



# Release Notes for Cisco ACNS Software, Release 5.3.3

---

August 4, 2005

ACNS Build 5.3.3-b7



**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

These release notes contain information about the Cisco Application and Content Networking System (ACNS) 5.3.3 software. These release notes describe the following topics:

- [Introduction, page 2](#)
- [New and Changed Information, page 2](#)
- [Important Notes, page 12](#)
- [Caveats, page 15](#)
- [Documentation Updates, page 40](#)
- [Related Documentation, page 42](#)
- [Obtaining Documentation, page 43](#)
- [Documentation Feedback, page 44](#)
- [Cisco Product Security Overview, page 45](#)
- [Obtaining Technical Assistance, page 46](#)
- [Obtaining Additional Publications and Information, page 47](#)



---

**Corporate Headquarters:**

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

Copyright © 2005 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.

These release notes are intended for administrators who will be configuring, monitoring, and managing devices that are running the ACNS 5.3.3 software. These release notes describe the new product features, the supported hardware, and the open and resolved caveats regarding the ACNS 5.3.3 software release.

## New and Changed Information

This section describes new and changed features in the ACNS 5.3.3 software release. It also lists the supported hardware.

## New Features in the ACNS 5.3.3 Software

This section describes the new features in the ACNS 5.3.3 software release and includes the following sections:

- [Introduction of the Wide-Area Application Engine, page 3](#)
- [Restoring Factory-Default Settings for Real Networks License Keys, page 3](#)
- [Enhancements to the Envivio-Cisco Streaming Engine Interoperability, page 4](#)
- [Support of Dynamic Content Routing, page 5](#)
- [Configuring TCP Memory Limits, page 8](#)
- [New Rule Command for Converting Hostnames to IP Addresses, page 9](#)
- [Modified Output of the show programs EXEC Command, page 10](#)

## Introduction of the Wide-Area Application Engine

The Wide-Area Application Engine (WAE) is an integrated hardware platform that provides a comprehensive set of services for the remote office. The WAE platform operates with either the ACNS or the Wide Area File Services (WAFS) software. When the ACNS software is installed, the WAE functions as a Content Engine or one of the other ACNS device modes, such as Content Router or Content Distribution Manager. When the WAFS software is installed, the WAE functions as a File Engine.



### Note

The ACNS 5.3.3 software supports three new WAE appliances: the WAE-511, the WAE-611, and the WAE-7326. The software shows the device as a CE-511, CE-611, or a CE-7326. For a complete list of the supported hardware, refer to the [“Hardware Supported” section on page 11](#).

In the ACNS 5.3.3 software, the Content Distribution Manager GUI supports Windows Media license keys and Real Networks Proxy and Subscriber license keys for the CE-511, the CE-611, and the CE-7326 in the following device group license settings windows:

- Devices > Device Groups > Applications > Streaming > Window Media > License
- Devices > Device Groups > Applications > Streaming > Real Networks > Real Proxy License
- Devices > Device Groups > Applications > Streaming > Real Networks > Real Subscriber License

## Restoring Factory-Default Settings for Real Networks License Keys

In the ACNS 5.3.3 software release, the ability to use the CLI or the Content Distribution Manager GUI to restore the Real Networks (RealProxy and RealSubscriber) license key settings to the factory defaults was added.

To restore the factory-default settings for RealProxy:

- From the Content Distribution Manager GUI, click the new Restore all files to factory defaults icon (see [Figure 1](#)) in the following two Content Distribution Manager GUI windows:
  - Devices > Devices > Applications > Streaming > Real Networks > Real Proxy License
  - Devices > Device Groups > Applications > Streaming > Real Networks > Real Proxy License

**Figure 1** *Restore Factory Defaults Icon in the Content Distribution Manager GUI*



- From the CLI, enter the new **rtsp real-proxy restore factory-default** EXEC command.

```
CONTENTENGINE# rtsp real-proxy restore ?
factory-default Restore real proxy configuration file and databases to default
```

To restore the factory-default settings for RealSubscriber:

- From the Content Distribution Manager GUI, click the new Restore all files to factory defaults icon in the following two Content Distribution Manager GUI windows:
  - Devices > Devices > Applications > Streaming > Real Networks > Real Subscriber License
  - Devices > Device Groups > Applications > Streaming > Real Networks > Real Subscriber License
- From the CLI, enter the new **rtsp real-subscriber restore factory-default** EXEC command.

```
CONTENTENGINE# rtsp real-subscriber restore ?
factory-default Restore real subscriber configuration file and databases to default
```

In the ACNS 5.3.3 software release, the **rtsp real-proxy default-configuration** and the **rtsp real-subscriber default-configuration** EXEC commands were replaced with the **rtsp real-proxy restore factory-default** and the **rtsp real-subscriber restore factory-default** EXEC commands. In the ACNS 5.3.1 software and earlier releases, when you entered the **rtsp real-proxy default-configuration** or the **rtsp real-subscriber default-configuration** EXEC command, only the RealProxy or RealSubscriber configuration files were restored to the default setting; the databases that contain the Real Networks license key settings were not restored to the factory defaults.

## Enhancements to the Envivio-Cisco Streaming Engine Interoperability

The Cisco Streaming Engine is a back-end RTSP server that can be enabled on a registered Content Engine. A Cisco Streaming Engine can be used to serve VoD files that are generated by Apple Computer's QuickTime VoD authoring tool. It can also relay live streams that are generated by QuickTime Live Broadcaster through RTP/RTSP.

The Envivio Broadcasting Studio creates contents that can be played back by the Cisco Streaming Engine and the Envivio Streaming Server. For the ACNS software, the Envivio Streaming Server implements a much larger set of the MPEG4 specifications in the industry than the QuickTime authoring tools and players.

The ACNS 5.3.3 software release includes the following enhancements that are related to Envivio-Cisco Streaming Engine interoperability:

- [Retention of m4e File Extensions for Envivio-Based Programs, page 4](#)
- [Content Engine Support for Publishing of Multicast SDP Files for Cisco Streaming Engine Live Programs, page 5](#)

### Retention of m4e File Extensions for Envivio-Based Programs

The ACNS software supports Envivio-based programs and IP/TV programs as a stream source. For IP/TV-ACNS programs, the program description is generated as a Session Description Protocol (SDP) file by the IP/TV Program Manager. The ACNS software uses this SDP file to distribute the program specifications to the appropriate Content Engines.

Envivio generates the program description as an .m4e file. In the ACNS 5.3.3 software and later releases, m4e extensions in the reference URLs are retained. This new functionality allows you to use the Envivio TV plugin to render streams that are encoded by the Envivio encoder using specific codecs such as H.264. For CLI-based programs, you can now publish broadcast\_id.m4e files if the source is an .m4e file.

## Content Engine Support for Publishing of Multicast SDP Files for Cisco Streaming Engine Live Programs

In previous releases of the ACNS software, multicast SDP files were not published for Cisco Streaming Engine programs that were created through the Content Distribution Manager or the Content Engine CLI. In previous releases, you could publish the SDP files from any HTTP/FTP server.

In the ACNS 5.3.3 software release, support for multicast reference URLs (Announce URLs) for programs that are created through the Content Distribution Manager or the CLI was added. The multicast reference URL, which is in the form of `http://Content Engine-IP address/ProgramID.sdp`, is resolved by the Content Engines that are serving the live program.

## Support of Dynamic Content Routing

In previous releases of the ACNS software, Content Routers used a static coverage zone file to describe the preferred routing path between Content Engines and client end systems.

A coverage zone is a mapping of client end-system IP addresses to Content Engines. The Content Router uses the Content Engine IP addresses to create a static redirection table that maps end-system IP addresses to Content Engines and provides information on the proximity of end systems to Content Engines. When content is requested by a client, the Content Router checks the client IP address to find the coverage zone that contains that IP address. The Content Router then selects the Content Engine that is serving this coverage zone.

In some ACNS network environments, Content Engine IP addresses keep changing, and coverage zones are dynamic instead of static. In such cases, the Content Router cannot create a static routing table, and it cannot successfully route the content.

When the following conditions are present, the content cannot be routed successfully by using static coverage zone tables in the Content Router:

- Multiple Content Engines are deployed in multiple locations.
- Each location contains a NAT firewall.
- One Content Router serves all locations.
- One root Content Engine serves all locations.
- Each location is configured with two uplink lines to the Internet for redundancy.
- Uplink lines for different locations can share an external public IP address pool so that the same IP address can be used by NAT firewalls in different locations at different times.

With multiple uplinks to the Internet, requests for content from clients and Content Engines that are in the same location can go out to the Content Router with different external IP addresses. The Content Router that is using static coverage zone files cannot accommodate sharing the same IP address pool among different locations.

In the ACNS 5.3.3 software and later releases, the Content Router can detect changes in Content Engine coverage zones and can dynamically adjust its routing tables.

### Enabling Dynamic Content Routing

For each Content Router that you want to configure for dynamic content routing, you must indicate that dynamic content routing is to be used over static content routing.

To configure dynamic content routing, follow these steps:

- 
- Step 1** From the Content Distribution Manager GUI, choose **Devices > Devices**.
  - Step 2** Next to the name of the Content Router that you want to configure, click the **Edit** icon.
  - Step 3** In the Contents pane, choose **Device Activation**. The Device Activation window appears.
  - Step 4** To indicate that dynamic content routing is to be used over static content routing, check the **Dynamic Content Routing** check box.
  - Step 5** To save the Content Router settings, click **Submit**.
- 

### Changing the Content Engine Metric Value for Dynamic Content Routing in the Coverage Zone File

In the ACNS 5.3.3 software, a new tag has been defined in the coverage zone file that allows you to change the metric which assigns a preference to a particular Content Engine in the routing table. This optional tag is the <dynamic> tag.

When a coverage zone file containing the <dynamic> tag and elements is assigned to a Content Router, the following applications are made:

- If dynamic content routing is enabled on a Content Router, the Content Router follows the specifications inside the <dynamic> tag, and it ignores the specifications in the <coverageZone> tag.
- If dynamic content routing is not enabled, the Content Router follows the specifications in the <coverageZone> tag, and it ignores the specifications in the <dynamic> tag.

The <dynamic> tag is a standalone tag; it is not defined as a subelement of the <coverageZone> tag. The subelements <CE> and <metric> must be defined within the <dynamic> tag. [Table 1](#) describes the elements of the <dynamic> tag.

**Table 1 Coverage Zone File Elements for Dynamic Content Routing**

Tag Name	Elements	Value	Description
<dynamic>			
	<CE> <sup>1</sup>	Content Engine name	Specifies the Content Engine for which the metric value is to be applied. The <dynamic> tag can contain the names of multiple Content Engines.
	<metric> <sup>1</sup>	Number	Value indicates the proximity of the Content Engine to the end user. The lower the value, the greater the preference given to the Content Engine.  If no metric is specified, the default value of 10 is applied.

1. This element is required.

The following example shows how the <dynamic> tag can be used in a coverage zone file:

```
<?xml version="1.0"?>
<CDNNetwork>
<revision>1.0</revision>
<dynamic>
<CE>hostname_of_ce</CE>----- NOTE: The tag is <CE> and not <ce>.
<metric>number</metric>
</dynamic>
</CDNNetwork>
```

The following example shows an invalid coverage zone file where the <dynamic> tag is written as a subelement of the <coverageZone> tag:

```
<?xml version="1.0"?>
<CDNNetwork>
<revision>1.0</revision>
<coverageZone>
<dynamic>
<CE>hostname_of_ce</CE>
<metric>number</metric>
</dynamic>
</coverageZone>
</CDNNetwork>
```

The following example shows that the <dynamic> tag and the <coverageZone> tag can exist together in a coverage zone file:

```
<?xml version="1.0"?>
<CDNNetwork>
<revision>1.0</revision>
<coverageZone>
<network>a.b.c.d/mask</network>
<CE>hostname_of CE</CE>
<metric>0</metric>
</coverageZone>
<dynamic>
<CE>name_of_ce</CE>
<metric>number</metric>
</dynamic>
</CDNNetwork>
```

The following example shows that the <dynamic> tag can appear multiple times in a coverage zone file:

```
<?xml version="1.0"?>
<CDNNetwork>
<revision>1.0</revision>
<dynamic>
<CE>hostname_of_ce1</CE>
<metric>number</metric>
</dynamic>
<dynamic>
<CE>hostname_of_ce2</CE>
<metric>number</metric>
</dynamic>
</CDNNetwork>
```

The following example shows that the <dynamic> tag can contain the names of multiple Content Engines:

```
<?xml version="1.0"?>
<CDNNetwork>
<revision>1.0</revision>
```

```

<dynamic>
<CE>hostname_of_ce1</CE>
<CE>hostname_of_ce2</CE>
<CE>hostname_of_ce3</CE>
<metric>number</metric>
</dynamic>
</CDNNetwork>

```

You can use a coverage zone file with the <dynamic> tag, for example, when a preference order has to be given for a set of Content Engines that are serving the same client base. The following example shows that ce1 is preferred over ce2 because the metric value for ce1 is lower than that of ce2:

```

<?xml version="1.0"?>
<CDNNetwork>
<revision>1.0</revision>
<dynamic>
<CE>hostname_of_ce1</CE>
<metric>20</metric>
</dynamic>
<dynamic>
<CE>hostname_of_ce2</CE>
<metric>30</metric>
</dynamic>
</CDNNetwork>

```

## Configuring TCP Memory Limits

In the ACNS 5.3.3 software release, the ability to use the CLI or the Content Distribution Manager GUI to configure TCP memory limits was added. The TCP memory limit settings allow you to control the amount of memory that can be used by the TCP subsystem's send and receive buffers.



### Caution

Do not modify the default values unless you know what you are doing. The default values are device dependent and have been chosen after extensive testing. They should not be changed under normal conditions. Increasing these values can result in the TCP subsystem using more memory, which might render the system unresponsive. Decreasing these values can result in increased response times and lower performance.

To configure TCP memory limit settings from the Content Distribution Manager GUI, choose **Devices > Devices (or Device Groups) > General Settings > Network > TCP**. The TCP Settings window appears.

To configure the TCP memory limit settings from the CLI, use the **tcp memory-limit** global configuration command.

Table 2 lists the TCP configuration fields that have been added under the TCP Memory Limit Settings heading in the Content Distribution Manager GUI and the corresponding CLI commands that were added in the ACNS 5.3.3 software release

**Table 2** TCP Memory Limit Settings

Content Distribution Manager GUI Parameter	Function	CLI Command
TCP Limit Low Water Mark	The lower limit (in MBytes) of memory pressure mode, below which TCP enters into normal memory allocation mode. The range is 4–600.	<b>tcp memory-limit low-water-mark</b> <i>megabytes</i>
TCP Memory Limit High Water Mark–Pressure	The upper limit (in megabytes) of normal memory allocation mode, beyond which TCP enters into memory pressure mode. The range is 5–610.	<b>high-water-mark-pressure</b> <i>megabytes</i>
TCP Memory Limit High Water Mark–Absolute	The absolute limit (in MBytes) on TCP memory usage. The range is 6–620.	<b>high-water-mark-absolute</b> <i>megabytes</i>

Table 3 describes the default values for each command parameter, which are based on the total amount of memory for the device.

**Table 3** Default TCP Memory Limit Settings

Total System Memory	Low	Pressure	Absolute
1 GByte, 2 GBytes, or 4 GBytes	360 MBytes	380 MBytes	400 MBytes
512 MBytes	180 MBytes	190 MBytes	200 MBytes
256 MBytes	25 MBytes	28 MBytes	30 MBytes

The following conditions must be satisfied whenever these default values are changed:

- The low water mark must be a number that is less than the high water mark pressure setting.
- The high water mark pressure must be a number that is less than the high water mark absolute setting:

```
low-water-mark < high-water-mark-pressure < high-water-mark-absolute
```

## New Rule Command for Converting Hostnames to IP Addresses

In the ACNS 5.3.1 software and earlier releases, the **use\_proxy** rule action and the **failover** option in the **use-proxy** rule action perform hostname to IP address translation at the time of the CLI configuration. If the IP address for the specified hostname were to change, the service rule would no longer function.

In the ACNS 5.3.3 software release, the **rule dns-resolve each-request** global configuration command was added. When this CLI command is enabled, the caching process on the Content Engine resolves the hostname each time that it processes the request and matches the pattern for the **use-proxy** rule action and the **failover** option in the **use-proxy** rule action.

For the ACNS 5.3.3 software and later releases, the caching process uses the initially resolved IP (done at the time of the CLI configuration) for processing the **use-proxy** rule action and the **failover** option in the **use-proxy** rule action when the **rule dns-resolve each-request** CLI command is disabled. For instance, the following is an example of the CLI command syntax for the yahoo and abc websites upon configuration with the ACNS 5.3.3 software:

```
ContentEngine(config)# rule action use-proxy www.yahoo.com 8080 failover pattern-list 10
ContentEngine(config)# rule action use-proxy www.abc.com 8090 pattern-list 20
```

In contrast, the following is an example of the CLI command syntax for the yahoo and abc websites upon configuration with the ACNS 5.3.1 software and earlier releases:

```
ContentEngine(config)# rule action use-proxy 66.94.230.42 8080 failover pattern-list 10
ContentEngine(config)# rule action use-proxy 199.181.132.250 8090 pattern-list 20
```

## Modified Output of the show programs EXEC Command

In the ACNS 5.3.1 software and earlier releases, the output of the **show programs EXEC** command does not include information about programs that were configured in local mode through the CLI. The command output only includes information about programs that were configured through the Content Distribution Manager GUI.

In the ACNS 5.3.3 software release, the command output for the **show programs** command was enhanced to include information about CLI-based programs (for example, information about CLI-based programs for both the Cisco Streaming Engine and WMT).

In the ACNS 5.3.3 software release, the output of the **show programs EXEC** command was also modified to add an “e-” for Envivio-based programs that have a reference URL that contains an .m4e filename extension.

## Hardware Supported

The ACNS 5.3.3 software supports the following hardware platforms.



### Note

All of the listed platforms also support the ACNS 5.3.1 software and the ACNS 5.2.x software releases except for the following three new Wide-Area Application (WAE) platforms that are only supported in the ACNS 5.3.3 software and later releases: the WAE-511, the WAE-611, and the WAE-7326.

- NM-CE-BP-SCSI
- NM-CE-BP-80G
- NM-CE-BP-40G
- NM-CE-BP
- CDM-4630
- CDM-4650
- CE-507
- CE-507AV
- CE-510-K9
- CE-510A-80GB-K9
- CE-510A-160GB-K9
- CE-511
- CE-566-K9
- WAE-511
- WAE-611
- CE-565-K9
- CE-565A-72GB-K9
- CE-565A-144GB-K9
- CE-590
- CE-590-DC
- CE-7320
- CE-7305-K9
- CE-7305A-K9
- CE-7325-K9
- CE-560
- CE-560AV
- CE-7325A-K9
- CE-7326
- WAE-7326
- CR-4430

# Important Notes

This section emphasizes important information regarding the ACNS 5.3.x software. It includes the following sections:

- [Eliminated Upgrade/Downgrade Paths, page 12](#)
- [Media File System Issues When Downgrading to ACNS 5.0 Software, page 12](#)
- [SmartFilter Issues When Upgrading or Downgrading to Another ACNS Software Release, page 13](#)
- [Websense Support, page 13](#)
- [Websense Issues When Downgrading to the ACNS 5.0 Software or ACNS 5.1 Software, page 13](#)
- [Interoperability with ICAP Vendors, page 14](#)
- [ICAP Performance, page 14](#)
- [Matrix of Supported Caching, Filtering, and Authentication Methods, page 15](#)

## Eliminated Upgrade/Downgrade Paths

In the ACNS 5.3.1 software release, the following upgrade and downgrade paths were eliminated:

- Upgrading from the ACNS 4.2 software to the ACNS 5.3 software
- Downgrading from the ACNS 5.3 software to the ACNS 4.2 software

## 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.

## Websense Support

In the ACNS 5.3.x software, Websense server Version 5.2 is supported on all Cisco Content Engine platforms. With Websense 5.2.0 software, you can use a local or remote Websense Policy Server to activate the local EIM Server, the local RADIUS Agent, the local eDirectory Agent, the local Network Agent, and the local User Service individually on a Content Engine.

For detailed information about configuring the Websense software, go to the following URL on the Websense website:

[http://ww2.websense.com/docs/support/documentation/setup/v52/WSPreinstall\\_CiscoCE\\_ACNS\\_53.pdf](http://ww2.websense.com/docs/support/documentation/setup/v52/WSPreinstall_CiscoCE_ACNS_53.pdf)

## 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.
-

## Interoperability with ICAP Vendors

The Internet Content Adaptation Protocol (ICAP) is an open standards protocol for content adaptation, typically at the network edge. Content adaptation includes virus scanning, content translation, content filtering, content insertion, and other ways 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, which filters and adapts 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 (respmod)—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 Internet Content Adaptation Protocol (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.

**Note**

---

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

---

## 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 5.3.x software. An asterisk (\*) indicates 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	*				*	*		

## Caveats

This section lists and describes the open and resolved Severity 1, 2, and 3 caveats in the ACNS 5.3.3 software. Caveats describe unexpected behavior in the ACNS 5.3.3 software. Severity 1 caveats are the most serious; Severity 2 caveats are less serious. Severity 3 caveats are moderate caveats.

## Open Caveats - ACNS 5.3.3 Software

This section lists caveats that have not been resolved in the ACNS 5.3.3 software release.

- 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.

- CSCec52221

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

Condition: This problem occurs if 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.

- CSCec52319

Symptom: Using FTP inside the .meta file to have the Content Engine obtain the .bin file for a Content Distribution Manager GUI-initiated upgrade is unsuccessful if the user's home directory differs from the FTP root.

Condition: Either you receive an error in the Content Distribution Manager GUI when you are creating the definition for the upgrade (when the .bin file does not exist in the user's home directory), or the Content Engine displays an error message on the upgrade (when the .bin file does not exist in the FTP root directory).

Workaround: Copy the .bin file to both the FTP root and the user's home directory, or use a user whose home directory is the FTP root.

- CSCed68360

Symptom: A constant stream of bandwidth error messages (one about every 2 seconds) is reported in the syslog. As the following sample messages indicate, these messages are not very useful.

```
Feb 11 13:24:26 webcache01 bandwd: %CE-BANDWD-3-115002: BANDWD: Trying again in two
seconds
Feb 11 13:24:28 webcache01 bandwd: %CE-BANDWD-3-115003: BANDWD: verification
registration failed, err=30
```

Condition: None.

Workaround: There is no known workaround.

- 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: There is no known workaround.

- 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.
- CSCee17283
 

Symptom: The cdnfs files are turned into directories (which are visible if you enter the **cdnfs browse EXEC** command on the Content Engine).

Conditions: This problem is rare and occurs only when the file system corruption has caused a directory entry to be a subdirectory when it should have been a file. This problem occurs only if multiple cdnfs entries are being updated and the Content Engine crashes (for example, the Content Engine crashes because of a power failure).

Workaround: Enter the **cdnfs cleanup start EXEC** command on the Content Engine.
- 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 with WMT live programs that have unicast access enabled. In this situation, streams can be accessible for up to 24 hours after the last playtime of the event if “Auto Delete” is set to true or can be accessible indefinitely if “Auto Delete” is set to false.

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

- CSCee40593

Symptom: Syslog messages contain the following text:

```
uns-server: %CE-CDNFS-0-480000: uns_read_meta: WOW! url mismatch:
wanted 'URL>', saw '^C'
```

Condition: This problem occurs because of file system corruption; the cdnfs metadata files have the wrong content (the content is internally consistent but is in the incorrect file). This problem occurs infrequently. For example, it can occur if the cdnfs content is being updated and a crash occurred because of a kernel panic (which occurs infrequently).

Workaround: Although there is no known workaround to stop the syslog messages shown above, lookups for the target URL (listed in the syslog message) may succeed if the ACNS software has created a new cdnfs entry for the target URL.

You can enter the **cdnfs lookup url EXEC** command to see if the URL is found. If the URL is not found, a way to force it to be replicated is to modify the file on the origin server (for example, by entering the **touch** command on a UNIX-based origin server).

Alternatively, you can enter the **acquisition-distribution database-cleanup start** command on the affected Content Engine to query the cdnfs for all the objects that are supposed to be on the Content Engine. Missing objects should be detected and replicated.

- CSCee49106

Symptom: The content replication status can show an incorrect manifest item count.

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

Workaround: There is no known workaround.

- CSCee67227

Symptom: If 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 is longer than 50 characters.

Workaround: For NTLM authentication, use a domain controller (DC) that has a domain name shorter than 35 characters.
- CSCee68339

Symptom: Proxy requests to the Content Engine proceed to allow mode (if allow mode is enabled) or are blocked (if allow mode is disabled) when the Websense URL filtering mechanism is configured to use the local Websense server.

Because the connections from the Content Engine to the Websense server time out, all requests go to allow mode until all 40 connections are exhausted. (This situation makes it appear as if the Websense server is not responding.) After all 40 connections are attempted, the Content Engine successfully connects to the Websense server and works properly thereafter.

Condition: This problem can occur under the following conditions:

  - The Content Engine is configured to use the local (internal) Websense server for URL filtering.
  - The local Websense server is running on the Content Engine.
  - There are long periods of inactivity.
  - The cache process has difficulty connecting to the local Websense server.

Workaround: Reconfigure Websense URL filtering on the Content Engine so that the Content Engine will attempt to establish new connections to the Websense server.
- CSCee71157

Symptom: Channel routing causes loops for several Content Engines.

Condition: This problem can 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 can develop within the system.

- CSCee78190

Symptom: When a root Content Engine is downgraded from the ACNS 5.2.x software to the ACNS 5.1 software, some channels are disabled and some content fails to be acquired.

Condition: This problem occurs when the manifest file URL is a Server Message Block (SMB) URL with a uniform naming convention (UNC) path format (for example, \\host\share\file), or when an item or crawl task specified in either the **src** or **start-url** attribute has a UNC path format.

Because the ACNS 5.1 software does not support SMB file acquisition, the root Content Engine running the ACNS 5.1 software is not able to fetch the manifest file or acquire content from the SMB shares.

Workaround: Either before or after you downgrade the root Content Engine from the ACNS 5.2.x software to the ACNS 5.1 software, remove the SMB URL from the Manifest URL field in the Channel configuration window of the Content Distribution Manager GUI and use a URL with supported protocols (HTTP, FTP, or HTTPS).




---

**Note** From an ACNS 5.1 Content Distribution Manager GUI, choose **Channels > Channels > Edit Channel**.

From an ACNS 5.2.x Content Distribution Manager GUI, choose **Content > Channels > Edit Channel > Channel Content**.

---

Edit the manifest file by removing content items and crawl tasks that have UNC formatted paths.

Use the **acquirer start-channel EXEC** command to initiate channel acquisition and verify that the workaround is successful.

- CSCee81376

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

Condition: This problem can occur 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: 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: There is no known workaround.
- 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: There is no known workaround.
- 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 switches.

Workaround: There is no known workaround. 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

The Content Engine becomes unresponsive, and it takes a long time for commands to be executed.

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 as many times as specified by the “repeatCount” setting.

Condition: This problem occurs only when RealPlayer Version 10 is used. The player exhibits the same behavior whether or not there is a Content Engine 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 only when the ICAP service is enabled on the Content Engine.

Workaround: There is no known workaround.
- CSCef57641

Symptom: The cache process on the Content Engine restarts.

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

Workaround: There is no known workaround.
- CSCef60282

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

Conditions: 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.
- 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.
- CSCef62968

Symptom: The Content Engine reboots suddenly when you are performing database maintenance.

Condition: The problem can occur because of a platform issue in the power supply of the device.

Workaround: Properly trim the power supply of the Content Engine.

- CSCef65567

Symptom: You are not able to download the control list or apply a policy (for example, the policies that control when the SmartFilter subscription or control list expire) to the SmartFilter 3.x plug-in.

Condition: This problem occurs if you use the SmartFilter 4.0 Administrator Console to define the SmartFilter 3.x plug-ins as part of a plug-in group.

Workaround: Use the SmartFilter 4.0 Administrator Console to define the SmartFilter 3.x plug-ins as individual plug-ins.

- 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.

- CSCeg04809
 

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

Condition: This problem can occur 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 only 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 can occur when the Websense server is enabled on the Content Engine.

Workaround: No user intervention is required. If this problem occurs, the Websense server functionality is not affected. After generating a core file, the Websense server will be automatically restarted 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 only 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.
- CSCeg49287
 

Symptom: When WCCP transparent redirection is being used to redirect RTSP client requests transparently to WCCP routers, the client receives an error stating that it is unable to locate the server when it attempts to retrieve the RTSP URL. This problem can occur because the URL presented to the client is a modified “bad” URL. This modified URL is the original URL with the Content Engine’s RTSP gateway IP address prepended before the domain name. For example, if the original RTSP URL is “rtsp://website.com.domain:554/url-path-info,” then the following modified “bad” URL is returned to the client:

*rtsp://ciscoRTSPG.ipaddress-of-rtsp-gateway.website.com.domain:554/url-path-info*

The reason that the client is unable to resolve the DNS is because the Content Engine is using the modified URL.

Condition: The problem can occur when the WCCP router list (**wccp router-list x.x.x.x** CLI command) on the Content Engine is configured with a router IP address that the router does not use in its WCCP “I See You” messages.

Workaround: Configure the WCCP router list to use the IP address that the WCCP router is using on its “I See You” messages.

- CSCeg51354  
Symptom: The Windows Media player goes into a buffering state for RTSPU-based file streaming.  
Condition: This problem can occur under the following circumstances:
  - The bandwidth between the client and the Content Engine is low.
  - The file used for streaming contains multiple audio streams.Workaround: Use RTSPT-based file streaming instead of RTSPU-based file streaming.
- CSCeg55742  
Symptom: Multiple connections are seen between the root Content Engine and the Windows Media server/encoder.  
Condition: This problem can occur if the root Content Engine is under a heavy load and multiple Content Engine children or clients connect to the root Content Engine to access a unicast stream. Because of timing issues, the root Content Engine can create multiple connections to the encoder/server. This problem does not adversely impact the clients that are watching the stream; however, one side effect is that more bandwidth will be used between the root Content Engine and the encoder/server.  
Workaround: There is no known workaround.
- CSCeg56075  
Symptom: RealPlayer crashes when the streams are switched over 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.
- CSCeg57195  
Symptom: After changing the DNS configuration, WMT fails and the WMT error logs show that there is a problem with resolving URLs.  
Condition: This problem occurs because WMT is not recognizing that a DNS change has occurred and is trying to use the old DNS configuration that may point to a server that is down or is inaccessible.  
Workaround: After you change the DNS configuration, reload the Content Engine to ensure that all of the processes will obtain the current DNS configuration when they start up.
- CSCeg60760  
Symptom: CPU usage on the Content Engine reaches 99 percent.  
Condition: This high CPU usage can occur if the Content Engine is serving numerous live-streaming requests and it is running the ACNS 5.1.11 software and later releases.  
Workaround: If you are not expecting a very high load on the Content Engine, you can turn off kernel optimization by entering the **no wmt accelerate live-split enable** global configuration command.

- CSCeg63788

Symptom: The local (internal) Websense server on the Content Engine is not responding to a block page message.

Condition: This problem can occur if certain clients do not behave properly and fail to send the requested data back to the Websense block page server. The block page server is not timing out these requests, reaches a limit, and then stops responding.

Workaround: Restart the internal Websense server or reboot the Content Engine to clear the connections.
- CSCeg68274

Symptom: SNMP management is not able to learn the standby interface in order to test the standby interface for accessibility.

Condition: This problem can occur if the Content Engine is configured with a standby interface and the SNMP management station uses an MIB query for ipAdEntAddr. The SNMP management system learns the addresses of the individual interfaces but not the address of the standby group.

Workaround: Configure real addresses for the interfaces on the Content Engine so that the SNMP management station can at least test that the interfaces on the Content Engine are active.
- CSCeg69790

Symptom: After you configure a live event through the ACNS 5.2 Content Distribution Manager GUI, the URL link generated by the Content Distribution Manager cannot be played.

Condition: This problem only occurs if the media filename or program name includes a blank space.

Workaround: Do not use a blank space in either the media filename or the program name when using the Content Distribution Manager to configure a live event. For example, use “-” or “\_” instead of a blank space.
- CSCeg74062

Symptom: Internet Explorer does not display the RealServer License Monitor window correctly. (This window is displayed by logging in to the RealServer administrative interface and then selecting **Logging & Monitoring** and **License Monitor**.)

Condition: This problem only occurs with Internet Explorer.

Workaround: Use the Firefox or Netscape browsers, which display the License Monitor window correctly.
- CSCeg74070

Symptom: Both Internet Explorer and Firefox browsers do not correctly display changed settings for the broadcast transmitter and receivers.

Condition: This problem occurs if the Content Engine is running the ACNS 5.2.x software and later releases, and is using RealServer as a back-end RTSP server.

Workaround: There is no known workaround.
- 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.

- 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:

- a. NTLM request authentication is enabled on the Content Engine.
- b. The request is sent after the Content Engine has been idle for a long period of time.
- c. 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.

- CSCeg84304

Symptom: The ICAP daemon that is running on the Content Engine generates a core file.

Condition: This problem can occur when there is a heavy load of HTTPS proxy traffic that is being processed by the Content Engine.

Workaround: There is no known workaround.

- 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 RTSP 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 can occur if a Content Router is being used for RTSP redirection.

Workaround: There is no known workaround.

- CSCeg88951

Symptom: When viewing a rich media stream, the video display may be black for a couple of minutes. After the video starts to play, if you click the progress bar in the Windows Media player to advance the video, the video display may go black again as though the video were starting over again.

Condition: This problem can occur if you are using a Windows Media 9 client to view a rich media stream.

Workaround: There is no known workaround.

- CSCeg90529

Symptom: Even though TACACS AAA accounting is enabled on the Content Engine, no command information is being received under the standard Cisco Access Control Server (ACS) TACACS headers.

Condition: This problem can occur if TACACS accounting is enabled on the Content Engine and it is reporting to a Cisco ACS 3.1 TACACS server.

Workaround: There is no known workaround.

- CSCeh06795

Symptom: A live channel may fail to be played from the clients. The replication fails as indicated by the output from the **show programs EXEC** command.

Condition: This problem can occur in the following condition:

- a. You are running the ACNS 5.2.1b7 software and later releases.
- b. You configure a live channel and then schedule it through the Content Distribution Manager GUI.
- c. You use uppercase letters when specifying the program name.

Workaround: Because uppercase letters are sometimes rejected, avoid using capital letters when specifying the program name in the Content Distribution Manager GUI.

- CSCeh20906

Symptom: Even though you have the transaction log sanitize feature enabled on the Content Engine, the RealProxy or RealServer access logs still display the client IP address even though 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. Even though you have entered the **transaction-logs sanitize** global configuration command, the RealProxy or RealServer access logs still display the client IP address even though it should be hidden.

Workaround: There is no known workaround.

- CSCeh21067

Symptom: Windows Media player files are not being downloaded properly.

Condition: This problem can occur if you have entered the **wmt disallowed-client-protocols http** global configuration command on the Content Engine and the Content Engine is rebooted.

Workaround: When the Content Engine is rebooted, reenter the **wmt disallowed-client-protocols http** command on the Content Engine.

- 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>.

- CSCeh28890
 

Symptom: When you perform a software upgrade or downgrade between the ACNS 5.3 software release and the ACNS 5.0 software release, the TCP Explicit Congestion Notification (ECN) configuration is not retained.

Condition: This problem can occur if you enter the **tcp ecn enable** global configuration command when the device is running the ACNS 5.0 software release, and then upgrade the device to the ACNS 5.3 software release.

Workaround: After upgrading the device to the ACNS 5.3 software release, reenter the **tcp ecn enable** command.
- CSCeh31111
 

Symptom: A core file is generated by the web server.

Condition: This problem can occur under the following condition:

  - a. In the Rules window of the Content Engine GUI, you choose **Cache** as the action and any pattern.
  - b. You fill in all the appropriate fields but leave the action Value string blank.
  - c. You click **Update**.

Workaround: Do not leave the action value field in the Rules windows blank.
- CSCeh31352
 

Symptom: The cache process generates a core file.

Condition: This problem can occur under the following condition:

  - a. The Content Engine has NTLM request authentication enabled.
  - b. One client (client A) requests an NTLM protected object from a origin server.
  - c. Another client (client B), whose user belongs to 500 groups, requests a plain object such as www.yahoo.com.
  - d. While client B is still waiting for all the groups to be retrieved, client A sends a request to www.google.com for plain objects.

Workaround: There is no known workaround.
- CSCeh34004
 

Symptom: When connected to an external ICAP server, the Content Engine may stop forwarding data. After the ICAP server timeout occurs, an error is reported to the HTTP client.

Condition: This problem can occur because of the timing of server responses.

Workaround: There is no known workaround.
- CSCeh34292
 

When the WMT player is being proxied to the Content Engine, the player stops and starts buffering several times when it is playing a media file.

Condition: This problem can occur under the following condition:

  - a. WMT is disabled on the Content Engine.
  - b. The media file is located on the Windows Media Series 9.1 server that will send back a keepalive header without a content-length header.

Workaround: Enter the **http ignore-resp-len-conn-hdr-check** global configuration command, which is a hidden CLI command, on the Content Engine.

- 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.

- CSCeh35997

Symptom: A file not found error message is generated for a pre-positioned IP/TV VoD file.

Condition: The problem can occur with a pre-positioned file that is moved from its origin server to another server, and then restored back to its original server location.

Workaround: Delete the on-demand program in the Program Manager GUI and define a new program to generate a fresh entry in the Manifest file.

- CSCeh37469

Symptom: You cannot configure the Websense server because of a synchronization problem. The output of the **show running EXEC** command shows that there are not any websense server configurations on the Content Engine, but the output of the **show websense-server EXEC** command shows that several websense components are installed on the Content Engine.

Condition: The problem can occur if you upgrade from the ACNS 5.2.x software to the ACNS 5.3.x software before there are any Websense server configurations on the Content Engine.

Workaround: To avoid the problem, before upgrading to a later version of the ACNS 5.x software, install at least one Websense component on the Content Engine. For example, enter the **websense service policy local activate** global configuration command on the Content Engine before upgrading to a later version of the ACNS 5.x software.

To recover from the problem, follow these steps:

- After upgrading the ACNS 5.x software, if the output of the **show running-config EXEC** command shows that there is no Websense server configuration on the Content Engine, remove the `/local1/WebsenseEnterprise/EIM/modules.txt` file on the disk.
- Enter the **write memory EXEC** command.
- Reload the Content Engine.

After reloading the Content Engine, the Content Engine should be back to its normal state and you can proceed to perform your planned Websense server configurations.

- CSCeh38741

Symptom: The Windows Media player is not able to stream content for more than one hour in the case of a cache hit.

Condition: This problem can occur when the Limit Player Timeout Inactivity value in the origin Windows Media server is set to the default value of 3600 seconds.

Workaround: Increase the Limit Player Timeout Inactivity value in the origin Windows Media server.
- CSCeh40432

Symptom: When the source of a WMT alias is changed to another source URL, the clients do not reflect the changes. The client is still connected to the old source stream even though the changes have been made. The user is watching a completely different stream than the one that is being sourced to the originating Content Engine. When using Windows Media streams in a cascaded hierarchy (one Content Engine that is pulling a stream from another and so on), if a client is pulling a stream from an alias and the alias that it is pointing to is changed to a different source, the client stream is not updated.

Condition: This problem occurs with the ACNS 5.1.13, 5.2 and 5.3 software.

Workaround: Delete and re-create the publishing point. When the source is an Encoder, if Encoder1 is provided as the source to the broadcast alias and the source is changed to Encoder2 while the client is playing the content, close Encoder1 to force the client to send a new request. After the client sends the new request, the client can obtain the stream from Encoder2.
- CSCeh41137

Symptom: The status of a Cisco Streaming Engine program continuously switches between playing and failed.

Condition: The problem can occur with a normal Cisco Streaming Engine program if a failing rebroadcast program already exists because the file had a filename or folder name that contained special characters.

Workaround: Delete the rebroadcast program that is failing because of the presence of special characters.
- CSCeh73477

Symptom: The acquirer experiences a problem with a samba crawl. The acquirer is recrawling the same crawl job.

Condition: This problem can occur if both of the following conditions exist:

  1. A channel contains a samba crawl from a Network Appliance file server, which contains such media files as .wmv files.
  2. The time to live (TTL) is set to recrawl the file at a fixed interval that is specified by the TTL attribute.

Workaround: There is no known workaround.

- CSCeh90085

Symptom: The media file system (mediafs) is borrowing more file space from the ACNS network file system (cdnfs) disk space than it should. The mediafs and cdnfs statistics files indicate that the underlying file system (which is shared by cdnfs and mediafs) is 100 percent full. Even though mediafs should only be allocated approximately 20 GBytes of space the output of the **show statistics mediafs** EXEC command shows that mediafs is consuming over 30 GBytes.

Condition: This problem can occur when mediafs is configured to use unused cdnfs disk space.

Workaround: Enter the **clear cache wmt** EXEC command to clear the WMT cache on the Content Engine.

- 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 can occur 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 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
```

- CSCei04025

Symptom: You cannot log on to the Content Engine and messages about mingetty being killed by signal 25 are being generated.

Condition: This problem can occur if the debug authentication feature (you have entered the **debug authentication user** EXEC command) has been enabled and is not disabled.

Workaround: Ensure that the debug authentication user feature is turned off by entering the **no debug authentication user** command on the Content Engine. Also, use the **delfile** EXEC command to delete the local1/service\_logs/pam-debug.log file and then run the **delfile service\_logs/pam-debug.log**. If you still cannot log in to Content Engine, contact Cisco Technical Assistance Center (TAC) for assistance.

- CSCei05034
 

Symptom: NTLM failover does not work properly. Client requests take approximately 2 minutes to time out because of an authentication failure, and the Content Engine never detects the domain controller (DC) failure.

Conditions: This problem can occur if both of the following conditions exist:

  - a. NTLM request authentication is enabled on the Content Engine.
  - b. The domain controller service hangs but the domain controller hardware is still operating.

Workaround: Bring up the domain controller service again, or restart the domain controller hardware, which will cause the Content Engine to fail over.
- CSCei06964
 

Symptom: The Windows Media player is not able to play the URL.

Condition: This problem can occur if the Content Engine is in between the Windows Media player and an ISA proxy, and NTLM authentication is enabled on the ISA proxy.

Workaround: There is no known workaround.
- CSCei62672
 

Symptom: When you click links from the table of contents or the index of the ACNS Content Distribution Manager online help, the links open in the same pane, that is, the left pane, which contains the table of contents and the index, instead of opening in the right pane, which contains the help topics.

Condition: This problem occurs after you install Microsoft security update MS05-026. This security patch disables cross-frame navigation features that are based on HTML Help ActiveX control (HHCTRL).

Workaround: To reenabte cross-frame navigation features that are based on HHCTRL, modify your Windows registry as explained in Microsoft Knowledge Base article 896905, which is available at this URL:

<http://support.microsoft.com/kb/896905/>
- CSCin54434
 

Symptom: Websense Manager cannot connect to the local Websense server (the Websense server runs 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 Websense Manager to connect to the local Websense server that is running on the Content Engine.

Workaround: There is no known workaround.
- CSCin59462
 

Symptom: An FTP client application stops receiving data for a data transfer operation such as a directory listing (ls) or file transfer (GET). The same symptom can occur for FTP-over-HTTP data transfers from the FTP server to the Content Engine.

Condition: For FTP client applications, the Content Engine must be using the FTP proxy through WCCP redirection, configured for following the FTP client's mode for establishing a data connection. The FTP client application must have also been set to use active mode to the FTP server.

```
ContentEngine(config)# wccp ftp router-list-num number
ContentEngine(config)# wccp version 2
ContentEngine(config)# ftp proxy active-mode enable
```

For FTP-over-HTTP data transfers, the Content Engine must be configured for an FTP incoming proxy and configured to use active mode to the FTP server. The client browser must be configured to use the Content Engine FTP proxy for FTP URLs.

```
ContentEngine(config)# ftp proxy incoming port
ContentEngine(config)# ftp proxy active-mode enable
```

The symptoms can occur with the configurations described above and when the FTP server starts sending data packets that are received out of order by the Content Engine before the Content Engine sends the TCP connection establishment SYN-ACK packet to the FTP server.

Workaround: Remove the Content Engine active mode configuration by entering the following global configuration command:

```
ContentEngine(config)# no ftp proxy active-mode enable
```

When this symptom occurs on an FTP client application, press **Ctrl-C** simultaneously to stop the partial data transfer operation.

When this symptom occurs on a browser configured for FTP-over-HTTP, click the **STOP** button to stop the partial data transfer operation.

- CSCin60029

Symptom: When a rule with the **redirect** action is configured with a URL of 0 and with a matching pattern (no replacing pattern), the cache process crashes if the request matches the pattern.

Condition: This problem occurs when you configure a numeric value of 0 for the redirected URL (for example, if *www.yahoo.com* is redirected to 0). If you want the Content Engine to redirect URL *x* to URL *y*, then you can configure the **rule redirect** action. While doing so, you must configure URL *x* and URL *y*.

Workaround: There is no known workaround.

- CSCin67818

Symptom: The manifest validator fails to fetch the XML file if the source is authenticated.

Condition: This problem occurs only if the file is located at an authenticated location.

Workaround: Put a copy of the manifest file in a nonauthenticated location to use the manifest validator.

## Resolved Caveats—ACNS 5.3.3 Software

This section lists the caveats that have been resolved in the ACNS 5.3.3 software release. The resolved caveats are grouped into the following categories:

- [Acquisition and Distribution Resolved Caveats, page 36](#)
- [ICAP Resolved Caveats, page 36](#)
- [Management Resolved Caveats, page 36](#)
- [Media and Streaming Resolved Caveats, page 37](#)
- [Proxy and Caching Resolved Caveats, page 38](#)
- [Rules Resolved Caveats, page 39](#)
- [Other Resolved Caveats, page 39](#)

## Acquisition and Distribution Resolved Caveats

- CSCeh40754  
The root Content Engine is not able to acquire content. The Content Distribution Manager GUI replication status window indicates that the Content Distribution Manager has no content, and the receiver Content Engines indicate “No Status Reported.” This problem can occur if the root Content Engine has recently experienced a failure that took it down, or it required a hard reboot that caused a database corruption on the root Content Engine, which in turn prevented the acquirer from acquiring the content.
- CSCeh44689  
The acquirer fails to load or start if the origin server requires NTLM authentication and the NTLM credentials are not provided to the acquirer.
- CSCeh45985  
The acquirer crashes and continues to restart while parsing the manifest file. This problem occurs in the following situation. The root Content Engine is configured to use an outgoing proxy with NTLM authentication, the Content Distribution Manager GUI is used to specify the NTLM parameter, and a relative source URL is used for the contents in the manifest file.
- CSCeh54906  
When the notFoundUrl attribute is set in a manifest file, a manifest parse error occurs.

## ICAP Resolved Caveats

- CSCeh96632  
The connection to the ICAP server is not terminated for up to 1.5 minutes after the server is unreachable. This problem occurs regardless of the keepalive timer setting.

## Management Resolved Caveats

- CSCeh48631  
The LocationApiServlet fails with a constraint exception when the name is not set.
- CSCeh55264  
The DeviceGroup TimeZone Settings with SummerTime set are overridden by each of the devices in the device group. This problem can occur if the CMS agent that is running on the Content Engine fails to properly parse the time zone configuration on the device and reports the time zone as having been changed from that of the Content Distribution Manager configuration. This situation causes the values to be overridden. This problem only occurs for the default time zone of UTC.
- CSCeh57366  
If you are running the ACNS 5.0 or 5.1 software on the Content Distribution Manager and one or more of the registered Content Engines are running the ACNS 5.2.x software or the ACNS 5.3.1 software, the NTLM server may appear out of order when you check the running configuration on the Content Engine. This problem can occur if you have specified both the primary and secondary domain servers for one of these Content Engines (or for a group that contains one of these Content Engines) through the NTLM Server Settings window of the Content Distribution Manager GUI.

- CSCeh58488  
Clients receive a “Page cannot be displayed” error message when they access a site that requires NTLM authentication. This problem can occur with chunked-encoded responses and responses with no content length header.
- CSCeh59273  
If you use the CLI to set the idle-timeout value to 60, the Content Distribution Manager GUI incorrectly interprets this setting as 120. This problem occurs if the Content Distribution Manager is running ACNS 5.3.1 software and the Content Engines are running the ACNS 5.3.3 software and later releases.
- CSCeh60484  
If you perform a software download from the Content Distribution Manager GUI and the download file is larger than 1 MByte, the GUI displays an incorrect status message about the software download (Download failed) while performing the software update.

## Media and Streaming Resolved Caveats

- CSCeh36052  
After a failover, multicasting does not occur on the root Content Engine and the child Content Engine if the WMT managed live event has redundant sources of publishing points in a Windows Media server. In this situation, unicast works properly.
- CSCeh41537  
The media player enters into a buffering state for managed live programs that are created with a broadcast publishing point as the source. This problem occurs with files that contain a large number of script events, which are used as the source for creating the publishing point in a Windows Media server.
- CSCeh43420  
A cache crash and core dump can occur on a Content Engine during a chunk-encoded object data transfer. However, when this problem occurs, the cache process is automatically restarted.
- CSCeh68970  
When the location leader for a WMT live multicast program fails, the other Content Engine (for example, CE2) in the same location does not start multicasting; however, it does serve the unicast request from the forwarder location.
- CSCeh72210  
There are some problems with the output of the **show programs prog-id/prog-name EXEC** command. For instance, the command output for WMT live programs shows the encoder and port number for the forwarded list but they are HTTP encoded (for example, the output is shown as “encoderip&port (10.77.140.10&8080)”). Another example of this display problem is that for live programs, an “e-” is appended to the unicast access URL.
- CSCeh72679  
Even though all of the NTLM credentials are provided, the proxy still fails authentication because the acquirer always uses unicode for the credentials.
- CSCeh79582  
The play duration is not available for pre-positioned media files. This problem can occur if the acquirer is used to acquire the media files and the play duration is not shown in the replication status and in the cdnfs lookup in the Content Engine.

- CSCeh94630  
The RealProxy administrator GUI shows garbled content. This problem can occur if you change the RealProxy configuration through the administrator GUI. A new window opens and displays garbled content.
- CSCei10904  
The output of the **show statistics wmt streamstat EXEC** command shows that the fast-cache acceleration bandwidth is being allocated for live HTTP requests. This problem can occur if the fast cache feature is enabled on the Content Engine for WMT requests and the Content Engine is running the ACNS 5.3.1 software or earlier releases. This problem was fixed in the ACNS 5.3.3 software release.

## Proxy and Caching Resolved Caveats

- CSCeh00314  
In the case of WMT live and content routing, the HTTP failover URL does not work. In the case of a WMT live using content routing, after the initial communication between the client and the Content Router, the client is redirected to the Content Engine. When the Content Engine receives this request, it sends the client an .asx file that contains two URLs (an MMS URL and an HTTP URL). In the case of WMT live, this HTTP URL is not valid. If the client fails over to this HTTP URL if the MMS URL fails, the stream will not be served by the Content Engine. This problem occurs on systems that are running the ACNS 5.1.x, 5.2.x, and 5.3.1 software. This problem was fixed in the ACNS 5.3.3 software release.
- CSCeh02627  
If a POST request includes an Expect: 100 Continue response, the Content Engine can experience problems in processing these POST requests properly.
- CSCeh15968  
The client receives an unexpected 400 bad request HTTP response from the origin server when the request is going through a Content Engine. This problem can occur if the client sends an unnecessary carriage-return and line feed (\r\n) in between the end of one request and the beginning of another request. These extra characters have been seen using the following version of the browser: Internet Explorer Version: 6.0.2800.1106.xpsp2.040919-1003, Cipher Strength: 128-bit, Update Versions: SP1; Q832894; Q837009; Q831167; Q823353; and Q871260.
- CSCeh48360  
The “rewrite” action fails for WMT requests if the “no-proxy” action is also configured for a matching pattern. This causes the “no-proxy” action to be executed first instead of the “rewrite” action being executed first. Such an example is shown below:

```
ContentEngine# show rule all
Rules Template Configuration
-----
Rule Processing Enabled
Actions :
rule action rewrite pattern-list 5
rule action no-proxy pattern-list 7
Pattern-Lists :
rule pattern-list 5 group-type or
rule pattern-list 5 url-regexp (mms.*://www.wm-server-1.com).* \1/pinball.wmv rule
pattern-list 7 group-type or rule pattern-list 7 dst-ip 10.77.157.169 255.0.0.0
```

In this case, 10.77.157.169 is the IP address of the www.wm-server-1.com.

If a request is given for `mmst://www.wm-server-1.com/100kbs.wmv`, it must be rewritten to the URL `mmst://www.wm-server-1.com/pinball.wmv`. However, because the “no-proxy” action is executed first such a “rewrite” does not occur.

- CSCeh55335

If the **http cache-vary-user-agent enable** global configuration command has been specified on the Content Engine, a cache crash can occur on the Content Engine.

- CSCeh69442

The Content Engine does not cache content and is not receiving any requests even though the router is redirecting traffic to the Content Engine. This problem can occur if the request header line in the packet is greater than 8 KBytes, which causes the Content Engine to reset the connection and to have an entry created in the bypass list.

- CSCeh73714

The cache process stops and the output of the **show tech-support EXEC** command shows a back trace.

- CSCei04882

Certain requests (for example, when you click on links from the results of a Goggle search) to the Content Engine time out without any response from the Content Engine. This problem can occur if all of the following conditions exist:

- a. The Content Engine is running the ACNS 5.3.1 software.
- b. The server response is noncacheable.
- c. The server transfer encoding is chunked.
- d. The Content Engine is configured to keep a persistent connection with the server.

This problem was fixed in the ACNS 5.3.3 software release.

## Rules Resolved Caveats

- CSCeh34039

The **no proxy** rule action does not work for transparently redirected proxy style requests. This problem occurs if there is a pattern configured for a domain name, such as `abccorp.com`, and a request is given to a source that is not a FQDN (for example, `http://www`). This problem was fixed in the ACNS 5.3.3 software release.

## Other Resolved Caveats

- CSCeh16755

For HTTP POSTs through a forward proxy, uploads of large files can be slower through the Content Engine and the Content Engine advertises a TCP receive window size that is much smaller than expected. This problem is caused because the TCP receive window decreases to 2 KBytes on a POST through a forward proxy for certain applications and operating systems.

- CSCeh34279

The Content Engine does not export the transaction logs when the transaction log export feature is enabled. This problem only occurs if there are Cisco Streaming Engine logs files in the `/local1/logs/cisco-streaming-engine` directory.

- CSCeh36106  
When you enter the **show inventory**, **show hardware**, and **show sysfs EXEC** commands, you can receive errors that indicate the operation is not permitted or that permission is denied. This problem can occur when you are logged in to the Content Engine as a normal-level administrator user (a user with a privilege level of 0).
- CSCeh41983  
The DNS process can hang after a corrupted DNS response is received.
- CSCeh48047  
The Content Engine hangs or enters kernel debug mode when there is high memory usage for TCP.
- CSCeh48187  
In rare circumstances, the Content Engine may not let anyone log in. This problem only occurs if all of the following conditions exist:
  - The system file system (sysfs) is not mounted on the Content Engine.
  - TACACS or RADIUS is enabled on the Content Engine and is the primary authentication mechanism.
  - Authentication failover is configured on the Content Engine.
  - The network is up and the TACACS or RADIUS server is reachable.
 This problem was fixed in the ACNS 5.3.3 software release.
- CSCeh66703  
The CLI configurations that were specified through the **ip route** global configuration command are not retained on a Content Engine NM-CE model after the Content Engine is reloaded.
- CSCeh69177  
A “Critical: Disk failure error occurred on *disk drive in Storage Array number*” alarm is displayed on the Content Distribution Manager even though the disk has not really failed. Even though the syslog.txt shows that the disk is reset and has returned to normal operation shortly after the alarm is raised, the alarm is not reset.  
  
If you enter a **show disks details EXEC** command, the command output shows the state of the drive as normal. If the drive is bad, the command output of the **show disks details** command would show that there is a problem with the disk. This problem occurs only on storage arrays that are attached to a Content Engine model CE-7325 that is running the ACNS 5.2.3 software.
- CSCeh82112  
The DNS service can crash or hang when it receives a certain type of maliciously coded DNS request from a client.

## Documentation Updates

This section describes documentation updates.

- [New WAE Platform Support in the ACNS 5.3.3 Software Release, page 41](#)
- [Enhancements to the Envivio-Cisco Streaming Engine Interoperability, page 41](#)
- [Support of Dynamic Content Routing Added in the ACNS 5.3.3 Software Release, page 41](#)

- [Content Distribution Manager GUI-Related Changes in the ACNS 5.3.3 Software Release](#), page 41
- [CLI-Related Changes in the ACNS 5.3.3 Software Release](#), page 42

## New WAE Platform Support in the ACNS 5.3.3 Software Release

This documentation update applies to the *Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.3*.

In the ACNS 5.3.3 software release, support for three new WAE appliances, the WAE-511, the WAE-611 and WAE-7326 was added. For more information, refer to the [“Introduction of the Wide-Area Application Engine”](#) section on page 3.

## Enhancements to the Envivio-Cisco Streaming Engine Interoperability

These documentation updates apply to the following two ACNS 5.3 software guides:

- *Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.3*
- *Cisco ACNS Software Command Reference, Release 5.3*

The ACNS 5.3.3 software release includes the following enhancements that are related to Envivio-Cisco Streaming Engine interoperability:

- [Retention of m4e File Extensions for Envivio-Based Programs](#), page 4
- [Content Engine Support for Publishing of Multicast SDP Files for Cisco Streaming Engine Live Programs](#), page 5

## Support of Dynamic Content Routing Added in the ACNS 5.3.3 Software Release

This documentation update applies to the *Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.3*.

In the ACNS 5.3.3 software and later releases, the Content Router can detect changes in Content Engine coverage zones and can dynamically adjust its routing tables. For more information about support of dynamic content routing, including how to use the Content Distribution Manager GUI to configure this new feature, refer to the [“Support of Dynamic Content Routing”](#) section on page 5.

## Content Distribution Manager GUI-Related Changes in the ACNS 5.3.3 Software Release

These documentation updates apply to the *Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.3*.

- In the ACNS 5.3.3 software release, the ability to restore the factory-default settings for Real Networks license keys through the Content Distribution Manager GUI was added. For more information, refer to the [“Restoring Factory-Default Settings for Real Networks License Keys”](#) section on page 3.
- In the ACNS 5.3.3 software release, the ability to use the Content Distribution Manager GUI to configure TCP memory limits was added. For more information, refer to the [“Configuring TCP Memory Limits”](#) section on page 8.

## CLI-Related Changes in the ACNS 5.3.3 Software Release

These documentation updates apply to the following two ACNS 5.3 software guides:

- *Cisco ACNS Software Configuration Guide for Locally Managed Deployments, Release 5.3*
- *Cisco ACNS Software Command Reference, Release 5.3*

In the ACNS 5.3.3 software release, the **rtsp real-proxy default-configuration** and the **rtsp real-subscriber default-configuration** EXEC commands were respectively replaced with the **rtsp real-proxy restore factory-default** and the **rtsp real-subscriber restore factory-default** EXEC commands. For more information on this topic, refer to the [“Restoring Factory-Default Settings for Real Networks License Keys” section on page 3](#).

In the ACNS 5.3.3 software release, the ability to use the CLI to configure TCP memory limits was added. For more information, refer to the [“Configuring TCP Memory Limits” section on page 8](#).

In the ACNS 5.3.3 software release, the **rule dns-resolve each-request** global configuration command was added. For more information, refer to the [“New Rule Command for Converting Hostnames to IP Addresses” section on page 9](#).

In the ACNS 5.3.3 software release, the output of the **show programs** EXEC command was modified. For more information, refer to the [“Modified Output of the show programs EXEC Command” section on page 10](#).

## 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 these release notes, the product documentation set includes:

- *Documentation Guide and License and Warranty for Cisco ACNS Software, Release 5.3.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 5.3.x* for a complete documentation roadmap and URL documentation links for this product.

## Hardware Documentation

- *Cisco Wide-Area Application Engine 511 and 611 Hardware Installation Guide*
- *Cisco Wide-Area Application Engine 7326 Hardware Installation Guide*
- *Cisco Content 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 5.3*
- *Cisco ACNS Software Command Reference, Release 5.3*
- *Cisco ACNS Software API Guide, Release 5.3*
- *Release Notes for Cisco IP/TV Broadcast Server and Viewer Software, Release 5.2.5*
- *Release Notes for Cisco ACNS Software Program Manager for IP/TV, Release 5.3*

## 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

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

### Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>

## Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Cisco will continue to support documentation orders using the Ordering tool:

- Registered Cisco.com users (Cisco direct customers) can order documentation from the Ordering tool:  
<http://www.cisco.com/en/US/partner/ordering/>
- Instructions for ordering documentation using the Ordering tool are at this URL:  
[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

## Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—[security-alert@cisco.com](mailto:security-alert@cisco.com)

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.htm](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.htm)

The link on this page has the current PGP key ID in use.

## Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

## Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

---

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

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, 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. (0502R)