



# Release Notes for Cisco ACNS Software, Release 5.4.3

---

September 4, 2006

ACNS Build 5.4.3 b17



Note

---

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

---

## Contents

This release note document contains information about the Cisco Application and Content Networking System (ACNS) 5.4.3 software. This release note describes the following topics:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [New and Changed Information, page 3](#)
- [Important Notes, page 9](#)
- [Caveats, page 13](#)
- [Related Documentation, page 39](#)
- [Obtaining Documentation, page 41](#)
- [Documentation Feedback, page 41](#)
- [Cisco Product Security Overview, page 42](#)
- [Obtaining Technical Assistance, page 43](#)
- [Obtaining Additional Publications and Information, page 44](#)



---

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

© 2006 Cisco Systems, Inc. All rights reserved.

# Introduction

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

This release note document is intended for administrators who will be configuring, monitoring, and managing devices that are running the ACNS 5.4.3 software. This document describes the new product features, the supported hardware, and the open and resolved caveats regarding the ACNS 5.4.3 software release.

## System Requirements

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

[Table 1](#) shows the hardware platforms that are supported in each ACNS software release. An “X” indicates that the software supports the hardware models listed in that row.

**Table 1** Hardware and ACNS Software Compatibility Matrix

Hardware Model	ACNS Software Support						
	5.3.1	5.3.3	5.3.7	5.4.1	5.4.3	5.5.1	5.5.3
CE-507 CE-560 CE-590 CR-4430 CDM-4630	X	X	X	X	X	X	X
CE-7320 CDM-4650	X	X	X	X	X	X	X
NM-CE-BP-SCSI NM-CE-BP-40G NM-CE-BP-80G	X	X	X	X	X	X	X
CE-510 CE-510A CE-565 CE-565A	X	X	X	X	X	X	X
CE-7305 CE-7305A CE-7325 CE-7325A	X	X	X	X	X	X	X
CE-511 CE-566	X	X	X	X	X	X	X
WAE-511 WAE-611		X	X	X	X	X	X
WAE-7326		X	X	X	X	X	X
WAE-512 WAE-612					X	X	X

**Note**

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

## Software Component Versions Supported in ACNS Software

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

**Table 2** *Component Versions Supported in ACNS Software Releases*

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

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

**Note**

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

## New and Changed Information

This section describes new and changed features in the ACNS 5.4.3 software release.

### New Features in the ACNS 5.4.3 Software

The ACNS 5.4.3 software includes the following new features, enhancements, and changes:

- [New Hardware Features, page 4](#)
- [SmartFilter Version 4.1 Integration, page 4](#)
- [FTP Service Disabled by Default, page 5](#)
- [Node Manager Process Enhancement, page 5](#)
- [New syslog Message Added, page 5](#)
- [Ability to Specify Addresses for Translog Files, page 5](#)
- [Controls for Monitoring Outgoing Proxy Servers, page 6](#)

- [Enhancements to ICAP Support, page 7](#)
- [New Rule Pattern to Filter Content Based on the X-Forwarded-For IP Address, page 8](#)
- [Support for Content Router Request Overflow Routing, page 9](#)

## New Hardware Features

The ACNS 5.4.3 release adds support for the WAE-512 and WAE-612 appliances. (For more information about hardware support in ACNS software, see [Table 1](#).)

The WAE-512 supports a single-disk hardware configuration.

## SmartFilter Version 4.1 Integration

The plug-in for SmartFilter software Version 4.1 has been integrated with ACNS 5.4.3 software. This version of SmartFilter has the following features:

- Listens on port 9014 for block page requests.  
The ACNS caching process listens on port 9015 for blocked pages and forwards the packets to port 9014 where SmartFilter listens.
- Provides advanced block pages with a new look and feel.
- Provides a new feature called temporary user override. (See the [“About the Temporary User Override Feature” section on page 4](#).)



### Note

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

## About the Temporary User Override Feature

In the ACNS 5.4.3 software release, the temporary user override is a new feature that is available with the SmartFilter software version 4.1. This feature allows the SmartFilter plugin to override the filtering mechanism that is being applied to the user group to which users have been added in the authentication server (in Step 3). You must configure this new feature through the SmartFilter Administrator Console (version 4.1.1).

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

- Step 1** Install the SmartFilter authentication server software on the machine that is running the SmartFilter Administrator Console or on a different machine.
- Step 2** From the SmartFilter Administrator Console, add the authentication server.
- Step 3** From the SmartFilter Administrator Console, add the users to the authentication server.
- Step 4** Deploy the changes to the authentication server.
- Step 5** From the SmartFilter Administrator Console, select the Content Engine, and add the configured authentication server to the Content Engine's list of authentication servers.

- Step 6** From the SmartFilter Administrator Console, add the users who should be allowed to override the filtering mechanism in the overrides for the Content Engine.
- Step 7** Deploy the changes to the Content Engine.
- 

## FTP Service Disabled by Default

To enable FTP proxy service on port 21, the FTP server service must be disabled on the Content Engine. You cannot have both FTP server and proxy services running on the Content Engine when the FTP proxy service is configured to use port 21.

In the ACNS 5.4.3 release, a code change has been made so that FTP service on the Content Engine is disabled by default. FTP is disabled by default in the following releases:

- ACNS 5.3.7 and later 5.3.x releases
- ACNS 5.4.3 and later 5.4.x releases
- ACNS 5.5.1 (b110) and later 5.5.x releases

On Content Engines that run ACNS software releases earlier than 5.3.7, 5.4.3, and 5.5.1 the FTP server service is enabled by default.

To enable FTP server service on Content Engines where the FTP server service is disabled, use the **ineted ftp enable** global configuration command.

## Node Manager Process Enhancement

In the ACNS 5.4.3 software release, the Content Engine Node Manager process (nodemgr) generates a core file that is useful for troubleshooting before it exits.

## New syslog Message Added

A new syslog message has been added to the ACNS 5.4.3 software. Multicast-in source objects in server-side playlists are not supported for Windows Media streaming. If you have such an unsupported configuration, the Windows Media stream will fail, and the problem will be identified in the syslog file, as shown in the following example:

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

## Ability to Specify Addresses for Translog Files

In the ACNS 5.4.3 software, the **transaction-logs** global configuration command was modified, and a new option **filename** and suboption **label** have been added. These new command options allow you to configure a customized string to appear in the transaction log in the transaction-logs filename label field, which replaces the IP address field. The length of the string cannot exceed 15 characters, and only alphanumeric characters and the period (.) character are allowed.

```
ce(config)# transaction-logs filename label custom_string
```

The following example configures the filename label as 10.77.155.160.

```
ce-14(config)# transaction-logs filename label 10.77.155.160
```

The following sample **show running-config** command output shows that the new filename label is configured:

```
ce-14# show running-config

! ACNS version 5.4.3
!
!
hostname ce-14
!
http anonymizer enable
http append x-forwarded-for-header
.....
.....
transaction-logs enable
transaction-logs archive interval 120
transaction-logs export enable
transaction-logs export compress
transaction-logs export interval 10
transaction-logs export ftp-server 172.19.228.125 admin **** /temp
transaction-logs filename label 10.77.155.160 <=====
```

The following **show transaction-logging** command output shows the new filename label as it appears in the transaction log:

```
ce-14# show transaction-logging

Transaction log configuration:
-----
Logging is enabled.
End user identity is visible.
File markers are disabled.
Archive interval: 120 seconds
Maximum size of archive file: 2000000 KB Log File format is squid.
Filename label string is 10.77.155.160 <=====
Windows domain is not logged with the authenticated username
Exporting files to ftp servers is enabled.
File compression is enabled.
Export interval: 10 minutes

.....
```

## Controls for Monitoring Outgoing Proxy Servers

The ACNS 5.4.3 software supports controls in both the CLI and in the Content Distribution Manager GUI to enable and disable the monitoring of outgoing proxy servers. The following three new CLI commands are available in the ACNS 5.4.3 software:

- **http proxy outgoing monitor enable**
- **ftp-over-http proxy outgoing monitor enable**
- **https proxy outgoing monitor enable**

To enable or disable outgoing proxy monitoring using the Content Distribution Manager GUI, follow these steps:

- 
- Step 1** Navigate to one of the following configuration windows:
- For HTTP connections, choose **Devices > Applications > Web > HTTP > HTTP Connections**.

- For FTP-over-HTTP connections, choose **Devices > Applications > Web > FTP > FTP-Over-HTTP Connections**.
  - For HTTPS connections, choose **Devices > Applications > Web > HTTPS > Proxy**.
- Step 2** Check or uncheck the **Enable Outgoing Proxy Monitor** check box.
- Step 3** Click **Submit** to save your changes.
- 

## Enhancements to ICAP Support

The Internet Content Adaptation Protocol (ICAP) is an open standards protocol for content adaptation, typically at the network edge. The ACNS 5.4.3 software supports the following enhancements for ICAP support:

- [ICAP Request Modification Support for HTTPS Requests, page 7](#)
- [Compatibility with the Data Trickling of WebWasher ICAP Server, page 7](#)
- [Support for Accessing Blank Pages over ICAP-Enabled Networks, page 7](#)
- [New CLI Command and GUI support for Configuring the ICAP Connection Timeout, page 7](#)

### ICAP Request Modification Support for HTTPS Requests

The ACNS 5.4.3 software supports an ICAP request modification (reqmod) for the HTTPS proxy-style requests. Support for ICAP reqmod processing allows proxy-style requests that use the HTTPS protocol to be modified as they are sent from the Content Engine to the ICAP server on their way to the origin server. For more information on ICAP support, see the [“Interoperability with ICAP Vendors”](#) section on page 11.

### Compatibility with the Data Trickling of WebWasher ICAP Server

The ACNS 5.4.3 software allows you to download large files over an ICAP-enabled network. Because of some compatibility issues with the data trickling feature of the WebWasher ICAP server, downloading large files over ICAP-enabled ACNS networks used to fail before the download was completed. However, starting with release 5.4.3, the ACNS software has become compatible with the data trickling feature of the WebWasher ICAP server. (See resolved caveat CSCsc29267.)

### Support for Accessing Blank Pages over ICAP-Enabled Networks

The ACNS 5.4.3 software allows you to access blank pages (null body pages, where there is no content) over an ICAP-enabled ACNS network. When you try to access blank pages, earlier versions of the ACNS software used to return error messages saying that the page could not be retrieved because the server was either unreachable or temporarily busy.

### New CLI Command and GUI support for Configuring the ICAP Connection Timeout

The ACNS 5.4.3 software allows you to configure a timeout value for ICAP connections. You can configure an ICAP connection timeout value using the following CLI command:

```
CE(config)#icap connection-timeout minutes
```

You can enter a number between 1 and 480 as the ICAP connection timeout interval in minutes to allow a longer timeout interval when you want to download large files from ICAP-protected sites.

Alternatively, you can configure the ICAP connection timeout from the Content Distribution Manager GUI.

To configure the ICAP connection timeout from the Content Distribution Manager GUI, follow these steps:

- 
- Step 1** Choose **Devices > Devices**. (Alternatively, choose **Devices > Device Groups**.)
  - Step 2** Click the **Edit** icon that corresponds to the Content Engine or device group for which you want to configure the ICAP timeout interval.
  - Step 3** Choose **Request Processing > ICAP**. The ICAP Settings window for the chosen device or device group appears.
  - Step 4** To configure the ICAP connection timeout interval, enter a number between 1 and 480 in the Connection-Timeout field. The default value is 20 minutes.
  - Step 5** To save the settings, click **Submit**.
- 

## New Rule Pattern to Filter Content Based on the X-Forwarded-For IP Address

The ACNS 5.4.3 software allows you to use a new rule pattern to filter content based on the x-forwarded-for IP address in the HTTP header. The x-forwarded-for attribute contains the IP address of the device from which the request originated. Only the use-server rule action is supported for the x-forwarded-for rule pattern. The use-server action sends server-style HTTP requests from the Content Engine to the specified IP address and port on a cache miss.

You can configure the x-forwarded-for rule pattern using the following CLI command:

```
CE(config)#rule pattern-list 1 header-field x-forwarded-for ip-address
```

Alternatively, you can configure the x-forwarded-for rule pattern from the Content Distribution Manager GUI.

To configure the rule pattern from the Content Distribution Manager GUI, follow these steps:

- 
- Step 1** Choose **Devices > Devices**. (Alternatively, choose **Devices > Device Groups**.)
  - Step 2** Click the **Edit** icon that corresponds to the Content Engine or device group for which you want to configure the rule pattern.
  - Step 3** In the Contents pane, choose **Request Processing > Service Rules**.
  - Step 4** In the taskbar, click the **Create New Service Rules** icon. The Creating New Service Rules window appears.
  - Step 5** Configure a pattern list and add a pattern to it by following these steps:
    - a. From the Rule Type drop-down list, choose **pattern-list**.
    - a. In the Rule Parameters field, configure the pattern list number and the pattern type as *list-num header-field x-forwarded-for IP Address*.
    - b. To save the settings, click **Submit**.
  - Step 6** Associate an action with an existing pattern list by following these steps:
    - a. In the Creating New Service Rule window (see [Step 1](#) through [Step 4](#)), choose **use-server** action type from the Rule Type drop-down list.




---

**Note** Only the use-server rule action is supported for the x-forwarded-for rule pattern.

---

- b. In the Rule Parameter field, enter the list number of the x-forwarded-for pattern list that you want associated with this action.
  - c. To save the settings, click **Submit**.
- 

For more information about creating rule patterns and configuring rule actions, see Chapter 16, “Configuring Request Processing Services” in the *Cisco ACNS Software Configuration Guide for Centrally Managed Deployments*, Release 5.5.

## Support for Content Router Request Overflow Routing

In the ACNS 5.4.1 implementation of load-based content routing, when all Content Engines in a domain became overloaded and the configured resource utilization thresholds were exceeded, the Content Router began dropping requests.

In the ACNS 5.4.3 release, when the original domain is overloaded, client requests can be redirected to an overflow or alternate domain. This feature applies to the following two situations:

- Load-based routing is configured and all Content Engines in the domain are overloaded.
- All Content Engines in the domain are offline. (Load-based routing does not have to be configured in this instance.)

**Note**


---

The request overflow routing feature must be configured on a per-domain basis.

---

When request overflow routing is not configured for the domain requested, requests that exceed Content Engine load-based thresholds or that are otherwise undeliverable, are redirected to an error notification message, and the requests are dropped.

Request overflow routing works dynamically when Content Engines are overloaded or deactivated. When the load of one or more Content Engines in the original host domain is reduced below threshold limits or Content Engines are reactivated, new requests are routed to the original host domain automatically.

Request overflow routing supports requests from RTSP, HTTP, and MMS clients.

## Important Notes

This section emphasizes important information regarding the ACNS 5.4.x software. It includes the following sections:

- [Multicast-In Sources in SSPLs Not Supported for Windows Media Streaming](#), page 10
- [No Downgrade Script to ACNS Releases Later than 5.3.3](#), page 10
- [RAM Requirements for ACNS 5.4 Software and Websense 5.5 Software](#), page 10
- [Websense Issues When Downgrading to the ACNS 5.0 Software or ACNS 5.1 Software](#), page 10
- [Media File System Issues When Downgrading to ACNS 5.0 Software](#), page 11
- [SmartFilter Issues When Upgrading or Downgrading to Another ACNS Software Release](#), page 11

- [Interoperability with ICAP Vendors, page 11](#)
- [ICAP Performance, page 12](#)
- [ICAP Maximum File Size Supported, page 12](#)
- [Matrix of Supported Caching, Filtering, and Authentication Methods, page 12](#)

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

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

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

## No Downgrade Script to ACNS Releases Later than 5.3.3

There is no downgrade script in the ACNS 5.4.3 code base to downgrade directly to ACNS 5.3.x releases that are later than ACNS 5.3.3. To downgrade from ACNS 5.4.3 software to ACNS 5.3.x software you must use the following guidelines:

- Use the Downgrade5\_4\_to\_5\_3\_3 downgrade script if you are downgrading from ACNS 5.4.3 to any ACNS 5.3 version that is greater than or equal to ACNS 5.3.3.
- Use the Downgrade5\_4\_to\_5\_3 downgrade script if you are downgrading from ACNS 5.4.3 to any ACNS 5.3 version that is earlier than ACNS 5.3.3.
- Before or after you run the downgrade script, you must install the version of ACNS 5.3.x software that you need.

## RAM Requirements for ACNS 5.4 Software and Websense 5.5 Software

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

## Websense Issues When Downgrading to the ACNS 5.0 Software or ACNS 5.1 Software

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

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

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

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

## Media File System Issues When Downgrading to ACNS 5.0 Software

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

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

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

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

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

## SmartFilter Issues When Upgrading or Downgrading to Another ACNS Software Release

When you upgrade or downgrade the Content Engine to a different release of the ACNS software, if there is a difference in the SmartFilter plug-in version, the SmartFilter database and configuration files are deleted and default configurations are loaded. This change occurs because the configuration details might be changed with each new version of SmartFilter software. After each upgrade or downgrade of the SmartFilter plug-in, a fresh database has to be downloaded from the SmartFilter Administration Console to the Content Engine. (For a description of which SmartFilter versions are supported in the ACNS software releases, see [Table 2](#).)

## Interoperability with ICAP Vendors

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

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

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

## ICAP Maximum File Size Supported

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

## Matrix of Supported Caching, Filtering, and Authentication Methods

Table 3 lists the caching, filtering, and authentication methods supported by Content Engines that are running the ACNS 5.4.x software. An asterisk (\*) indicates that a feature is supported for that particular protocol.

Table 3 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	*							

**Table 3** Caching, Filtering, and Authentication Methods and Related Protocol Support (Continued)

Protocol	Filtering				Proxy Authentication			
	Caching	N2H2	Websense	SmartFilter	RADIUS	LDAP	NTLM	TACACS+
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 5.4.3 software. Caveats describe unexpected behavior in the ACNS 5.4.3 software. Severity 1 caveats are the most serious; Severity 2 caveats are less serious. Severity 3 caveats are moderate caveats.

## Open Caveats

This section lists caveats that have not been resolved in the ACNS 5.4.3 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 is chosen for content acquisitions from such a site, the acquirer error statistics will contain a 401 (Unauthorized) error code, and the acquirer error log will display the following error message:

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

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



**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 the following 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.

- 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 i4-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.

- 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.

- 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.
- 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.
- 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.

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

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

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

- 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 under the following conditions:

- 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.
- CSCeg56075
 

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

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

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

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

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

Workaround: 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 under the following conditions:

  - 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.

- CSCeg86386

Symptom: In a Content Router environment, users are not able to choose RTSPU (UDP) or RTPST(TCP) by requesting with `rtspu://` or `rtsp://` 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.

- 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.

- 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>.

- 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:

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

```

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

```

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

- CSCeh73477

Symptom: The acquirer experiences a problem 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.

- 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
```

- 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.

- CSCei18400

Symptom: There is a problem with playing high definition/high bit rate video on-demand streams.

Condition: This problem can occur if there are more than 14 unique 2-Mbps streams with two clients per stream (28 connections).

Workaround: There is no known workaround.

- CSCei28716

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

Condition: This problem occurs very rarely.

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

- 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.

- CSCsb61528

Symptom: The Content Engine sends the redirect assign message before it receives the “I see you” message from the router.

Condition: Because the Content Engine sends the redirect assign message before it receives the “I See You” message, the redirect assign message will always have a bad rcv-id. This problem occurs because the rcv-id is incremented as part of the router processing the “Here I am” message. Consequently, the value in the redirect assign message will be behind by 1.

Workaround: No workaround is required because although the redirect assign message will have a bad rcv-id (it will be behind by 1), the redirect assign message is resent by the Content Engine and is accepted by the router without affecting the WCCP service.

- CSCsb65952

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

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

Workaround: There is no known workaround.

- CSCsb69794

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

Condition: The problem can occur in the following situation:

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

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

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

- CSCsb72030

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

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

Workaround: There is no known workaround.

- CSCsb79685
 

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

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

Workaround: When you are using Microsoft producer to publish the content, select publish to **My Computer** and when you select the **Choose publish settings for different audiences** option do not check the **Enable rich-media Streaming** option. When the content is pre-positioned, all content that is created in publishing should be pre-positioned.
- CSCsc00804
 

Symptom: When the primary Content Distribution Manager is upgraded to the ACNS 5.3.3 software or a later release, the WCCP service to all of the registered Content Engines is interrupted. Only some of the Content Engines recover from this interruption in the WCCP service.

Condition: This problem can occur if all of the registered Content Engines are running the ACNS 5.3.3 software or a later release, and then you upgrade the Content Distribution Manager to the ACNS 5.3.3 software or a later release.

Workaround: There is no known workaround.
- CSCsc05348
 

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

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

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

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

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

Workaround: There is no known workaround.
- CSCsc14022
 

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

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

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

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

- CSCsc15499

Symptom: HTTP POST requests, which are received through HTTP1.0, can fail and a 400 Bad request error message is generated.

Condition: This problem can occur if the POST request contains an additional CRLF pair following the announced Content-Length. There are certain clients that are known to append this data to a request.

Workaround: Disable HTTP 1.0 at the client.
- CSCsc25501

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

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

Workaround: Reboot the Content Engine.
- CSCsc26852

Symptom: There is a cache assert in the `icap_in_pending_list`.

Condition: This problem can occur if the Content Engine is running the ICAP process.

Workaround: No workaround is required because the cache process automatically restarts on the Content Engine.
- CSCsc42786

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

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

Workaround: Downgrade the Content Engine to the ACNS 5.2.x software or an earlier software release.
- CSCsc44106

Symptom: The configured rules for a device group are randomized when they are applied to the Content Engine that joins the device group.

Condition: This problem occurs because the Content Distribution Manager GUI sorts the configured device group rules by the name of the rule. When you use the Content Distribution Manager GUI to configure rules for a device group, you cannot specify the precedence of a configured rule.

Workaround: There is no known workaround.
- CSCsc45058

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

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

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

- CSCsc71576

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- CSCsc81316

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

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

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

Workaround: Reload the Content Engine.

- CSCsc83129

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

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

Workaround: There is no known workaround.

- CSCsd14159

Symptom: The ICAP daemon crashes and produces core files.

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

Workaround: There is no known workaround. The ICAP daemon restarts.

- CSCsd14626

Symptom: The Content Engine sends an Internet Mail Server (IMS) request to the server well before the configured TTL period expires.

Condition: This problem occurs when the rule action **cache-non-cacheable** is configured, an HTTPS server is configured for SSL termination, and an HTTPS request is issued that matches the HTTPS server configured and also matches the pattern configured for the rule action **cache-non-cacheable**. The first request is cached, and the TTL is set as configured in the rule action **cache-non-cacheable**. However, well before the configured TTL expires, a second request is issued to the same URL that matches the rule and HTTPS server configured.

Workaround: There is no known workaround.

- CSCsd17740
 

Symptom: Stale connections are found within internal processes for pre-positioned content. The Content Engine runs out of connections and stops functioning. The stale connections accumulate at a rate of about 1K per week. The limit is 16K. These symptoms become visible after about 10 weeks.

Condition: This condition occurs when the customer is running ACNS 5.3.5b6 software and uses the Content Distribution Manager to pre-position content on the Content Engines.

Workaround: Use a script to run the **service restart cache** command every 2-3 weeks to clean up the stale connections.
- CSCsd20346
 

Symptom: The customer sees blips and experiences delays at the client that are directly related to upstream proxy failures.

Condition: This problem occurs when the ACNS 5.3.5.6 software is running on a CE-7325 that is streaming content at a rate of 400-1000 transactions per second (TPS). The downstream proxy Content Engines stream to outgoing upstream Content Engines. Each downstream Content Engine has 1 or 2 upstream Content Engines configured for failover purposes.

Workaround: None.
- CSCsd21974
 

Symptom: Changes to rules take a long time to complete.

Condition: This condition occurs when you change a rule and submit it using the Content Distribution Manager GUI, and a large number of rules are already configured.

Workaround: None. The changes will eventually complete.
- CSCsd27358
 

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

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

Workaround: There is no known workaround.

Additional Information: Because of a design limitation in the proxy cache process, the Content Engine is designed to perform a graceful close on the client end, even if the server closes the connection abruptly by sending a reset.
- CSCsd30356
 

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

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

Workaround: Restart the authmod process by using the **service restart http\_authmod** command.
- CSCsd47916
 

Symptom: HTTPS request filtering does not work properly.

Condition: This problem occurs when HTTPS request filtering is configured where WCCP transparent redirection is being used. When users request https://domain, they receive a “page cannot be displayed” 443 error message and are blocked.

Workaround: There is no known workaround.

- CSCsd57046  
Symptom: RTSP statistics show incorrect values.  
Condition: This problem occurs in cache hit cases.  
Workaround: There is no known workaround.
- CSCsd58836  
Symptom: HTTPS requests to the HTTPS proxy in the Content Engine are not served. The browser shows that the page is continuously loading. The TCP traces show that the Content Engine accepts the connection and the request, but it does not respond.  
Condition: This problem occurs when the Content Engine is using ACNS 5.3 or 5.4 software, and the HTTPS requests are coming in at 20 TPS or greater.  
Workaround: Downgrade the Content Engine to ACNS 5.2 software.
- CSCsd60376  
Symptom: Bypass servers (static or dynamic) are not accessible with WCCP enabled.  
Condition: This problem occurs when you use WCCP with an L2 mask assignment on a WCCP router. When a bypass entry is added either dynamically or statically to the Content Engine, then the site is no longer accessible through a browser.  
Workaround: There is no known workaround.
- CSCsd62968  
Symptom: The Content Distribution Manager reports the following error:  

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

  
Condition: This error occurs after upgrading to ACNS 5.4.1 software.  
Workaround: There is no known workaround.
- CSCsd66331  
Symptom: The **dns pin cname** global configuration command does not take effect on the Content Engine until after the DNS caching service is restarted.  
Condition: This problem occurs when the DNS pin configuration has changed, but the DNS queries do not reflect that configuration change.  
Workaround: Disable and then enable the DNS cache by using the **dns disable** command followed by the **dns enable** command.
- CSCsd66674  
Symptom: The RTSP gateway fails.  
Condition: The conditions that produce this problem are not known.  
Workaround: There is no known workaround.
- CSCsd66739  
Symptom: A core file from the unified error log daemon process is generated. The process restarts immediately, but any application error log messages generated during the brief period when the process is restarting are not logged.  
Condition: The conditions that produce this problem are not known.  
Workaround: There is no known workaround. The process restarts automatically.
- CSCsd69636  
Symptom: The Content Engine serves connections even when its not configured as an HTTP proxy.

Condition: This problem occurs when the Content Engine is configured as a proxy in the browser client for port 80, an HTTP request is issued to fetch content that is pre-positioned in the Content Engine, and the **http proxy incoming port** command is not configured.

Workaround: There is no known workaround.

- CSCsd72312

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

Condition: This condition occurs because there is no way to disable the DNS lookup.

Workaround: There is no known workaround.

- CSCsd78318

Symptom: Client proxy requests in a persistent connection are forwarded without modification to the origin server, and responses are not cached.

Condition: This condition occurs after the origin server responds with an HTTP status 207 error message on the previous request.

Workaround: Use the rule action **no-persistent-connection server-only** to disable persistent connections.

- CSCsd81866

Symptom: The Content Engine unexpectedly reloads.

Condition: This problem occurs when the Node Manager process (nodemgr) exits after receiving an unexpected signal, such as a signal 11 (SIGSEGV).

The syslog.txt file contains an error message and a stack backtrace of the process at the time of the exit, such as the following:

```
Nodemgr: %CE-NODEMGR-1-330065: nodemgr: signal 11 received
```

The Content Engine has been reloaded automatically by the Node Manager after it has exited once due to an unexpected signal.

Workaround: None. The problem should be reported to Cisco TAC and the syslog sent to Cisco TAC for analysis.

- CSCsd82649

Symptom: TVout programs exhibit audio skipping.

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

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

- CSCsd87378

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

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

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

- CSCsd89303

Symptom: After running for a while, the Content Engine stops serving the live stream.

Condition: The conditions that produce this problem are not known.

Workaround: Reload the Content Engine.

- CSCsd90755  
Symptom: The Content Engine stops functioning completely.  
Condition: This problem occurs under no special conditions.  
Workaround: None.
- CSCsd90763  
Symptom: The Content Engine stops functioning.  
Condition: The conditions that produce this problem are not known.  
Workaround: There is no known workaround. A power cycle is required to reload the Content Engine.
- CSCsd94410  
Symptom: Output from the show **alarms history detail** command shows the following alarm message: “The cache service died.”  
Condition: This problem occurs on the WAE-73xx and WAE-5xx appliances that are using the ACNS 5.4.1 SPECIAL4 B5 image, within 2 minutes of reloading the appliance with this software image.  
Workaround: There is no known workaround.
- CSCsd95049  
Symptom: The following major alarm is seen from the Content Distribution Manager or from the CLI for the **show alarm** command, and a core file for the exec\_show\_running-config process exists in the /local1/core\_dir directory:  
Major Alarms:  
-----  

Alarm ID	Module/Submodule	Instance
1 core_dump	sysmon	core

  
Condition: No specific conditions are known. This problem is possibly related to the multiprocessor platform, such as a CE-7325, that has been upgraded from ACNS 5.3.x to ACNS 5.4.1 software and then downgraded to ACNS 5.3.x.  
Workaround: There is no known workaround.  
An unconfirmed workaround is to reset the BIOS settings to the factory defaults during the reload sequence. This workaround requires manual intervention from the system administrator and console access to the Content Engine during the reload.
- CSCse03969  
Symptom: The SecureComputing Software “Administration Console” and “Administration Server” are not acting as expected.  
Condition: This problem occurs in SmartFilter Versions: 4.1.0.01 on Windows XP, using the ACNS 5.3.3.b8 software. The Content Engine ignores a customized download server and defaults to the list.smartfilter.com server.  
Workaround: Download SmartFilter from the default location only.
- CSCse04951  
Symptom: The Content Engine sometimes fails to serve an FTP-over-HTTP request.  
Condition: This problem occurs when an application makes an FTP-over-HTTP request for data.  
Workaround: Restart the application.

- CSCse05693

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

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

Workaround: There is no known workaround.
- CSCse08263

Symptom: Websense creates a core file every 4 minutes and causes high CPU usage.

Condition: This problem occurs when a Content Engine that is running ACNS 5.3.5.6 is taken out of the cache farm and is idle. If Websense is enabled, the CPU usage begins to climb and a core file is created every 4 minutes.

Workaround: Disable Websense.
- CSCse12310

Symptom: WMT streams that use the RTSP protocol are failing.

Condition: This problem occurs with Content Engines that are configured as Internet or Intranet proxies and all of the outbound streams are split on the outside Content Engines. The issue appears to be related to one particular website because other RTSP streams through the same Content Engines do not have this problem. Requests made directly to the site over RTSP without using the Content Engine as a proxy do not exhibit this problem.

Workaround: Disallow the RTSPT and RTSPU protocols by using the **wmt disallowed-client-protocols RTSPT RTSPU** command, and the event is streamed successfully over MMS.
- CSCse13530

Symptom: The Websense Enterprise Client Policy Manager has not been posted in the Cisco ACNS 5.4 software download site.

Condition: Without this software you cannot administer the Websense policies.

Workaround: Download the Websense Enterprise Client Policy Manager directly from Websense:  
<http://www.websense.com/global/en/Downloads/>
- CSCse19593

Symptom: The Content Engine returns a 400 bad request error message.

Condition: This condition occurs when the Content Engine receives a 304 response with a TCP FIN flag from the server.

Workaround: There is no known workaround.
- CSCse20926

Symptom: HTTPS connections are getting dropped in the middle of a transfer.

Condition: This problem occurs when CPU profiling is enabled and a large number of HTTPS requests are requested.

Workaround: Disable the CPU profiling.

- CSCse21312
 

Symptom: Devices are not able to receive configuration updates and send statistics or status information to or from the Content Distribution Manager. About 1200 Content Engines are showing as offline in the Content Distribution Manager GUI.

Condition: This communication failure occurs because the Content Engines are unable to authenticate with the Content Distribution Manager when they try to establish an SSL session. The devices are marked offline because they cannot communicate with the Content Distribution Manager.

Workaround: Restart the certmgr service by enabling and disabling RPC debugging on the device using the **debug rpc detail EXEC** command on all affected devices.
- CSCse24172
 

Symptom: Some **show** commands stop functioning and are not listed in the CLI.

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

Workaround: Reload the Content Engine to restart the parser server.
- CSCse26141
 

Symptom: LDAP authentication fails even though the correct credentials are being used.

Condition: This problem occurs when LDAP authentication is enabled on the Content Engine.

Workaround: There is no known workaround. The problem eventually corrects itself.
- CSCse30532
 

Symptom: The Content Engine hangs and produces core files for the MMS server.

Condition: This problem occurs with ACNS 5.3.5.6 software that is running on a CE-7325 and possibly on a CE-560 and CE-590.

Workaround: Reload the Content Engine.
- CSCse37329 CDM GUI:
 

Symptom: When you enter a **show** command from Content Distribution Manager a null pointer exception is issued and the command fails.

Condition: This problem occurs when you use the “Activate all Inactive CEs” icon in the Content Distribution Manager GUI Device Listing window to activate the Content Engine.

Workaround: To workaround this problem, follow these steps:

  - a. Choose **Devices > Device Activation**.
  - b. Check the **Enable Request Routing** check box.
  - c. Click **Submit**.
  - d. Uncheck the **Enable Request Routing** check box.
  - e. Click **Submit**.

You can now successfully enter **show** commands from Content Distribution Manager GUI.
- CSCse90369
 

Symptom: The Content Engine experiences an SNMP server core dump.

Condition: This problem occurs rarely and inconsistently when an SNMP query searches for the item, “actastorVersion” to fetch the version of WAFS that is running on the device. This query is valid only when the device is running WAFS, not ACNS software.

Workaround: There is no known workaround.

## Resolved Caveats—ACNS 5.4.3 Software

This section lists the caveats that have been resolved in the ACNS 5.4.3 software release.

- CSCeg60760  
Symptom: CPU usage on the Content Engine reaches 99 percent.
- CSCei91572  
Symptom: The IP ACL indexing is incorrect while moving and editing post save.
- CSCsb81163  
Symptom: The browser displays an error message that the requested URL could not be retrieved.
- CSCsb95697  
Symptom: The SNMP client is experiencing counters and gauge values of zero.
- CSCsc13494  
Symptom: A disk is marked as “bad” when a disk error threshold is reached after a transient disk failure.
- CSCsc22469  
Symptom: The Altiris RapiDeploy feature does not work with the Content Engine, but it does work with IIS.
- CSCsc75289  
Symptom: Usernames are not being used by the Websense Network Agent for user-based policy filtering.
- CSCsd02269  
Symptom: The user is unable to upload the manifest file from the Content Distribution Manager GUI.
- CSCsd04224  
Symptom: The Manifest validator hangs for large files.
- CSCsc81507  
Symptom: The Content Engine may lose the configured routes.
- CSCsc97711  
Symptom: If the configured **wmt max clients** value is equal to the default value, it will not show in the running config output.
- CSCse21542  
Symptom: The primary outgoing proxy cannot be defined from the GUI.
- CSCsd06577  
Export of transaction logs does not work.
- CSCsd06561  
Symptom: The **show transaction log** output shows false archived files.
- CSCsd11891  
Symptom: Nonbreaking spaces entered in the rule text field produce question marks (?) in the CLI.

- CSCsd20115  
Symptom: The proxy cache returns a 406 error message when the **icap append-x-headers x-server-ip** command is configured.
- CSCsd28066  
Symptom: When performing the initial setup for a Content Engine using the ACNS CLI, you cannot configure the domain name server IP address with the number 255 in the IP address.
- CSCsd30034  
Symptom: The Content Distribution Manager GUI does not recognize the entry limitations of the static bypass list.
- CSCsd38167  
Symptom: The Content Engine is in a deadlock state and is not caching the content.
- CSCsd40679  
Symptom: A formatting change in the error log is causing parsing problems.
- CSCsd42056  
Symptom: After upgrading to the ACNS 5.4.1 software and SmartFilter 4.1.0, the CPU usage jumps to 100 percent.
- CSCsd47637  
Symptom: The RTSP VoD program fails if the RTSP source URL uses a hostname.
- CSCsd47975  
Symptom: Binary uploads fail when ICAP is enabled on the Content Engine.
- CSCsd54886  
Symptom: WCCP-redirected HTTP requests on ports other than port 80 fail to play for MMS-over-HTTP.
- CSCsd57339  
Symptom: A non-admin SFTP login allows access to a UNIX filesystem.
- CSCsd57898  
Symptom: If a Program Manager is taken off line and restored, and the manifest file for a pre-positioned channel is checked before the Program Manager database is restored, then the root and edge Content Engines will not show any media left in their channels.
- CSCsd58287  
Symptom: When reverse DNS lookup is configured for uncategorized requests in SmartFilter, the Content Engine CPU usage reaches 100 percent.
- CSCsd58837  
Symptom: When you add a standby Content Distribution Manager to a large group of managed Content Engines, the process of adding a new or replacement standby Content Distribution Manager and the database update required causes the primary Content Distribution Manager to show multiple Content Engines as offline.
- CSCsd59596  
Symptom: The cache process stops communicating with the ICAP daemon.

- CSCsd61442  
Symptom: The Content Engine does not send a transaction log to the Windows Media Server in the case of a cache hit for RTSP or MMS requests.
- CSCsd65189  
Symptom: The ICAP daemon is not handling HTTP 304 requests properly.
- CSCsd66292  
Symptom: The time stamp in the acquisition and distribution transaction log is incorrect.
- CSCsd66384  
Symptom: A 400 Bad request error message is displayed in the client browser after receiving a 200 OK message with the TCP FIN flag set.
- CSCsd69378  
Symptom: The MMS server crashes while parsing PLAY messages.
- CSCsd70190  
Symptom: The HTTP cache process fails and restarts when user authentication and rules are enabled.
- CSCsd73961  
Symptom: The **show statistics http savings** output in the CLI shows the cache hit ratio as a percentage, while the Content Distribution Manager GUI (**Devices > Statistics > Content Engines > HTTP**) shows the HTTP cache hit ratio as a decimal. The statistic should be shown as a percentage in the GUI to match the output in the CLI.
- CSCsd76836  
Symptom: The requirement to send the 0-carousel pass file automatically during a multicast program is no longer needed.
- CSCsd78727  
Symptom: The ACNS software is accepting proxy-style requests on ports 553 and 554.
- CSCsd78914  
Symptom: The ACNS Content Distribution Manager and Content Engines appear to be down, even though they are running.
- CSCsd82687  
Symptom: The Content Engine reboots with the following error in the syslog:  

```
%CE-NODEMGR-0-330045: Rebooting the device because service 'dataserver' is dead
```
- CSCsd86169  
Symptom: The Content Engine shows as offline in the Content Distribution Manager GUI. The device is not accessible through the LAN, but responds to console access. The hostname and default gateway configuration settings are lost.
- CSCsd91249  
Symptom: The Websense User Service cannot enumerate common names with commas.
- CSCsd75392  
Symptom: After upgrading to the ACNS 5.4.1 software, some .asf content no longer streams.

- CSCse07773  
Symptom: Add limit checking for the metaR & metaS processes so that these processes can be restarted once a certain limit is reached.
- CSCse21498  
Symptom: A core file is generated when you attempt to play content that is no longer available.
- CSCse21941  
Symptom: The service “rpc\_httpd” stops with the following messages seen in the syslog.txt:  

```
%CE-NODEMGR-3-330025: Service 'rpc_httpd' died due to signal 25: File size limit exceeded %CE-NODEMGR-5-330032: Stopping service: 'rpc_httpd'.
```
- CSCse22837  
Symptom: The ACNS Windows Media Server serves certain WMV files with audio only and no video.
- CSCse14327  
Symptom: The proxy returns a 400 bad request error message to the client.
- CSCse21941  
Symptom: Writing to the /local1/logs/apache/error\_log.rpc file fails because the file size is greater than 2 GB.
- CSCse26956  
Symptom: Large file downloads fail when ICAP is enabled.
- CSCse34873  
Symptom: The MMS server generates a core file when a broadcast alias in the Content Engine is created with a server-side playlist (SSPL) that has a multicast-in source.  
The core file problem is resolved; however, multicast-in for SSPL is not supported. A new syslog message has been added to the ACNS 5.4.3 software to identify this issue.  
If this unsupported configuration is used, the player remains in a buffering state, and the Content Engine generates the following syslog message:  

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

## 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 following documents are included in the product documentation set:

- *Documentation Guide and License and Warranty for Cisco ACNS Software, Release 5.4.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 5.4.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 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 5.4*
- *Cisco ACNS Software Command Reference, Release 5.4*
- *Cisco ACNS Software API Guide, Release 5.4*
- *Cisco ACNS software Program Manager for IP/TV User Guide, Release 5.4*
- *Release Notes for Cisco ACNS Software Program Manager for IP/TV, Release 5.4*

## Online Help

- 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

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML 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= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

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

## Ordering Documentation

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/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at [tech-doc-store-mkpl@external.cisco.com](mailto:tech-doc-store-mkpl@external.cisco.com) or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

## 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 submit comments about Cisco documentation 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 will find information about how to:

- 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, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at 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 have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—[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.

- For 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 (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.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.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

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

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

## 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)**—An existing 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 operations 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 the network is impaired, while 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.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

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

- 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, 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, 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, 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. (0601R)