Monitoring and Troubleshooting the ACNS Network

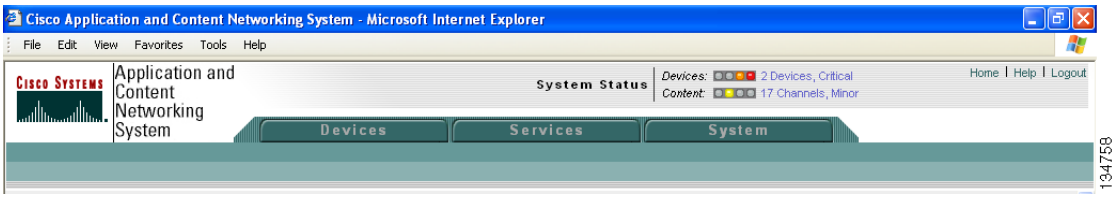
This chapter provides information on monitoring and troubleshooting devices and content replication in the ACNS network, and on using the system message logs, transaction logs, and SNMP.

This chapter contains the following sections:

Monitoring System Status

The ACNS 5.5 Content Distribution Manager GUI displays the system status in a system status bar that is located above the navigation tabs in every window. The system status bar presents the overall device and content health of the system. You can use this feature to monitor devices and content replication in your ACNS network. The system status bar helps you immediately identify any problems on the network, allowing you to act and respond to problems quickly. (See Figure 21-1.)

Figure 21-1 System Status Bar



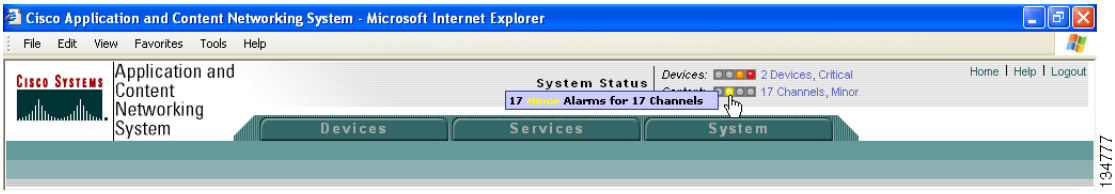
The system status reporting mechanism uses four alarm lights to identify problems that need to be resolved. Each light represents a different alarm level, as follows:

- Green—No alarms (the system is in excellent health)
- Yellow—Minor alarms

- Orange—Major alarms
- Red—Critical alarms

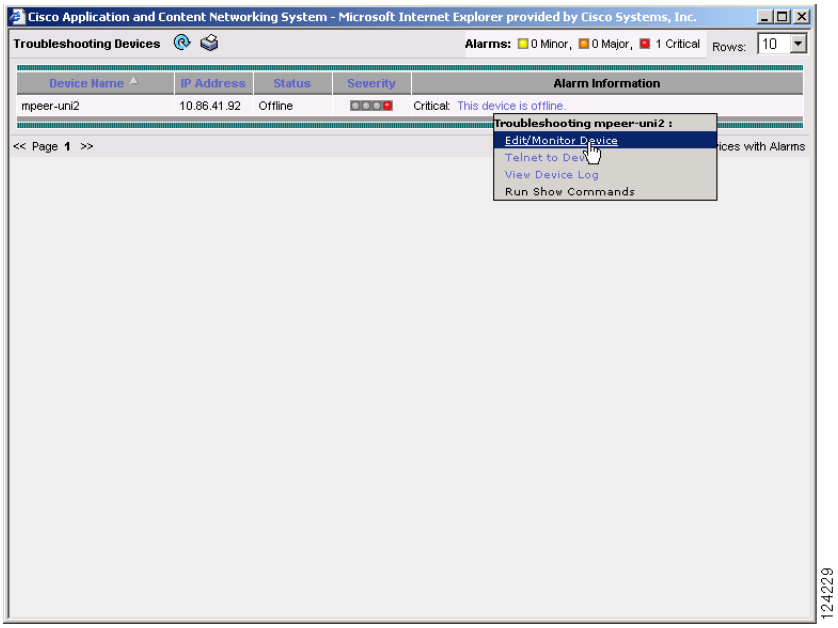
When you roll your mouse over an alarm light in the system status bar, a popup message provides further details about the device or channel status. (See Figure 21-2.) When you click the alarm light, a troubleshooting window opens (Troubleshooting Devices or Troubleshooting Content), listing the individual devices or channels that need attention.

Figure 21-2 Status Details



When you roll your mouse over an item under the Alarm Information column in the Troubleshooting Devices or Troubleshooting Content window, a contextual popup menu appears. The popup menu provides links to all the diagnostic tools, troubleshooting tools, logs, and monitoring applications for troubleshooting and resolving the problem. Figure 21-3 shows the troubleshooting tools menu for device alarms.

Figure 21-3 Troubleshooting Tools Menu



Device Alarms

Device alarms are associated with device objects and pertain to applications and services running on Content Engines, Content Routers, and Content Distribution Managers. Device alarms are defined by the reporting application or service. Device alarms can also reflect reporting problems between the device and the Content Distribution Manager. (See Table 21-1.)

Table 21-1 Device Alarms for Reporting Problems

Alarm	Alarm Severity	Device Status	Description
Device is offline	Critical	Offline	The device has failed to communicate with the Content Distribution Manager.
Device is pending	Major	Pending	The device status cannot be determined.
Device is inactive	Minor	Inactive	The device has not yet been activated or accepted by the Content Distribution Manager.
Device has lower software version	Minor	Online	The device is not interoperable with the Content Distribution Manager because it has an earlier software version.

Troubleshooting Devices Using the System Status Bar

To troubleshoot a device from the system status bar, follow these steps:

Step 1 In the system status bar, click the Devices alarm light or click the alarm message next to the Devices alarm light panel. The Troubleshooting Devices window pops up as a separate window.

Step 2 In the Alarm Information column, hold your mouse over the alarm message until the Troubleshooting tools menu appears. (See Figure 21-3.)

Step 3 Choose the troubleshooting tool that you want to use, and click the link. The link takes you to the appropriate window in the Content Distribution Manager GUI. Table 21-2 describes the tools available for all device alarms.

Table 21-2 Troubleshooting Tools for Device Alarms

Item	Navigation	Description
Get Alarm Description(s)	None	Replaces alarm counts with alarm descriptions
Telnet to Device	Opens a Telnet window	Initiates a Telnet session using the device IP address
View Device Logs	**Devices > Device Monitoring > Logs**	Displays system message logs filtered for this device
Edit Device	Device Home	Displays device home window for configuration
Monitor Device	Device Home	Displays device home window for monitoring
Run Show Commands	**Devices > Device Monitoring > Show/Clear Commands > Show Commands**	Displays device show command tool

Using the Content Distribution Manager GUI show Command Tool

To use the Content Distribution Manager GUI **show** command tool, follow these steps:

Step 1 From the Content Distribution Manager GUI, choose **Devices > Devices**.

Step 2 Click the **Edit** icon next to the name of the device for which you want to issue a **show** command.

Step 3 In the Contents pane, choose **Device Monitoring > Show/Clear Commands** and then click **Show Commands**.

Step 4 From the drop-down list, choose a **show** command.

Step 5 Enter arguments for the command, if any. (Refer to the *Cisco ACNS Software Command Reference, Release 5.x* publication for more command information.)

Step 6 To display the **show** command output, click **Submit**. A window appears, displaying the **show** command output for that device.

Content Alarms

Content alarms pertain to content replication problems and are associated with channels. Content alarms are raised by the Content Distribution Manager based on replication status reports or by the node health manager based on acquisition and distribution errors.

If the same fault is reported by replication status and by node health manager, the Content Distribution Manager GUI reports both; one appears as the true alarm and the other as an error. The Content Distribution Manager does not corollate nor attempt to consolidate the errors generated by replication status and by node health manager.

To view the content alarms, click the **Content** alarm light or click the **Channels** link next to the alarm light in the status bar. The Troubleshooting Content window pops up. (See Figure 21-4.) Table 21-3 lists the content alarms.

Figure 21-4 Troubleshooting Content—Content Alarms

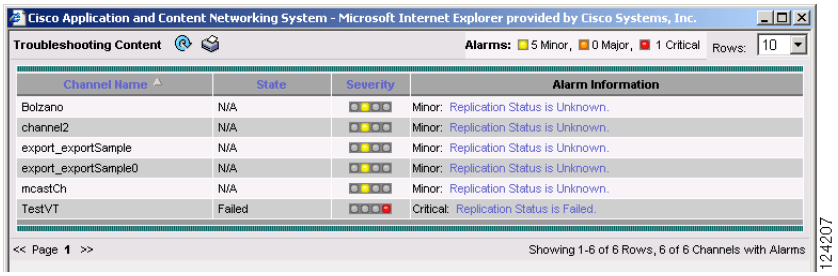


Table 21-3 Content Alarms for Channel Replication Status

Alarm	Severity	Description
Replication Status is Failed	Critical	The number of Content Engines in the channel that failed to replicate the content is greater than zero.
Replication Status is Pending	Minor	The number of Content Engines in the channel with content replication status unknown is greater than zero.

Troubleshooting Content Replication Issues Using the System Status Bar

To troubleshoot content replication issues from the system status bar, follow these steps:

Step 1 In the system status bar, click the Content alarm light or click the alarm message next to the Content alarm light panel. The Troubleshooting Content window pops up as a separate window.

Step 2 In the Alarm Information column, hold your mouse over the alarm message until the Troubleshooting tools menu appears.

Step 3 Choose the troubleshooting tool that you want to use, and click the link. The link takes you to the appropriate window in the Content Distribution Manager GUI. Table 21-4 describes the tools available for all content alarms.

Table 21-4 Troubleshooting Tools for Content Alarms

Item	Navigation	Description
View Replication Status	**Content > Channels > Replication Status**	Displays second-level replication status for a channel.
Edit Channel	**Content > Channels > Definition**	Opens the Modifying Channel window.

Monitoring System Events Using the System Message Log

Use the ACNS system logging feature to set specific parameters for the system log file (syslog). This file contains authentication entries, privilege level settings, and administrative details. System logging is always enabled. The system log file is located on the system file system (sysfs) partition as /local1/syslog.txt.

You can use either of the following methods to configure the Content Engine to send varying levels of event messages to disk, console, or host.

- Content Distribution Manager GUI, as described in the "Configuring System Event Logging Using the Content Distribution Manager GUI" section on page 21-5
- Content Engine CLI, as described in the "Configuring System Event Logging Using CLI Commands" section on page 21-8

Configuring System Event Logging Using the Content Distribution Manager GUI

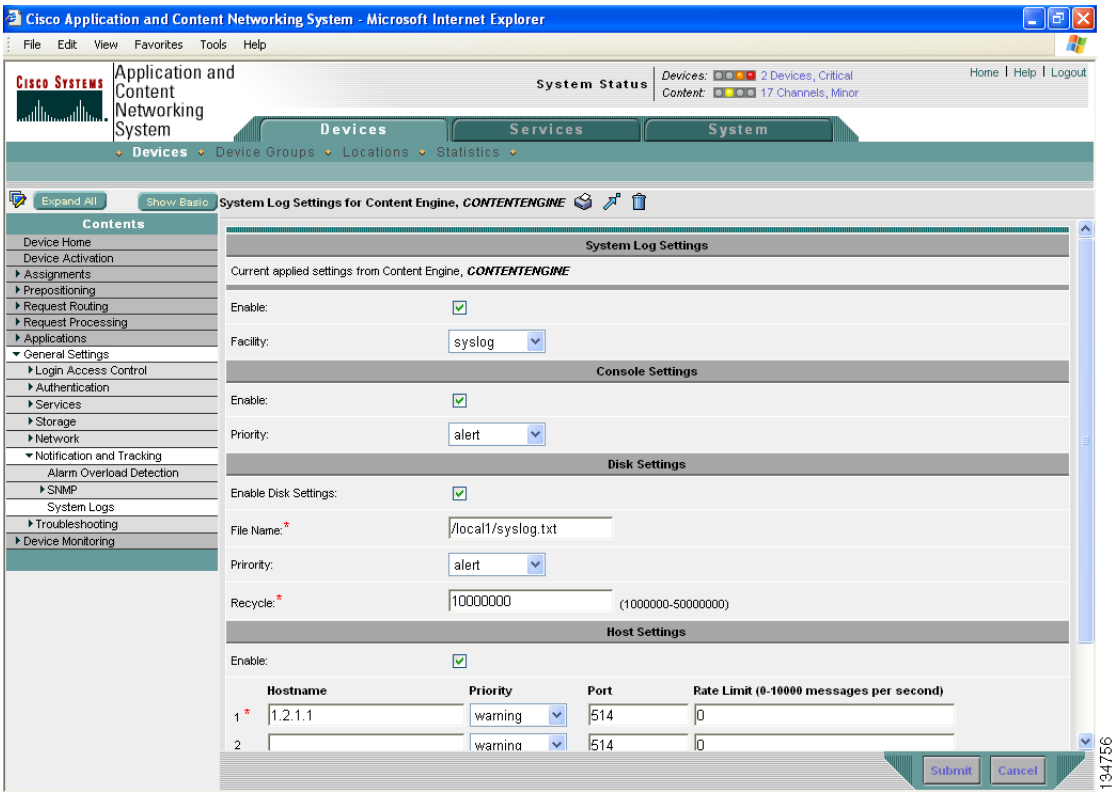
To enable system logging, follow these steps:

Step 1 From the Content Distribution Manager GUI, choose **Devices > Devices**.

Step 2 Click the **Edit** icon next to the Content Engine for which you want to enable system logging. The Contents pane appears on the left.

Step 3 From the Contents pane, choose **General Settings > Notification and Tracking > System Logs**. The System Log Settings for Content Engine window appears. (See Figure 21-5.)

Figure 21-5 Syslog Settings Window



Step 4 Under the System Log Settings heading, check the **Enable** check box to enable system logging.

Step 5 From the Facility drop-down list, choose the appropriate facility.

Step 6 To save the settings, click **Submit**.

You can enable sending syslog files to the console, disk, or a host.

To enable syslog files to be sent to the console, follow these steps under Console Settings:

Step 1 Check the **Enable** check box to enable sending syslog files to the console.

Step 2 From the Priority drop-down list, choose the severity level of the message that should be sent to the specified remote syslog host. The default priority-code is “warning” (level 4). Each syslog host is capable of receiving a different level of event messages. (See Table 21-6 for a list of priority levels.)

Step 3 To save the settings, click **Submit**.

To enable syslog files to be sent to disk, follow these steps under Disk Settings:

Step 1 Check the **Enable Disk Settings** check box to enable sending syslog files to disk.

Step 2 In the File Name field, enter a path and a filename where the syslog files will be stored on disk.

Step 3 From the Priority drop-down list, choose the severity level of the message that should be sent to the specified remote syslog host. The default priority-code is "warning" (level 4). Each syslog host is capable of receiving a different level of event messages. (See Table 21-6 for a list of priority levels.)

Step 4 In the Recycle field, specify the size of the syslog file (in bytes) that can be recycled when it is stored on disk. The default value of the file size is 10000000.

Whenever the current log file size surpasses the recycle size, the log file is rotated. (The default recycle size for the log file is 10,000,000 bytes.) The log file cycles through at most five rotations, and each rotation is saved as *log_file_name.[1-5]* under the same directory as the original log.

The rotated log file is configured in the File Name field (or by using the **logging disk filename** command).

Step 5 To save the settings, click **Submit**.

To enable syslog files to be sent to a host, follow these steps under Host Settings:

Step 1 Check the Enable Host Settings check box to enable sending syslog files to a host. You can configure up to four hosts to which syslog messages can be sent. (See the next section, "About Multiple Hosts for System Logging.")

Step 2 In the Hostname field, enter a host name or IP address of the remote syslog host. Specify up to three more remote syslog hosts in the Hostname fields 2 through 4. You must specify at least one host name if you have enabled system logging to a host.

Step 3 From the Priority drop-down list, choose the severity level of the message that should be sent to the specified remote syslog host. The default priority-code is "warning" (level 4). Each syslog host is capable of receiving a different level of event messages. (See Table 21-6 for a list of priority levels.)

Step 4 In the Port field, specify the destination port on the remote host to which the Content Engine should send the message. The default port number is 514.

Step 5 In the Rate Limit field, specify the number of messages that are allowed to be sent to the remote syslog host per second. To limit bandwidth and other resource consumption, messages to the remote syslog host can be rate limited. If this limit is exceeded, the specified remote syslog host drops the messages. There is no default rate limit, and by default all syslog messages are sent to all of the configured syslog hosts.

Step 6 To save the settings, click **Submit**.

About Multiple Hosts for System Logging

Each syslog host can receive different priority levels of syslog messages. Therefore, you can configure different syslog hosts with a different syslog message priority code to enable the Content Engine to send varying levels of syslog messages to the four external syslog hosts. For example, the Content Engine can be configured to send messages that have a priority code of "error" (level 3) to the remote syslog host that has an IP address of 172.31.2.160 and messages that have a priority code of "warning" (level 4) to the remote syslog host that has an IP address of 172.31.2.161.

However, if you want to achieve syslog host redundancy or failover to a different syslog host, you must configure multiple syslog hosts on the Content Engine and assign the same priority code to each configured syslog host (for example, assigning a priority code of "critical" (level 2) to sylog host 1, sylog host 2, and syslog host 3).

In addition to configuring up to four logging hosts, you can also configure the following for multiple syslog hosts:

- A port number different from the default port number, 514, on the Content Engine to send syslog messages to a logging host.
- A rate limit for the syslog messages, which limits the rate at which messages are sent to the remote syslog server (messages per second) to control the amount of bandwidth used by syslog messages.

Configuring System Event Logging Using CLI Commands

Use the **logging** command to set specific parameters for the system log file (syslog). This file contains authentication entries, privilege level settings, and administrative details. System logging is always enabled. The system log file is located in the system file system (sysfs) storage area as /local1/syslog.txt.

Logging can be configured to send messages to the console, to disk, or to an external syslog host. See Table 21-5 for a list of the key system logging parameters, descriptions, and CLI commands.

Table 21-5 System Logging Parameter Settings

GUI Parameter	Function	CLI Command
Host Server	IP address or host name of the host that receives syslog messages from the device group.	**logging host** *hostname* or *ip-address*
Console	Enables sending syslog files to the console.	**logging console enable**
Disk	Enables sending syslog files to disk.	**logging disk enable**
Priority	Determines priority level when system logging is enabled to disk, console, or host.	**logging disk priority, logging console priority, logging host priority**
Syslog file	Path of the syslog file on the hard drive.	**logging disk filename** *filename*
Recycle	Rewrites the syslog file when it surpasses the specified recycle size.	**logging recycle** *size*

Logging can be configured to send various levels of messages to disk, console, or host using the **priority** option of the logging command. Table 21-6 lists the different priority levels of detail to send to the recipient of the syslog messages for a corresponding event.

Table 21-6 System Logging Priority Levels and Descriptions

Priority Code	Condition	Description
0	Emergency	System is unusable.
1	Alert	Immediate action needed.
2	Critical	Critical condition.
3	Error	Error conditions.
4	Warning	Warning conditions.
5	Notice	Normal but significant conditions.

Table 21-6 System Logging Priority Levels and Descriptions (continued)

Priority Code	Condition	Description
6	Information	Informational messages.
7	Debug	Debugging messages.

Viewing the System Message Log

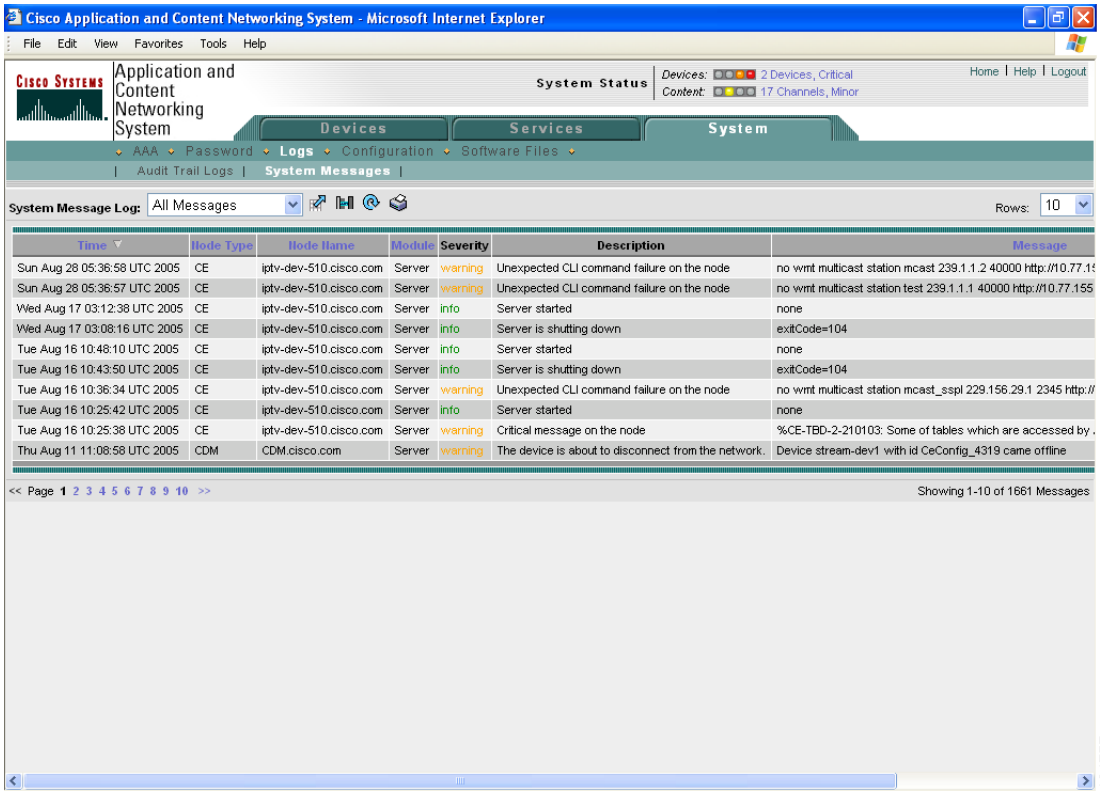
Using the system message log feature of the Content Distribution Manager GUI, you can view information about events that have occurred in your ACNS network.

To view logged information for your ACNS network, follow these steps.

Note The Content Distribution Manager logs messages only of the severity level "critical" or higher from registered nodes.

Step 1 From the Content Distribution Manager GUI, choose **System > Logs > System Messages**. The System Message Log window appears. (See Figure 21-6.)

Figure 21-6 System Message Log (Showing All Messages)



Step 2 Choose one of the following types of messages to display from the System Message Log drop-down list:

- All
- CLI
- Critical
- Database

A table listing and describing each message is displayed.

Step 3 To sort the messages chronologically, click a column heading by node type, node name, module, severity, or message text. By default, messages are listed chronologically. (See Figure 21-6.)

Note If no name is available for a node, the name displayed is "Unavailable." This might occur if the node has been deleted or has been reregistered with Cisco ACNS software.

Step 4 If you have many event messages, you might need to view multiple pages to view the activity in which you are interested. Click the forward (>>) and back (<<) buttons to move between pages. Alternatively, click the link for a specific page number to jump to that page.

Note You can choose the number of rows to be displayed in the System Message Log window by choosing a number from the Rows drop-down list.

Alarm Overload Detection

Content Engines that are running ACNS software can track the rate of incoming alarms from the Node Health Manager. If the rate of incoming alarms exceeds a certain threshold that is configured as the high water mark (HWM), then the Content Engine enters an alarm overload state. This condition occurs when multiple applications raise alarms at the same time to report error conditions. When a Content Engine is in an alarm overload state, then the following events occur:

- SNMP traps for subsequent alarm raise-and-clear operations are suspended. The trap for the raise alarm-overload alarm and the clear alarm-overload alarm are sent. However, traps related to alarm operations between the raise-alarm-overload alarm and the clear-alarm-overload alarm operations are suspended.
- Alarm overload raise-and-clear notifications are not blocked. The alarm overload state is communicated to SNMP and the Configuration Management System (CMS). However, in the alarm overload state, SNMP and the CMS are not notified of individual alarms. Individual alarm information is available from the CLI only.
- The Content Engine remains in an alarm overload state until the rate of incoming alarms decreases to the point that the alarm rate is less than the low water mark (LWM).
- If the incoming alarm rate falls below the LWM, the Content Engine comes out of the alarm overload state and begins to report the alarm counts to SNMP and the CMS.

When the Content Engine is in an alarm overload state, the Node Health Manager continues to record the alarms being raised on the Content Engine and keeps track of the incoming alarm rate. Alarms that have been raised on a Content Engine can be listed by using the Content Engine CLI commands shown

in Table 21-7. These CLI commands allow you to systematically drill down to the source of an ACNS software alarm (the cause of the problem). You can use these CLI commands to identify the source of a problem without wading through numerous ACNS software logs.

Table 21-7 Viewing Content Engine Alarms

Command	Syntax	Description
show alarms		Displays a list of all currently raised ACNS software alarms (critical, major, and minor alarms) on the Content Engine.
	show alarms critical	Displays a list of only currently raised ACNS software critical alarms on the Content Engine.
	show alarms major	Displays a list of only currently raised ACNS software major alarms on the Content Engine.
	show alarms minor	Displays a list of the currently raised ACNS software minor alarms on the Content Engine.
	show alarms detail	Displays detailed information about the currently raised ACNS software alarms.
	show alarms history	Displays a history of ACNS software alarms that have been raised and cleared on the Content Engine. The CLI retains the last 100 alarm raise and clear events only.
	show alarms status	Displays the counts for the currently raised ACNS software alarms on the Content Engine. Also lists the alarm overload state and the alarm overload settings.

Configuring Alarm Overload Detection Settings for the Content Engine

To configure alarm overload detection for a Content Engine, follow these steps:

Step 1 Choose **Devices > Devices**. The Devices window appears, listing all the device types configured in the ACNS network.

Step 2 Click the **Edit** icon next to the name of the Content Engine for which you want to configure the alarm overload state. The Device Home for Content Engine window appears.

Step 3 In the Contents pane, choose **General Settings > Notification and Tracking > Alarm Overload Detection**. The Alarm Overload Detection Settings for Content Engine window appears.

Step 4 Uncheck the **Enable Alarm Overload Detection** check box if you do not want to configure the Content Engine to suspend alarm raise and clear operations when multiple applications report error conditions. This check box is checked by default.

Step 5 In the Alarm Overload Low Water Mark (Clear) field, enter the number of incoming alarms per second below which the Content Engine comes out of the alarm overload state. Low water mark is the level to which the number of alarms must drop before alarms can be restarted. The default value is 1. The low water mark value should be less than the high water mark value.

Step 6 In the Alarm Overload High Water Mark (Raise) field, enter the number of incoming alarms per second above which the Content Engine enters the alarm overload state. The default value is 10.

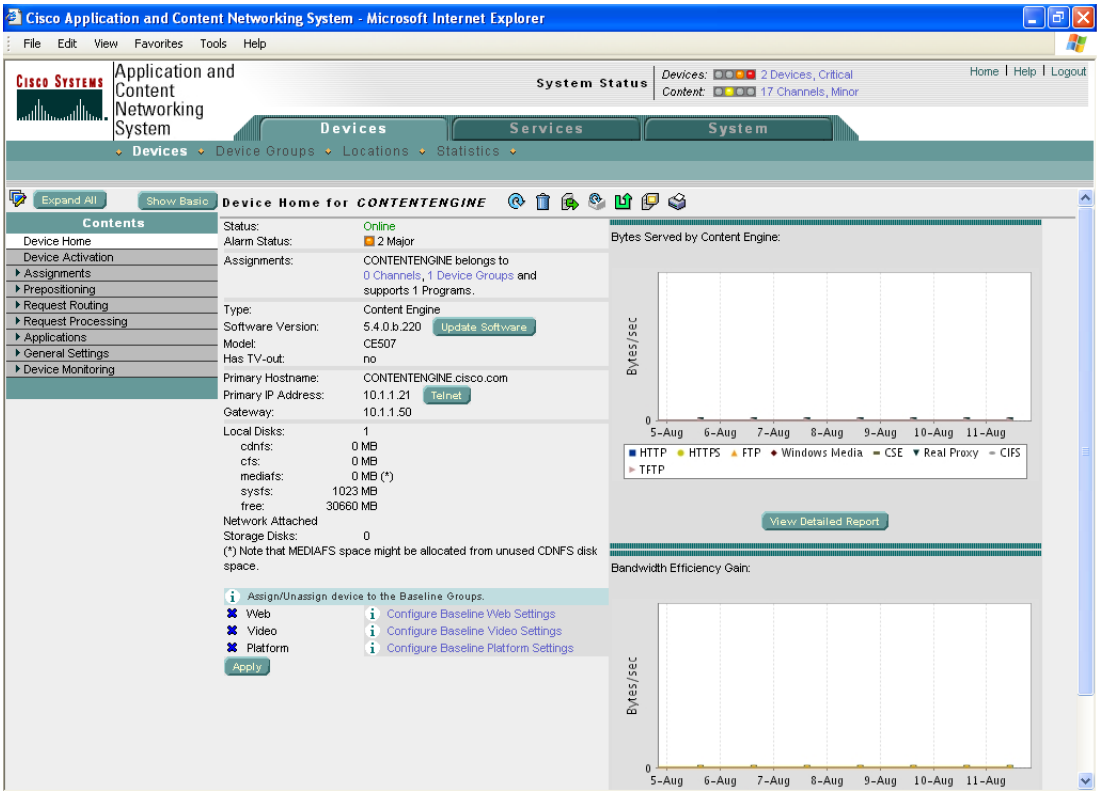
Step 7 To save the settings, click **Submit**

If you try to leave this window without saving the modified settings, a warning dialog box prompts you to submit the changes. This dialog box appears only if you are using the Internet Explorer browser.

Monitoring Device Status

The Device Home window provides device and alarm status for individual devices. (See Figure 21-7.)

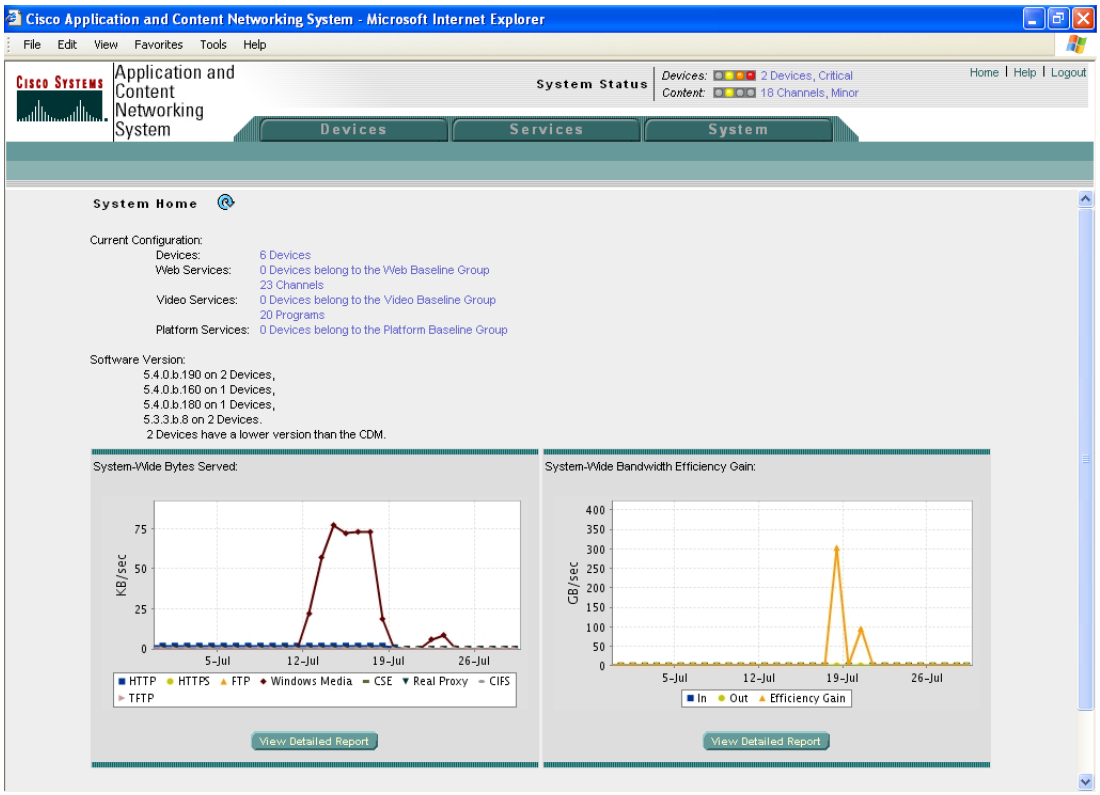
Figure 21-7 Monitoring Device Status



Monitoring Device Performance

It is often useful to be able to assess the performance of Content Engines across your network. You can do this using the Content Engine statistics feature in the Content Distribution Manager GUI. The System Home window displays system-wide statistics in a graphical form and enables you to view, at a glance, which Content Engines are online, as well as assess their available resources, the volume of traffic being routed to them, and their performance in serving requests. (See Figure 21-8.)

Figure 21-8 System Home



The information displayed is based on a snapshot of your ACNS network that represents the state of your Content Engines at the end of every two polling periods. You can configure the interval between polls in the Content Distribution Manager GUI (**System > Configuration > System Properties > System.datafeed.pollRate**). The default polling rate is 300 seconds (5 minutes).

The Content Distribution Manager GUI also allows you to view statistics for Content Engines, device groups, and Content Routers in tabular form based on the type of server. (See the next three sections.)

Viewing Content Engine Statistics

To view Content Engine statistics in tabular form, follow these steps:

Step 1 From the Content Distribution Manager GUI, choose **Devices > Statistics**.

Step 2 In the Contents pane, click **Content Engines**, and then choose one of the following submenu options to view the Content Engine statistics for that option:

- Cisco Streaming Engine
- HTTP
- RTSP
- Windows Media

Table 21-8 explains the meaning of each Content Engine statistic presented in the GUI.

Step 3 To print the statistics data, click the **Printer** icon.

Table 21-8 Content Engine and Device Group Statistics

Content Engine Property	Description
Cisco Streaming Engine	
Bandwidth (bits/sec)	Current bandwidth output by the server in bits per second.
Total Bytes	Total bytes output by the server since it was started.
Total Packets	Total packets output by the server since it was started.
RTSP Connections	Number of clients currently connected over RTSP.
All Connections	Number of clients currently connected since startup.
Updated	Time stamp indicating when the statistics were updated.
HTTP	
Requests/Sec	Number of requests per second.
Bytes/Sec	Number of bytes per second.
Request Latency	Average number of seconds per HTTP request. Corresponds to the output from the **show statistics http performance** EXEC command as the "Seconds / Request Avg."
Hit Rate	Average number of content items per minute successfully served from the cache of the Content Engine or from all the Content Engines in the channel or virtual ACNS network during the preceding quarter hour.
Updated	Time stamp indicating when the statistics were updated.
RTSP	
Requests	Number of requests. Corresponds to the output from the **show statistics rtsp proxy media-real savings** command.
Bytes	Number of bytes. Corresponds to the output from the **show statistics rtsp proxy media-real savings** command.

Table 21-8 Content Engine and Device Group Statistics (continued)

Content Engine Property	Description
Hit Rate	Average number of content items per minute successfully served from the cache of the Content Engine or from all the Content Engines in the channel or virtual ACNS network during the preceding quarter hour.
Updated	Time stamp indicating when the statistics were updated.
Windows Media	
Concurrent Requests	Number of simultaneous requests the WMT proxy/server is serving at the current time.
Kbits/Sec	Number of kilobits per second.
Cache Hit Rate	Average number of content items per minute successfully served from the cache of the Content Engine or from all the Content Engines in the channel or virtual ACNS network during the preceding quarter hour.
Updated	Time stamp indicating when the statistics were updated.

Viewing Device Group Statistics

To view device group statistics for your ACNS network, follow these steps:

Step 1 From the Content Distribution Manager GUI, choose **Devices > Statistics**.

Step 2 In the Contents pane, click **Device Groups**, and then choose one of the following submenu options to view the Content Engine statistics for that option:

- Cisco Streaming Engine
- HTTP
- RTSP
- Windows Media

Statistics for device groups are the same as for Content Engines. (See Table 21-8 for an explanation of the meaning of each device group statistic presented in the GUI.)

Step 3 To print the statistics data, click the **Printer** icon.

Viewing Routing Statistics

To view routing statistics for Content Routers and routing Content Engines, follow these steps:

Step 1 From the Content Distribution Manager GUI, choose **Devices > Statistics**.

Step 2 In the Contents pane, click **Routing Statistics**, and then choose one of the following submenu options to view the Content Engine statistics for that option:

- Routing Requests
- Routing Redirects

Table 21-9 explains the meaning of each Content Router statistic presented in the GUI.

Table 21-9 Content Router Statistics

Content Router Property	Description
Routing Requests	
Total Requests	Total number of content requests received by simplified hybrid routing.
Http Requests	Number of ASX and traditional HTTP web requests received.
Rtsp Requests	Number of RTSP requests received.
Updated	Time stamp indicating when the statistics were updated.
Routing Redirects	
Total Requests	Total number of content requests received by simplified hybrid routing.
Reqs Redirected	Total number of content requests received by simplified hybrid routing that were redirected.
Reqs Not Directed	Total number of content requests received by simplified hybrid routing that were not redirected.
Updated	Time stamp indicating when the statistics were updated.

Step 3 To print the statistics data, click the **Printer** icon.

You can also view additional content routing statistics through the Content Distribution Manager GUI using the **show** command tool. (See the "Using the Content Distribution Manager GUI show Command Tool" section on page 21-4.) The **show** commands are further documented in the *Cisco ACNS Software Command Reference, Release 5.5* publication.

Viewing Streaming Statistics

CLI commands provide the following statistical information for incoming streams and multicast streams:

- Incoming statistics
- Outgoing statistics

- Multicast statistics
- Bandwidth Savings

The following statistics are not provided:

- Unicast per-stream statistics
- Multicast per-program statistics

Incoming Statistics

Incoming stream statistics are provided in following EXEC commands:

- **show statistics rtsp server cisco-streaming-engine bytes incoming**

  The output shows incoming bytes for both unicast and multicast streams.

  - For unicast, the command output shows the total incoming bytes and incoming packets and the aggregate bytes and packets for both RTSP and UDP source streams.
  - For multicast, the command output shows the total incoming bytes and total incoming packets.

- **show statistics rtsp server cisco-streaming-engine usage**

  The output of this command shows the incoming unicast connection details, incoming unicast bandwidth, and incoming multicast bandwidth statistics.

  - For unicast incoming connection statistics, the command output provides statistics for current RTSP connections, current RTP connections, total RTSP connections, and total RTP connections.
  - For unicast incoming bandwidth statistics, the command output provides statistics for current and average RTP bandwidth for RTSP source streams, current and average UDP bandwidth for UDP source streams, and the aggregate current and average bandwidth for both RTSP and UDP source streams.
  - For multicast incoming statistics, the command output provides statistics for current and average multicast incoming bandwidth.

Outgoing Statistics

Outgoing stream statistics are provided in following EXEC commands:

- **show statistics rtsp server cisco-streaming-engine bytes outgoing**

  The output shows outgoing bytes for both unicast and multicast streams.

  - For unicast, the command output shows total and aggregate outgoing bytes and packets for VOD and live streams.
  - For multicast, the command output shows total outgoing bytes and packets.

- **show statistics rtsp server cisco-streaming-engine usage**

  The command output shows unicast outgoing connection details, unicast outgoing bandwidth, and multicast outgoing bandwidth statistics.

  - For Unicast outgoing connection statistics, the command output shows statistics for current and total RTSP connections, current and total RTP connections, current RTP-over-RTSP connections, and current and total RTSP connections for VOD and live streams.
  - For unicast outgoing bandwidth statistics, the command output shows statistics for current and average RTP bandwidth.

  - For multicast outgoing statistics, the command output shows statistics for current and average multicast outgoing bandwidth.

Multicast Statistics

Multicast stream statistics are provided in the following EXEC commands:

- **show statistics rtsp server cisco-streaming-engine bytes incoming**
- **show statistics rtsp server cisco-streaming-engine bytes outgoing**
- **show statistics rtsp server cisco-streaming-engine usage**

The command output provides the following statistical information:

- Total incoming bytes and total incoming packets.
- Current and average incoming bandwidth.
- Total outgoing bytes and total outgoing packets.
- Current and average outgoing bandwidth.

Bandwidth Savings Statistics

Bandwidth savings statistics for unicast live splitting are provided in the following EXEC command:

- **show stat rtsp server cisco-streaming-engine bw-savings**

  The command output shows statistics for total incoming, outgoing, and saved bytes.

Revised Command Syntax

The following existing commands have been modified to resemble the **wmt** command syntax:

```
CE# show statistics rtsp server cisco-streaming-engine ?
  all         Display all statistics
  bytes       Display bytes statistics
  requests    Display unicast request statistics
  bw-savings  Display unicast savings statistics
  usage       Display usage statistics
  performance Display server performance

CE# show statistics rtsp server cisco-streaming-engine bytes ?
  incoming    Display incoming bytes statistics
  outgoing    Display outgoing bytes statistics
  <cr>
```

Clearing the Statistics

The following commands clear all Cisco Streaming Engine statistics without restarting the streaming server:

- **clear statistics rtsp server cisco-streaming-engine**
- **clear statistics all**

Configuring Report Options

The Content Distribution manager GUI provides four different monitoring reports. Report data is available in both tabular and graphical form.

Bytes Served Report

The Bytes Served report allows you to view Content Engine usage over time and to identify usage trends. To view the Bytes Served report and configure the reporting options, follow these steps:

Step 1 Choose **Devices > Devices**.

Step 2 Click the **Edit** icon for the Content Engine that you want to view or configure.

Step 3 In the Contents pane, choose **Device Monitoring > Statistics > Bytes Served**. The Bytes Served Report for Content Engine window appears, displaying the statistical data.

Step 4 To change the report parameters and display characteristics, modify the report options as desired.

Step 5 To reset the report parameters, click **Update**.

Bandwidth Efficiency Gain Report

After a Content Engine has been in use for some time and has collected statistics, the bandwidth efficiency gain report can demonstrate the value of the Content Engine in terms of bandwidth savings.

To view the Bandwidth Efficiency Gain report and configure the reporting options, follow these steps:

Step 1 Choose **Devices > Devices**.

Step 2 Click the **Edit** icon for the Content Engine that you want to view or configure.

Step 3 In the Contents pane, choose **Device Monitoring > Statistics > Bandwidth Efficiency Gain**. The Bandwidth Efficiency Gain Report for Content Engine window appears, displaying the statistical data.

Step 4 To change the report parameters and display characteristics, modify the report options as desired.

Step 5 To reset the report parameters, click **Update**.

Streaming Sessions Report

The Streaming Sessions report lists the total number of streaming sessions in progress at the collection time. It allows you to plan for future hardware provisioning and licensing requirements based on utilization data.

To view the Streaming Sessions report and configure the reporting options, follow these steps:

Step 1 Choose **Devices > Devices**.

Step 2 Click the **Edit** icon for the Content Engine that you want to view or configure.

Step 3 In the Contents pane, choose **Device Monitoring > Statistics > Streaming Sessions**. The Streaming Sessions Report for Content Engine window appears, displaying the statistical data.

Step 4 To change the report parameters and display characteristics, modify the report options as desired.

Step 5 To reset the report parameters, click **Update**.

CPU Utilization Report

To view the CPU Utilization report and configure the reporting options, follow these steps:

Step 1 Choose **Devices > Devices**.

Step 2 Click the **Edit** icon for the Content Engine that you want to view or configure.

Step 3 In the Contents pane, choose **Device Monitoring > Statistics > CPU Utilization**. The CPU Utilization Report for Content Engine window appears, displaying the statistical data.

Step 4 To change the report parameters and display characteristics, modify the report options as desired.

Step 5 To reset the report parameters, click **Update**.

Monitoring Specified HTTP URLs

ACNS 5.5 software supports HTTP URL monitoring using either the Content Distribution Manager GUI or the CLI. This feature allows you to specify the time interval (in seconds) for monitoring the specified URL(s), as well as the acceptable delay (in seconds) before the URL is retrieved. You can monitor up to 10 HTTP URLs.

To configure HTTP URL monitoring using the Content Distribution Manager, follow these steps:

Step 1 From the Content Distribution manager GUI, choose **Devices > Devices** or **Devices > Device Groups**.

Step 2 Click the **Edit** icon next to the name of the Content Engine (or device group) that you want to configure for URL monitoring.

Step 3 In the Contents Pane, choose **Applications > Web > HTTP > HTTP Monitor URL**. The HTTP Monitored URLs window appears.

Step 4 To add a URL to the list of monitored URLs, click the **Create New HTTP Monitored URL** icon in the taskbar. The Creating New HTTP Monitor URL window appears.

Step 5 In the HTTP URL field, enter the URL that you want to monitor.

Step 6 To configure the time interval for monitoring the specified URL, enter a number from 1 to 3600 (seconds) in the Monitoring Interval field. The default setting is 60 seconds.

Step 7 To configure the acceptable delay before the URL is retrieved, enter a number from 1 to 3600 (seconds) in the Acceptable Delay field. The default setting is 60 seconds.

Step 8 To save the settings, click **Submit**.

To configure a Content Engine to monitor the performance of specific URLs using the CLI, use the **http monitor url** *url* global configuration command.

This command enables you to specify up to 10 URLs that you want the Content Engine to monitor. The Content Engine maintains statistics about the various response characteristics for each of the monitored URLs. (You can use the new **show statistics http monitor** command to view these statistics, as described later in this section.)

```
ContentEngine(config)# http monitor url ?
  WORD  URL for monitoring
```

The **http monitor url** *url* command has two command options, the **acceptable-delay** and **interval** options. As the following sample output indicates, the **acceptable-delay** option is used to specify the acceptable delay in seconds (the maximum number of seconds that the specified monitored URL should be retrieved within). The default acceptable delay is 60 seconds.

```
ContentEngine(config)# http monitor url http://www.abc.com/ ?
  acceptable-delay  Threshold time in seconds before which the URL should be
  retrieved.(default is 60 seconds)
  interval          Interval in seconds for monitoring the URL.(default is 60 seconds)
  <cr>
```

As the following sample command output indicates, the **acceptable-delay** option is used to specify the acceptable delay, which is the maximum number of seconds that the specified URL should be retrieved within.

```
ContentEngine(config)# http monitor url http://www.abc.com/ acceptable-delay ?
  <1-3600>  Acceptable delay in seconds
```

Note If you use the **http monitor url** *url* command to configure the same URL with a different interval or acceptable-delay setting, the most recently configured setting takes precedence and overrides any previously configured settings for that particular URL.

As the following sample command output indicates, the **interval** option specifies the monitoring interval (that is, how frequently the Content Engine should monitor requests for a specific URL). The monitoring interval is specified in seconds. The default monitoring interval is 60 seconds.

```
ContentEngine(config)# http monitor url http://www.abc.com/ acceptable-delay 100
interval ?
  <1-3600>  Monitor interval in seconds
```

In the following example, the Content Engine is configured to monitor the URL named "http://www.abc.com/" using the default values (an interval of 60 seconds and an acceptable delay of 60 seconds):

```
http monitor url http://www.abccorp.com/
```

In the following example, the Content Engine is configured to monitor the URL named "http://www.abc.com/." The Content Engine is configured to wait up to 100 seconds for the URL to be retrieved and to monitor requests for this URL every 100 seconds.

```
ContentEngine(config)# http monitor url http://www.abc.com/ acceptable-delay 100
interval 100
```

If it takes more than 100 seconds for the URL to be retrieved, the specified acceptable delay is exceeded. The Content Engine tracks the response time (minimum and maximum delay time) as well as the number of times that the acceptable delay is exceeded for a particular URL. These statistics are shown in the output from the new **show statistics http monitor** EXEC command. (An example of the output from the **show statistics http monitor** EXEC command is provided below.)

To display statistics for the monitored URLs, use the **statistics http monitor** EXEC command. The following example shows the statistics that are reported for each of the monitored URLs:

```
ContentEngine# show statistics http monitor
HTTP Monitor URL statistics
---------------------------

Monitor URL                              = http://www.abc.com/
Total requests                           = 118
Failed requests                          = 30
Requests above acceptable delay          = 37
Minimum response time                    = 8.183 seconds
Maximum response time                    = 210.021 seconds

Monitor URL                              = http://www.abccorp.com/
Total requests                           = 275
Failed requests                          = 44
Requests above acceptable delay          = 26
Minimum response time                    = 0.071 seconds
Maximum response time                    = 164.061 seconds
```

In the command output shown above, note the following information:

- "Failed requests" are requests that did not succeed (for example, the request failed to resolve the domain name of that URL).
- "Requests above acceptable delay" are the requests that took longer than the specified acceptable delay (the maximum number of seconds specified by the acceptable-delay setting).

The output of the **show running-configuration** EXEC command includes information about the URL monitoring configuration. In the following excerpt from the **show running-configuration** command output, this particular information is highlighted in bold:

```
ContentEngine# show running-configuration
! ACNS version 5.2.3
!
!
hostname sust-7320-ce1
!
http persistent-connections timeout 300
http proxy incoming 8080
http proxy outgoing preserve-407
http tcp-keepalive enable
http monitor url http://www.abc.com/ interval 100 acceptable-delay 100
http monitor url http://www.abccorp.com/
!
ftp proxy incoming 8080
!
clock timezone US/Eastern -5 0
!
!
.
.
.
```

Only the non-default values are displayed in the output from the **show running-configuration** command. Consequently, because the Content Engine was configured to use the default values to monitor the URL "http://www.abccorp.com," the above sample output does not display these values for that URL.

To display a list of monitored URLs, including the interval and acceptable delay setting for each monitored URL, use the **show http monitor** EXEC command:

```
ContentEngine# show http monitor

Monitor URL: http://www.abc.com/
Monitor Interval: 100
Acceptable Delay: 100

Monitor URL: http://www.abccorp.com/
Monitor Interval: 60
Acceptable Delay: 60
```

Enabling Kernel Debugger

Cisco ACNS software allows you to enable or disable access to the kernel debugger (kdb) from the Content Distribution Manager GUI. Once enabled, kernel debugger is automatically activated when kernel problems occur, or you can manually activate it from the local console for the ACNS device by pressing the required key sequence.

To enable the kernal debugger from the Content Distribution Manager GUI, follow these steps:

Step 1 From the Content Distribution Manager GUI, choose **Devices > Devices**.

Step 2 Click the **Edit** icon next to the name of the Content Engine that you want to debug.

Step 3 In the Contents Pane, choose **General Settings > Troubleshooting > Kernal Debugger**. The Kernal Debugger window appears.

Step 4 To enable the kernal debugger, check the **Enable** check box, and click **Submit**.

To enable the kernal debugger from the CLI, use the **kernal kdb** global configuration command.