



# Release Note for Cisco ACNS Software, Release 5.5.7

---

February 4, 2009



**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 contains information about the Cisco Application and Content Networking System (ACNS) 5.5.7 software. The ACNS software combines the technologies of demand-pull caching and pre-positioning for accelerated delivery of web applications, objects, files, and streaming media; the ACNS software runs on Cisco Content Engines, Content Distribution Manager, and Content Router hardware platforms, as well as Cisco Wide Area Application Engine appliances.

This release note is intended for administrators who will be configuring, monitoring, and managing devices that are running the ACNS 5.5.7 software. This release note describes the new product features, the supported hardware, and the open and resolved caveats regarding the ACNS 5.5.7 software.

This release note contains the following topics:

- [Hardware and Software Components Supported, page 2](#)
- [Network Module Support, page 3](#)
- [HTTP Follow-Redirect Feature, page 4](#)
- [Operating Condition for ACNS Content Preloading, page 8](#)
- [Open Caveats in Software Version 5.5.7, page 8](#)
- [Resolved Caveats in Software Version 5.5.7, page 23](#)
- [Related Documentation, page 26](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 26](#)



---

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

© 2006 Cisco Systems, Inc. All rights reserved.

# Hardware and Software Components Supported

This section describes which hardware and software products are compatible with the ACNS 5.5.7 software. This section includes the following topics:

- [Hardware Platforms Supported in ACNS Software, page 2](#)
- [Software Component Versions Supported in ACNS Software, page 3](#)

## Hardware Platforms Supported in ACNS Software

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


**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.

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

Hardware Model	ACNS Software Support							
	5.3.1	5.3.3	5.3.7	5.4.1	5.4.3	5.5.1	5.5.5	5.5.7
CE-507 CE-560 CE-590 CR-4430 CDM-4630	X	X	X	X	X	X	X	X
CE-7320 CDM-4650	X	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	X
CE-510 CE-510A CE-565 CE-565A	X	X	X	X	X	X	X	X
CE-7305 CE-7305A CE-7325 CE-7325A	X	X	X	X	X	X	X	X
CE-511 CE-566	X	X	X	X	X	X	X	X
WAE-511 WAE-611		X	X	X	X	X	X	X
WAE-7326		X	X	X	X	X	X	X

**Table 1** Hardware and ACNS Software Compatibility Matrix (continued)

Hardware Model	ACNS Software Support							
	5.3.1	5.3.3	5.3.7	5.4.1	5.4.3	5.5.1	5.5.5	5.5.7
WAE-512 WAE-612					X	X	X	X
NME-WAE-502-K9								X

## Software Component Versions Supported in ACNS Software

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

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

ACNS Software Release	SmartFilter Version Supported	Websense Version Supported
ACNS 5.2.1	Version 4.0.1	Version 5.2
ACNS 5.3.x	Version 4.0.1	Version 5.2
ACNS 5.4.1	Version 4.0.1	Version 5.5.2 <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
ACNS 5.5.5	Version 4.1.1	Version 5.5.2
ACNS 5.5.7	Version 4.1.1	Version 5.5.2

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

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 may lead to a communication failure.

## Network Module Support

The ACNS 5.5.7 software provides support for the Cisco NME-WAE-502-K9 network module. The network module is a standalone Wide Area Application Engine (WAE) that plugs into a host Cisco access router that runs Cisco IOS software. The ACNS 5.5.7 software, a Linux system-based application, resides on the network module and has its own startup and run-time configurations that are independent of the Cisco IOS configuration on the router.

Because the network module does not have an external console port, you must configure the network module by initiating a Telnet session or by initiating a configuration session from the router CLI. For more information about configuring the network module, see the *Configuring Cisco Access Routers and NME-WAE Network Modules for ACNS Deployments* document.

After initial setup, which requires using router configuration commands, configure the NME-WAE in the same manner as other ACNS devices, with the following exceptions:

- The NME-WAE cannot serve as a Content Distribution Manager for other ACNS devices.
- The NME-WAE does not support device mode configuration. The device mode configuration prompt has been removed from the NME-WAE startup script.
- Websense URL-filtering is not supported for the NME-WAE-502.

The ACNS software does not support the following hardware-related features for the network module:

- USB port
- Compact Flash utilization LED
- Software reset button

**Note**

Although the software does not support the software reset button, the hardware will reset if you press the reset button for more than 4 seconds.

## HTTP Follow-Redirect Feature

The ACNS 5.5.7 software supports a new HTTP and HTTPS filtering option (**http follow-redirect**) that allows the Content Engine to access content objects from a list of servers that match the hostname (or IP address) and URL path prefix that you specify in the configuration. This feature allows ACNS to host content and provide accelerated delivery for third-party applications that use dynamically-generated access URLs.

This section describes the HTTP follow-redirect feature and contains the following configuration information:

- [Configuring HTTP Follow-Redirect Filtering Using the Content Distribution Manager GUI](#)
- [Configuring HTTP Follow-Redirect Filtering Using the Content Engine CLI](#)
- [Viewing HTTP Follow-Redirect Filtering Statistics](#)
- [Configuring a Custom Error Page](#)

To implement this feature, three new global configuration commands have been added to the CLI and corresponding configuration settings have been added to the Content Distribution Manager GUI. You must enter all three of these new commands to configure the Content Engine to intercept and follow the HTTP or HTTPS 302 redirect responses.

If you enable this feature, but do not configure all of these commands, then the 302 response from the issuing server is sent directly to the client instead of to the Content Engine, and the location of the origin server is exposed to the client. The result occurs when the CLI-configured hostname does not match the hostname in the request from client or when the CLI-configured path prefix does not match the prefix in the 302 redirect URL received by the Content Engine.

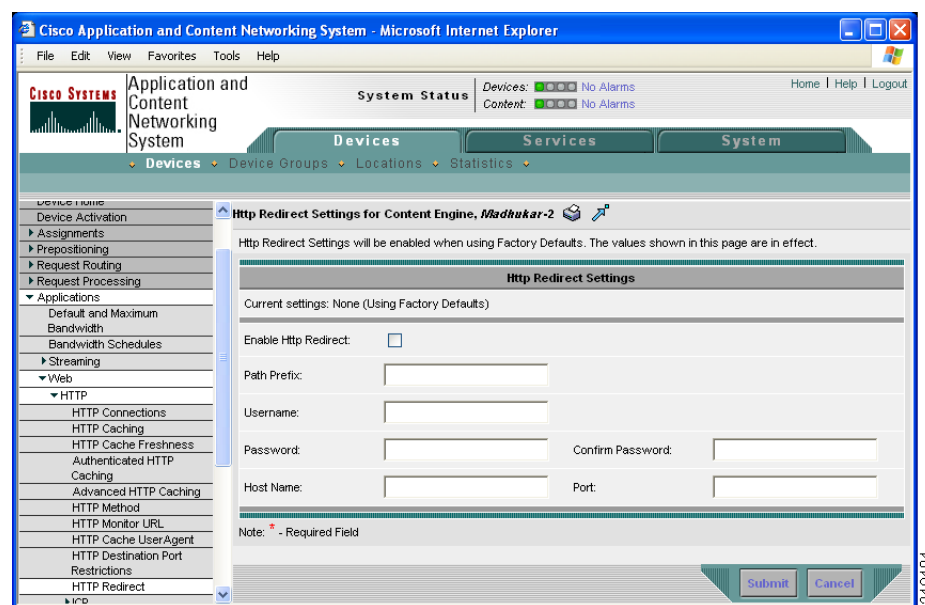
If you do not configure the username and password, or if the username or password is rejected by the origin server, the server sends a standard 500 class error code to the client. In ACNS 5.5.7 software, you may configure the Content Engine to download and send a customized error message page instead of the standard error message.

## Configuring HTTP Follow-Redirect Filtering Using the Content Distribution Manager GUI

To configure a Content Engine or Device Group to intercept and follow HTTP or HTTPS 302 redirect responses, follow these steps:

- Step 1** From the Content Distribution Manager GUI, choose **Devices > Devices** (or **Device Groups**).
- Step 2** Click the **Edit** icon next to the Content Engine or Device Group that you want to configure. The Contents pane appears on the left.
- Step 3** Choose **Applications > Web > HTTP > HTTP Redirect**. The HTTP Redirect Settings window appears. (See [Figure 1](#).)

**Figure 1** HTTP Redirect Settings Window



- Step 4** To enable the Content Engine to intercept and follow 302 redirect responses from a specified server or servers, check the **Enable Http Redirect** check box.
- Step 5** In the Path Prefix field, enter the prefix of the URL to be followed if a match occurs. You may enter a maximum of 255 characters.
- Step 6** To allow the Content Engine to authenticate itself with the origin server, do the following:
  - Enter a valid username in the Username field. You may enter 1 to 127 characters. The following special characters are not allowed in the username field: + = ; ? < >
  - Enter a password string in the Password field. To confirm the password, reenter the same string in the Confirm Password field. You may enter 1 to 127 characters. The password field does not restrict special character usage.
- Step 7** In the Host Name field, enter the hostname of the server sending the redirect responses that the Content Engine is to follow. You may enter hostnames for a maximum of 8 different servers.

This field instructs the Content Engine to follow 302 redirect responses from these servers only.

- Step 8** In the Port Field, enter the port number from which the server sends redirect responses. The port range is 1 to 65535.
- You may configure the Content Engine to follow the 302 redirects for HTTPS content by configuring an HTTPS port (such as, 443 or 8443) in this field.
- Step 9** To save your settings, click **Submit**.

## Configuring HTTP Follow-Redirect Filtering Using the Content Engine CLI

To use the CLI to configure the Content Engine to intercept and follow HTTP 302 redirect responses, enter all three of the global configuration mode commands shown in Table 3. All three commands are mutually exclusive and may be entered in any order.

**Table 3** Configuring the HTTP Follow-Redirect Feature

GUI Parameter	Function	CLI Command
Enable Http Redirect	Enables special handling of HTTP 302 responses. The default is disabled.	<b>http follow-redirect enable</b>
Path Prefix	Applies special follow-redirect handling of 302 responses to URLs that contain the specified prefix only. The prefix field may contain 1 to 255 characters.	<b>http follow-redirect server</b> { <i>server-ip</i>   <i>hostname</i> } <i>port</i> <b>path-prefix</b> <i>prefix</i>
Username Password	Configures the username and password used by the Content Engine to authenticate itself with the origin server when retrieving the content. Supports basic and MD5 digest authentication.  The <i>username</i> and <i>password</i> fields may contain 1 to 127 characters.  Valid characters for <i>username</i> are alphanumeric characters (a-z, A-Z, 0-9) and the following special characters: ! @ # \$ % ^ & ( ) - _ { } . ~ `.  The following special characters are not valid for <i>username</i> : + = : ; ? < >	<b>http follow-redirect server-authentication</b> <i>username password</i>
Host Port	Applies special follow-redirect handling of 302 responses generated by the server and port that are specified.  You may configure the Content Engine to follow the 302 redirects for HTTPS content by configuring an HTTPS port (such as, 443 or 8443) in this field.  You may configure a maximum of 8 servers by using this command. Each server must be configured separately in its own command line.	<b>http follow-redirect server</b> { <i>server-ip</i>   <i>hostname</i> } <i>port</i>

## Viewing HTTP Follow-Redirect Filtering Statistics

To view statistics for the HTTP follow-redirect filtering feature, use the **show statistics http follow-redirect** EXEC mode command. Use this command to monitor or troubleshoot HTTP follow-redirect filtering.

Table 4 describes the fields in the **show statistics http follow-redirect** display.

**Table 4** Field Descriptions for the **show statistics http follow-redirect** Command

Field	Description
Total Requests received	Total number of HTTP and HTTPS requests received by the Content Engine.
Host match	Number of requests that matched the host and port configured through the <b>http follow-redirect</b> configuration mode command.
Redirects Received	Number of host- and port-matched requests that received a 302 reply.
Total Redirects Followed	Number of requests that matched host and port and received a 302 reply for which the prefix was also matched.
Prepositioned Follow Redirect Content	Number of followed requests that were pre-positioned.
Cache Hit Follow Redirect Content	Number of followed requests that were cache hits.
Cache Miss Follow Redirect Content	Number of followed requests that were cache misses.
Basic Authentication required	Number of followed requests that needed Basic authentication.
Digest Authentication required	Number of followed requests that needed Digest authentication.
Unsupported Authentication scheme	Number of followed requests for which a 401 error was received for an authentication scheme which was neither Basic nor Digest.
Authentication failure	Number of followed requests for which authentication was required but the credentials configured through the <b>http follow-redirect server-authentication</b> configuration command did not work.
Error responses	Number of followed requests for which the Content Engine was not able to retrieve the content and returned a 500 error.  For example, the followed request may have failed because of an authentication failure or an object was not present.

## Configuring a Custom Error Page

ACNS 5.5.7 software supports the ability to download a customized error message page that the Content Engine sends when the HTTP follow-redirect URL fails. To configure the Content Engine to download and send a custom error page, use the **http custom-error-page** EXEC mode command.

**http custom-error-page download http-follow-redirect-failed** *file\_url*

In the *file\_url* field, enter the URL from the location where the file is to be retrieved. The file size limit is 16K. When you issue this command, the error message page is downloaded to the Content Engine. The Content Engine sends this page instead of the standard error page, which states, “HTTP follow redirect failed.”

## Operating Condition for ACNS Content Preloading

ACNS software parses HTTP URLs for username and password, but does not parse FTP URLs for username and password. By design, ACNS software supports authentication for HTTP requests only. We recommend that you use anonymous FTP URLs or use an HTTP server for preloading content. Only anonymous FTP URLs may be preloaded.

## Open Caveats in Software Version 5.5.7

This section lists the open caveats in the ACNS 5.5.7 software. The open caveats are grouped into the following categories:

- [Windows Media Open Caveats, page 8](#)
- [Miscellaneous Open Caveats, page 13](#)

### Windows Media Open Caveats

- CSCeg86386  
Symptom: In a Content Router environment, you cannot choose RTSPU (UDP) or RTPST (TCP) when you request `rtspu://` or `rtspt://` from Windows Media Players. In addition, when you request an RTSPU stream, an RTSPT stream is returned instead. When you specify the **wmt disallowed-client-protocols rtspu** global configuration command, it does not prevent clients from being served for a request `rtspu://crfqdn/file.asf` and returns an RTSP stream instead of an error.  
Condition: This problem occurs when you use a Content Router for RTSP redirection.  
Workaround: The restricted protocol cannot be played; however, as a partial solution, another protocol is chosen instead of returning an error message.
- CSCsb79685  
Symptom: When a WMT stream is pre-positioned, the audio works but the playback of embedded slides in the pre-positioned WMT stream are not displayed.  
Condition: This problem occurs if you use Microsoft presenter to create a WMT stream that has embedded slides. When this content is pre-positioned, WMT opens and the audio works but the slides never appear.  
Workaround: When you are using Microsoft producer to publish the content, choose publish to **My Computer**. When you choose the **Choose publish settings for different audiences** option, do not check the **Enable rich-media Streaming** option. When the content is pre-positioned, all content that is created in publishing should be pre-positioned.

- CSCsc07702
 

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

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

Workaround: Use a QuickTime player instead of a PacketVideo player.
- CSCsd63199
 

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

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

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

Symptom: The RTSP request fails.

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

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

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

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

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

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

Contact your IXIA support specialist for further IXIA IXLoad support information.
- CSCsd98883
 

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

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

Workaround: This problem affects statistics only; it does not affect functionality.

- CSCsd98892
 

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

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

Workaround: None.
- CSCsd99636
 

Symptom: More outgoing bandwidth is consumed than expected.

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

Workaround: The bandwidth allocation is reset as soon as playback ends for that stream.
- CSCse00701
 

Symptom: Outgoing bytes are not getting incremented in a timely fashion.

Condition: Outgoing byte statistics are incremented in the CLI only when control events (such as pauses or stops) occur on active streams. This condition occurs during VoD, proxy, or live playback for Windows Media streams.

Workaround: Click any control event, such as pause, and then view the bytes being incremented by using the **show statistics wmt bytes outgoing EXEC** command.
- CSCse06358
 

Symptom: Even when a multicast station is removed from the Content Engine, the Current field of the Number of Concurrent Active Multicast Sessions section in the **show statistics wmt multicast** command output shows a value. The field is not cleared even after you enter the **clear statistics wmt** command. This problem does not affect the functionality.

Condition: This condition occurs when a multicast station is stopped and removed from the Content Engine.

Workaround: None.
- CSCse07034
 

Symptom: The incoming bandwidth does not restrict the multicast source.

Condition: This condition occurs when an RTSP source is directed to the multicast station.

Workaround: Use an HTTP source for the multicast station.
- CSCse07737
 

Symptom: The outgoing bytes keep incrementing.

Condition: When a multicast station is started and stopped quickly 10 times or more, the Outgoing Bytes field of the **show statistics wmt multicast** command keeps incrementing even though multicasting is stopped. Also, the Aggregate Multicast-out Bandwidth field is not cleared until you restart the WMT program.

Workaround: Avoid rapid multiple starts and stops during a WMT multicast program.

- CSCse08370
 

Symptom: The Windows Media Player stays in the buffering state and then disconnects.

Condition: In a very high-latency network (>100 ms), when playback is over RTSP (UDP) for a multi-bit-rate stream, retransmission requests may lag behind and cause this problem.

Workaround: The workaround consist of the following three methods:

  - a. Request the file stream again.
  - b. Reduce the latency in your network.
  - c. Use rtspt:// in the URL.
- CSCse15691
 

Symptom: The incoming bandwidth usage statistics for broadcast server-side-playlists continue to increment.

Condition: This problem occurs when there are more than 100 requests for a server-side-playlist that switches streams every 1 minute. This condition is not seen for a lower number of requests.

Workaround: None.
- CSCse21472
 

Symptom: The Content Engine appears to be in a hung state and does not respond to ping, Telnet, or to requests.

Condition: This condition occurs when a Content Engine receives 200 live-splitting requests for a combination of fast-switching server-side playlists that have streams switching every 1 minute and that have their multi-bit-rate encoder source encoded with 8 different bit rates.

Workaround: Stop incoming requests from clients. If the software does not recover, reload the Content Engine.
- CSCsf97988
 

Symptom: The wmt\_be process generates a core file during the server\_parse phase.

Condition: This problem occurs during VoD stress testing for pass-through content when you use the Windows Media load simulator.

Workaround: If this problem occurs, save the core files and the WMT error logs to assist TAC in debugging the problem.
- CSCsh15218
 

Symptom: The wmt\_be process generates a core file.

Condition: This problem occurs during stress testing of a managed live unicast out-only program with a live SSPL source.

Workaround: If this problem occurs, save the core files and the WMT error logs to assist TAC in further debugging the problem.
- CSCsh16683
 

Symptom: The wmt\_be process hangs in the read phase, and outgoing bandwidth is not fully released.

Condition: This problem occurs during proxy VoD stress testing after two to three hours of testing.

Workaround: Use the **clear wmt incoming (outgoing)** command to clear the session.

- CSCsh36505

Symptom: UNS resolution fails for WMT managed live multicast program.

Condition: This occurs when the domain name of the Content Engine, which is the root for the live multicast program, is configured as the os-fqdn of a channel other than the one that is assigned to the managed live multicast.

Workaround: Use the root Content Engine's domain name or IP address as the os-fqdn of a channel that will be assigned to the managed live multicast out program. Use the root Content Engine's IP address (instead of domain name) if it is going to be assigned as the os-fqdn of a channel other than one that will be assigned to a WMT multicast out program.

- CSCsi29474

Symptom: The Windows Media Managed Live Program start time increments or decrements by one hour when the program is scheduled near the start or end of the daylight savings transition. Although the GUI displays the incorrect program start time, the value in the CDM database shows correctly. This incorrect schedule time occurs when the GUI tries to retrieve the program schedule from the CDM database.

Condition: When any program is configured on March 11, between 1 and 7 o'clock, it is automatically incremented by one hour. When the program is configured for Nov. 4, between 2 and 6 o'clock during the ending of DST time, the program is decremented by one hour. This behavior is also seen for 2008 DST, both for the starting and the ending time period.

Workaround: During these transition time periods, programs may be scheduled by entering a start time of one hour less during the DST start period, or one hour more during the DST end period. For example, if the program is to begin March 11, at 6:00, then enter March 11, 5:00 in the CDM GUI. Similarly, if the program is to begin Nov. 4, at 6:00, then enter Nov. 4, 7:00 in the CDM GUI.

- CSCsj58290

Symptom: Windows Media Player displays one of the following error messages when trying to view specific WMV files through the ACNS WMT server.

- With WMP version 10: Windows Media Player encountered an unknown error. This error may occur when another program or operating system component encounters a problem but does not communicate the nature of the problem to the Player.
- With WMP version 9: Windows Media Player encountered an unknown error.

Condition: The problem happens when Windows Media Player is set to use only TCP and is applicable for the RTSP protocol (which might also be used for mms:// URLs).

Workaround: Set Windows Media Player to use only the UDP option (though this might not work due to firewall or NAT issues). Alternatively, use ACNS version 5.5.5 or later, on which the problem could not be reproduced.

## Miscellaneous Open Caveats

- CSCdy82311

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

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

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

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

Workaround: Use one of these workarounds:

- Use weak authentication.
- On the secure server, use a certificate that was generated by one of the standard certificate authorities. Refer to the certificate list in the *Cisco ACNS Software Upgrade and Maintenance Guide, Release 5.x* document to determine which CA certificate to install on your origin servers. Note that the certificate list differs based on the version of the ACNS software.

- CSCea51815

Symptom: When a Content Engine model CE-565 is attached to a Storage Array SA-7 device, if the cache file system (cfs) partition is allocated a large portion of the disk space (approximately 160 GB or greater), 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. The Storage Array device is used for the cache file system (cfs).

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

- CSCed68727

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

Condition: This problem occurs if there is a coverage zone configuration change that causes already-imported coverage zone files to refer to invalid Content Engines.

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

- CSCed77655

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

Condition: The **http l4-switch spoof-client-ip enable** global configuration command turns on IP spoofing on a Content Engine that is functioning as a caching engine. When a **rule action use-server** global configuration command is used, the Content Engine stops spoofing the client IP address and instead uses its own IP address to retrieve 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 IP address for the physical addresses. You then configure a real IP address that floats between the two interfaces. If you then configure SNMP traps, the traps are being sourced from the dummy IP address and not the routable IP address. Therefore, the NMS host does not know from where the trap originates.

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 IP address of the SNMP agent.
- CSCee67330

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

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

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

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

Condition: This problem occurs rarely. In 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 disabled. In such cases, NTLM authentication still occurs, although the output of the **show running EXEC** command shows that the NTLM server is disabled on the Content Engine.

Workaround: reenter the **no ntlm server enable** global configuration command on the Content Engine.
- CSCee92698

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

Condition: This problem occurs when the Content Engine is running the ACNS 5.5.7 software, and you configure two or more ICAP services to subscribe to the same vectoring point (the response modification [RESPMOD] vectoring point).

Workaround: None. This problem has not been seen in any of our customer sites; the scenario was assumed by our testing team in an attempt to provide support in future releases.

- 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: None. This problem has not been seen in any of our customer sites; the scenario was assumed by our testing team in an attempt to support this scenario in future releases based on the need.

- CSCef60282

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

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

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

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

- CSCef67934

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

Condition: This problem occurs in the following circumstances:

- 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:

The system had trouble processing your last request.

This situation occurs in the following circumstances:

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

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

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

- CSCeg56075

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

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

Workaround: Set the reconnect to manual instead of automatic.

- CSCeg82405

Symptom: The Internet Explorer client retrieves a partial (incomplete) customized error page and displays it along with 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: Use a non-IE client browser. This problem does not occur with non-IE client browsers.

- CSCeg84004

Symptom: NTLM authentication for a valid user may take a longer period than usual (approximately two minutes) if the client sends the request when the Content Engine has been idle for 12 or more hours.

Condition: This problem occurs in the following circumstances:

- NTLM request authentication is enabled on the Content Engine.
- The request is sent after the Content Engine has been idle for 12 or more hours.
- The client machine has some malfunctioning program (for example, spyware or a virus) and is sending HTTP requests to the Content Engine along with the first request from the browser. The user agent is named Tioga, and the request is as follows:

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

where *somehostname* is a hostname.

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

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

- CSCeh23466

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

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

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

- CSCeh35923

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

Condition: This problem only occurs under the following condition:

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

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

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

- CSCei01668

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

Condition: This problem occurs 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 inside the firewall 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 fail at the firewall.

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

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

- CSCei28716

Symptom: The system stops functioning and there are kernel core dumps.

Condition: This problem occurs rarely.

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

- CSCsb69794

Symptom: There is no option available in the Websense GUI for configuring the Winix NTLM Settings (Windows NT Directory/Active Directory [Mixed Mode]).

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

Workaround: None.

- 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 after the initial failure to load a page occurs, subsequent reloads will succeed.

- CSCsc14022

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

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

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

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

- CSCsc25501

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

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

Workaround: Reload the Content Engine.
- CSCsc45058

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

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

Workaround: Use the QuickTime player or a VLC client to view the content from a Microsoft Windows computer.
- CSCsc81316

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

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

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

Workaround: Reload the Content Engine.
- CSCsc83129

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

Condition: This problem occurs when a Content Engine 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: You must upgrade to a version of the ACNS 5.4.x software in which this issue has not been seen.
- CSCsd66331

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

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

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

- CSCsd69768

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

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

Workaround: Enter the **https server server\_name host FQDN** global configuration command on the Content Engine after you have modified the IP address that corresponds to the HTTPS server host FQDN on the DNS server.
- CSCsd72312

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

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

Workaround: None.
- CSCsd82649

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

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

Workaround: Downgrade to the ACNS 5.1.9.5 software.
- CSCsd87378

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

```
Network name cannot be found
```

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

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

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

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

Workaround: None.
- CSCsg8356

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

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

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

- CSCsh46848  
Symptom: The Content Engine cache process restarts continuously and creates core dumps.  
Condition: This problem occurs when ACNS 5.5.5 software is running on a Content Engine with an external storage array and a CFS partition size that is greater than 440 GB. This defect is not seen on Content Engines running versions prior to the ACNS 5.5.5 release. This caveat is not seen on Content Engines running the ACNS 5.5.5 software that are using the internal disk drives because the maximum CFS partition size for internal disks is 384 GB.  
Workaround: Reduce the CFS partition size to less than 440 GB.
- CSCsi10052  
Symptom: A core file is generated in the ftp\_ctlpxy.  
Condition: The Content Engine is operating as an FTP proxy.  
Workaround: None. The process is restarted after a few tries.
- CSCsi47286  
Symptom: A cache core file is seen in the /local1/core\_dir. The core file is located in sf\_lookup\_ldap\_groups.  
Condition: Smartfilter is enabled.  
Workaround: None. The cache process restarts on its own.
- CSCsj07968  
Symptom: Database corruption occurs when a large number of Content Engines are added to a new device group or channel, or are registered to the Content Distribution Manager.  
Condition: The site has about 2,200 Content Engines, but the exact number of Content Engines that cause the database corruption has not been identified yet.  
Workaround: Perform database maintenance regularly, and especially before adding Content Engines to a channel, by using this CLI command: **cms database maintenance full**
- CSCsj07986  
Symptom: An SNMP core file is generated.  
Condition: This problem occurs in a lab environment with very little traffic. A MIB walk was done just before the core was generated.  
Workaround: None.
- CSCsj08016  
Symptom: The webserver module caused a crash.  
Workaround: None.
- CSCsj21531  
Symptom: Retrieving objects on HTML pages causes long delays (from 3 to 15 or more seconds).  
Condition: This problem occurs when the first configured name server is down and replies with ICMP unreachable for the DNS queries.  
Workaround: Either remove the first name server from the configuration, or fix the server problem.

- CSCsj26798  
Symptom: An SNMP core file is generated.  
Condition: This situation occurs rarely, when no one is working on the device.  
Workaround: None.
- CSCsj27748  
Symptom: An SNMP core file is generated.  
Condition: This problem occurs when there is an unexpected null pointer.  
Workaround: None.
- CSCsj49720  
Symptom: When deleting a reference to a PAC file template, the other previously configured PAC file template references stop working.  
Condition: This problem occurs after a CDN update.  
Workaround: Delete all the PAC file templates and reregister them, or reregister the deleted PAC file template.

## Resolved Caveats in Software Version 5.5.7

This section lists the caveats that have been resolved in the ACNS 5.5.7 software.

- CSCsc10623—In the **show http-authcache** display, the domain is displayed in lower case.
- CSCsd91271—Requests are forwarded to the outgoing proxy on port 65533, regardless of the configured port.
- CSCsd99435—Windows Media Player displays, “Attempting to reconnect,” when playing server-side playlists that contain multi-bit-rate (MBR) streams using RTSP.
- CSCse02533—The remote HTTP source counter increments for the multicast-in source.
- CSCse12809—The Content Engine sends an HTTP 500 error to one of the clients during a live split of a managed live unicast program.
- CSCse17190—The Windows Media Player attempts to reconnect when it reaches an end of stream (EOS) of the broadcast alias.
- CSCsf28637—Unexpected message output is displayed after disabling debug.
- CSCsg25802—A wmt\_mbe core file is generated by the rebroadcast program.
- CSCsg51735—Smartfilter Control List download fails often.
- CSCsg60334—The IP address of a shutdown interface is used in WCCP updates.
- CSCsg60700—The Content Engine may not remain in the device group when placed in the group from the GUI.
- CSCsg82905—The wmt\_be process generates a core file during stress testing.
- CSCsg83562—The Content Router returns a 404 response for RTSP for a large number of registered Content Engines.
- CSCsg85869—The wmt process loops in a particular scenario.
- CSCsg87468—The advertised TCP window is limited to 32 KB.
- CSCsg92691—The wmt process loops and leads to 100 percent CPU usage.

- CSCsg92978—A problem occurs with the X-Forwarded-For-Header information.
- CSCsg97879—The dataserver generates a core file during the notification process.
- CSCsg99340—A slow response is seen for On-Demand and MediaFile pages on the Program Manager.
- CSCsh05777—No sound plays from the Microsoft Webinar when the Content Engine is used as a proxy.
- CSCsh11356—FTP preload does not follow the subdirectories.
- CSCsh11650—The **use-http-proxy** option does not work.
- CSCsh15386—The wmt\_mbe process generates core files in a specific scenario.
- CSCsh21894—The wmt\_be sessions are not exiting properly, and outgoing bandwidth is not released.
- CSCsh23907—Transparent requests for proxy autoconfig file enter bypass mode.
- CSCsh29889—The **custom-header** option for the **test-url** command causes a host not found error.
- CSCsh33309—Packets for existing connections are not returned to the router, but are dropped.
- CSCsh34984—The wmt\_be process generates core files in the OpWMSsetParameter under ACNS 5.5.5.4.
- CSCsh35131—VOD file has streams with IDs greater than 31, causing a loop in WMT.
- CSCsh36139—An out-of-memory condition in the Content Engine causes the Content Engine to enter KDB mode after killing its processes.
- CSCsh38163—After upgrading to ACNS 5.5.5, MEDIAFS disk usage exceeds the allocated limit.
- CSCsh41316—The **show https all** command did not display the servers configured.
- CSCsh46848—The cache process restarts continuously on a Content Engine with an attached storage array.
- CSCsh52266—The Content Engine enters KDB mode.
- CSCsh54645—The wmt stream\_scheduler dies due to signal 3.
- CSCsh54679—ACNS Content Distribution Manager must support 2007 Daylight Savings Time Compliance.
- CSCsh56641—Pre-positioned content in the Content Engine does not support range-header requests.
- CSCsh59532—The Content Router does not log a proper response for an IPv6 query.
- CSCsh60096—DNS queries only the primary domain, not other configured domains.
- CSCsh63113—Core files are generated in the UniReceiver.
- CSCsh67515—A blocked page is not being served by the Content Engine.
- CSCsh69225—The **show bypass list** command displays the server port entry in the client side.
- CSCsh69267—The Content Engine entered KDB mode after an upgrade from version 5.4.3.
- CSCsh71625—A cache core is generated in xact\_done\_send\_error\_msg.
- CSCsh72641—Flow protection uses GRE with the L2-redirect WCCP service.
- CSCsh81534—False SNMP traps are sent without a configuration change.
- CSCsh82514—The WMT program schedule time increments by one hour after the daylight savings transition period.

- CSCsh98250—KDB mode occurs during the wmt\_be session.
- CSCsi00029—The **cache reset** command does not reset the cache.
- CSCsi08998—A syslog message is logged for every blocked HTTPS proxy connection.
- CSCsi12257—WCCP Healing Transactions are not logged.
- CSCsi15770—You cannot preload any WMV video files.
- CSCsi16380—The message type “Unexpected” is logged in syslog on the Content Engine.
- CSCsi16500—Pre-position of WMF files is not working; the error is “Unable to scan for play length.”
- CSCsi16813—For FTP-over-HTTP requests, the URL filtering module should be bypassed.
- CSCsi18571—Replication Content Engines have the wrong content counts after a huge content deletion occurs.
- CSCsi26436—NTLM-protected objects are not served when ICAP respmod is enabled.
- CSCsi32332—The online learning application stops when you take the chapter tests and you cannot go to next section.
- CSCsi35189—With Slow-Start enabled in a single Content Engine, only one bucket is assigned for each redirect assign.
- CSCsi36041—The Windows Media Player causes an error when serving cached content while an inactivity timeout is configured.
- CSCsi40391—The content for a META REFRESH request is improperly formatted.
- CSCsi42284—A wmt core file is generated by rtspd.
- CSCsi43638—Some proxy exclude list entries match unexpected domain names.
- CSCsi44425—Packets redirected to the Content Engine are getting incremented, instead of packets sent to the router.
- CSCsi45898—The **type-tail** command does not search correctly.
- CSCsi45941—The non-Location Leader Content Engine fails to issue an intact NSC file for a live multicast program.
- CSCsi47104—The cache process loops when retrieving chunked encoded content, and the server responds with malformed content.
- CSCsi52102—Engineering mode access should not be allowed.
- CSCsi57705—Websense cannot identify users.
- CSCsi58489—A JavaScript error occurs in the Audit Logs page.
- CSCsi60502—The **show memory** command fails to display the application memory usage information.
- CSCsi71104—The **find** command options do not work.
- CSCsi75165—With X-Forward configured, the 127.0.0.1 IP address is appended as the IP address.
- CSCsi83884—The ftp-export process generates a core file when using the SFTP server, and an invalid directory is specified.
- CSCsi85380—The wmt\_be process generates a core file in the fe\_msg sector.
- CSCsi87691—When content is being pre-positioned, the play duration field is interpreted as seconds when it is minutes.

- CSCsi91019—The wmt\_be process generates core files when the player is trying to reconnect after a connection failure.
- CSCsi91320—The wmt\_be process generates a core file in the data\_write sector.
- CSCsi97636—The cache process crashes when the header size exceeds 16 KB.
- CSCsi97871—The wmt\_be process is consuming CPU bandwidth because of a hang in the parser\_scan sector.
- CSCsj12288—WMT failover between Content Engines fails.
- CSCsj19799—An HTTPS proxy outgoing failure occurs after a reload.
- CSCsj47274—WMT crashes in data\_write from an HTTP stream with ACNS 5.5.5.b4.
- CSCsj47345—The Content Engine revalidates each request regardless of whether content is stale or not.
- CSCsj52850—Bypass auth-traffic is not working when an ICAP server is configured.
- CSCsj53163—Bypass auth-traffic does not work when error handling is reset or a send-cache error is configured.
- CSCsi85829—The Content Engine shows 100 percent CPU usage without an actual load after running for 12 or more hours.

## Related Documentation

- *Configuring Cisco Access Routers and NME-WAE Network Modules for ACNS Deployments*
- *Cisco ACNS Software Upgrade and Maintenance Guide, Release 5.x*
- *Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.5*
- *Cisco ACNS Software Command Reference, Release 5.5*
- *Cisco ACNS Software API Guide, Release 5.5*
- *Cisco Network Modules Quick Start Guide*
- *Cisco Network Modules and Interface Cards Regulatory Compliance and Safety Information*

The Content Distribution Manager GUI and the Content Engine GUI both have context-sensitive online help that may be accessed by clicking the **HELP** button.

## Obtaining Documentation, Obtaining Support, and Security Guidelines

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

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

---

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

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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

