logs are stored in the internal camera SDRAM, all existing logs in the camera are lost after a camera reboot, power-up, or power-down.

The following sections describe the Log windows in detail:

Log Setup Window

The Log Setup window provides options for configuring the log file and an optional Syslog server on which to store log files.

To display the Log Setup window, perform the following steps:

Procedure

Step 1 From the IP camera user interface, click the **Setup** link.

Step 2 Click **Log** to expand the menu.

Step 3 From the Log menu, click **Setup**.

The Log Setup window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

Table 10-1 describes the options in the Log Setup window.

Table 10-1 Log Setup Window Options

Option	Description
Local Log Settings Area	
Minimum Log Severity	Choose the minimum severity of messages that the appear in the log file. The system logs all messages of this severity and higher. Message severities, from highest to lowest, are: • **Emergency**—The system is unusable. • **Alert**—A situation occurred that requires immediate action. • **Critical**—A situation occurred that requires action soon. • **Error**—An error occurred, but it does not necessarily affect the ability of the system to function. • **Warning**—A undesirable condition occurred. • **Notice**—Notification about a system condition that is not necessarily an error condition. • **Informational**—Information about a system activity. • **Debug**—Information about a system activity with detailed technical information. Includes messages of every other severity. The default severity is Informational.
Maximum Log Entries	Maximum number of entries that the log file maintains. When the log file reaches this limit, it begins overwriting entries, starting with the oldest one. The default value is 100.
Syslog Settings Area	
Enable Syslog	Check this check box to send the log information to a designated Syslog server. The selected information also is maintained on the IP camera until it is overwritten. This option is useful for consolidating logs in deployments with several IP cameras and for retaining logs.
Primary Syslog Server	Identify the primary Syslog server by choosing **IP Address** or **Hostname** from the drop-down list and entering the IP address or host name in the corresponding field.
Primary Syslog Server Port	Enter the primary Syslog server port number that receives the logs. Valid values are 514 and 1024 through 65535. The default Syslog port is 514.
Facility	Enter the system facility that receives logs on the Syslog server.

Table 10-1 Log Setup Window Options (continued)

Option	Description
Minimum Log Severity	Choose the minimum severity of messages that are sent to the Syslog server. The system sends all messages of this severity and higher. Message severities, from highest to lowest, are: • **Emergency**—The system is unusable. • **Alert**—A situation occurred that requires immediate action. • **Critical**—A situation occurred that requires action soon. • **Error**—An error occurred, but it does not necessarily affect the ability of the system to function. • **Warning**—A undesirable condition occurred. • **Notice**—Notification about a system condition that is not an error condition. • **Informational**—Information about a system activity. • **Debug**—Information about a system activity with detailed technical information. Includes messages of every other severity. The default severity is Informational.
Secondary Syslog Server	Identify an optional secondary Syslog server by choosing **IP Address** or **Hostname** from the drop-down list and entering the IP address or host name in the corresponding field.
Secondary Syslog Server Port	Enter the port number that receives the logs on the secondary Syslog server. Valid values are 514 and 1024 through 65535. The default Syslog port is 514.
Facility	Enter the system facility that receives logs on the Syslog server.
Minimum Log Severity	Choose the minimum severity of messages that are sent to the secondary Syslog server. The system sends all messages of this severity and higher. Message severities, from highest to lowest, are: • **Emergency**—The system is unusable. • **Alert**—A situation occurred that requires immediate action. • **Critical**—A situation occurred that requires action soon. • **Error**—An error occurred, but it does not necessarily affect the ability of the system to function. • **Warning**—An undesirable condition occurred. • **Notice**—Notification about a system condition that is not an error condition. • **Informational**—Information about a system activity. • **Debug**—Information about a system activity with detailed technical information. Includes messages of every other severity.

Local Log Window

The Local Log window lets you view the log file that is stored on the IP camera.

To display the Local Log window, perform the following steps:

Procedure

Step 1 From the IP camera user interface, click the **Setup** link.

Step 2 Click **Log** to expand the menu.

Step 3 From the Log menu, click **Local Log**.

The Local Log window appears.

Table 10-2 describes the options in the Local Log window.

Table 10-2 Local Log Window Options

Option	Description
Log List Area	
Rows per page	Choose the number of log entry rows to display per page and click the **Go** button to the right of this option to update the display.
Filter	Choose the type of log message to include in the display. To include messages of every severity, choose **All**.
Since	Choose the time period for which you want to view log messages.
Go button	Update the log display based on the values in the Filter and Since fields.
Severity	An icon in this column indicates the severity of the corresponding log message: —Emergency message —Alert message —Critical message —Error message —Warning message —Notice message —Informational message —Debug message To display log messages in order of severity with the least severity first, click the Severity column heading. Click the heading again to reverse the display order.
Date/Time	Date and time that the logged activity occurred. By default, log messages appear in the order that the activity occurred with the oldest message first. To reverse this display order, click the Date/Time column heading.

Table 10-2 Local Log Window Options (continued)

Option	Description
Description	Message that describes the logged activity. For detailed information about log messages, see Table 10-3 on page 10-5.
Page controls	Let you move through the log file entries: Page field—Enter a page number and press Enter.  —Go to first page  —Go to previous page  —Go to next page  —Go to last page

Table 10-3 describes the messages that can appear in the IP camera log file. When you view the log file, each message includes the date and time that it was logged. In this table:

- Messages appear in alphabetical order
- Angle brackets (<>) indicate items that are replaced by appropriate information when the message appears. *Italic text* describes these items.
- Severity indicates the severity of the message:
  - 0—Emergency (the system is unusable)
  - 1—Alert (a situation occurred that requires immediate action)
  - 2—Critical (a situation occurred that requires action soon)
  - 3—Error (an error occurred, but it does not necessarily affect the ability of the system to function)
  - 4—Warning (an undesirable condition occurred)
  - 5—Notice (notification about a system condition that is not an error condition)
  - 6—Informational (information about a system activity)
  - 7—Debug (information about a system activity with detailed technical information)

Table 10-3 Log Messages

Message Name	Description that Appears in Log File	Explanation	Severity
AUTHENTICATION_FAILED	Access authentication to <*web server, streaming server, or SSH server*> by user <*user*> <*IP address or hostname*> failed.	An attempt to log in or authenticate to the IP camera failed.	3
AUTHENTICATION_FAILED	Access authentication to <*server type*> server <*server IP address or hostname*> failed.	The IP camera was unable to access an SNTP, Syslog, DNS, SMTP, HTTP, or 802.1x server.	4
AUTHORIZATION_FAILED	Unauthorized address <*IP address or hostname*> attempted to access camera.	An attempt was made to access the IP camera by using invalid user credentials from an IP address that has been configured for no access.	3

Table 10-3 Log Messages (continued)

Message Name	Description that Appears in Log File	Explanation	Severity
CODEC_LOST	Connection to Codec/Sensor module was lost. Internal module is either down or not responding.	The IP camera codec/sensor module is not responding.	4
CONFIG_SAVE_FAILED	Saving configuration to user <*user*> <*IP address or hostname*> failed.	A user attempt to save the IP camera configuration failed.	3
CONFIG_SAVED	Configuration saved by user <*user*> <*IP address or hostname*>.	The IP camera configuration was saved by a user.	5
CONFIG_UPLOAD_FAILED	Uploading configuration failed from user <*user*> <*IP address or hostname*>.	A user attempt to import the IP camera configuration failed.	3
CONFIG_UPLOADED	Configuration uploaded from user <*user*> <*IP address or hostname*>.	The IP camera configuration was imported by a user.	5
DEFAULTS_FAILED	Restoring factory defaults failed for user <*user*> <*IP address or hostname*>.	An attempt to reset the IP camera to its factory default configuration failed.	3
DEFAULTS_RESTORED	Factory defaults restored successfully by user <*user*> <*IP address or hostname*>.	The IP camera was reset to its factory default configuration.	5
DEVICE_REBOOT_AUTO	Device rebooted.	The IP camera rebooted automatically.	5
DEVICE_REBOOT_MANUAL	Device was rebooted manually by user <*user*> <*IP address or hostname*>.	The IP camera was rebooted by a user.	5
DHCP_LEASE	DHCP lease renewal was successful.	The IP camera renewed its DHCP lease.	6
DSP_ENCODING_HALTED	The Codec/Sensor module's DSP encoding was halted. Either the analog image signal from the sensor has been lost, or an internal encoding error has occurred.	The DSP of the IP camera codec/sensor module DSP stopped encoding. The analog image signal from the sensor may be lost or an internal encoding error may have occurred.	2
EMAIL_TRIGGERED	Event triggered: email sent to <*email address*>.	An event occurred and email notification of the event was sent.	5
ETH_BER	Bit Error Rate (BER) exceeded specified threshold of <*threshold*>.	The bit error rate (BER) exceeded the specified threshold.	4
ETH_SIGNAL_DEGRADE	Ethernet signal degrading.	The IP camera detected a degrading Ethernet signal.	4
FRAMES_DROPPED	Output frame rate does not match the camera's configured frame rate.	The IP camera is sending video at a frame rate that does not match the configured frame rate.	3
FW_UPGRADE_FAILED	Upgrading firmware failed from user <*user*> <*IP address or hostname*>.	An attempt to upgrade the IP camera firmware failed.	0
FW_UPGRADED	Firmware upgraded successfully from user <*user*> <*IP address or hostname*>.	The IP camera firmware was updated.	5
HTTP_TRIGGERED	Event triggered: notification sent to HTTP server <*IP address or hostname*>.	An event occurred and HTTP notification of the event was sent.	5

Table 10-3 Log Messages (continued)

Message Name	Description that Appears in Log File	Explanation	Severity
INPUT_ONE_CHANGED	Input port one changed to <*high/low*>.	Input port 1 on the IP camera changed state.	5
INPUT_ONE_RESET	Input port one reset to <*high/low*>.	Input port 1 on the IP camera reset to its default state.	5
INPUT_TWO_CHANGED	Input port two changed to <*high/low*>.	Input port 2 on the IP camera changed state.	5
INPUT_TWO_RESET	Input port two reset to <*high/low*>.	Input port 2 on the IP camera reset to its default state.	5
IP_CONFLICT	IP Address conflict for <*IP address*>.	IP camera experienced an IP address conflict.	4
IR_FILTER_DAY_AUTO	IR filter changed to day automatically.	The IP camera enabled its day filter automatically.	6
IR_FILTER_DAY_MANUAL	IR filter manually changed to day by user <*user*> <*IP address or hostname*>.	The IP camera day filter was enabled by a user.	6
IR_FILTER_NIGHT_AUTO	IR filter changed to night automatically.	The IP camera enabled its night filter automatically.	6
IR_FILTER_NIGHT_MANUAL	IR filter changed to night by user <*user*> <*IP address or hostname*>.	The IP camera night filter was enabled by a user.	6
LOG_IN	User <*user*> <*IP address or hostname*> logged in to <*web server or SSH server*>.	A user logged in to the IP camera.	5
LOG_OUT	User <*user*> <*IP address or hostname*> logged out of <*web server or SSH server*>.	A user logged out of the IP camera.	5
MOTION_DETECTED	Motion detected in region <*region index*>.	The IP camera detected motion in its video field.	5
MOTION_STOPPED	Motion in region <*region index*> stopped.	The IP camera stopped detecting motion in its video field.	5
OUTPUT_ONE_RESET	Output port one reset to <*high/low*>.	Output port 1 on the IP camera reset to its default state.	5
OUTPUT_ONE_TRIGGERED	Output port one triggered to <*high/low*>.	Output port 1 on the IP camera changed state.	5
POWER_SUPPLY_FAILURE	DC power supply failure.	The DC power for the IP camera failed.	2
SERVER_CONTACTED	Communication established with <*server type*> server <*server or IP address*>.	The IP camera established communication with an SNTP, DHCP, Syslog, DNS, SMTP, HTTP, or 802.1x server.	6
SERVER_LOST	Communication lost with <*server type*> server <*server or IP address*>.	The IP camera lost communication with an SNTP, DHCP, Syslog, DNS, SMTP, HTTP, or 802.1x server.	4
SERVER_UNREACHABLE	Failed to contact <*server type*> server <*server or IP address*>.	The IP camera was unable to contact an SNTP, DHCP, Syslog, DNS, SMTP, HTTP, or 802.1x server or a gateway.	4

Table 10-3 Log Messages (continued)

Message Name	Description that Appears in Log File	Explanation	Severity
START_STREAM	Channel <*channel ID*> started streaming to user <*user*> <*IP address or hostname*>.	The IP camera began streaming video to a user device.	6
STOP_STREAM	Channel <*channel ID*> stopped streaming to user <*user*> <*IP address or hostname*>.	The IP camera stopped streaming video to a user device.	6
TEMP_THRESHOLD_T1	Current temperature, <*temperature*>, <*exceeds/is below*> <*high temperature/low_temperature*> threshold.	The internal temperature of the IP camera is lower than 59°F (15°C) or higher than 149°F (65°C).	2
TEMP_THRESHOLD_T2	Current temperature, <*temperature*>, <*exceeds/is below*> <*high temperature/low_temperature*> threshold.	The internal temperature of the IP camera is lower than 32°F (0°C) or higher than 176°F (80°C).	4
TEMP_THRESHOLD_T3	Current temperature, <*temperature*>, <*exceeds/is below*> <*high temperature/low_temperature*> threshold.	The internal temperature of the IP camera is lower than 5°F (–15°C) or higher than 194°F (90°C).	5
TIME_DST_SWITCH	Time switched to Daylight Savings time with an offset of <*offset*> minutes.	The IP camera internal clock switched to daylight saving time.	6
TIME_REG_SWITCH	Time switched from Daylight Savings time with an offset of <*offset*> minutes.	The IP camera internal clock switched to standard time.	6
UNEXPECTED_EXCEPTION	Unexpected exception occurred. Could not <read/write> <*to/from*> repository by user <*user*> <*IP address or hostname*>.	IP camera could not read or write information to its internal repository.	2