



Release Notes for Cisco ACNS Software, Release 5.5.5

December 29, 2006

ACNS Release 5.5.5 b4

Revised: March 20, 2008



Note

The most current Cisco documentation for released products is available on Cisco.com.

Contents

This release note contains information about the Cisco Application and Content Networking System (ACNS) 5.5.5 software. This release note contains the following topics:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [New and Changed Information, page 3](#)
- [Design Limitation for ACNS Object Transfers, page 10](#)
- [Caveats, page 10](#)
- [Related Documentation, page 31](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 32](#)



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

© 2006 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; the ACNS software runs on Cisco Content Engines, Content Distribution Manager, and Content Router hardware platforms, as well as Cisco Wide Area Application Engine appliances.

This release note is intended for administrators who will be configuring, monitoring, and managing devices that are running the ACNS 5.5.5 software. This release note describes the new product features, the supported hardware, and the open and resolved caveats regarding the ACNS 5.5.5 software release.

System Requirements

Table 1 shows the hardware platforms supported in each ACNS software release. 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	5.5.5
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
WAE-7326		X	X	X	X	X	X
WAE-512 WAE-612					X	X	X

**Note**

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.

Software Component Versions Supported in ACNS Software

Table 2 describes which integrated 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
ACNS 5.5.5	Version 4.1.1	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), the ACNS software requires a minimum of 1 GB of RAM.

**Note**

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 and Changed Information

This section describes the following new and changed features in the ACNS 5.5.5 software release:

- [Websense 6.2 Support](#)
- [WCCP Layer 2 Return Support](#)
- [New and Changed Commands in the ACNS 5.5.5 Software](#)
- [SmartFilter Version 4.1 Integration](#)

Websense 6.2 Support

The ACNS 5.5.5 release supports URL filtering using an external Websense server with Websense Version 6.2. To configure your Content Engines for Websense URL filtering in a centrally managed deployment, see the “[Using a Websense Enterprise Server](#)” section. To configure your Content Engines for Websense URL filtering in a locally managed deployment, see the “[Configuring Standalone Content Engines for Websense URL Filtering](#)” section.



Note

Websense Version 6.2 is not supported as an integrated feature in the ACNS 5.5.5 software.

For more detailed information about configuring the Websense software, go to the following website: <http://www.websense.com>.

WCCP Layer 2 Return Support

The ACNS 5.5.5 software introduces a new option (**l2-return**) for the **wccp** global configuration command that provides Layer 2 packet return support. The Layer 2 return option allows you to override the default Layer 3 GRE return path; packets are returned from the Content Engine to the WCCP-enabled router at Layer 2 instead.

A Content Engine can reject and return packets in the following typical situations:

- The Content Engine is filtering packets based on certain conditions that make processing packets unproductive, for example, when IP authentication has been enabled.
- The Content Engine has a static bypass list configured on it.
- The Content Engine is overloaded, and the **load bypass enable** command is configured on it.



Note

The Layer 2 return feature is supported in all ACNS devices that support the ACNS 5.5.5 software in Content Engine device mode.

The packet return method can be configured independently of the packet forwarding method. For example, you can configure the following methods for packet forwarding and packet return:

- GRE packet forwarding (Layer 3 redirection) with Layer 2 packet return
- Layer 2 redirection with Layer 2 packet return

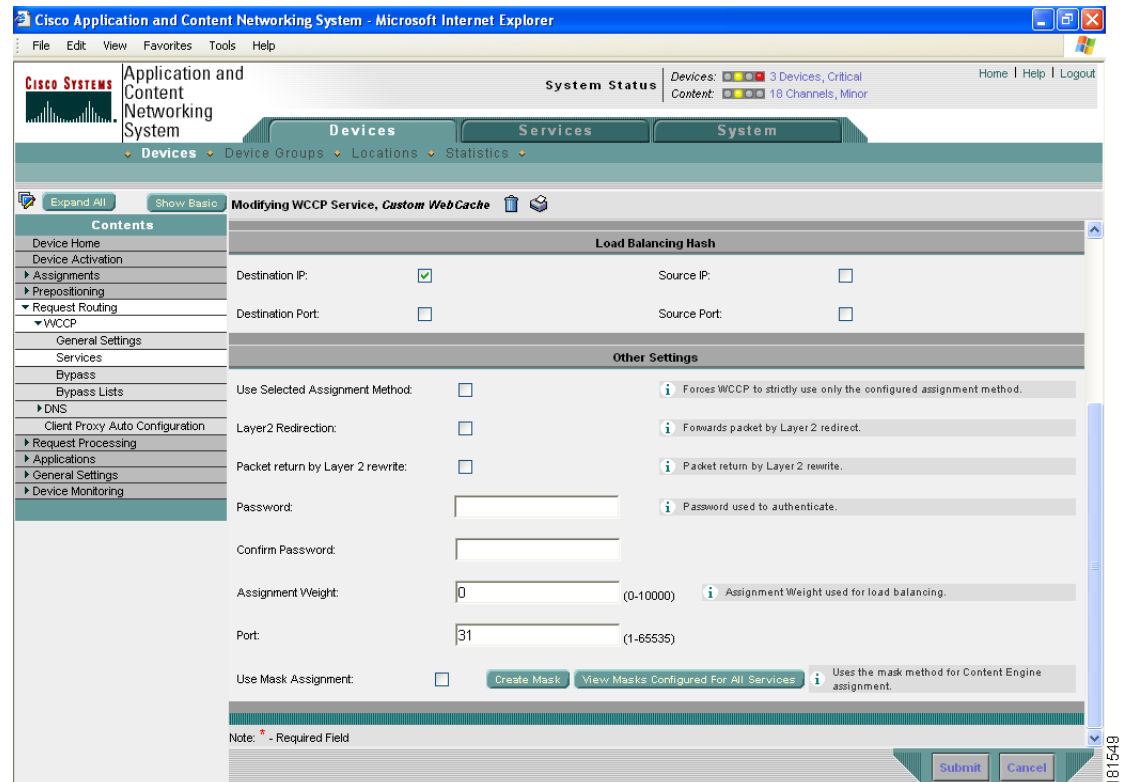
The Layer 2 return option is available for all WCCP services listed in the **wccp** command. Some sample configurations are as follows:

```
WAE(config)# wccp reverse-proxy router-list-num 1 l2-return
WAE(config)# wccp rtsp router-list-num 1 l2-return
WAE(config)# wccp wmt router-list-num 1 hash-source-port l2-redirect l2-return
WAE(config)# wccp ftp-native router-list-num 1 l2-redirect l2-return
WAE(config)# wccp https-cache router-list-num 1 l2-redirect l2-return
WAE(config)# wccp service-number 91 router-list-num 1 port-list-num 1 application cache
l2-redirect l2-return
```

To configure the Layer 2 packet return option from the Content Distribution Manager GUI, follow these steps:

- Step 1** Choose **Devices > Devices (or Device Groups)**. The Devices (Device Groups) window appears, listing all the device types (or device groups) configured in the ACNS network.
- Step 2** Click the **Edit** icon next to the Content Engine (or device group) for which you want to configure WCCP service settings:
 - For single devices, the Device Home for Content Engine window appears.
 - For device groups, the Modifying Device Group window appears.
- Step 3** In the Contents pane, choose **Request Routing > WCCP > Services**. The WCCP Service Settings window appears.
- Step 4** Choose the WCCP service that you want to modify by clicking the **Edit** icon next to the service. Alternatively, you can create a new service by clicking the **Create New WCCP Service Setting** icon in the taskbar.
- Step 5** In the WCCP Service configuration window, enable the Layer 2 return feature by checking the **Packet return by Layer 2 rewrite** check box under the Other Settings heading. (See [Figure 1](#).)

Figure 1 Enabling Packet Return by Layer 2 Rewrite



- Step 6** To disable the Layer 2 return feature, uncheck the **Packet return by Layer 2 rewrite** check box.
- Step 7** To apply your WCCP service settings, click **Submit**.

New and Changed Commands in the ACNS 5.5.5 Software

This section describes the new and changed commands in the ACNS 5.5.5 software release. Changes are described for both the command line interface and the Content Distribution Manager GUI.

Table 3 lists the commands and options that have been added in this release.

Table 3 CLI Commands Added in ACNS 5.5.5 Software

Mode	Command and Syntax	Description
EXEC	core-dump backtrace { all <i>filename</i> }	Generates a backtrace of a given core file. This command applies to cache, FTP, ICAP, and WMT process core files only.
	core-dump service { acquisition authentication cache cms content-routing cse distribution dns ftp icap real-proxy real-server rtspd websense wmt pid number } force	Forces a core dump from the CLI for a particular service. The wmt option requires a process identification number (PID) from 1 to 65535.
EXEC	debug dfs { all api diskcache memcache rawio }	Enables debugging for a specified Diamond File System (DFS) subsection. The command options perform the following actions: <ul style="list-style-type: none"> • all—Enables debugging for all DFS subsections. • api—Enables debugging for the XFS-to-DFS API interface (the top-level application interface to the disk-storage management subsystem). • memcache—Enables debugging statements for in-memory object storage/retrieval and management. • diskcache—Enables debugging statements for on-disk object storage, retrieval, and management. • rawio—Enables debugging statements for raw data block transfers between the DFS disk cache manager and the raw physical disk drivers.

Table 3 CLI Commands Added in ACNS 5.5.5 Software (continued)

Mode	Command and Syntax	Description
EXEC	<p>debug malloc authmod {all caller-accounting catch-double-free catch-free-null check-boundaries check-free-chunks clear-on-alloc statistics }</p> <p>debug malloc cache-app {all caller-accounting catch-double-free catch-free-null check-boundaries check-free-chunks clear-on-alloc statistics }</p> <p>debug malloc dns-server {all caller-accounting catch-double-free catch-free-null check-boundaries check-free-chunks clear-on-alloc statistics }</p> <p>debug malloc icap {all caller-accounting catch-double-free catch-free-null check-boundaries check-free-chunks clear-on-alloc statistics }</p>	<p>Provides informational analysis on a running system that helps identify sources of corruption and memory allocation mismanagement.</p> <p>The memory allocation debugging feature allows you to view the system memory allocation for a particular service and to check or log certain activities for each service.</p> <p>The debug malloc command provides memory allocation debugging for the following services:</p> <ul style="list-style-type: none"> • authmod—Authmod service • cache-app—HTTP cache service • dns-server—DNS caching service • icap—ICAP service <p>The command options perform the following actions:</p> <ul style="list-style-type: none"> • all—Enables all memory allocation debugging options. • caller-accounting—Collects statistics for every distinct allocation call stack. • catch-double-free—Logs any attempt to release unallocated memory. • catch-free-null—Logs any attempt to release a NULL pointer. • check-boundaries—Runs scribble checking for over and under boundaries. • check-free-chunks—Checks if free chunks are overwritten after the release. • clear-on-alloc—Ensures all memory allocations are cleared to zero. • statistics—Provides a summary of use statistics for the service.

Table 3 CLI Commands Added in ACNS 5.5.5 Software (continued)

Mode	Command and Syntax	Description
EXEC	debug malloc log-directory <i>dir_path</i>	Designates a directory pathname for the memory allocation log.
	service { acquisition authentication cache cms cse distribution dns ftp icap real-proxy real-server websense wmt } restart	Restarts a particular service.
	sysreport { acquisition-distribution authentication cms cse dns ftp http https icap real rules url-filter wmt } [date-range <i>start end filename</i>] [<i>filename</i>]	Generates a compression file that contains syslogs for troubleshooting a particular service module. You can specify a date range for the system report. Dates must conform to the yyyy/mm/dd format.
	top [-] [d <i>delay</i>] [p <i>pid</i>] [c] [S] [s] [i] [n <i>iter</i>]	Identifies the specific process that is consuming CPU usage. The top command is a Linux command that is now available in the ACNS software in EXEC mode. All options except the b (batch mode) option are available. The command options perform the following actions: <ul style="list-style-type: none"> • d—Specifies the delay between screen updates. You can change the delay by using the s interactive command. • p—Monitors processes with the given process ID (PID) only. This flag can be used up to 20 times. This option is not available interactively, and it cannot be put into the configuration file. • S—Specifies cumulative mode, where each process is listed with the CPU time that it and its dead children have spent. • s—Specifies secure mode. This option disables the interactive commands. • i—Ignores any idle or zombie processes. • c—Displays the command line instead of the command name only. • n—Specifies the number of iterations. Updates the display a given number of times and then exits.

Table 4 lists the commands and options that have changed in this release.

Table 4 CLI Commands Changed in ACNS 5.5.5 Software

Mode	Command and Syntax	Description
EXEC	<code>show cfs url <i>url</i></code>	Shows whether the specified URL is in the Content Engine cache or not.
	<code>show tech-support list-files <i>dir_name</i> [recursive]</code>	Displays recursive directory information for important directories. This option allows you to display a list of the files and subdirectories in a particular directory. You must use the absolute path for the directory name (for example, <code>/local1/logs</code>).
	<code>show tech-support service {acquisition-distribution authentication cms cse dns ftp http https icap kernel real rules url-filter wccp wmt}</code>	Displays the show tech-support output based on a particular service module.
	<code>debug http advanced {client-ip <i>ipaddress</i> server-ip <i>ipaddress</i>}</code>	Allows debug messages to be filtered based on the IP address.
Config	<code>wccp <i>service_name</i> router-list-num <i>number</i> l2-return</code>	Uses Layer 2 instead of Layer 3 GRE to return packets that are rejected by the Content Engine to the WCCP-enabled router.

SmartFilter Version 4.1 Integration

The plug-in for SmartFilter software Version 4.1 has been integrated with the ACNS 5.5.5 software. This version of SmartFilter has the following features:

- Listens on port 9014 for block page requests.
The ACNS caching process listens on port 9015 for blocked pages and forwards the packets to port 9014 where SmartFilter listens.
- Provides advanced block pages with a new look and feel.
- Provides a new feature called temporary user override. (See the [“About the Temporary User Override Feature”](#) section on page 9.)



Note

To configure SmartFilter Version 4.1 features, you must obtain the SmartFilter Administration Console version 4.1.1, which can be downloaded from the Secure Computing website.

About the Temporary User Override Feature

In the ACNS 5.5.5 software release, the temporary user override is a new feature that is available with the SmartFilter software version 4.1. This feature allows the SmartFilter plugin to override the filtering mechanism that is being applied to the user group to which users have been added in the authentication server (in Step 3). You must configure this new feature through the SmartFilter Administrator Console (version 4.1.1).

To use the temporary user override feature, follow these steps:

-
- Step 1** Install the SmartFilter authentication server software on the machine that is running the SmartFilter Administrator Console or on a different machine.
 - Step 2** From the SmartFilter Administrator Console, add the authentication server.
 - Step 3** From the SmartFilter Administrator Console, add the users to the authentication server.
 - Step 4** Deploy the changes to the authentication server.
 - Step 5** From the SmartFilter Administrator Console, select the Content Engine, and add the configured authentication server to the Content Engine's list of authentication servers.
 - Step 6** From the SmartFilter Administrator Console, add the users who should be allowed to override the filtering mechanism in the overrides for the Content Engine.
 - Step 7** Deploy the changes to the Content Engine.
-

Design Limitation for ACNS Object Transfers

By design, ACNS software does not handle the transfer of objects larger than 2 GB. When an object transfer reaches the 2-GB limit, the Content Engine closes the connection to both the client and the server.

Caveats

This section lists and describes the new, open, and resolved Severity 1, 2, and 3 caveats in the ACNS 5.5.5 software. Caveats describe unexpected behavior in the ACNS 5.5.5 software. Severity 1 caveats are the most serious; Severity 2 caveats are less serious. Severity 3 caveats are moderate caveats.

This section contains information about the open and closed caveats:

- [Open Caveats—ACNS 5.5.5 Software](#)
- [Resolved Caveats—ACNS 5.5.5 Software](#)

Open Caveats—ACNS 5.5.5 Software

This section lists caveats that have not been resolved in the ACNS 5.5.5 software release. The open caveats are grouped into the following categories:

- [Windows Media Open Caveats, page 11](#)
- [Other Open Caveats, page 15](#)

Windows Media Open Caveats

- CSCeg86386

Symptom: In a Content Router environment, you cannot choose RTSPU (UDP) or RTPST (TCP) when you request rtspu:// or rtspt:// from Windows Media Players. In addition, when you request an RTSPU stream, an RTSPT stream is returned instead. Also, when you specify the **wmt disallowed-client-protocols rtspu** global configuration command, it does not prevent clients from being served for a request rtspu://crfqdn/file.asf and returns an RTSP stream instead of an error.

Condition: This problem can occur if you use a Content Router for RTSP redirection.

Workaround: The restricted protocol cannot be played; however, as a partial solution, another protocol is chosen instead of returning an error message. We are working to provide a complete solution to this issue.
- 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 you use Microsoft presenter 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, choose publish to **My Computer**. When you choose 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.
- CSCsd63199

Symptom: Camiant server request validation fails for live content when the URL is requested again.

Condition: This problem occurs when the .asx URL is requested again without the browser cache being cleared.

Workaround: Clear the browser cache after every request.
- CSCsd75279

Symptom: The RTSP request fails.

Condition: This problem occurs when the publishing point on a Windows Media server is a URL to source content published on a Content Engine, and the Windows Media server is requesting the content using an RTSPU URL (rtspu://).

Workaround: For the above configuration, Microsoft recommends using RTSPT as the protocol for the URL to the remote source (rtspt://).
- CSCsd92288

Symptom: The IXIA Windows Media load tool client does not interoperate with ACNS 5.5.x WMT using RTSP.

Condition: IXIA Windows Media load tool clients are not compatible with the ACNS 5.5.x software because the ACNS 5.5.x software does not start sending RTP packets until after it receives the RTSP SET_PARAMETER logconnectstats. The problem does not occur with Windows Media Players because Windows Media Players send the connectstats.

Workaround: Use IXLoad version 3.10 software to allow IXLoad media clients to generate WMT traffic to RealMedia servers. You must configure each IXLoad WMT client manually to set the appropriate parameters.

For example, use the SET_PARAMETER command that was introduced in IXLoad 3.10 to add the set parameter into the client IXLoad stream, and use Option1 as the argument. The IXLoad client will connect to an RTSP Windows Media server and request the content through a Content Engine.

Contact your IXIA support specialist for further IXIA IXLoad support information.

- CSCsd98883

Symptom: The RTSPU disallowed counter, in the output of the **show statistics wmt error** command, does not get incremented when RTSPU is disallowed on the Content Engine. However, the RTSPU request will be blocked.

Condition: This problem occurs with some versions of Windows Media Players 9 and 10.

Workaround: This problem affects statistics only; it does not affect functionality. We are working to resolve this problem.

- CSCsd98892

Symptom: The live splitting statistics in the output of the **show statistics wmt savings** command do not get incremented for broadcast-alias requests.

Condition: This problem occurs only when the broadcast alias is configured with a video on demand (VoD) or a proxy source.

Workaround: There is no known workaround at this time. We are working to resolve this problem.

- CSCsd99435

Symptom: Windows Media Player displays “Attempting to reconnect” when playing server-side playlists that contain multi-bit-rate (MBR) streams using RTSP.

Condition: When playing a server-side playlist using RTSP, the Windows Media Player requests an MBR stream switch because of insufficient bandwidth and then later requests the next entry in the server-side-playlist.

Workaround: Start the play again.

- CSCsd99636

Symptom: More outgoing bandwidth is consumed than expected.

Condition: This problem occurs when Fast Cache (FC) is enabled on the client and on the Content Engine. Because FC is supported only for cache-hit cases, the outgoing bandwidth should be calculated with consideration for FC for cache-hit cases only. (Outgoing bandwidth is calculated with consideration for FC because data is sent at a higher rate when FC is enabled on the client and on the Content Engine.) However, this problem occurs because the outgoing bandwidth is being calculated with consideration for FC even for cache-miss cases.

Workaround: There is no known workaround. The bandwidth allocation is reset as soon as playback ends for that stream.

- 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: Use a QuickTime player instead of a PacketVideo player.

- CSCse00701
Symptom: Outgoing bytes are not getting incremented in a timely fashion.
Condition: Outgoing byte statistics are incremented in the CLI only when control events (such as pauses or stops) occur on active streams. This condition occurs during VoD, proxy, or live playback for Windows Media streams.
Workaround: Click any control event, such as pause, and then view the bytes being incremented by using the **show statistics wmt bytes outgoing** EXEC command.
- CSCse02533
Symptom: The remote HTTP source counter increments for the multicast-in source.
Condition: When a multicast-in source is used for a broadcast alias in the Content Engine, then the By Source of Content field in the **show statistics wmt requests** command output shows the remote HTTP counter incrementing instead of the multicast counter. This condition is seen in the ACNS 5.5.x software.
Workaround: There is no known workaround. This problem does not impact the performance of this product. We are working to resolve this problem in a future release.
- CSCse06358
Symptom: Even when a multicast station is removed from the Content Engine, the Current field of the Number of Concurrent Active Multicast Sessions section in the **show statistics wmt multicast** command output shows a value. The field is not cleared even after you enter the **clear statistics wmt** command. This problem does not affect the core functionality.
Condition: This condition can occur when a multicast station is stopped and removed from the Content Engine.
Workaround: There is no known workaround at this time. We are working to resolve this problem.
- CSCse07034
Symptom: The incoming bandwidth does not restrict the multicast source.
Condition: This condition occurs when an RTSP source is directed to the multicast station.
Workaround: An HTTP source can be used for the multicast station.
- CSCse07737
Symptom: The outgoing bytes keep incrementing.
Condition: When a multicast station is started and stopped quickly 10 times or more, the Outgoing Bytes field of the **show statistics wmt multicast** command keeps incrementing even though multicasting is stopped. Also, the Aggregate Multicast-out Bandwidth field is not cleared until the WMT program is restarted.
Workaround: Avoid rapid multiple starts and stops during a WMT multicast program.
- CSCse07977
Symptom: The Windows Media Player stays in the buffering state.
Condition: A stream encoded with video only is played using RTSPU (that is, either the URL is `rtspu://` or the URL is `rtsp://`), and the player advanced statistics indicate that the protocol in use is RTSP (UDP).
Workaround: Use the RTSPT protocol as the protocol for the URL (`rtspt://`).

- CSCse08370
Symptom: The Windows Media Player stays in the buffering state and then disconnects.
Condition: In a very high-latency network (>100 ms), when playback is over RTSP (UDP) for a multi-bit-rate stream, retransmission requests can lag behind and cause this problem.
Workaround: Request the file stream again. Reduce the latency in your network. Use rtsp:// in the URL.
- CSCse12809
Symptom: The Content Engine sends a 500 error message to one of the clients during a live split of a managed live unicast program.
Condition: This error occurs when the source for the program is an SSPL.
Workaround: The user on the client that receives a 500 error message should request the program again.
- CSCse15691
Symptom: The incoming bandwidth usage statistics for broadcast server-side-playlists continue to increment.
Condition: This problem is seen when there are more than 100 requests for a server-side-playlist that switches streams every 1 minute. This condition is not seen for a lower number of requests.
Workaround: There is no known workaround at this time. We are working to resolve this problem.
- CSCse16536
Symptom: The player goes into the buffering state and hangs.
Condition: This problem occurs during a multicast-in-multicast-out play forever program after the end of the first loop.
Workaround: Use the encoder source content instead of the VoD content.
- CSCse17190
Symptom: The Windows Media Player attempts to reconnect when it reaches an end of stream (EOS) of the broadcast alias.
Condition: This condition occurs only when a multicast stream is used as the source for the broadcast alias in the Content Engine.
Workaround: Use unicast instead of multicast as the source for your broadcast alias. We are working to resolve this problem.
- CSCse21472
Symptom: The Content Engine appears to be in a hung state and does not respond to ping, Telnet, or to requests.
Condition: This condition occurs when a Content Engine receives 200 live-splitting requests for a combination of fast-switching server-side playlists that have streams switching every 1 minute and that have their multi-bit-rate encoder source encoded with 8 different bit rates.
Workaround: Stop incoming requests from clients. If the software does not recover, reload the Content Engine.

- CSCsf97988
Symptom: The wmt_be process generates a core file during the server_parse phase.
Condition: This problem occurs during VoD stress testing for pass-through content when you use the Windows Media load simulator.
Workaround: There is no known workaround. If this problem occurs, save the core files and the WMT error logs to assist TAC in further debugging the problem.
- CSCsh15218
Symptom: The wmt_be process generates a core file.
Condition: This problem occurs during stress testing of a managed live unicast out-only program with a live SSPL source.
Workaround: There is no known workaround. If this problem occurs, save the core files and the WMT error logs to assist TAC in further debugging the problem.
- CSCsh16683
Symptom: The wmt_be process hangs in the read phase, and outgoing bandwidth is not fully released.
Condition: This problem occurs during proxy VoD stress testing after two to three hours of testing.
Workaround: Use the **clear wmt incoming (outgoing)** command to clear the session.
- CSCsh21894
Symptom: The wmt_be sessions are not exiting properly, and outgoing bandwidth is not released.
Condition: This problem occurs during proxy VoD stress testing when you use the Windows Media load simulator.
Workaround: Use the **clear wmt incoming (outgoing)** command to clear the session.

Other Open Caveats

- CSCdy82311
Symptom: Content cannot be acquired using strong authentication from secure origin servers that use certificates from nonstandard certificate authorities (CAs). If strong authentication was chosen for content acquisitions from such a site, the acquirer error statistics will contain a 401 (Unauthorized) error code, and the acquirer error log contains 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.



Note 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 (for example, a certificate has expired, certificate is not yet valid, and a subject issuer mismatch has occurred) are allowed during certificate verification.

Workaround: Use one of these workarounds:

- Use weak authentication.
- On the secure server, use a certificate that was generated by one of the standard certificate authorities. ACNS network administrators should refer to the following information to determine which CA certificate to install on their origin servers. Note that the certificate list differs based on the version of the ACNS software. For the ACNS 5.1.x software release or later, refer to the certificate list in the *Cisco ACNS Software Upgrade and Maintenance Guide, Release 5.x*.

- 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 is observed.

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.



Note The Storage Array device is used for the cache file system (cfs).

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

- CSCed68727

Symptom: The Content Distribution Manager only checks if coverage zone files refer to invalid Content Engines after there is a fresh import. When there is a configuration change that can cause already 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 if there is a coverage zone configuration change that causes already-imported coverage zone files to refer to invalid Content Engines.

Workaround: Whenever the hostname of a Content Engine is changed or the Content Engine is removed from the network, the current information about the device has to be updated in the corresponding coverage zone file or files.

- 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 where SNMP traps are coming from.

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. You 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 type 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.
- 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 is longer than 50 characters.

Workaround: For NTLM authentication, use a domain controller (DC) that has a domain name shorter than 35 characters.
- CSCee90245

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

Condition: This problem occurs very rarely. In very rare situations, even though you entered the **no ntlm server enable** global configuration command to disable NTLM proxy authentication on the Content Engine, NTLM proxy authentication is still not turned off. In such cases, NTLM authentication can still occur, although the output of the **show running EXEC** command shows that the NTLM server is not enabled on the Content Engine.

Workaround: Enter the **no ntlm server enable** global configuration command again 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 can occur 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: Currently, we do not have a workaround for this problem. This problem has not been seen in any of our customer sites; the scenario was assumed by our testing team in an attempt to support this scenario in future releases based on the need.
- 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 only when the ICAP service is enabled on the Content Engine.

Workaround: Currently, we do not have a workaround for this problem. This problem has not been seen in any of our customer sites; the scenario was assumed by our testing team in an attempt to support this scenario in future releases based on the need.

- CSCef60282

Symptom: Even though you entered a **write memory** command, after an immediate reload, a prompt appears that the configuration has been changed.

Condition: This problem occurs if the following conditions are met:

- You have enabled Websense on the Content Engine.
- The IP address of the Content Engine is removed or changed.
- You enter a **write memory** command on the Content Engine.
- You 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.

- 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 can occur in the following condition:

- a. You have specified values in the Client Proxy Autoconfig Device Group window of the Content Distribution Manager GUI.
- b. You override these values through the Client Proxy Autoconfig Device window of the Content Distribution Manager GUI.
- c. You revert the Content Engine back to the device group settings (you click the **Force device group settings** button in the device group window or you select 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.
```

This situation can occur under the following circumstances:

- 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.

Condition: This problem occurs only when there is a slow connection between the Content Distribution Manager and your browser and you perform any of the unsupported actions described above.

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.

- CSCeg56075

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

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

Workaround: Set the reconnect as manual instead as 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: There is no known workaround. This problem does not occur with non-IE client browsers.

- CSCeg84004

Symptom: NTLM authentication for a valid user may take a longer period than usual (approximately two minutes) if the client sends the request when the Content Engine has been idle for a long period of time.

Condition: This problem can occur in the following condition:

- NTLM request authentication is enabled on the Content Engine.
- The request is sent after the Content Engine has been idle for a long period of time.
- The client machine has some 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 as follows:

```
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.

- 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, which contains 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, which is available 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 only occurs under the following condition:

- You are trying to install the ACNS software image on a CE-7326.
- 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.

- CSCei01668

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

Condition: This problem can occur if 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 inside with a source port of TCP 8999 going to the NAT address of the clients.

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

```

- CSCei28716

Symptom: The system crashes and there are kernel core dumps.

Condition: This problem occurs very rarely.

Workaround: No workaround is required because the Content Engine will reboot and the system will work normally after the reboot.

- CSCsb69794

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

Condition: The problem can 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 can occur when the content has been pre-positioned on the Content Engine.

Workaround: Although we do not have a workaround, we are working to fix this issue.

- 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.

- 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 in the following situation. 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 can 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 if you enter the **no rule enable** command and then 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: Reload the Content Engine.

- 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 actual 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.

- 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 can occur 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 can occur in the following situation. 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: There is no known workaround. You must upgrade to a version of ACNS 5.4.x software in which this issue has not been seen.

- CSCsd66331

Symptom: The DNS pin of a host does not take effect on the Content Engine until you reload the DNS caching service on the Content Engine.

Condition: This problem occurs when the DNS pin configuration has been changed but the DNS queries do not reflect the configuration changes.

Workaround: Disable and enable the DNS cache on the Content Engine.

- CSCsd69768

Symptom: The Content Engine does not reflect a change in the IP address of the HTTPS server host.

Condition: This problem occurs when you have changed the IP address for the HTTPS server host FQDN in the DNS server after the HTTPS server host FQDN has been configured to resolve to an IP address on the Content Engine.

Workaround: Enter the **https server server_name host FQDN** global configuration command on the Content Engine after you have modified the IP address that corresponds to the HTTPS server host FQDN on the DNS server.

- CSCsd72312

Symptom: Before sending a request to the Internet Content Adaptation Protocol (ICAP) server, the Internet Content Adaptation Protocol (ICAP) client contacts the DNS.

Condition: This problem occurs when the ICAP feature has been enabled.

Workaround: Although we do not have a workaround, we are working to fix this issue.
- CSCsd82649

Symptom: The Content Engine may skip audio and video streams in MPEG2 files.

Condition: This problem occurs in the Content Engine running ACNS versions later than 5.1.9.5.

Workaround: Downgrade to the ACNS 5.1.9.5 software.
- CSCsd87378

Symptom: The Content Engine is unable to use a Common Internet File System (CIFS) sharename called global and responds with this error message:

```
Network name cannot be found
```

Condition: This problem occurs when you try to map a drive to the pre-positioned content for a manifest file or a simple pre-positioned file with a Common Internet File System (CIFS) sharename called global.

Workaround: Use any other Common Internet File System (CIFS) sharename except global.
- CSCse05693

Symptom: The **show stat dns-cache** CLI command does not reflect the statistics of the DNS caching.

Condition: This problem occurs when the request is routed through WCCP and the **dns-cache statistics** command is not updated. The statistics are updated when the Content Engine is used as a proxy.

Workaround: Although there is no known workaround, we are working on a solution to update the statistics in WCCP mode.
- CSCsg8356

Symptom: RTSP requests to the Content Router return an RTSP 404 error message. The media file fails to play in the player, and the player displays an error message.

Condition: This problem occurs when the Content Router has more than 100 Content Engines registered in the ACNS network.

Workaround: No workaround is possible with the single Content Router. You must add an additional Content Router to balance the load.
- CSCsh46848

Symptom: The Content Engine cache process restarts continuously and creates core dumps.

Condition: This problem occurs when you have ACNS 5.5.5 software on a Content Engine with an external storage array and a CFS partition size that is greater than 440 GB. This defect is not seen on Content Engines running ACNS software prior to the 5.5.5 release. Neither is this defect seen on Content Engines running ACNS 5.5.5 software that are using the internal disk drives because the maximum CFS partition size for internal disks is 384 GB.

Workaround: Reduce the CFS partition size to less than 440 GB.

- CSCsh33309
Symptom: 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.
Condition: This problem occurs when you have multiple Content Engines in the farm with a redirection policy mask assigned, a mask value of 0xfd, and a static bypass list configured. The incoming requests are matching the configured bypass list.
Workaround: Configure a different mask value.

Resolved Caveats—ACNS 5.5.5 Software

This section lists the caveats that have been resolved in the ACNS 5.5.5 software release. The resolved caveats are grouped into the following categories:

- [2007 Daylight Savings Time Compliance, page 25](#)
- [Acquisition, page 25](#)
- [Cache, page 25](#)
- [CLI, page 26](#)
- [CMS, page 26](#)
- [Content Engine, page 26](#)
- [Disk, page 27](#)
- [Distribution, page 27](#)
- [GUI, page 27](#)
- [HTTP, page 27](#)
- [HTTPS, page 27](#)
- [ICAP, page 28](#)
- [Logs, page 28](#)
- [Program Manager, page 28](#)
- [RealProxy, page 28](#)
- [RTSP, page 28](#)
- [Rules, page 29](#)
- [SmartFilter, page 29](#)
- [SNMP, page 29](#)
- [SSL, page 29](#)
- [URL Filtering, page 29](#)
- [Websense, page 29](#)
- [WMT, page 30](#)

2007 Daylight Savings Time Compliance

- CSCse61326
Symptom: Starting in calendar year 2007, daylight savings summer-time rules may cause ACNS to generate timestamps (such as in syslog messages) that are off by one hour.

Acquisition

- CSCse87989
Symptom: The Manifest Validator does not show the error and warning messages after 1000 lines of debug error message text.

Cache

- CSCsd78318
Symptom: In a persistent connection, the responses to the client proxy requests are not cached and are forwarded without modification to the origin server.
- CSCse04147
Symptom: The max-obj-size limiting has failed.
- CSCse14327
Symptom: The Content Engine proxy returns a 400 bad request error message.
- CSCse19593
Symptom: The Content Engine returns a 400 bad request error message on receiving a 304 response with TCP FIN from the server.
- CSCse21941
Symptom: The service “rpc_httpd” stops, and the following message is displayed in the syslog file:

```
%CE-NODEMGR-3-330025: Service 'rpc_httpd' died due to signal 25: File size limit exceeded %CE-NODEMGR-5-330032: Stopping service: 'rpc_httpd'.
```
- CSCse23710
Symptom: The cache process crashes.
- CSCse46706
Symptom: The cache process stops and crashes continuously without serving requests.
- CSCse51849
Symptom: 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.
- CSCse56693
Symptom: Multiple cache cores are seen when ICAP is enabled.
- CSCse82279
Symptom: Core files are created when the header length is abnormal and contains multiple E tags.
- CSCsg13942
Symptom: The cache process crashes when RADIUS, TACACS, or LDAP authentication is enabled, and the client responds with an NTLM header.

- CSCg40085
Symptom: The cache process does not handle X-Forwarded-For headers properly and creates core files.

CLI

- CSCsg08530
Symptom: The **ntlm server domain** global configuration command does not allow domain names that start with a number.

CMS

- CSCsc97711
Symptom: The default value for the **wmt max-concurrent-sessions** command does not appear in the running configuration.
- CSCse21312
Symptom: Content Engines are marked as offline because they cannot communicate with the Content Distribution Manager. Content Engines cannot authenticate the Content Distribution Manager when they try to establish an SSL session.
- CSCse41396
Symptom: The primary Content Distribution Manager configuration shows the configuration for the standby Content Distribution Manager. The standby Content Distribution Manager might lose network connectivity.
- CSCse49236
Symptom: The Content Distribution Manager GUI accepts a bandwidth rate that is greater than 180 Mbps for the CE-590. If you enter a value that is greater than 180 Mbps, the CLI will fail in the CE-590, and the configuration will be removed from the GUI the next time that the Content Distribution Manager requests a full device statistics update from the CE-590 Content Engine.

Content Engine

- CSCsc19566
Symptom: A Content Engine can hang or go into kernel debug mode if the kernel debug feature is enabled on the Content Engine.
- CSCsc81507
Symptom: The Content Engine may lose the configured routes.
- CSCsd90763
Symptom: The Content Engine stops functioning.
- CSCsd95049
Symptom: A core file for the `exec_show_running-config` process exists in the `/local1/core_dir` directory, and a major alarm is seen in the Content Distribution Manager GUI or in the Content Engine CLI when you enter the **show alarm** command.

Disk

- CSCsc13494
Symptom: A disk is marked as “bad” when a disk error threshold is reached after a transient disk failure.

Distribution

- CSCse07773
Symptom: Acquisition and distribution processes leave a log and restart when the maximum amount of memory is exceeded.
- CSCsg02290
Symptom: Core files are created when you enter the **pgmrategen** or **pgmratemon EXEC** commands.
- CSCef93883
Symptom: The multicast connectivity test tool cannot use the second network interface.

GUI

- CSCsd21974
Symptom: When you change or modify a rule from the Content Distribution Manager GUI, you experience a considerable delay before the changes take effect.
- CSCse21542
Symptom: When multiple outgoing proxies are listed through the GUI, the actual CLI written to the Content Engine is different from what was entered in the GUI.
- CSCsc44106
Symptom: The configured rules for a device group are randomized when they are applied to the Content Engine that joins the device group.

HTTP

- CSCse39453
Symptom: The number of Apache server versions or modules disclosed is limited.
- CSCse39881
Symptom: The HTTP anonymizer causes blank pages or extra characters at the top or bottom of a web page to appear.

HTTPS

- CSCsd58836
Symptom: The Content Engine accepts the TCP connection but does not respond to HTTPS requests. The browser will appear to be loading the HTTPS request.

- CSCse94542
Symptom: HTTPS requests are not served properly when the **wccp spoof-client-ip** command is enabled.

ICAP

- CSCsd14159
Symptom: The ICAP daemon crashes and produces core files.
- CSCse26956
Symptom: Large file downloads fail when ICAP is enabled.
- CSCse41883
Symptom: The running configuration randomly loses some configured ICAP servers that are present in the startup configuration.
- CSCse84251
Symptom: A 502 error message, “Unknown ICAP error number (out of range, too high)” is seen.

Logs

- CSCsd05772
Symptom: When you export log files from the archive to an external server using FTP, some of the log files are not exported.
- CSCse40191
Symptom: Translog does not work when the compression option is enabled.

Program Manager

- CSCse73495
Symptom: The Program Manager returns an ‘Invalid Audio/Video Bandwidth’ error when you try to configure an MPEG file-based scheduled program.

RealProxy

- CSCsg04691
Symptom: You cannot configure HTTP proxy on port 8002 when RealProxy service is enabled on the same Content Engine.

RTSP

- CSCse18576
Symptom: The URL signature validation fails for a Camiant server RTSP request.
- CSCse18874
Symptom: Windows Media RTSP does not work.

Rules

- CSCsd27100
Symptom: A memory allocation library that can track memory leaks is needed in the code base.

SmartFilter

- CSCsd58287
Symptom: When you enable SmartFilter, the Central Processing Unit (CPU) indicates 100 percent usage.
- CSCse22425
Symptom: The Content Engine enters the kernal debugger mode.

SNMP

- CSCsb95697
Symptom: The SNMP client is experiencing counters and gauge values of zero.

SSL

- CSCsg10276
Symptom: The ACNS software is susceptible to the following security vulnerability: CVE-2006-3747.

URL Filtering

- CSCsd47916
Symptom: The HTTPS traffic that uses transparent redirection is not filtering properly.
- CSCsf06645
Symptom: A core file is created in the webserver when the Content Engine is reloaded from the Content Engine GUI.
- CSCsg27387
Symptom: The Content Engine reloads and creates a core file when a URL is passed to SmartFilter.

Websense

- CSCsc75289
Symptom: Usernames are not being used by the Websense Network Agent for user-based policy filtering.

WMT

- CSCeh38741
Symptom: The Windows Media Player is not able to stream content for more than one hour in the case of a cache hit.
- CSCse05481
Symptom: The Duration field in the **show statistics wmt streamstat** command output shows a large value for some of the streams.
- CSCse09222
Symptom: The Windows Media Player plays the stream without a problem. However, the **show statistics wmt streamstat** command shows that the bandwidth consumption is 0 (zero) and that the stream is in the TEARDOWN state. Also, the bandwidth used by this stream is not counted in the bandwidth consumption statistics, even though the bandwidth is being used. After the user stops playing the stream, no further impact is seen.
- CSCse12607
Symptom: The WMT server process crashes and causes temporary service disruption. This problem occurs under stress conditions when a large number of simultaneous requests for VoD files are sent.
- CSCse14195
Symptom: A core file has been seen while running stress testing for server-side play lists (SSPL) with multi-bit-rate (MBR) live content.
- CSCse14384
Symptom: The cache-hit counter in the output of the **wmt statistics** command does not increment.
- CSCse15623
Duplicate of CSCse09222.
- CSCse16525
Symptom: The incoming bandwidth usage statistics (viewed by using the **show statistics wmt usage** command) are incremented for every stream switch made by the live stream. The Content Engine also continues to pull old bit rate selections of the live stream and new bit rate selections, in anticipation of the need to split the stream for new clients requesting the older bit rate selection.
- CSCse16537
Symptom: The Windows Media Player enters the waiting state after a play/pause/play sequence of control events. This problem is seen only when the HTTP protocol is used for a live publishing point hosted on the Windows Media Server.
- CSCse48068
Symptom: RTSP live requests fail when the publishing point contains a forward slash (/) in the name.
- CSCse73398
Symptom: URLs with a colon (:) character in the query string cause Window Media managed live core dumps.
- CSCse74668
Symptom: An HTTP transaction log for a long filename causes a core dump.

- CSCsf05668
Symptom: a null pointer access error causes a core dump on the Content Engine when WMT streams are playing.
- CSCsg01291
Symptom: Unicast stream splitting with ACNS 5.5.1 and WMP V8 does not work.
- CSCsg06844
Symptom: Bandwidth errors occur when a client requests streaming content.
- CSCsg47285
Symptom: WMT license limits are being reached because idle streams are not being cleared.

Related Documentation

Your product shipped with a minimal set of printed documentation. The printed documentation provides enough information for you to install and initially configure your product.

Product Documentation Set

In addition to this release note, the following documents are included in the product documentation set:

- *Documentation Guide and License and Warranty for Cisco ACNS Software, Release 5.5.x*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*

Refer to the *Documentation Guide and License and Warranty for Cisco ACNS Software, Release 5.5.x* for a complete documentation roadmap and URL documentation links for this product.

Hardware Documentation

- *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*

Software Documentation

- *Cisco ACNS Software Upgrade and Maintenance Guide, Release 5.x*
- *Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.5*
- *Cisco ACNS Software Command Reference, Release 5.5*
- *Cisco ACNS Software API Guide, Release 5.5*
- 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

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



Note

The term *locally deployed Content Engine* refers to a Content Engine that was initially configured with the autoregistration feature turned off so that the Content Engine would not automatically register with the Content Distribution Manager. Because the Content Engine did not register with the Content Distribution Manager, it can be individually managed through the Content Engine CLI or GUI as a locally deployed device. The Content Engine GUI allows you to remotely configure, manage, and monitor locally deployed Content Engines through your browser.

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.

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>

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0812R)

© 2006, 2007 Cisco Systems, Inc. All rights reserved.