CHAPTER 8

CPE History and Troubleshooting

This chapter describes how to use device information for troubleshooting. Among the features available for this purpose are:

Device History

This section describes the Device History feature, which provides a detailed history of significant events that occur in a device-provisioning lifecycle. This feature can be helpful for troubleshooting.

You can view device history through the API or through the administrator user interface.

- To retrieve the history of a specific device, invoke the following API:
  `com.cisco.provisioning.cpe.api.ipdevice.history getHistory` `(DeviceID` *`deviceID`*`)`
- To retrieve the history of a specific device using the administrator user interface, see Viewing Device History, page 16-12.

Table 8-1 details the specific record types supported by the Cisco BAC Device History feature:

Table 8-1 Supported Device History Records

Record Type	Description	Message Format
AddedAutomatically	Recorded when a previously unregistered device is automatically added to Cisco BAC after contacting the DPE.	*time*: Device record was automatically created.

	Example:
	`Tue Jul 11 18:41:42 EDT 2006:`
	`Device record was automatically created.`	

AddedViaAPI	Recorded when a device is added to Cisco BAC by using the client API.	*time*: Device record was added via API by user *username*.
	Example: Tue Jul 11 18:41:42 EDT 2006: Device record was added via API by user "admin".	

Table 8-1 Supported Device History Records (continued)

Record Type	Description	Message Format
UpdatedViaAPI	Recorded when a device record stored at the RDU was modified using the client API.	*time*: Device record was updated *reason* by user *username*.
	Example: Tue Jul 11 18:41:42 EDT 2006: Device record was updated via API command "IPDevice.changeClassOfService" by user "admin".	
FirstContact	Recorded when a device first contacts Cisco BAC.	*time*: Device made first contact with Cisco BAC.
	Example: Tue Jul 11 18:41:42 EDT 2006: Device made first contact with Cisco BAC.	
CPEDiscoveredData Updated	Recorded when a device reports new values for a device parameter, which are tracked by the RDU as discovered data. For details on discovered parameters, see Discovering CPE Parameters, page 4-4.	*time*: Recorded updates of *number* parameter values discovered from device.

	Example:
	`Tue Jul 11 18:41:42 EDT 2006:`
	`Recorded updates of 2 parameter values discovered from device.`	

ConfigGenRequested	Recorded when device instruction regeneration is initiated for a device. The resulting instructions are sent to all DPEs in the device's provisioning group.	*time*: Device policy instructions regeneration initiated as a result of *reason* by user *username*.

	Example:
	`Tue Jul 11 18:41:42 EDT 2006:`
	`Device policy instructions regeneration initiated as a result of execution of API Command "IPDevice.performOperation" by user "admin".`	

ConfigUpdated	Recorded when Cisco BAC activates a new configuration on a device.	*time*: Device was configured according to configuration version: *configuration revision*.

	Example:
	`Tue Jul 11 18:41:42 EDT 2006:`
	`Device was configured according to configuration version: 215438bb.`	

UpdatedConfig Available	Recorded when new configuration instructions for the device have been sent from the RDU to the DPEs.	*time*: Configuration policy for device was updated; new version: *configuration revision*.

	Example:
	`Tue Jul 11 18:41:42 EDT 2006:`
	`Configuration policy for device was updated; new version: 215438bb.`	

Table 8-1 Supported Device History Records (continued)

Record Type	Description	Message Format
ReportedNewConfig	Recorded when a device reports using a new configuration using the *ParameterKey* contained in the Inform message.	*time*: Device reported new configuration version: *configuration revision*.

	Example:
	`Tue Jul 11 18:41:42 EDT 2006:`
	`Device reported new configuration version: 215438bb.`	

NewOperationQueued	Recorded when a new device operation is initiated through the client API or the administrator user interface and is queued by Cisco BAC for execution on a device.	*time*: On-connect operation *operation name* with ID *operation ID* was queued by user *username*.

	Example:
	`Tue Jul 11 18:41:42 EDT 2006:`
	`On-connect operation "SetParamValues" with ID "15e2ccd:10c5f4b2ad0:80000024" was queued by user "admin".`	

OperationExecuted	Recorded when an operation initiated through the client API or the administrator user interface is successfully executed on a device.	*time*: *Operation mode operation name* with ID *operation id* was executed on the device.

	Example:
	`Tue Jul 11 18:41:42 EDT 2006:`
	`On-connect operation "SetParamValues" with ID "15e2ccd:10c5f4b2ad0:80000024" was executed on the device.`	

OperationRemoved	Recorded when a device operation queued within Cisco BAC is removed.	*time*: On-connect operation *operation name* with ID *operation id* was removed.

	Example:
	`Tue Jul 11 18:41:42 EDT 2006:`
	`On-connect operation "GetParamValues" with ID "15e2ccd:10c5f4b2ad0:80000025" was removed.`	

ReportedNewFirmware	Recorded when a device reports by using new firmware using the Inform message.	*time*: Device reported new firmware/software version: *firmware/software version*.

	Example:
	`Tue Jul 11 18:41:42 EDT 2006:`
	`Device reported new firmware/software version: 6d9bfec2.`	

UpdatedFirmwareRules Available	Recorded when new firmware rules for the device have been sent from the RDU to the DPEs.	*time*: Firmware rules for device were updated; new version: *firmware rules revision*.

	Example:
	`Tue Jul 11 18:41:42 EDT 2006:`
	`Firmware rules for device were updated; new version: 6d9bfec2.`	

Configuring Device History

You use the Device History feature to record significant events in a device-provisioning lifecycle. This section describes how to enable or disable this feature.

Enabling Device History

Device History is, by default, enabled. To enable or disable this feature from the API, change the `SERVER_DEVICE_HISTORY_ENABLE_KEY` property.

Note Every time Device History is enabled or disabled, a message is logged in *audit.log*. Device history is also stored in the troubleshooting log.

To enable or disable Device History through the administrator user interface:

Step 1 Choose **Configuration** on the Primary Navigation bar or Main Menu page.

Step 2 Choose **Defaults** on the Secondary Navigation bar.

The Configure Defaults page appears.

Step 3 Click **System Defaults**.

Step 4 On the defaults page, against Device History, click the **Enabled** radio button.

Note To disable the device history feature, click the **Disabled** radio button. When Device History is disabled, no new updates to any existing device or details of any new device are recorded in the device history. However, existing events are retained.

Step 5 Click **Submit**, or click **Reset** to return to default values.

Viewing Device History

To view the device history from the administrator user interface:

Step 1 From the **Devices** page, locate the device whose history you want to view. You can use one of the search types for this purpose.

Step 2 Click the **View Details** icon () corresponding to the correct device.

The Device Details page appears.

Step 3 Against View Device History Details, click the **View Details** icon.

The Device History Details page appears.

You can retrieve device history by using the API command `IPDevice.getDeviceHistory()`.

Configuring Device History Size

To configure the maximum number of device history entries from the administrator user interface, choose **Configuration > Defaults > System Defaults**. Enter a value in the field corresponding to Maximum Device History Entries. The default number of entries is 40.

To configure this number from the API, set the `SERVER_MAX_DEVICE_HISTORY_SIZE` property.

If you reduce the value of the Maximum Device History Entries, the existing records which exceed the limit do not get purged until a new device history is recorded. At that point, the device's history is updated according to the limit on maximum device history entries that the administrator sets.

If the maximum number has been increased, the older entries are retained. If the maximum number has been decreased, the oldest entries are deleted.

Device History Records

The device history records are logged in a rolling list. When the list reaches the limit that the administrator specifies, the oldest entry is removed. However, the following records are never deleted:

- AddedViaAPI (in the case of preregistered devices)
- AddedAutomatically (in the case of unregistered devices)
- FirstContact

To optimize Cisco BAC performance that extensive recording of device activity might impact, you can enable or disable specific event types with the following system properties from the API:

Note These properties are, by default, disabled. These options impact device history only if you have enabled the Device History feature.

- `SERVER_DEVICE_HISTORY_IMMEDIATE_OP_ENABLE_KEY`

  Records OperationExecuted history for immediate operations.

- `SERVER_DEVICE_HISTORY_PROXY_OP_ENABLE_KEY`

  Records the NewOperationQueued, OperationRemoved, and OperationExecuted history for on-connect device operations.

Note If you disable the `SERVER_DEVICE_HISTORY_IMMEDIATE_OP_ENABLE_KEY` property and enable the `SERVER_DEVICE_HISTORY_PROXY_OP_ENABLE_KEY` property, the immediate operation is disabled and the on-connect operation is enabled.

- `SERVER_DEVICE_HISTORY_GEN_CONFIG_ENABLE_KEY`

  Records ConfigGenRequested history.

To enable or disable these properties from the administrator user interface:

Step 1 Choose the **Configuration > Defaults** page.

Step 2 Click the **System Defaults** link on the left corner of the screen.

Step 3 Click the radio buttons corresponding to the operation you want to enable or disable:

- To enable recording the history of immediate operations, click the **Enabled** radio button corresponding to Immediate Operation History.
- To enable recording the history of on-connect operations, click the **Enabled** radio button corresponding to On-Connect Operation History.
- To enable recording the history of configuration generation, click the **Enabled** radio button corresponding to Instruction Generation History.

To disable these operations, click the corresponding **Disabled** radio button.

Step 4 Click **Submit**.

Device Faults

In large installations, devices with recurring faults can cause bottlenecks and affect performance. Recurring faults can result from a device malfunction or misconfiguration of Cisco BAC. You can use Cisco BAC to detect recurring faults occurring at the RDU and the DPE servers through the Recurring Device Faults feature.

You can also configure Cisco BAC to ignore and not store the CWMP faults reported by the CPE. The fault values must be specified in the *dpe.properties* file with comma separation, for example, */dpe/cwmp/fault/ignore=9003, 9801*.

The DPE will filter the CPE faults with fault codes 9003 and 9801 while reporting the faults. This feature is helpful when faults from Customer Premises Equipment (CPE) to Cisco BAC are expected for certain standard operations such as a reboot or recurrent faults.

A recurrent fault is one that occurs many times over a short period of time, or one with high chances of occurring repeatedly. For instance, a fault may occur when an attempt is made to configure a device and if the device is missing a parameter.

Such a fault qualifies as recurring even if it happens only once, because this operation is executed on every device contact. However, if a one-time device operation is initiated from the API and results in a fault, this fault is returned to the API client in the operation response and is not considered to be recurring.

Also, consider the following scenarios:

- A configuration template at the RDU may refer to a property that was deleted from the system. Every time the RDU tries to generate instructions for devices by using this template, an error occurs. This error qualifies the device as the one causing a recurring fault and is reported to the user.
- A device sends an invalid or incomplete Inform message because of a bug in the device firmware. The same Inform is generated on every device contact. This problem also qualifies as a recurring fault.

This feature provides details about the last fault for given devices as well as aggregated fault statistics for the system as a whole, the RDU server, and each DPE server.

The following operations monitor device faults on the RDU and the DPE:

At the RDU:
Failures during instruction generation.
Failures during extension execution.
At the DPE:
Violations of the CPE WAN Management Protocol.
Failures during DataSync instruction processing, which is responsible for discovering data from a device and updating the RDU.
Failures during FirmwareRules instruction processing, which is responsible for executing firmware rules configured in the RDU firmware rules templates.
Failures during ConfigSync instruction processing, which is responsible for updating device configuration according to RDU configuration templates.
Failures during UnknownDevice instruction processing, which is responsible for processing unknown or unregistered devices.

The RDU and the DPE maintain a list of recurring faults. Each fault contains the date and time of occurrence, the ID of the device, and a fault description.

Faults automatically expire and are purged from the system as soon as their lifetime expires. After a fault is purged from the system, the statistics are adjusted accordingly.

Note Cisco BAC limits the number of devices returned in the device fault list on the administrator user interface to 1,000. If the number of devices with faults exceeds 1,000, the operator will see a message stating that more devices have faults that just those on the screen.

To avoid impacting performance, Cisco BAC does not store fault information on the disk. If you restart the server, you will lose fault data that was maintained by that server in its memory. However, if faults repeat again, they are reported.

Retrieving Device Faults

Device fault information is available using the API and the administrator user interface.

From the API, you can call the following properties:

- `Configuration.getRDUDetails`—Returns the list of devices with faults at the RDU.
- `Configuration.getDPEDetails`—Returns the list of devices with faults at the DPE.
- `IPDevice.getDetails`—Returns information about faults related to the device.

From the administrator user interface, choose:

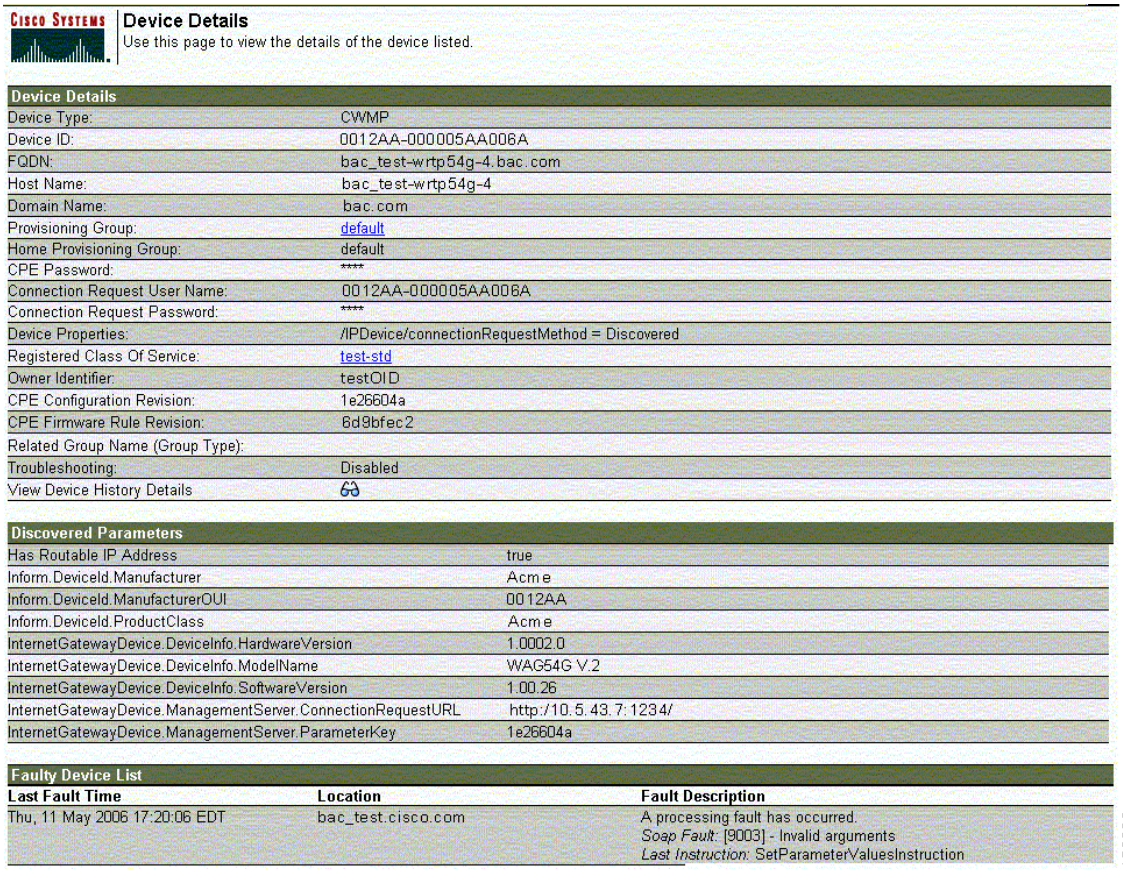
- **Servers > RDU—**Displays device fault statistics at the RDU level and aggregated for all DPEs. Statistics appear for the following periods of time by default: 1, 3, 12, and 72 hours.
- **Servers > Provisioning Groups > Manage Provisioning Groups > View Provisioning Group Details**—Displays device fault statistics for each DPE in a provisioning group.

- **Servers > DPEs > Manage Device Provisioning Engines > View Device Provisioning Engines Details**—Displays the number of devices with faults, if any. Against Device with Faults, click the **View Details** icon. The Device Details page appears, detailing device fault statistics at the DPE level.

Note The Device with Faults option, along with the **View Details** icon, appears on the **View Device Provisioning Engines Details** page only if there are devices with faults.

- **Devices > Manage Devices > Device Details**—Displays the last fault, if any, for the selected device, as described in Figure 8-1.

Figure 8-1 Fault Description on Device Details Page



Device Details
Use this page to view the details of the device listed.

Device Details	
Device Type:	CWMP
Device ID:	0012AA-000005AA006A
FQDN:	bac_test-wrtp54g-4.bac.com
Host Name:	bac_test-wrtp54g-4
Domain Name:	bac.com
Provisioning Group:	default
Home Provisioning Group:	default
CPE Password:	****
Connection Request User Name:	0012AA-000005AA006A
Connection Request Password:	****
Device Properties:	/IPDevice/connectionRequestMethod = Discovered
Registered Class Of Service:	test-std
Owner Identifier:	testOID
CPE Configuration Revision:	1e26604a
CPE Firmware Rule Revision:	6d9bfec2
Related Group Name (Group Type):	
Troubleshooting:	Disabled
View Device History Details	

Discovered Parameters	
Has Routable IP Address	true
Inform.DeviceId.Manufacturer	Acme
Inform.DeviceId.ManufacturerOUI	0012AA
Inform.DeviceId.ProductClass	Acme
InternetGatewayDevice.DeviceInfo.HardwareVersion	1.0002.0
InternetGatewayDevice.DeviceInfo.ModelName	WAG54G V.2
InternetGatewayDevice.DeviceInfo.SoftwareVersion	1.00.26
InternetGatewayDevice.ManagementServer.ConnectionRequestURL	http://10.5.43.7:1234/
InternetGatewayDevice.ManagementServer.ParameterKey	1e26604a

Faulty Device List

Last Fault Time	Location	Fault Description
Thu, 11 May 2006 17:20:06 EDT	bac_test.cisco.com	A processing fault has occurred. *Soap Fault:* [9003] - Invalid arguments *Last Instruction:* SetParameterValuesInstruction

156328

Cisco BAC maintains details of the most recent device with fault at each server. On account of DPE redundancy, a specific device over time will contact multiple DPEs, and may make it to a fault list on one or each of those DPEs.

The same device may also have recurring faults at the RDU. Cisco BAC provides an aggregated view of device faults at all servers. However on each server, no more than one fault for each device is tracked at any given time. Any device with faults is removed from the memory when it expires.

Managing Chatty Clients

In this release of Cisco BAC, you can use the Chatty client feature to detect devices that make an excessive number of TR-069 or HTTP file server calls. You can use this feature to reduce the adverse impact of Chatty devices on services that are provided to other devices.

Using this feature, you can detect the Chatty devices and throttle their access to the DPE. This feature is enabled by default on the DPE. You can disable this feature from the DPE CLI, using the **`chatty-client filter enabled`** {*true* | *false*} command. (See the *Cisco Broadband Access Center 3.7 DPE CLI Reference* for more details.)

The following properties are used to configure this feature on the DPE:

- SampleTimeInterval—Indicates the duration, in seconds, for which the DPE monitors the activity of a device. The default is 30 seconds.
- SampleHitsToThrottle—Indicates the number of events received from the device during the sample time interval. The default is 15.
- QuietTimeInterval—Indicates the duration, in seconds, for which the DPE monitors the activity of a throttled device. The default is 10 seconds.
- QuietHitsToLeaveThrottled—Indicates the number of events received from the device during the quiet time interval. The default is 5.

You can configure these properties using the DPE CLI. For more information, see the *Cisco Broadband Access Center 3.7 DPE CLI Reference*.

Cisco BAC uses the Chatty client filter to monitor the CPE events based on the device identifier. If the number of events received from the device during the sample time interval is greater than the value configured for the Sample-hits-to-throttle property, the DPE throttles the device. When a device is in a throttled state, all events that the device generates, are discarded.

Cisco BAC continues to monitor the activity on the throttled device to determine whether the device can be restored to the Normal state. If the device generates fewer events than the value configured for the Sample-hits-to-throttle property, the DPE moves the device to the Quiet state.

While in the Quiet state,

- If the number of events received from the device during the Quiet time interval is greater than the value configured for the Quiet-hits-to-leave-throttled property, the DPE moves the device to throttled state.
- If the number of events received from the device during the quiet time interval is less than the value configured for the Quiet-hits-to-leave-throttled property, the DPE restores the device to the Normal state.

Device Troubleshooting

You can use this feature to collect highly detailed troubleshooting information about one or multiple specific devices. Troubleshooting information includes all server interactions related to a given device or a group of devices. This information includes administrator user interface operations, RDU API operations, DPE interactions with the CPE, and inter-server DPE-to-RDU interactions.

You can enable or disable troubleshooting for one or a number of specific devices without turning logging on, and without searching through log files for specific device information.

Cisco BAC maintains a list of devices, based on the device identifier, for which detailed troubleshooting information is collected.

Troubleshooting information is stored centrally at the RDU and is maintained for each device. The DPEs do not store this data. Instead, the DPE forwards this information to the RDU which writes it to the device log file, troubleshooting.log, in the BPR_DATA/rdu/logs directory when it receives this information.

If the connection from the DPE to the RDU is lost, any new troubleshooting events occurring on the DPE are discarded. The logging of troubleshooting information resumes only after the RDU-DPE connection is restored.

The troubleshooting.log file is different from other log files such as rdu.log, dpe.log, and audit.log. The troubleshooting.log file only logs detailed troubleshooting information relating to a specific set of devices in the troubleshooting mode.

Note The tracking feature is turned off until one or more devices are added to the troubleshooting group.

When you enable or disable troubleshooting on a specific device, the change takes place immediately at all servers (RDU and DPEs); you do not have to reboot the RDU or the DPEs. The log files on the respective servers lists the current list of devices in the troubleshooting mode.

Caution Additional memory and disk space is required whenever the device troubleshooting feature is used. As the number of tracked devices increases, so does the amount of memory and disk space that is required to support the number of logs that are created.

Configuring Device Troubleshooting

The Device Troubleshooting feature is disabled until one or more devices are put into troubleshooting mode. This section describes how you can enable or disable troubleshooting for a device from the administrator user interface. It also describes how to view a list of devices in troubleshooting mode and how to view troubleshooting log for a given device.

You can configure the maximum number of devices in troubleshooting mode to prevent inadvertently putting too many devices in this mode, and thus, diminishing server performance. By default, this number is set at 100.

To configure the maximum number of the devices allowed in troubleshooting mode from the administrator user interface, click the Systems Defaults page using the **Configuration > Defaults** tabs. Enter a value in the Maximum Troubleshooting Device Count field.

Enabling Troubleshooting for a Device

To enable troubleshooting for a device, the device must be preregistered in the Cisco BAC RDU. If the device is not yet preregistered, add the device from the Manage Devices page by clicking the **Add** button. For information on adding devices, see Adding Device Records, page 16-11.

To enable troubleshooting for a device that already resides in the RDU database:

Step 1 From the Manage Devices page, click the Search Type drop-down list, and select the Device Identifier Option Search option. You can use the wildcard function for this search. (See Table 16-1.)

Step 2 Click **Search**.

A list of devices appears.

Step 3 Click the Identifier link corresponding to the device that you want to track.

The Modify Device page appears, listing various device parameters.

Step 4 Click the **Enabled** radio button corresponding to the Troubleshooting parameter.

Step 5 Click **Submit**. Troubleshooting is now enabled for the device.

To verify if a given device is enabled for troubleshooting, you can access the Device Details page, and view status against Troubleshooting.

Disabling Troubleshooting for a Device

To disable troubleshooting for a device:

Step 1 From the **Devices** tab, locate the device that you want to delete. You can use one of the search types for this purpose.

Step 2 Click the Identifier link corresponding to the device that you want to delete from the troubleshooting list.

The Modify Device page appears.

Step 3 Against the Troubleshooting parameter, click the **Disabled** radio button.

Step 4 Click **Submit**.

Viewing List of Devices in Troubleshooting Mode

When you enable troubleshooting for a device, the device is automatically added to a special device group which contains a list of devices in troubleshooting mode. The group type is **system** and the group name is **troubleshooting**. You can access the list of devices in this group from the API or the administrator user interface.

To view a list of devices currently enabled for troubleshooting:

Step 1 From the **Manage Devices** page, click the Search Type drop-down list, and select **Group Search**.

Step 2 From the Group (Group Type) drop-down list, select the troubleshooting (system) option to view all the devices in troubleshooting mode.

Step 3 Click **Search**.

You can also see the list of devices in troubleshooting mode is by viewing the RDU log (*rdu.log*) and the DPE log (*dpe.log*). The list of devices is logged whenever the server is started and whenever there is a change in the list of devices that are enabled for troubleshooting.

The devices enabled for troubleshooting appear in the log files with the log level of 5-notification. For more details on log files, see Logging, page 20-2.

Viewing Device Troubleshooting Log

You can view the troubleshooting log file of a specific device in one of two ways.

- Complete the procedure described in Viewing List of Devices in Troubleshooting Mode, page 8-11. Then, follow these steps:

Step 1 When a list of the devices in troubleshooting mode appears, click the **View Details** icon corresponding to a specific device.

The Device Details page appears.

Step 2 Against View Troubleshooting Log, click the **View Details** icon.

The View Log File Contents page appears.

- Complete the following procedure:

Step 1 From the Manage Details page under the **Devices** tab, click the Search Type drop-down list, and select the Device Identifier Option Search option. You can use the wildcard character (*) for this search.

Step 2 Click **Search**.

A list of devices appears.

Step 3 Click the View Details icon corresponding to the device whose log file you want to check.

The Device Details page appears.

Step 4 Against View Troubleshooting Log, click the **View Details** icon.

The View Log File Contents page appears.

The color coding for the device troubleshooting log entries is:

- BAC-TROUBLESHOOTINGINFO—Informational messages are marked in white.
- BAC-TROUBLESHOOTINGINPUT—Details of messages received by Cisco BAC servers are marked in grey.
- BAC-TROUBLESHOOTINGOUTPUT—Details of messages sent by Cisco BAC servers are marked in green.
- BAC-TROUBLESHOOTINGERROR—Error messages are marked in red.