



Release Note for Cisco ACNS Software, Release 5.4.5

October 30, 2007



Note

The most current Cisco documentation for released products is available at Cisco.com at <http://www.cisco.com>. The online documents may contain updates and modifications made after the hardcopy documents were printed.

Contents

This release note document contains information about the Cisco Application and Content Networking System (ACNS) 5.4.5 software. This release note describes the following topics:

- [Introduction, page 2](#)
- [Hardware Platforms Supported in ACNS Software, page 2](#)
- [Software Component Versions Supported in ACNS Software, page 3](#)
- [New Command in ACNS 5.4.5, page 3](#)
- [Operating Considerations, page 4](#)
- [Open Caveats in Software Version 5.4.5, page 7](#)
- [Resolved Caveats in Software Version 5.4.5, page 22](#)
- [Related Documentation, page 27](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 28](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Introduction

The ACNS software combines the technologies of demand-pull caching and pre-positioning for accelerated delivery of web applications, objects, files, and streaming media.

This release note document is intended for administrators who will be configuring, monitoring, and managing devices that are running the ACNS 5.4.5 software. This document describes the new product features, the supported hardware, and the open and resolved caveats regarding the ACNS 5.4.5 software release.

Hardware Platforms Supported in ACNS Software

The ACNS software runs on Cisco Content Engine, Content Distribution Manager, Content Router, and Wide Area Application Engine (WAE) hardware platforms.

The ACNS 5.4.3 release is the required minimum software release for the WAE-512 and WAE-612 appliances. The ACNS 5.3.3 release is the required minimum software release for the WAE-511, WAE-611, and WAE-7326 appliances.

Table 1 shows the hardware platforms and the minimum ACNS software release in which each is supported. An “X” indicates that the software supports the hardware models listed in that row.

Table 1 Hardware and ACNS Software Compatibility Matrix

Hardware Model	ACNS Software Support						
	5.3.1	5.3.3	5.3.7	5.4.1	5.4.3	5.5.1	5.5.3
CE-507 CE-560 CE-590 CR-4430 CDM-4630	X	X	X	X	X	X	X
CE-7320 CDM-4650	X	X	X	X	X	X	X
NM-CE-BP-SCSI NM-CE-BP-40G NM-CE-BP-80G	X	X	X	X	X	X	X
CE-510 CE-510A CE-565 CE-565A	X	X	X	X	X	X	X
CE-7305 CE-7305A CE-7325 CE-7325A	X	X	X	X	X	X	X
CE-511 CE-566	X	X	X	X	X	X	X
WAE-511 WAE-611		X	X	X	X	X	X

Table 1 Hardware and ACNS Software Compatibility Matrix (continued)

Hardware Model	ACNS Software Support						
	5.3.1	5.3.3	5.3.7	5.4.1	5.4.3	5.5.1	5.5.3
WAE-7326		X	X	X	X	X	X
WAE-512					X	X	X
WAE-612							

Software Component Versions Supported in ACNS Software

Table 2 describes which SmartFilter and Websense versions are supported in the ACNS software releases.

Table 2 Component Versions Supported in ACNS Software Releases

ACNS Software Release	SmartFilter Version Supported	Websense Version Supported
ACNS 5.2.1	Version 4.0.1	Version 5.2
ACNS 5.3.x	Version 4.0.1	Version 5.2
ACNS 5.4.1	Version 4.0.1	Version 5.5.2 ¹
ACNS 5.4.3	Version 4.1.1	Version 5.5.2
ACNS 5.5.1	Version 4.0.1	Version 5.5.2

1. The integrated Websense Enterprise software Version 5.5 in the ACNS 5.4 software requires a minimum of 512 MB of RAM. We recommend that you upgrade the RAM on your device to 512 MB or greater, or move your integrated Websense server to another device that has at least 512 MB of RAM. When additional Websense components are enabled (such as the Network Agent), ACNS software requires a minimum of 1 GB of RAM.

Performance is optimal when Websense Enterprise Manager, the Websense Policy Server, and all other Websense components are situated in the same LAN. If all components are not in the same LAN, you might experience communication latency between Websense Enterprise Manager and other components. A significant increase in latency can lead to a communication failure.

New Command in ACNS 5.4.5

Table 3 describes the new command added in the ACNS 5.4.5 software release.

Table 3 CLI Command Added in ACNS 5.4.5

Mode	Syntax	Description
Global configuration	snmp-server trap-source <i>interface</i>	This command allows you to specify the interface with its corresponding IP address from which a Simple Network Management Protocol (SNMP) trap should originate.

Operating Considerations

This section describes operating considerations for ACNS 5.4.x software. It includes the following sections:

- [Multicast-In Sources in SSPLs Not Supported for Windows Media Streaming, page 4](#)
- [No Downgrade Script to ACNS Releases Later than 5.3.3, page 4](#)
- [RAM Requirements for ACNS 5.4 Software and Websense 5.5 Software, page 4](#)
- [Websense Issues When Downgrading to the ACNS 5.0 Software or ACNS 5.1 Software, page 5](#)
- [Media File System Issues When Downgrading to ACNS 5.0 Software, page 5](#)
- [SmartFilter Issues When Upgrading or Downgrading to Another ACNS Software Release, page 5](#)
- [Interoperability with ICAP Vendors, page 6](#)
- [ICAP Performance, page 6](#)
- [ICAP Maximum File Size Supported, page 6](#)
- [Matrix of Supported Caching, Filtering, and Authentication Methods, page 6](#)

Multicast-In Sources in SSPLs Not Supported for Windows Media Streaming

Multicast-in source objects in server-side playlists are not supported for Windows Media streaming. If you have such an unsupported configuration, the Windows Media stream will fail, and the problem will be identified in the syslog file, as shown in the following example:

```
Jul 9 21:30:09 new-stream-ce2-158-3 mms_server: %CE-WMT-2-512078: Multicast-in with SSPL source is not supported
```

No Downgrade Script to ACNS Releases Later than 5.3.3

There is no downgrade script in the ACNS 5.4 code base to downgrade directly to ACNS 5.3.x releases that are later than ACNS 5.3.3. To downgrade from ACNS 5.4 software to ACNS 5.3.x software you must use the following guidelines:

- Use the Downgrade5_4_to_5_3_3 downgrade script if you are downgrading from ACNS 5.4 to any ACNS 5.3 version that is greater than or equal to ACNS 5.3.3.
- Use the Downgrade5_4_to_5_3 downgrade script if you are downgrading from ACNS 5.4 to any ACNS 5.3 version that is earlier than ACNS 5.3.3.
- Before or after you run the downgrade script, you must install the version of ACNS 5.3.x software that you need.

RAM Requirements for ACNS 5.4 Software and Websense 5.5 Software

The integrated Websense Enterprise software Version 5.5 in the ACNS 5.4 software requires a minimum of 512 MB of RAM. We recommend that you upgrade the RAM on your device to 512 MB or greater, or move your integrated Websense server to another device that has at least 512 MB of RAM.

WebSense Issues When Downgrading to the ACNS 5.0 Software or ACNS 5.1 Software

If the local (internal) Websense server is enabled on the Content Engine and you downgrade from the ACNS 5.2.x software to either ACNS 5.0 software or ACNS 5.1 software, the WebsenseEnterprise directory is removed from the Content Engine and the local Websense server stops working. The ACNS 5.2.x software does not generate an error message indicating that the WebsenseEnterprise directory has been removed. However, in the ACNS 5.3.1 software and later releases, the following error message is displayed to notify you about this Websense downgrade issue:

```
WARNING:
Websense does not support downgrade
Hence removing /local/local1/WebsenseEnterprise
Websense will stop working after copy ftp install
```

To avoid this problem when downgrading from the ACNS 5.3.x or ACNS 5.2.x software to either ACNS 5.1.x software or ACNS 5.0.x software, follow these steps:

-
- Step 1** Disable the local (internal) Websense server on the Content Engine.
 - Step 2** Deactivate the Websense services on the Content Engine.
 - Step 3** Install the ACNS 5.1 software or ACNS 5.0 software downgrade image on the Content Engine.
-

Media File System Issues When Downgrading to ACNS 5.0 Software

If you have configured the media file system (mediafs) with the ACNS 5.1 software and later releases, and then downgrade to the ACNS 5.0 software, the mediafs disk space assignment is lost and reverts to the ACNS network file system (cdnfs) disk space. (The mediafs is used for on-demand content that is fetched through the two streaming protocols [RTSP and WMT]. The cdnfs is used for pre-positioned content in the ACNS network.)

This situation occurs because of a design change that was implemented in the ACNS 5.1 software. Because the ACNS 5.0 software is not compatible with this change, the disk space becomes assigned to cdnfs instead of mediafs. To work around this problem, follow these steps:

1. After you downgrade to the ACNS 5.0 software, use the CLI (**disk config EXEC** command) or the GUI to assign the mediafs disk space.

Use the Content Distribution Manager GUI for Content Engines that are registered with a Content Distribution Manager. Use the Content Engine GUI for standalone Content Engines (Content Engines that are not registered with a Content Distribution Manager and are being managed through the Content Engine GUI or CLI).

2. Reboot the Content Engine for the disk configuration changes to take effect.

SmartFilter Issues When Upgrading or Downgrading to Another ACNS Software Release

When you upgrade or downgrade the Content Engine to a different release of the ACNS software, if there is a difference in the SmartFilter plug-in version, the SmartFilter database and configuration files are deleted and default configurations are loaded. This change occurs because the configuration details

might be changed with each new version of SmartFilter software. After each upgrade or downgrade of the SmartFilter plug-in, a fresh database has to be downloaded from the SmartFilter Administration Console to the Content Engine. (For a description of which SmartFilter versions are supported in the ACNS software releases, see [Table 2](#).)

Interoperability with ICAP Vendors

The Internet Content Adaptation Protocol (ICAP) is an open standards protocol for content adaptation, used typically at the network edge. Content adaptation includes virus scanning, content translation, content filtering, content insertion, and other methods of improving the value of content to end users. ICAP specifies how a Content Engine, acting as an HTTP proxy server, can communicate with an external device that is acting as an ICAP server to filter and adapt the requested content.

ICAP provides two content-processing modes for HTTP services. These modes define the transactions that can occur between a Content Engine acting as an ICAP client and an ICAP server. The two modes are as follows:

- Request modification (reqmod)—Allows modification of requests as they are sent from the Content Engine to the ICAP server on their way to the origin server. The ICAP server can modify these requests depending on the services requested.
- Response modification (respmo)—Allows modification of requests after they return from the origin server. The ICAP server only acts on requested objects after they return from the origin server.

The following is a complete list of the ICAP vendors that have been certified to interoperate with the Content Engine:

- TrendMicro for reqmod and respmod
- Symantec for respmod

ICAP Performance

With the respmod vectoring point, which is used by virus-scanning ICAP vendors, the performance of the Content Engine model CE-7305 will be 300 transactions per second.

With the reqmod-precache vectoring point, which is used by URL filtering ICAP vendors, the performance of the Content Engine model CE-7305 will drop 20 percent from the rated performance.

The performance of the Content Engine will be limited by the performance of the ICAP server.

ICAP Maximum File Size Supported

For ACNS 5.4.x software and later, the maximum file size that is supported in the ACNS software is 2 GB. Files that exceed this size limit are not supported for ICAP processing.

Matrix of Supported Caching, Filtering, and Authentication Methods

[Table 4](#) lists the caching, filtering, and authentication methods supported by Content Engines that are running the ACNS 5.4.x software. An asterisk (*) indicates that a feature is supported for that particular protocol.

Table 4 Caching, Filtering, and Authentication Methods and Related Protocol Support

Protocol	Filtering				Proxy Authentication			
	Caching	N2H2	Websense	SmartFilter	RADIUS	LDAP	NTLM	TACACS+
HTTP	*	*	*	*	*	*	*	*
FTP-over-HTTP	*	*	*	*	*	*	*	*
HTTPS-over-HTTP	*	*	*	*	*	*	*	*
RTSPG	*							
MMSU	*							
MMST	*							
MMS-over-HTTP	*				*	*		
HTTP-WCCP	*		*	*	*	*	*	*
FTP-WCCP (native FTP)	*							
HTTPS-WCCP	*		*	*				
RTSPG-WCCP	*							
MMSU-WCCP	*							
MMST-WCCP	*							
MMS-over-HTTP -WCCP	*				*	*		

Open Caveats in Software Version 5.4.5

This section lists the open caveats in software version 5.4.5.

- CSCdy82311

Symptom: Content cannot be acquired using strong authentication from secure origin servers that use certificates from nonstandard certificate authorities (CAs). If strong authentication is chosen for content acquisitions from such a site, the acquirer error statistics will contain a 401 (Unauthorized) error code, and the acquirer error log will display the following error message:

```
Strong Cert Authentication rejects certificate due to error: ssl error code
```

Condition: This problem occurs if the origin server uses a certificate that is not known as a standard certificate to the ACNS software acquirer. For content acquisition from secure sites over HTTPS using strong authentication, only sites with certificates from standard certificate authorities are supported.

With strong authentication, if any errors occur during certificate verification by the ACNS acquirer, then content from that site will not be acquired. With weak authentication, certain errors are allowed during certificate verification (for example, a certificate has expired, certificate is not yet valid, and a subject issuer mismatch has occurred).

Workaround: Use one of the following workarounds:

- Use weak authentication.
- On the secure server, use a certificate that was generated by one of the standard certificate authorities. To determine which CA certificate to install on an origin server, refer to the certificate lists in the *Cisco ACNS Software Upgrade and Maintenance Guide, Release 5.x*. Certificate lists differ based on the version of the ACNS software.

- CSCea51815

Symptom: When a Content Engine model CE-565 is attached to a Storage Array SA-7 device, if too large a cache file system (cfs) partition is configured, and a combined streaming and caching workload is used, then a lower HTTP performance will result.

Condition: This problem occurs when the CE-565 has Windows Media Technologies (WMT) enabled, a combined streaming and caching workload is used, and the Content Engine is attached to an SA-7 device.

Workaround: Allocate less space to the cfs if a Storage Array is attached to the Content Engine.

- CSCec52221

Symptom: After you downgrade from the ACNS 5.1b300 software to the ACNS 5.0.7b8 software, Windows Media Technologies (WMT) is enabled with no media file system (mediafs).

Condition: This problem occurs when you upgrade from the ACNS 5.0.7b8 to the ACNS 5.1bx software, configure the disk, and then downgrade to the ACNS 5.0.7b4 software.

Workaround: Reconfigure the disk with a mediafs partition and reload the software.

- CSCed68727

Symptom: The Content Distribution Manager only checks if coverage zone files refer to invalid Content Engines after there is a fresh import. When a configuration change causes imported coverage zone files to refer to invalid Content Engines, the Content Distribution Manager does not check or display the correct error message until the next fresh import.

Condition: This problem occurs when a configuration change causes imported coverage zone files to refer to invalid Content Engines.

Workaround: None.

- CSCed77655

Symptom: The Content Engine stops spoofing the client IP address and uses its own IP address to fetch content from the origin server.

Condition: The **http l4-switch spoof-client-ip enable** global configuration command turns on IP spoofing on a Content Engine that is functioning as a caching engine. When a **rule action use-server** global configuration command is used, the Content Engine stops spoofing the client IP address and instead uses its own IP address to fetch the content.

Workaround: Remove the rule configurations.

- CSCed84227

Symptom: The network management system (NMS) host does not know the location from which SNMP traps are originating.

Condition: This problem occurs if there are two interfaces and you configure interface redundancy using both interfaces. You must use a dummy address for the physical addresses, and then configure a real address that floats between the two interfaces. If you then configure SNMP traps, the traps are being sourced from the dummy address and not the routable address. Therefore, the NMS host does not know where the trap is coming from.

Workaround: Configure the Content Engine to generate SNMP version 2c trap messages. Because the SNMP version 2c trap message does not contain the IP address of the SNMP agent, the NMS software will use the source IP address of the UDP message to identify the address of the SNMP agent.

- CSCee25042

Symptom: Even though you entered the **url-filter wmt bad-sites-deny** global configuration command on the Content Engine, the Content Engine is not filtering requests for content that is pre-positioned in its wmt_vod directory.

Condition: This problem occurs in the following situation:

- a. You pre-position a file (for example, file.asf) on the Content Engine in its wmt_vod directory.
- b. After pre-positioning the file, you configure the bad site list for URL filtering using `mmst://Content Engine IP address/wmt_vod/file.asf`.
- c. A user makes a content request for this URL (`mmst://Content Engine IP address/wmt_vod/file.asf`).

Workaround: Configure the bad site list using `mmst://127.0.0.1/wmt_vod/file.asf` instead of `mmst://Content Engine IP address/wmt_vod/file.asf`.

- CSCee38190

Symptom: A WMT live stream in a managed live event environment is accessible for a period longer than the scheduled duration.

Condition: This problem occurs only when WMT live programs have unicast access enabled. In this situation, if “Auto Delete” is set to true, streams are accessible for a maximum of 24 hours after the last playtime of the event. If “Auto Delete” is set to false, streams are accessible indefinitely.

Workaround: Control the live-stream source through the schedule for the event. Typically, this process involves starting and stopping the WMT encoder.

- CSCee49106

Symptom: The content replication status may show an incorrect number of acquired files.

Condition: This problem may occur if too many channels share the same content (for example, if over 100 channels share the same 30 files in each channel). Even though all 100 channels should show the 30 files that were acquired and distributed, it takes an extended period (days) before the correct manifest item count is displayed.

Workaround: Reduce the number of channels that share the same contents.

- CSCee56998

Symptom: The CPU usage on the Content Engine hits a peak of 100 percent.

Condition: This problem may occur if the internal (local) Websense server is enabled on the NM-CE-BP models.

Workaround: None.

- CSCee67227

Symptom: When you specify foo as a folder URL in the manifest file, and there is a single item redirection from foo to foo/ by the web server, the ACNS acquirer fails to process such redirections and generates a 716 error message. If you are using the quick crawl tool in the Channel Content window, some of the files also report 716 error messages.

Condition: This problem occurs if you are using the quick crawl tool and there is a single item redirect from foo to foo/. However, if foo is a link from a crawl job, single item redirections from foo to foo/ are allowed.

Workaround: Specify foo/ in the manifest file, or specify a crawl job instead of using the quick crawl tool.
- CSCee67330

Symptom: Microsoft NT LAN Manager (NTLM) authentication fails and the pop-up window is displayed again.

Condition: This problem occurs if NTLM authentication is being used and the specified domain name contains more than 50 characters.

Workaround: For NTLM authentication, use a domain controller (DC) that has a domain name with fewer than 35 characters.
- CSCee71157

Symptom: Channel routing causes loops for several Content Engines.

Condition: This problem may occur if there are Content Engines that are running the ACNS 5.1.x software or earlier, and these Content Engines are registered with a Content Distribution Manager that is running the ACNS 5.2.x software.

Workaround: Upgrade the Content Engines to the ACNS 5.2.x software. Currently, a Content Distribution Manager that is running the ACNS 5.2.x software does not propagate some configuration changes to Content Engines that are running an ACNS software release earlier than the ACNS 5.2.x software. Therefore, Content Engines that are running the ACNS 5.1.x software or earlier, may not recognize that the root Content Engine was changed from one Content Engine to another. Consequently, routing loops may develop within the system.
- CSCee81376

Symptom: The CMS service on the Content Distribution Manager cannot start and fails to create the CMS database backup file.

Condition: This problem occurs if the ACNS network configuration is very large (for example, with 2000 configured Content Engines) and the sysfs partition is 2 GB or less.

Workaround: Create a sysfs partition that is greater than 2 GB.
- CSCee90245

Symptom: Microsoft NT LAN Manager (NTLM) authentication occurs even though you disabled it on the Content Engine.

Condition: In rare situations, NTLM proxy authentication remains enabled when you enter the **no ntlm server enable** global configuration command, although the output of the **show running EXEC** command shows that the NTLM server is not enabled on the Content Engine.

Workaround: Reenter the **no ntlm server enable** global configuration command on the Content Engine.

- CSCee92698

Symptom: The ICAP service is enabled on the Content Engine, but the Content Engine is unable to retrieve the content.

Condition: This problem occurs if the Content Engine is running the ACNS 5.x software, and you configure two or more ICAP services to subscribe to the same vectoring point (the response modification [RESPMOD] vectoring point).

Workaround: None.
- CSCee92917

Symptom: A cleanup of the sysfs partition removes all pre-positioned RealMedia contents from the /local1/real_vod/ directory on the Content Engine.

Condition: This problem occurs if the sysfs partition is saturated because of the population of content in the real_vod directory.

Workaround: None.
- CSCef11091

Symptom: The WCCP cache farm (a cluster of Content Engines that are running WCCP) is formed using the assignment method even though you specified the **mask-assignment assign-method-strict** option when configuring the WCCP service.

Condition: This problem occurs if the WCCP cache farm is associated with Cisco routers instead of Cisco switches.

Workaround: None. Mask assignment was only designed for Catalyst 6500 series switches and is not supported by Cisco routers.
- CSCef16345

Symptom: The stream scheduler in the edge Content Engine retrieves stale Session Description Protocol (SDP) information from its forwarder and stores it in its local1/cse_live/ucast folder if the encoding is modified through IP/TV Program Manager. All further RTSP requests are served with this stale SDP content.

Condition: This problem occurs if the stream scheduler retrieves stale SDP information from its forwarder because the program has been edited and the encoding changed for a program. This situation occurs if the Content Distribution Manager notification at the edge Content Engine triggers the stream scheduler before the same occurs at the root Content Engine. Consequently, the edge Content Engine obtains the SDP content from its forwarder, which is valid content at that moment.

Workaround: Reload the Content Engine.
- CSCef37606

Symptom: The Content Engine becomes unresponsive, and commands take 16000 milliseconds or more to execute.

Condition: This problem occurs when the load that is running on the Content Engine is almost as high as the maximum permissible load for a Content Engine, and you then enable ICAP (especially with request modification [REQMOD] transactions). This situation causes the Content Engine to go into an overload state and not recover easily.

Workaround: The load on the Content Engine with ICAP enabled (for the response modification [respmod] transactions) should be kept to 50 percent of the load that it can handle without ICAP.

- CSCef37947

Symptom: A URL in the Synchronized Multimedia Integration Language (SMIL) file that has the “repeatCount” value set may not be requested the number of times specified by the “repeatCount” setting.

Condition: This problem occurs when RealPlayer Version 10 is used. The player exhibits the same behavior regardless of whether a Content Engine exists between the client and the origin server.

Workaround: Use RealOne player instead of RealPlayer Version 10, or request the SMIL file again. The URL will be played at least once in the player.
- CSCef44709

Symptom: An HTTP 1.0 request that is received by the Content Engine from a client web browser is sent as an HTTP 1.1 request by the Content Engine to the origin server.

Condition: This problem occurs when the ICAP service is enabled on the Content Engine.

Workaround: None.
- CSCef57641

Symptom: The cache process on the Content Engine restarts.

Condition: This problem occurs if a large volume of HTTP, HTTPS, and FTP traffic is being directed to the Content Engine operating in transparent mode.

Workaround: None.
- CSCef60282

Symptom: When you enter the **write memory** command and immediately reload the Content Engine, a prompt appears showing that the configuration has been changed.

Condition: This problem occurs when you perform the following configuration sequence:

 - a. Enable Websense on the Content Engine.
 - b. Remove or change the IP address of the Content Engine.
 - c. Enter a **write memory** command on the Content Engine.
 - d. Reload the Content Engine.

Workaround: Note that ACNS functionality is not affected if this problem occurs. However, if a prompt appears stating that the configuration has been changed, enter **yes** to save the configuration.
- CSCef61845

Symptom: Unicast access to a live program does not work.

Condition: This problem occurs only when you use special characters (“?” and “#”) in the unicast reference URL.

Workaround: To publish a live event, use URLs that do not contain special characters.
- CSCef67934

Symptom: The proxy autoconfiguration file is missing from the Content Engine after you switch from group settings to device settings, and then switch back to group settings.

Condition: This problem occurs when you perform the following configuration sequence:

 - a. Specify values in the Client Proxy Autoconfig Device Group window of the Content Distribution Manager GUI.
 - b. Override these values through the Client Proxy Autoconfig Device window of the Content Distribution Manager GUI.

- c. Revert the Content Engine back to the device group settings by clicking the **Force device group settings** button in the device group window or by selecting the device group from the drop-down menu in the device window. The autoconfiguration file is not found but the proxy autoconfiguration feature is shown as enabled.

Workaround: Return to the device window in the Content Distribution Manager GUI, delete the values from the proxy autoconfiguration fields in the device window, and then select **device group** from the drop-down menu.

- CSCef67938

Symptom: When using the quick start tool in the Content Distribution Manager GUI, if you repeatedly click the **Add-Router to List** button before the window completely loads in your browser, the following message appears in your browser:

```
The system had trouble processing your last request.
```

Condition: This problem occurs when there is a slow connection between the Content Distribution Manager and your browser, and any of the following unsupported actions take place:

- You click the **BACK** or **REFRESH** browser buttons.
- Multiple browser windows from the same client machine are accessing the Content Distribution Manager GUI.
- Another user deletes the item that you are working with in the Content Distribution Manager GUI.

Workaround: Return to the Content Distribution Manager GUI and wait until the window is completely loaded in your browser before you click the **Add-Router to List** button.

- CSCeg04809

Symptom: HTTP VoD file statistics are not being updated correctly.

Condition: This problem occurs if you enter the **show statistics wmt requests EXEC** command while you are using the HTTP protocol to play a stream. The command output shows the total unicast requests field as 2 but shows the other types of requests (for example, the number of served streaming requests) as 1.

Workaround: Wait until the stream ends before you enter the **show statistics wmt requests EXEC** command.

- CSCeg22697

Symptom: The Websense EIM server that is running on the Content Engine generates a core file.

Condition: This problem occurs when the Websense server is enabled on the Content Engine.

Workaround: No user intervention is required. The Websense server functionality is not affected. After generating a core file, the Websense server restarts automatically, and the functionality is restored.

- CSCeg47793

Symptom: If you modify a Content Engine GUI page and reload the page without first clicking the Update button, the new (unsaved) values are displayed on the page instead of the old (saved) values.

Condition: This problem occurs if you are using the latest versions of the Netscape browser (Version 7.0 or later) to access the Content Engine GUI.

Workaround: Go to another Content Engine GUI page, and then return to the same Content Engine GUI page instead of reloading the page. The redisplayed Content Engine GUI page will display the old (saved) values instead of the new (unsaved) values.

- CSCeg56075

Symptom: RealPlayer crashes when the streams are switched from the first stream to the second stream.

Condition: This problem occurs if you have set the reconnect as automatic for broadcast redundancy.

Workaround: Set the reconnect as manual instead of automatic.
- CSCeg82405

Symptom: The Internet Explorer client retrieves a partial (incomplete) customized error page and displays it along with some partial HTML code.

Condition: This problem occurs if a customized error page is configured on the Content Engine and an Internet Explorer client requests a nonexistent HTTPS URL, which causes the customized error page to be returned.

Workaround: None.
- CSCeg84004

Symptom: After a client boots and sends the first request from the browser, the NTLM authentication prompt may take approximately two minutes to appear.

Condition: This problem occurs under the following conditions:

 - a. NTLM request authentication is enabled on the Content Engine.
 - b. The client machine has a malfunctioning program (for example, spyware or a virus) and is sending HTTP requests to the Content Engine along with the first request from the browser. The user agent is named Tioga, and the request is similar to the following example:


```
GET http://somehostname/Zone-UVWXYZ/config.cfg HTTP/1.0\r\n
Request Method: GET
Accept: /*/*\r\n
User-Agent: Tioga\r\n
Host: somehostname\r\n
Pragma: no-cache\r\n
```

where *somehostname* is a hostname.

The user will be authenticated after waiting approximately two minutes. After reporting a failure to the browser, the Content Engine uses the same credential and retrieves the group information for that user from its HTTP authentication cache.

Workaround: On the Content Engine, configure a rule to either reject requests from the user agent named Tioga, or configure the **no-auth** rule to bypass authentication for this user agent.
- CSCeg86386

Symptom: In a Content Router environment, users are not able to choose RTSPU (UDP) or RTPST(TCP) by requesting with `rtspu://` or `rtspt://` from their Windows Media players. Another symptom is that an RTSPT stream is returned when an RTSPU stream is requested. A third symptom is that even though you specified the **wmt disallowed-client-protocols rtspu** global configuration command, it is not preventing clients from being served for a request `rtspu://crfqdn/file.asf`, which will return an RTSP stream instead of an error.

Condition: This problem may occur if a Content Router is being used for RTSP redirection.

Workaround: None.

- CSCeh20906

Symptom: Although you have the transaction log sanitize feature enabled on the Content Engine, the RealProxy or RealServer access logs display the client IP address when it should be hidden.

Condition: This problem is caused because the **transaction-logs sanitize** CLI command is not working properly for the RealProxy and RealServer.

Workaround: None.

- CSCeh23466

Symptom: The table of contents and the index of the ACNS Content Distribution Manager online help are not functioning. When you open the online help window, the left pane containing the table of contents and index appears blank.

Condition: This problem is caused by the Windows Security Update MS05-001. This security patch prevents the creation of an instance of the HTML Help ActiveX control that is served in HTML content from outside the Local Machine zone.

Workaround: Because the ACNS Content Distribution Manager is part of your internal network, you may modify the Windows registry to allow execution of ActiveX controls that are served from within the intranet zone. For more information on modifying the registry to workaround this issue, refer to Microsoft Knowledge Base article 892675 at this URL: <http://support.microsoft.com/kb/892675>.

- CSCeh35923

Symptom: When you are trying to install the ACNS software on a Content Engine, DMA errors are displayed.

Condition: This problem occurs under the following two conditions:

- a. You are trying to install the ACNS software image on a CE-7326.
- b. You select Option 7 from the Installer main menu as follows:

```
Installer Main Menu:
 1. Configure Network
 2. Manufacture flash
 3. Install flash cookie
 4. Install flash image from network
 5. Install flash image from cdrom
 6. Install flash image from disk
 7. Wipe out disks and install .bin image
 8. Exit (and reboot)
Choice [0]: 7
```

Workaround: The DMA errors are displayed four to five times in sequence and then the normal operation of the Content Engine continues without any user intervention.

- CSCeh73477

Symptom: The acquirer experiences a problem when accessing files from the Samba share.

Condition: This problem occurs when the following two conditions exist:

1. A channel contains a Samba crawl from a Network Appliance file server that is running a version prior to version 7.0.
2. The root Content Engine is running ACNS 5.3 or later.

Workaround: The Network Appliance file server that is running a version older than 7.0 has problems with the Samba versions used in ACNS 5.3 and later. Upgrade the Network Appliance file server to version 7.0 or higher or downgrade ACNS to version 5.2.

- CSCeh93212

Symptom: The Websense Manager cannot connect to the local (internal) Websense server that is running on the Content Engine, and clients receive the following error: “Failed to connect, the server is not yet fully started. please try again in a little while”.

Condition: This problem occurs if a standby IP address is used on both the primary and secondary interfaces, which prevents the Websense Manager from connecting to the Content Engine.

Workaround: Disable the standby IP group and use a single IP address on the interface.

- CSCei01668

Symptom: The firewall shows that there is an excessive amount of traffic originating from the Content Engine over TCP port 8999.

Condition: This problem occurs when the Content Engine is on the outside of the firewall (connected to the internet gateway router). The Content Engine is constantly attempting to reset the connections to the client inside the firewall with a source port of TCP 8999 going to the NAT address of the client.

Because the port translation timer has expired on the Content Engine, the Content Engine uses port 8999 to return the message to the client. Because there is no NAT address configured on the firewall with the TCP port 8999, these messages/requests fail at the firewall.

Workaround: Configure the following global configuration CLI commands on the Content Engine:

```
ContentEngine(config)# http tcp-keepalive enable
ContentEngine(config)# tcp keepalive-timeout 60
ContentEngine(config)# tcp keepalive-probe-interval 60
```

- CSCin54434

Symptom: The Websense Manager cannot connect to the Websense server that is running as a separate process on the Content Engine instead of running on a separate system.

Condition: This problem occurs if an external IP address is used from the Websense Manager to connect to the local Websense server that is running on the Content Engine.

Workaround: None.

- CSCsb65952

Symptom: There is a local Network Agent core file on the Content Engine. The local Network Agent is one of the services of the local Websense server and runs on the Content Engine.

Condition: This problem occurs when the local Network Agent is enabled on the Content Engine.

Workaround: None.

- CSCsb69794

Symptom: The Websense GUI does not contain an option for configuring the Winix NTLM Settings (Windows NT Directory/Active Directory [Mixed Mode]).

Condition: The problem may occur in the following situation:

- The Content Engine is running the ACNS 5.3.1.5 software or a later release and the integrated Websense software.
- More than 24 hours have elapsed since you originally configured the Winix NTLM setting.

Workaround: Reinstall the user service component of Websense on the Content Engine. For example, enter the following two global configuration commands:

```
ContentEngine(config)# no websense-server service user activate
ContentEngine(config)# websense-server service user activate
```

- CSCsb72030

Symptom: The Content Engine is returning a 200 OK response when it should be returning a 304 message.

Condition: This problem occurs when the content has been pre-positioned on the Content Engine.

Workaround: None.
- CSCsb79685

Symptom: When a WMT stream is pre-positioned, the audio works but the playback of embedded slides in the pre-positioned WMT stream are not displayed.

Condition: This problem occurs if Microsoft presenter was used to create a WMT stream that has embedded slides. When this content is pre-positioned, WMT opens and the audio works but the slides never appear.

Workaround: When you are using Microsoft producer to publish the content, select publish to **My Computer** and when you select the **Choose publish settings for different audiences** option, do not check the **Enable rich-media Streaming** option. When the content is pre-positioned, all content that is created in publishing should be pre-positioned.
- CSCsc05348

Symptom: During ICAP REQMOD precache processing, a significant amount of server errors occur.

Condition: The server errors are being generated because the existing connections are closed when the internal connection to the Content Engine receives an error.

Workaround: No workaround is required because even though the clients whose requests are going through the Content Engine will experience one failure to load a page, their attempt to reload a page will succeed.
- CSCsc07702

Symptom: A PacketVideo player cannot play back a Helix Mobile Producer-encoded media file.

Condition: This problem occurs when the files are pre-positioned. This problem does not occur if the QuickTime player (Version 6.0.5 or Version 7.0.2) is used to play back the files.

Workaround: None.
- CSCsc14022

Symptom: The Windows Media player reports an error when the user attempts to play a URL that requires authorization by the Camiant ICAP server.

Condition: This problem occurs when a request fail authorization with the ICAP server occurs, and the Camiant ICAP server has its alternate URL configured as a content-routed FQDN (for example, http://<cr-fqdn>/filename.asf).

Workaround: The Windows Media player will not report an error and will successfully play the alternate URL that is configured on the Camiant ICAP server if you configure the alternate URL in one of the following formats:

 - A Windows Media player meta file that will be content-routed to a Content Engine (for example, http://<cr-fqdn>/filename.asf.asx). This URL may also be specified using the RTSP protocol.
 - A file that resides on an external Windows Media server (a Windows Media server that does not reside on a Content Engine).

- CSCsc25501

Symptom: After you remove the **no-auth** rule on the Content Engine, the Content Engine continues to apply the rule even when you enter the **no rule enable** command and remove all of the pattern lists.

Condition: This problem occurs if the **no auth** rule has been configured and then you remove it from the Content Engine.

Workaround: Reboot the Content Engine.
- CSCsc42786

Symptom: Websense logging on the Content Engine does not show the usernames for LDAP/NTLM queries.

Condition: This problem occurs if the Content Engine is running the ACNS 5.3.x software release or a later software release.

Workaround: Downgrade the Content Engine to the ACNS 5.2.x software or an earlier software release.
- CSCsc45058

Symptom: The Windows version of the PacketVideo player does not display video output. The player indicates that buffering is occurring but no video or audio is rendered.

Condition: This problem occurs if the client is a PacketVideo player (a Windows simulator) and the source is a PacketVideo server. The mobile phone-based PacketVideo client plays video/audio properly for the same program.

Workaround: Use the QuickTime player or a VLC client to view the content from a Microsoft Windows computer.
- CSCsc71576

Symptom: The Content Router does not redirect requests to Content Engines in less specific network routes when all Content Engines in the more specific network routes have reached their load threshold.

Condition: This problem occurs when all of the following conditions exist:

 - The Content Router is configured to redirect requests based on the load of the Content Engines.
 - The coverage zone file has some Content Engines serving a more specific network route and some Content Engines serving a less specific network route, as shown in the following example:

```

<coverageZone>
<network>10.86.0.0/16</network> -----> More specific network route
<CE>ce1</CE>
<metric>10</metric>
</coverageZone>

<coverageZone>
<network>10.77.0.0/16</network> -----> More specific network route
<CE>ce2</CE>
<metric>10</metric>
</coverageZone>

<coverageZone>
<network>10.0.0.0/8</network> -----> Less specific network route
<CE>ce3</CE>
<metric>10</metric>
</coverageZone>

```

Content Engine ce3 is configured to serve the network 10.0.0.0/8 which is less specific to the network 10.86.0.0/16 served by Content Engine ce1 and 10.77.0.0/16 served by Content Engine ce2.

- All the Content Engines serving the more specific network have reached their load threshold.
- The Content Router receives a request from a client in the more specific network.

Workaround: The coverage zone file should be reconfigured in such a way that all Content Engines serving the less specific network route should be configured for the more specific network route with a higher metric value, as shown in the following example:

```
<coverageZone>
<network>10.86.0.0/16</network> -----> More specific network route with lower metric
<CE>ce1</CE>
<metric>10</metric>
</coverageZone>

<coverageZone>
<network>10.77.0.0/16</network> -----> More specific network route with lower metric
<CE>ce2</CE>
<metric>10</metric>
</coverageZone>

<coverageZone>
<network>10.86.0.0/16</network> -----> More specific network route with higher metric
<CE>ce3</CE>
<metric>20</metric>
</coverageZone>

<coverageZone>
<network>10.77.0.0/16</network> -----> More specific network route with higher metric
<CE>ce3</CE>
<metric>20</metric>
</coverageZone>
```

In this example, Content Engine ce3 (initially configured for the 10.0.0.0/8 network route) is now configured for both the more specific network routes 10.86.0.0/16 and 10.77.0.0/16 with a metric value 20, which is higher than the metric value of 10 configured for Content Engine ce1 and Content Engine ce2.

If the Content Router receives a request from network 10.77.0.0/16, and if Content Engine ce2 has reached its load threshold, the Content Router will redirect the request to Content Engine ce3.

Similarly, if the Content Router receives a request from network 10.86.0.0/16, and if Content Engine ce1 has reached its load threshold, the Content Router will redirect the request to Content Engine ce3.

- CSCsc81316

Symptom: At the Content Engine, the client is refused access to the RealProxy client. The Content Engine is also logging the following types of error messages:

```
Sep 2 11:50:30 prx03 wccp: %CE-WCCP-3-500001: RTSP Proxy may be down, keepalives
halted!
Sep 2 11:50:30 prx03 rtspd: %CE-WCCP-3-500057: wccp_liveness_update(): Could not send
alivemessage (tries 1). Success
Sep 2 11:50:38 prx03 MCM: Plugin MC_REAL_ERRORPLUGIN: 72: Error retrieving URL
`broadcast/.../reflector:35134' (Invalid path)
Sep 2 11:50:39 prx03 MCM: Plugin MC_REAL_ERRORPLUGIN: 74: Error retrieving
URL`broadcast/.../reflector:35137' (Invalid path)
```

Condition: This problem occurs if RealProxy is enabled on a Content Engine that is running the ACNS 5.x software.

Workaround: Reload the Content Engine.

- CSCsc83129

Symptom: ACNS pre-positioned downloads are slower than downloads from the origin server. For example, if you download a pre-positioned file from a Content Engine, the maximum download speed is 3.5 Mbps. If you download the same file directly from the origin server, the maximum download speed is 10 Mbps.

Condition: This problem occurs when a Content Engine model CE-7305 is running the ACNS 5.3.5 software or a later release, and the pre-positioned file is downloaded over a Gigabit Ethernet interface with an HTTP bit rate set to 0 (unrestricted).

Workaround: None.

- CSCsd27358

Symptom: The Content Engine closes the TCP connection gracefully at the client side, even when the connection is aborted on the server side.

Condition: This problem occurs when the Content Engine is acting as a proxy and the origin server is resetting (RST) the connection due to some failure condition.

Workaround: None. The Content Engine is designed to perform a graceful close on the client end, even if the server closes the connection abruptly by sending a reset.

- CSCsd30356

Symptom: The Content Engine hangs and does not authenticate NTLM users or pass traffic. NTLM servers show as DEAD in the **show statistics ntlm** command output.

Condition: This problem occurs when the Content Engine is running NTLM or other authmod authentication.

Workaround: Restart the authmod process by using the **service restart http_authmod** command.

- CSCsd60376

Symptom: Bypass servers (static or dynamic) are not accessible with WCCP enabled.

Condition: This problem occurs when you use WCCP with an L2 mask assignment on a WCCP router. When a bypass entry is added either dynamically or statically to the Content Engine, then the site is no longer accessible through a browser.

Workaround: None.

- CSCsd62968

Symptom: The Content Distribution Manager reports the following error:

```
Cache service died kernel crash and or user core files detected.
```

Condition: This error occurs after upgrading to ACNS 5.4.1 software.

Workaround: None.

- CSCsd66331

Symptom: The **dns pin cname** global configuration command does not take effect on the Content Engine until after the DNS caching service is restarted.

Condition: This problem occurs when the DNS pin configuration has changed, but the DNS queries do not reflect that configuration change.

Workaround: Disable and then enable the DNS cache by using the **dns disable** command followed by the **dns enable** command.

- CSCsd72312

Symptom: The ICAP client contacts the DNS server every time before sending the request to the ICAP server.

Condition: This condition occurs because the DNS lookup cannot be disabled.

Workaround: None.
- CSCsd82649

Symptom: TVout programs exhibit audio skipping.

Condition: This problem occurs in ACNS builds above 5.1.9.5 and in ACNS 5.4.1, which exhibits video skipping, as well. This problem does not occur in ACNS build 5.1.9.5.

Workaround: Downgrade to ACNS 5.1.9.5 software, which does not exhibit this problem.
- CSCsd87378

Symptom: The ACNS 5.3.5 or 5.4.1 software returns an error message when you use “global” as the CIFS sharename.

Condition: This problem occurs when you use either a manifest file or a simple pre-positioned file to map a drive to the pre-positioned content using “global” as the CIFS sharename.

Workaround: Use a sharename other than “global.” If you use any name in the configuration other than “global,” the drive is able to map successfully.
- CSCse05693

Symptom: DNS cache statistics are not updated. The output for the **show statistics dns-cache** command does not reflect the actual statistics of DNS caching; however, the DNS caching occurs without any issues.

Condition: This problem occurs when the request is routed using WCCP. When the Content Engine is used as proxy, the statistics are updated properly.

Workaround: None.
- CSCse24172

Symptom: Some **show** commands disappear from the CLI and stop functioning.

Condition: There is no known condition under which this problem occurs.

Workaround: Reload the Content Engine to restart the parser server.
- CSCsg26390

Symptom: Core files are detected in the dispatcher.

Condition: This problem occurs when the Content Engine is running CSM.

Workaround: None. The Content Engine recovers on its own immediately.
- CSCsi29474

Symptom: The Windows Media managed live program begins one hour later than scheduled or one hour earlier than scheduled.

Condition: This behavior occurs when a program is configured on March 11, 2007 between 1:00 and 7:00 a.m. or on November 4, 2007 between 2:00 and 6:00 a.m. only. This behavior also occurs for programs that are configured on the 2008 daylight savings transition dates and times.

Workaround: During these transition periods, adjust program schedules by one hour to compensate for the time change. For example, if you are configuring the program on March 11, at 6:00 a.m., set the start time in the GUI for one hour earlier. If you are configuring the program on November 4, at 6:00 a.m., set the start time in the GUI for one hour later.

Resolved Caveats in Software Version 5.4.5

This section lists the caveats that have been resolved in software version 5.4.5.

- **CSCsc06562**—The Content Distribution Manager GUI shows confusing license information for a Content Engine that joins a device group without a license.
- **CSCsc41449**—The syslog is filled with kernel-level error messages, such as, assertion `!atomic_read`.
- **CSCsc71063**—The file system on a Network Module running WAFS or ACNS may be corrupted.
- **CSCsc72789**—The ACNS syslog file is flooded with the following level-4 warning messages: `sym0:0:0:phase change 6-7`.
- **CSCsd05772**—Some archive files are not exported from the log directory.
- **CSCsd14159**—The ICAP daemon crashes and produces core files.
- **CSCsd21974**—Changes made to rules in the Content Distribution Manager GUI take a long time to complete.
- **CSCsd47916**—HTTPS request filtering using transparent redirection does not work properly.
- **CSCsd47925**—The `show cdp neighbors` command shows the local host as being on an unknown interface and on port “lo”.
- **CSCsd58836**—HTTPS requests to the HTTPS proxy in the Content Engine are not returned. The browser shows that the page is continuously loading. The TCP traces show that Content Engine accepts the connection and the requests, but it does not return the content.
- **CSCsd78318**—Client proxy requests in a persistent connection are forwarded without modification to the origin server, and responses are not cached.
- **CSCsd91307**—Usernames and user groups are sent with the wrong server names to the ICAP server.
- **CSCsd95164**—The cache process restarts.
- **CSCsd98458**—SSL terminated requests are getting the following error message: `All outgoing Proxy has failed to serve the request`.
- **CSCse02187**—When you configure rules with url-regex patterns and then try to delete the second pattern from the pattern list, the Content Engine deletes the first configured pattern instead.
- **CSCse03969**—The SecureComputing Software “Administration Console” and “Administration Server” are not operating as expected.
- **CSCse08147**—When you try to configure WCCP dynamic services using the GUI, the configuration is sometimes lost in both the GUI and the CLI. When you configure WCCP dynamic services from the CLI, the configuration is reflected in the CLI but not in the GUI.
- **CSCse12310**—The Content Engine closes the connection to the player.
- **CSCse13530**—The Admin GUI for Websense has not been posted in the ACNS 5.4 section. Without the Admin GUI you cannot administer the Websense policies.
- **CSCse15564**—The WMT general settings are overridden when you configure the WMT bitrate outgoing and incoming settings with the maximum value.
- **CSCse19593**—The Content Engine returns a 400 bad request error message on receiving a 304 response with a TCP FIN flag from the server.
- **CSCse21090**—When you try to override the device group configuration using the CLI, the changes you make in the CLI are lost, and the original device group configuration is used.

- **CSCse21312**—Content Engines cannot communicate with the Content Distribution Manager, and they are marked offline.
- **CSCse21373**—Attackers bypass HTTP filtering by using a technique known as HTTP request smuggling.
- **CSCse23710**—The cache process crashes.
- **CSCse26762**—The cache process is coring and restarting.
- **CSCse30677**—The cache process restarts.
- **CSCse32153**—When you configure the standby interface errors field with the maximum value, the errors field in the **show interface standby** command shows a negative value.
- **CSCse34826**—The Content Engine returns a proxy authentication failure.
- **CSCse35943**—The ICAP daemon crashes.
- **CSCse37518**—The **show users** administrative command does not display the privileged level of all users.
- **CSCse39453**—An HTTP GET or HEAD to an ACNS appliance returns the Apache server version and the underlying OS, disclosing information that might be used by an attacker to target the specific version or OS running on the appliance.
- **CSCse43176**—A SCSI error “DEVICE INTERNAL RESET” causes the drive to be removed from the volume and generates error messages.
- **CSCse43723**—The WAE cannot connect to the Cisco 3750 switch, and the WAE link LED lights are off.
- **CSCse45100**—The **show version pending** command displays an error message. The **show version last** command displays nothing.
- **CSCse46645**—The interface shuts down when the **cdm ip** command is already configured with a hostname, and then you enable autoregistration.
- **CSCse51800**—In transparent mode, the status code is logged as 000 when the outgoing proxy is not reachable, the proxy monitor is disabled, and the failure to origin server is not enabled. In proxy mode, the status code is logged as 500.
- **CSCse51849**—When multiple clients connect to the origin server, the IP address seen on the origin server is the IP address of the client that originally established the connection.
- **CSCse57138**—The number of objects shown on the access Content Engine does not agree with the number shown on the parent (forwarder) Content Engine or the Root Content Engine for a particular channel.
- **CSCse61326**—Beginning in calendar year 2007, daylight savings summertime rules may cause ACNS to generate timestamps (such as in syslog messages) that are off by one hour.
- **CSCse62186**—Some of the configurations are lost when you assign and unassign device groups for ICAP servers.
- **CSCse73296**—The ICAP server configurations are lost when you change the aggregate setting from **no** to **yes**.
- **CSCse73311**—When you try to modify the device group configuration a separate entry is created in the GUI.
- **CSCse74534**—When you change the log filename label, an empty log file is created.
- **CSCse82185**—When the primary source fails and the alternate-source URL configured is a multicast stream, the multicast station does not start.

- **CSCse82279**—When the request header length is abnormal, the cache process creates a core dump.
- **CSCse83867**—When the RADIUS key is removed, the Content Engine contacts the RADIUS server with some default key, and the RADIUS server fails to respond.
- **CSCse84251**—The message, “Unknown ICAP error number (out of range, too high)” is shown when the ICAP server resets the connection.
- **CSCse90369**—An SNMP server produced a core dump.
- **CSCse94542**—The **wccp spoof-client-ip** command for HTTPS does not display any data.
- **CSCse99190**—The Samba configuration indicates that it has the ability to perform digital signing when in fact, it does not support it and fails in fetching data from the Windows shares in the Windows 2003 server.
- **CSCsf02694**—The CIFS website is not removed in the CLI when the user deletes the website in the GUI.
- **CSCsf04020**—The cache process crashes when ICAP and failover to origin server is enabled.
- **CSCsf05195**—The device group configuration is not reflected in the Content Engine CLI.
- **CSCsf06645**—Core files are created in the webserver when the Content Engine is reloaded from the Content Engine GUI.
- **CSCsf13428**—The device went into KDB mode.
- **CSCsf16324**—An invalid argument error message is given for valid commands. The following CLI commands fail:

```
wmt multicast station-configuration test failover retry-count
wmt multicast station-configuration test failover retry-interval
```

- **CSCsf17528**—Inetd FTP and TFTP support is needed in the Content Distribution Manager GUI.
- **CSCsf18895**—The **ip default-gateway** command does not get applied in the WAE.
- **CSCsf23063**—The mms_server process produces core files,
- **CSCsf27490**—The mms_server process produces core files,
- **CSCsf30455**—ICAP is restricted to 400 MB of memory on the 566 platform, which is 160 MB less than the actual memory limit for the platform.
- **CSCsf30502**—Both Content Engines in the same location are multicasting.
- **CSCsf30647**—The device group configuration is not reflected in the CLI, and there is ambiguity between the CLI and GUI device group configuration.
- **CSCsf96197**—The Content Distribution Manager GUI loses its hostname when you enter invalid information in the TFTP directory page.
- **CSCsf96355**—A core file is generated.
- **CSCsf97055**—The Cisco Security Response document responds to the multiple security advisories published by the OpenSSL Project.
- **CSCsg01017**—The **clear statistics all** command displays the following error message:

```
CDM1-7326# clear statistics all
Item Not Found. (Error 4)
CDM1-7326# story not found
```

- **CSCsg02290**—Core files are created when you use the **pgmrategen** or **pgmratemon** commands in the ACNS 5.4.3 software.
- **CSCsg02469**—Some requests are not sent through the ICAP server but are directly forwarded to the outgoing proxy.
- **CSCsg02568**—The **show tech-support** command lists irrelevant bypass statistics for the Content Router.
- **CSCsg03573**—WCCP and FTP fields need to be removed from the IP ACL feature page for the Content Router. These fields are not supported in the CLI and should be removed from the GUI.
- **CSCsg04691**—You cannot configure the HTTP proxy to listen on port 8002 when RealProxy service is enabled on the same Content Engine.
- **CSCsg08530**—The **ntlm server domain** global configuration command does not allow you to configure a domain name that starts with a number.
- **CSCsg10276**—ACNS might be susceptible to the following vulnerability: CVE-2006-3747.
- **CSCsg11427**—Failover takes a long time.
- **CSCsg13726**—Transaction log settings from the device group are lost when you assign a device to a device group that has WMT, Real Networks, RTSP, and transaction logs configured.
- **CSCsg13942**—The cache process creates a core dump when authentication is enabled (RADIUS, TACACS, or LDAP) and the client responds with an NTLM header.
- **CSCsg16478**—In the **show wccp gre** command, the Packets Dropped Due to Bad Buckets field is incrementing.
- **CSCsg21479**—When you are using L2 redirect with WCCP, the Content Engine changes the source IP address and the port number on DNS replies.
- **CSCsg24404**—Under rare conditions, the snmpcd process creates a core file on a Content Engine.
- **CSCsg25703**—When you set the Inetd FTP default value from the GUI, the setting is not reflected in the CLI.
- **CSCsg27387**—The webserver generates a core file.
- **CSCsg33927**—ACNS is not using the outgoing interface address as the source of the SNMP trap.
- **CSCsg37345**—The ICAP daemon goes into an overloaded state.
- **CSCsg39174**—The aggregate setting is not disabled when you remove the device group configuration using the CLI.
- **CSCsg39853**—Multicast replication is not occurring properly on 512 and 612 devices with dual interfaces.
- **CSCsg40085**—The cache process does not handle the X-Forwarded-For header properly and generates core files.
- **CSCsg41935**—When a non-cacheable object is being transferred, the Content Engine abruptly closes the destination connection.
- **CSCsg43011**—A clean shut down of WCCP during device reload causes excessive WCCP protocol messages to be exchanged with the Catalyst 6000 switch.
- **CSCsg47105**—When you use the local database method for authentication, you are not able to view more than ten administrators.
- **CSCsg51735**—Downloading the SmartFilter control list fails halfway through the download. The initial download of the SmartFilter control list succeeds, but subsequent downloads fail at about 40 MB.

- **CSCsg55732**—The Cisco Security Response document responds to the multiple security advisories published by the OpenSSL Project.
- **CSCsg56968**—The TCP connection hangs.
- **CSCsg60504**—Several ICAP daemon threads go into a read/select loop and use 100 percent of the CPU.
- **CSCsg63876**—The stream scheduler fails to restart the program, and the program fails to play.
- **CSCsg64978**—Requests are returned with authentication failure.
- **CSCsg65145**—When WCCP with spoofing is enabled and a request is added to the bypass list, in the transaction log the request is marked with a 200 error response instead of a 500 error response.
- **CSCsg65332**—The **show user username** command displays only two entries for the user, whereas the **show http-authcache** command displays all entries for a user.
- **CSCsg65596**—The ACNS 5.5.4-b151 software cannot be loaded on the Content Distribution Manager, Content Router, and certain Content Engines because the image requires 106 sectors, and these devices have only 105 sectors.
- **CSCsg72936**—The cache process crashes when rules related to groupname pattern-list are configured, LDAP authentication is enabled, and the Content Engine runs for a long time.
- **CSCsg73684**—You cannot configure the WAE 7326 to utilize 100 percent of the disk space.
- **CSCsg85798**—The cancel and reset buttons do not work.
- **CSCsg87466**—The output of the **show user username** command is contradictory.
- **CSCsg87468**—The TCP connection cannot utilize the available network bandwidth.
- **CSCsg88293**—When you are using CIFS file sharing, the file /var/log/unexpected.tdb, located on the RAM drive, grows without limits and uses all available space.
- **CSCsg91568**—The rule action **no-url-filtering** is not applied to client requests, resulting in the action not being performed on matching requests.
- **CSCsh05657**—Under rare conditions, the Content Engine reports the following error messages:
WCCP: %CE-WCCP-3-500011: WCCP: Malformed view component-incorrect length.
- **CSCsh07135**—The cache process crashes.
- **CSCsh11650**—The proxy is not accessed when the **use-http-proxy** option is used with the **test-url** command.
- **CSCsh13565**—The **wccp assign-method-strict** configuration does not persist after an upgrade.
- **CSCsh13624**—HTTP monitor will not monitor the configured URL if the Ctrl+C keys are pressed.
- **CSCsh13797**—A 7325A device went into KDB mode during upgrade/downgrade testing.
- **CSCsh16510**—The network CIFS server functionality is not working.
- **CSCsh18781**—When the X-Forwarded-For header contains false information, authentication fails even though you send the credentials.
- **CSCsh12033**—When the X-Forwarded-For header contains false information, an invalid IP address is stored in the authcache.
- **CSCsh20203**—No hash buckets are assigned to the WAE.
- **CSCsh33309**—Packets for existing connections are not returned to the router, but are dropped. The field, “Packets dropped due to bad buckets” is incremented in the output of the **show wccp gre** command.
- **CSCsh36139**—The Content Engine enters KDB mode after randomly shutting down processes.

- **CSCsh53369**—WCCP statistics for non-GRE and non-WCCP statistics keep increasing for no apparent reason.
- **CSCsh53396**—The Catalyst 6500 series switch shows high CPU usage.
- **CSCsh69225**—When WCCP is enabled, the client is bypassed.
- **CSCsh71625**—The cache process produces core files in the xact_done_send_error_msg.
- **CSCsh72641**—TCP connections are broken when a new Content Engine is added to the WCCP group.
- **CSCsh82514**—When a Windows Media managed live program is set to begin after the daylight savings transition date, the program begins one hour later than scheduled.
- **CSCsi26436**—NTLM protected objects are not served when ICAP respmod is enabled.
- **CSCsh57242**—Specific type of prepositioned files fail xs when requested by client. Files that are affected include PDF documents.

Related Documentation

The ACNS documentation set includes the following:

- [Hardware Documentation](#)
- [Software Documentation](#)
- [Online Help](#)

Hardware Documentation

ACNS documentation includes the following hardware guides:

- *Cisco Wide Area Application Engine 512 and 612 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 511 and 611 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 7326 Hardware Installation Guide*
- *Cisco Content Engine 7305 and 7325 Hardware Installation Guide*
- *Cisco Content Engine 511 and 566 Hardware Installation Guide*
- *Cisco Content Engine 510 and 565 Hardware Installation Guide*
- *Cisco Content Engine 500 Series Hardware Installation Guide*
- *Cisco Content Distribution Manager 4630 Hardware Installation Guide*
- *Cisco Content Router 4430 Hardware Installation Guide*
- *Cisco Content Networking Hardware Installation Guide for the Seven-Rack Unit Chassis*
- *Cisco Regulatory Compliance and Safety Information for the Content Networking Product Series*

Software Documentation

ACNS documentation includes the following software guides:

- *Cisco ACNS Software Upgrade and Maintenance Guide, Release 5.x*
- *Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.4*
- *Cisco ACNS Software Command Reference, Release 5.4*
- *Cisco ACNS Software API Guide, Release 5.4*
- *Cisco ACNS Software Program Manager for IP/TV User Guide, Release 5.4*
- *Release Notes for Cisco ACNS Software Program Manager for IP/TV, Release 5.4*

Online Help

The Content Distribution Manager GUI and the Content Engine GUI both have context-sensitive online help that can be accessed by clicking the **HELP** button. ACNS software includes the following online help systems:

- Content Distribution Manager GUI online help system for centrally managed ACNS networks
- Content Engine GUI online help system for locally deployed Content Engines

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0612R)