# Release Notes for Cisco ACNS Software, Release 5.5.1

**May 12, 2006**

**ACNS Release 5.5.1-b7**

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

## Contents

These release notes contain information about the Cisco Application and Content Networking System (ACNS) 5.5.1 software. These release notes describe the following topics:




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

# Introduction

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

These release notes are intended for administrators who will be configuring, monitoring, and managing devices that are running the ACNS 5.5.1 software. These release notes describe the new product features, the supported hardware, and the open and resolved caveats regarding the ACNS 5.5.1 software release.

# System Requirements

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

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

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

**Note** The ACNS 5.5.1 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 |
| ACNS 5.5.1 | Version 4.0.1 | Version 5.5.2 |

# New and Changed Information

This section describes new and changed features in the ACNS 5.5.1 software release.

## New Features in the ACNS 5.5.1 Software

The ACNS 5.5.1 software includes the following new features, enhancements and changes:


- FTP Service Disabled by Default, page 3
- Enhancements to ICAP Support, page 4
- New Rule Pattern to Filter Content Based on the X-forwarded-for IP Address, page 5
- Support for Content Router Request Overflow Routing, page 6
- Support for Channel Priming for Faster Video Startup, page 6
- List of the Windows Media Technologies Command Options Not Supported in ACNS 5.5 Software, page 7


### 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 5.5.1 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 relelases
- ACNS 5.5.1 and later 5.5.x releases

On Content Engines that run ACNS software releases earlier than 5.3.7 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 **inetd ftp enable** global configuration command.

## 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 5.5.1 software supports the following enhancements for ICAP support:



### ICAP Request Modification Support for HTTPS Requests

The ACNS 5.5.1 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 14.

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

The ACNS 5.5.1 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 5.5.1, the ACNS software has become compatible with the data trickling feature of the WebWasher ICAP server. (See resolved caveats CSCeh34004 and CSCsc29267.)

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

The ACNS 5.5.1 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 5.5.1 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 5.5.1 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. To configure a pattern list, follow 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** Next, associate an action with an existing pattern list.

- **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.

**Step 7** To save settings, click **Submit**.

For more information on 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 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 5.5 release, when the original domain is overloaded, client requests can be redirected to an overflow or alternate domain. This feature is applicable in the following two cases:

- 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.

**Note** Even though ACNS 5.5 software does not support the MMS protocol, request overflow routing supports requests from MMS clients because the overflow domain can be another Content Engine or any Windows Media server or third-party server.

## Support for Channel Priming for Faster Video Startup

The ACNS 5.5 software release allows channels for unicast managed live programs to be primed for faster startup times. When a live channel is primed, a unicast-out stream is pulled from the origin server to a Content Engine before a client ever requests the stream. When the first request for the stream goes out, the stream is already in the channel.

## List of the Windows Media Technologies Command Options Not Supported in ACNS 5.5 Software

This section lists the **wmt** global configuration command options that are not supported in ACNS 5.5.1 or later releases. If you have these command options configured in an earlier ACNS release, and then you upgrade to ACNS 5.5.1 or later, the MMS configurations are removed. If you downgrade to an earlier release, the MMS configurations are not restored.

**Note** You must plan to save your configurations before you upgrade your software to ACNS 5.5.x, if you want to restore MMS configurations after a downgrade.

The following **wmt** command options are not supported in ACNS 5.5.1 software:

```
Wmt-ce(config)# wmt cache ?
unique-stream-key  Use unique stream ID as the cache key

mt-ce(config)# wmt disallowed-client-protocols ?
  mmst   disallow streaming over mmst protocol (mmst://)
  mmsu   disallow streaming over mmsu protocol (mmsu://)

wmt-ce(config)# wmt incoming ?
  <1-65531>  Port to listen for MMS requests

wmt-ce(config)# wmt proxy outgoing ?
  mms   Out-going MMS proxy configuration

wmt-ce# show services ?
  ports Display services by port
  summary Display services summary
```

**Note** The range of ports between 1755–1759 from both the **show services ports** and **show services summary** commands are not supported in the ACNS 5.5.1 software.

# Design Limitation for ACNS Object Transfers

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

# Operating Considerations

This section describes information regarding the ACNS 5.5.x software. It includes the following sections:



## Protocol Support for Windows Media Streaming Has Changed

ACNS 5.5 software no longer supports the MMS protocol for acquiring or distributing Windows Media content between servers. If you are using MMS-based streaming, you must migrate to RTSP-based streaming or HTTP-based streaming before you upgrade to the ACNS 5.5 software release. (See the *Cisco ACNS Software Upgrade and Maintenance Guide, Release 5.x* publication for the ACNS 5.5 release.)

## MMS Configurations are Removed on Upgrade

Because the MMS protocol is no longer supported in ACNS 5.5.1 or later releases, command options in the Content Engine CLI and Content Distribution Manager GUI that configure the MMS protocol have been removed. If you have these command options configured in an earlier ACNS release, and then you upgrade to ACNS 5.5.1 or later, the MMS configurations are removed. If you downgrade to an earlier release, the MMS configurations are not restored.

You must plan to save your configurations before you upgrade your software to ACNS 5.5.x, if you want to restore MMS configurations after a downgrade.

The Content Distribution Manager automatically creates a database backup file, which you can find in the CLI root directory with a filename similar to the following:

```
cms-db-03-13-2006-08-30.dump
```

The filename contains the date and time that the backup was made. In the example, 03-13-2006 is the date and 8:30 is the time that this data was saved. We recommend that you export a copy of the database backup file before you upgrade your Content Distribution Manager or Content Engines to ACNS 5.5 software.

**Note** For a complete list of commands that have been changed or removed in the ACNS 5.5.x software release, see the "List of the Windows Media Technologies Command Options Not Supported in ACNS 5.5 Software" section on page 7.

# Multicast Station NSC Reference URL Configurations in a Mixed Network

If you are using a Content Distribution Manager that is running a release prior to ACNS 5.5 (such as ACNS 5.3.x or ACNS 5.4.x) and you are using it to manage Content Engines that are running ACNS 5.5 software, the Content Distribution Manager does not recognize the **nsc-reference** option of the **wmt multicast station-configuration** global configuration command. This option is new to the ACNS 5.5.1 release.

If you configure an ACNS 5.5 Content Engine using the **wmt multicast station-configuration** command without configuring the **nsc-reference** option, the configuration can be successfully managed by the Content Distribution Manager.

If you configure an ACNS 5.5 Content Engine using the **wmt multicast station-configuration** command and the **nsc-reference** option, the configuration is not recognized by the Content Distribution Manager.

If you configured an ACNS 5.5 Content Engine using the **wmt multicast station-configuration** command without configuring the **nsc-reference** option, and later you attempt to modify the configuration by adding an NSC reference URL for this station from the Content Engine CLI, the lower version Content Distribution Manager removes the multicast station during the next management system update.

# Using Mixed Versions of Windows Media Server

Windows Media Server prior to Version 9.x does not support RTSP, so you cannot use an RTSP source URL with older versions of Windows Media Server. If you have Windows Media Servers in your ACNS network that do not support RTSP, you must use HTTP as the source URL for Windows Media streaming.

# Windows Media Managed Live Programs

In ACNS releases prior to ACNS 5.5, MMST was the protocol used for communications between Content Engines for managed live programs. In the ACNS 5.5 release, the protocol for communication between Content Engines has changed to RTSPT. If you are using ACNS 5.5 software on some Content Engines and are using earlier versions of software on other Content Engines in your network, Windows Media managed live programs will fail because the ACNS 5.5 Content Engine will not be able to communicate with ACNS 5.4 or 5.3 Content Engines. If you are migrating to ACNS 5.5 software, you must upgrade all the Content Engines in the Windows Media live channel to ACNS 5.5 software for successful delivery of managed live programs.

HTTP unicast delivery (Unicast in-Unicast out) to the client is not supported for managed live streaming; only RTSP URLs are supported. In the Live Source URL field in the Content Distribution Manager GUI (**Services > Video > Programs > Live Streaming**), you can have an HTTP or RTSP URL, but in the Unicast URL Reference field and in the Customized URL field only RTSP URLs are allowed.

If MMS is configured in the Live Streaming window (**Services > Video > Programs > Live Streaming**) before the upgrade, the configuration remains the same after the upgrade to ACNS 5.5 software; however, you cannot modify the source URLs in this window without changing the protocol from MMS to one of the supported protocols in ACNS 5.5 software.

The Content Distribution Manager GUI returns an error message if you try to modify the settings in this window when the MMS protocol is included from a previous release.

## Windows Media Services Streaming Media Acquisition

In prior releases, ACNS software supported Content Engine acquisition of Windows Media streaming content. In ACNS 5.5 software, the Content Engine cannot acquire and pre-position Windows Media streaming content.

If an MMS URL is specified as the source URL for a content item in the Channel Content window (**Services > Web > Channels > Channel Content**) before the upgrade, the configuration remains the same after the upgrade to ACNS 5.5 software; however, you cannot modify the content items in this window until you change the protocol of the URL from MMS to one of the supported protocols in ACNS 5.5 software.

The Content Distribution Manager GUI returns an error message if you try to modify the settings in this window when the MMS protocol is included from a previous release.

## WCCP Transparent Redirection for MMS

In the ACNS 5.5 release, WCCP Service 81 and Service 82 for MMS redirection are still valid. If your network is set up for WCCP redirection for MMS, and an MMS request is redirected to the Content Engine, the Content Engine accepts the request and immediately closes the connection. This operation forces the Windows Media client to rollover to RTSP or HTTP to serve the stream.

**Note** URLs starting with mmsu:// or mmst:// cannot be rolled over. You must replace these URLs with rtsp:// or http://. We recommend that you explicitly reconfigure your MMS settings to RTSP.

## Using Windows Media Encoder or Mixed Versions of Windows Media Player

HTTP is supported for communications between Windows Media Player and the Windows Media Encoder or between a Content Engine and the Windows Media Player; however, it is not supported for communications between Content Engines.

HTTP is the only mode of data delivery supported by Windows Media Encoders. RTSP is not supported by Windows Media Encoders. ACNS software supports live streams that have Windows Media Encoders as their source. Support for HTTP allows Content Engines to communicate with the Windows Media Encoder.

If Windows Media Player Version 9, or a later version, issues an explicit mmst:// or mmsu:// URL request, the ACNS 5.5 software sends an error message and will not play the stream. If a request contains an mms:// URL, the player uses RTSP or HTTP instead.

When connecting to a publishing point using the MMS protocol, a rollover method is used to obtain the best connection. When a URL in Windows Media Player Version 9, or a later release, specifies an MMS URL (mms://), the Windows Media Player attempts to use the following protocols for media delivery, in the order shown:

1. RTSPU (RTSP using UDP)
2. RTSPT (RTSP using TCP)
3. HTTP
4. MMSU (MMS using UDP)
5. MMST (MMS using TCP)

**Note** If you have different versions of Windows Media Player in your network, you should configure HTTP proxy in all versions of Windows Media Player to allow Windows Media streaming over HTTP, which is supported across all versions of software.

# Windows Media Services License Key Interoperability Issues

Licenses purchased for Windows Media Services (WMS) in the ACNS 5.5 software and later releases are not supported in ACNS 5.4.x software or earlier releases. However, a Content Distribution Manager running ACNS 5.4 software can configure licenses for both ACNS 5.4 and ACNS 5.5 devices.

One caveat is that an ACNS 5.4 Content Distribution Manager cannot correctly validate ACNS 5.5 license keys. Because the license keys in ACNS 5.5 software are new, they are not recognized by earlier software versions. When you attempt to run a validation check on an ACNS 5.5 WMS license key from the ACNS 5.4 Content Distribution Manager GUI, you will receive an error message stating that you have entered the key incorrectly. (License key validation is optional in the Content Distribution Manager GUI.) (See Table 3.)

*Table 3 Content Distribution Manager Interoperability Matrix*

| Content Distribution Manager Software | | ACNS 5.4 WMS Licenses | ACNS 5.5 WMS Licenses | Later ACNS 5.5.x Licenses |
|---|---|---|---|---|
| **ACNS 5.4** | Configure | Yes | Yes | Yes |
| | Validate | Yes | No | No |
| **ACNS 5.5** | Configure | Yes | Yes | Yes |
| | Validate | No | Yes | Yes |

You should not attempt to validate ACNS 5.5 license keys with an ACNS 5.4 Content Distribution Manager. You, however, can submit the license key and successfully configure the WMS license for the ACNS 5.5 release from an ACNS 5.4 Content Distribution Manager. To verify that WMT is enabled on a Content Engine in this situation, use the **show wmt** EXEC command.

If you attempt to configure an ACNS 5.5 (or later release) WMS license key on an appliance that is running ACNS 5.4 software or an earlier release, the license key will fail, and Windows Media Services will not be enabled on that appliance. This failure is logged and can be viewed from **Devices > Device Monitoring > Logs** in the Content Distribution Manager GUI.

If you have a mixture of ACNS 5.4 and ACNS 5.5 devices in your network and you want to configure licenses by device groups, we recommend that you group devices in the Content Distribution Manager separately by software release in order to avoid an issue with license incompatibility.

**Note** When you upgrade from ACNS 5.4 to ACNS 5.5 software, any WMS license keys that you configured in ACNS 5.4 will continue to be valid after the upgrade.

# Content Distribution Manager Interoperability Issues

A Content Distribution Manager running ACNS 5.4 software can provide a centralized interface for configuring and managing ACNS networks in which some or all of the Content Engines are running ACNS 5.5 software.

A Content Distribution Manager running ACNS 5.5 software can provide a centralized interface for configuring and managing ACNS networks in which all of the Content Engines are running ACNS 5.5 software only. (See Table 4.)

*Table 4 Content Distribution Manager Interoperability Matrix*

| Content Distribution Manager Software | ACNS 5.4.x Appliances | ACNS 5.5.1 Appliances | Later ACNS 5.5.x Appliances |
|---|---|---|---|
| ACNS 5.4 | Yes | Yes | Yes |
| ACNS 5.5 | No | Yes | Yes |

If you are migrating your network to the ACNS 5.5 release, observe the following requirements:

- Ensure that your Content Distribution Manager is running a version of ACNS 5.4 software.
- Always upgrade your Content Engines and Content Routers to ACNS 5.5 before you upgrade the Content Distribution Manager to ACNS 5.5.
- Always upgrade your Content Distribution Manager to ACNS 5.5 last, after all other appliances in your network are using ACNS 5.5 software.
- Follow the migration procedure outlined in the *Cisco ACNS Software Upgrade and Maintenance Guide, Release 5.x* publication for the ACNS 5.5 release.

# RAM Requirements for ACNS 5.5 Software and Websense 5.5 Software

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

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

If the local (internal) Websense server is enabled on the Content Engine and you downgrade from the ACNS 5.2.x software to either ACNS 5.0 software or ACNS 5.1 software, the WebsenseEnterprise directory is removed from the Content Engine and the local Websense server stops working. The ACNS 5.2.x software does not generate an error message indicating that the WebsenseEnterprise directory has been removed.

However, in the ACNS 5.3.1 software and later releases, the following error message is displayed to notify you about this Websense downgrade issue:

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

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

**Step 1** Disable the local (internal) Websense server on the Content Engine.

**Step 2** Deactivate the Websense services on the Content Engine.

**Step 3** Install the ACNS 5.1 software or ACNS 5.0 software downgrade image on the Content Engine.

# Media File System Issues When Downgrading to ACNS 5.0 Software

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

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

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

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

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

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

When you upgrade or downgrade the Content Engine to a different release of the ACNS software, if there is a difference in the SmartFilter plug-in version, the SmartFilter database and configuration files are deleted and default configurations are loaded. This change occurs because the configuration details might be changed with each new version of SmartFilter software. After each upgrade or downgrade of the SmartFilter plug-in, a fresh database has to be downloaded from the SmartFilter Administration Console to the Content Engine.

**Note** The ACNS software release 5.5.1 uses the SmartFilter Version 4.0.1 plug-in.

# ICAP Services

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

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

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

## Interoperability with ICAP Vendors

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

- TrendMicro for reqmod and respmod
- Symantec for respmod

## ICAP Performance

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

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

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

### Maximum File Size Supported for ICAP Processing

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.

For releases prior to ACNS 5.4.x software, the maximum file size that is supported in the ACNS software in pass-through mode is 2 GB. Files that exceed this size limit are not supported for ICAP processing.

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

Table 5 lists the caching, filtering, and authentication methods supported by Content Engines that are running the ACNS 5.5.x software. An asterisk (*) indicates that a feature is supported for that particular protocol.

*Table 5 Caching, Filtering, and Authentication Methods and Related Protocol Support*

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

# Caveats

This section lists and describes the new, open, and resolved Severity 1, 2, and 3 caveats in the ACNS 5.5.1 software. Caveats describe unexpected behavior in the ACNS 5.5.1 software. Severity 1 caveats are the most serious; Severity 2 caveats are less serious. Severity 3 caveats are moderate caveats.

# Open Caveats—ACNS 5.5.1 Software

This section lists caveats that have not been resolved in the ACNS 5.5.1 software release. The open caveats are grouped into the following categories:


- Windows Media Open Caveats, page 16
- Other Open Caveats, page 21


## Windows Media Open Caveats

- 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.

- CSCsd63199

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

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

  Workaround: Clear the browser cache after every request.

- CSCsd75279

  Symptom: The RTSP request fails.

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

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

- CSCsd92288

  Symptom: The IXIA Windows Media load tool client does not interoperate with ACNS 5.5.1 WMT using RTSP.

  Condition: IXIA Windows Media load tool clients are not compatible with the ACNS 5.5.1 software because the ACNS 5.5.1 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: There is no known workaround.

- CSCsd98883

  Symptom: The RTSPU disallowed counter, in the output of the **sh stat 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: There is no known workaround.

- 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 VoD or a proxy source.

  Workaround: There is no known workaround.

- CSCsd99435

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

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

  Workaround: Start the play again.

- CSCsd99636

  Symptom: More outgoing bandwidth is consumed than expected.

  Condition: Usually, outgoing bandwidth is calculated with consideration for Fast Cache (FC), since data is sent at a higher rate if FC is enabled on the client and on the Content Engine. Since FC is supported only for cache-hit cases, the outgoing bandwidth should be calculated with consideration for FC for cache hit cases only. However, the outgoing bandwidth is calculated with consideration for FC even for cache-miss cases. The bandwidth allocation is reset as soon as playback ends for that stream.

  Workaround: There is no known workaround.

- CSCse00701

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

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

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

- CSCse02533

  Symptom: The remote HTTP source counter increments for the multicast-in source.

  Condition: When a multicast-in source is used for a broadcast alias in the Content Engine, then the By Source of Content field in the **show statistics wmt requests** command output shows the remote HTTP counter incrementing instead of the multicast counter. This condition is seen in the ACNS 5.5.1 software.

  Workaround: There is no known workaround.

- CSCse04147

  Symptom: The max-obj-size limiting has failed.

  Condition: This problem occurs when the max-obj-size is limited and a request is given to the Content Engine.

  Workaround: There is no known workaround.

- CSCse05481

  Symptom: The Duration field in the **show statistics wmt streamstat** command output shows a large value for some of the streams.

  Condition: This condition occurs in the ACNS 5.5.1 software under stress conditions.

  Workaround: There is no known workaround.

- 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.

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

  Workaround: There is no known workaround.

- CSCse07034

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

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

  Workaround: An HTTP source can be used for the multicast station.

- CSCse07737

  Symptom: The outgoing bytes keep incrementing.

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

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

- CSCse07977

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

  Condition: A stream encoded with video only is played using RTSPU (that is, either the URL is rtspu:// or the URL is rtsp:///), and the player advanced statistics indicate that the protocol in use is RTSP (UDP).

  Workaround: Use the RTSPT protocol as the protocol for the URL (rtspt://).

- CSCse08174

  Symptom: The CE-510, CE-510A, CE-565, and CE-565A platforms go into an inaccessible state during a live split.

  Condition: This problem occurs when Windows Media Players request a live stream encoded with multiple bit rates using RTSP (UDP) and not all players are requesting the same bit rate. This problem occurs when the network has high latency and there are increased numbers of RTSP-UDP retransmission requests showing in the player advanced statistics field.

  This problem can occur in a few minutes or after many hours, depending on the network conditions, the number of bit rates encoded in the live stream, the number of bit rates requested by the clients, and the number of clients requesting the stream.

  This problem has been seen in the ACNS 5.3, ACNS 5.4, and ACNS 5.5 software releases.

  This problem has not been seen on any other platforms or if the player uses RTSP (TCP).

Workaround: Reload the Content Engine. Use RTSP (TCP) instead of RTSP (UDP) in the live-split condition.

- CSCse08370

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

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

  Workaround: Try the file stream again. Try to alleviate the latency problem. Use rtspt:// in the URL.

- CSCse09222

  Symptom: The Windows Media Player plays the stream without a problem. However, the **show statistics wmt streamstat** command shows that the bandwidth consumption is 0 (zero) and that the stream is in the TEARDOWN state. Also, the bandwidth used by this stream is not counted in the bandwidth consumption statistics, even though the bandwidth is being used. After the user stops playing the stream, no further impact is seen.

  Condition: This problem occurs during a long play of pre-positioned content when RTSP is the transport protocol for a multi-bit-rate file, and the Windows Media Player requests multiple stream switches between the bit rates.

  Workaround: There is no known workaround.

- CSCse09560

  Symptom: The Windows Media Player attempts to reconnect to the stream.

  Condition: This problem occurs occasionally when control events such as fast-forward, fast-reverse, or seek are executed on the Windows Media Player for VoD or proxy content playback using MMS-over-HTTP.

  Workaround: The Windows Media Player recovers from the error automatically, and there is no disruption in the playback except for a momentary break when the player reconnects to the stream.

- CSCse12607

  See CSCse14195.

- CSCse12809

  Symptom: The Content Engine sends a 500 error message to one of the clients during a live split of a managed live unicast program.

  Condition: This error occurs when the source for the program is a SSPL.

  Workaround: If the client receives a 500 error message, send a new request.

- CSCse14195

  Symptom: A core file has been seen while running stress testing for server-side play lists (SSPL) with multi-bit-rate (MBR) live content.

  Condition: A core file was seen during stress testing of SSPL and MBR live.

  Workaround: There is no known workaround.

- CSCse14384

  Symptom: The cache-hit counter in the output of the **wmt statistics** command does not increment.

  Condition: There are no specific conditions for this problem.

  Workaround: There is no known workaround.

- CSCse15623

  See CSCse09222.

- CSCse15691

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

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

  Workaround: There is no known workaround.

- CSCse16514

  Symptom: The RTSP cache-hit playback fails in an outgoing proxy scenario if the URL contains a query string.

  Condition: This problem occurs only for URLs of the form rtsp://hostname/filename?name=value in a cache-hit scenario. It will not be seen if the URLs are of the form rtsp://hostname/publishing_point_name/filename?name=value.

  Workaround: There is no known workaround.

- CSCse16525

  Symptom: The incoming bandwidth usage statistics (viewed by using the **show statistics wmt usage** command) are incremented for every stream switch made by the live stream. The Content Engine also continues to pull old bit rate selections of the live stream and new bit rate selections, in anticipation of the need to split the stream for new clients requesting the older bit rate selection.

  Condition: This condition occurs when the user is playing back a multi-bit-rate live stream, and the Windows Media Player selects different stream selections during the playback period.

  Workaround: There is no known workaround.

- CSCse16536

  Symptom: The Windows Media Player goes into the buffering state and hangs.

  Condition: This problem occurs during a multicast-in and multicast-out play forever program after the end of the first loop.

  Workaround: There is no known workaround.

- CSCse16537

  Symptom: The Windows Media Player enters the waiting state after a play/pause/play sequence of control events. This problem is seen only when the HTTP protocol is used for a live publishing point hosted on the Windows Media Server.

  **Note** A publishing point is the point of client access to the Windows Media Server that is hosting all of the media items in a playlist. A client accesses the streaming content from the Windows Media Server by connecting to the publishing point.

  Condition: This problem occurs when pause and play is used for a live publishing point from Windows Media Server.

  Workaround: Instead of using the live publishing point on the Windows Media Server as the source stream, use Windows Media Encoder as the source for the live program.

- CSCse17190

  Symptom: The Windows Media Player attempts to reconnect when it reaches an end of stream (EOS) of the broadcast alias.

  Condition: This condition occurs only when a multicast stream is used as the source for the broadcast alias in the Content Engine.

  Workaround: There is no known workaround.

- CSCse18576

  Symptom: The URL signature validation fails for a Camiant server RTSP request.

  Condition: This problem occurs when you enter the **clear stat all** or **clear stat wmt** command. The next Camiant server RTSP request will fail.

  Workaround: Reconfigure one url-signature key ID after you clear the statistics, to ensure that further requests are validated correctly.

- CSCse18874

  Symptom: Windows Media RTSP does not work.

  Condition: This problem occurs when the user configures ports 5004 and 5005 for another application.

  Workaround: Use ports other than 5004 and 5005 for other applications, and allow 5004 and 5005 to be used by Windows Media RTSP.

- 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.

## Other Open Caveats

- CSCdy82311

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

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

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

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

Workaround: Use one of these workarounds:

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

- CSCea51815

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

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

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

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

- CSCed68727

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

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

  Workaround: There is no known workaround.

- CSCed77655

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

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

  Workaround: Remove the rule configurations.

- CSCed84227

  Symptom: The network management system (NMS) host does not know where SNMP traps are coming from.

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

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

- 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 in the following condition:

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

     The autoconfiguration file is not found but the proxy autoconfiguration feature is shown as enabled.

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

- CSCef67938

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

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

  This situation can occur under the following circumstances:

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

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

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

- CSCeg04809

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

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

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

- CSCeg22697

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

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

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

- CSCeg47793

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

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

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

- CSCeg56075

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

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

  Workaround: Set the reconnect as manual instead as automatic.

- CSCeg82405

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

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

  Workaround: There is no known workaround.

- CSCeg84004

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

  Condition: This problem can occur in the following condition:

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

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

     where *somehostname* is a hostname.

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

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

- CSCeg86386

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

  Condition: This problem 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 Windows Media 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.

- CSCeh38741

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

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

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

- 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:

  a. A channel contains a samba crawl from a Network Appliance file server, which contains such media files as .wmv files.
  b. 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.

- CSCsb95697

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

Condition: This problem can occur if the Content Engine is running the ACNS 5.2.7 software or a later release, and it has not been rebooted for several weeks.

Workaround: There is no known workaround.

- 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.

- CSCsc13494

  Symptom: A disk is marked as "bad" when a disk error threshold is reached after a transient disk failure.

  Condition: This problem occurs only rarely and can only occur if the Storage Array device is attached to a model CE-7325 that is running the ACNS 5.3.3.8 software or a later release.

  Workaround: After the disk is marked "bad," you can enter the **disk mark** ***diskname*** **good** EXEC command on the Content Engine to mark the disk as "good."

- 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.

- CSCsc19566

  Symptom: A Content Engine can hang or go into kernel debug mode if the kernel debug feature is enabled on the Content Engine.

  Condition: This problem can occur with a model CE-7325 that is running the ACNS 5.2.7.7 software or a later release.

  Workaround: Reload the 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.

- 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.

- CSCsc72072

  Symptom: With MMS URLs, WCCP hits for pre-positioned WMV files fail.

  Condition: This problem occurs because UNS resolution fails.

  Workaround: Substitute an IP address for the fully-qualified domain name (FQDN).

- CSCsc75289

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

  Condition: This problem occurs if the Websense Network Agent is configured on the Content Engine.

  Workaround: There is no known workaround.

- 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.

- CSCsc81507

  Symptom: The Content Engine may lose the configured routes.

  Condition: This problem can occur if you have manually entered the routes.

  Workaround: Reenter the routes.

- 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.

- CSCsc97711

  Symptom: The default value for **wmt max-concurrent-sessions** does not show up in running config mode.

  Condition: This problem occurs when the configured value for the wmt max clients is equal to that of the dynamic default value of **wmt max-concurrent-sessions**.

  Workaround: Configure a different value for **wmt max-concurrent-sessions**.

- CSCsd05772

  Symptom: When you export log files from the archive to an external server using FTP, some of the log files are not exported.

  Condition: Because filenames in /logs/real-subscriber-logs, /logs/real-proxy, and /logs/cisco-streaming-engine directories do not include an underscore and use a combination of the Content Engine IP address and year, the first 15 characters of the filenames are identical. The FTP export status file (ftp_export.status) saves the i-node of the archived log file and the first 15 characters of the filename. If a log file by the same name was deleted earlier by the user and if there is an entry for the deleted file in ftp_export.status, the log file does not get exported.

  Workaround: Manually delete the file ftp_export.status in the log directory. All log files get exported during the next scheduled or forced attempt.

- CSCsd14626

  Symptom: The Content Engine appears to send IMS request to the server before the configured time-to-live (TTL) period expires.

  Condition: When you configure the cache-non-cacheable rule action and the HTTPS server for a secure socket layer (SSL) termination and issue a HTTPS request matching the configuration, the first request is cached and the second request is issued before the time-to-live (TTL) expires.

  Workaround: There is no known workaround.

- CSCsd17740

  Symptom: The Content Engine shows a change to a large number of stale connections between the proxy cache and the integrated Apache server for pre-positioned content. An increase in the number of stale connections might cause the Content Engine to exceed the limit of connections (16000) and to stop functioning.

  Condition: Stale connections increase at about 1000 connections per week. At this rate, it might take a few weeks before you experience any problem with the Content Engine's functioning.

  Workaround: Run the **service restart cache** command once every 2 or 3 weeks to clean up the stale connections.

- CSCsd20346

  Symptom: The failover of the upstream HTTP request to the backup Content Engine causes a delay that results in a proxy failure.

  Condition: This problem occurs on a Content Engine 7325 running ACNS 5.3.5.6 with a failover backup to another Content Engine

  Workaround: There is no known workaround.

- CSCsd21974

  Symptom: When you change or modify a rule from the Content Distribution Manager GUI, you experience a considerable delay before the changes take effect.

  Condition: This problem occurs when you have a large number of rules already configured on the device.

  Workaround: There is no known workaround.

- CSCsd27358

  Symptom: Sometimes, when you download a file using HTTP, and if the download takes more than 20 minutes, the Content Engine closes the TCP connection and fails to complete the download.

  Condition: This problem occurs if your file download requires ICAP processing.

  Workaround: There is no known workaround.

- CSCsd30356

  Symptom: The Content Engine stops authenticating NTLM users and stops responding and passing traffic. NTLM servers show up as dead when you enter the **show statistic ntlm** CLI command.

  Condition: This problem occurs on Content Engines that run NTLM or some other authmode authentication services.

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

- CSCsd58287

  Symptom: When you enable SmartFilter, the Central Processing Unit (CPU) indicates 100 percent usage.

  Condition: This problem occurs when you configure reverse dnslookup for uncategorized requests in Smartfilter.

  Workaround: Disable reverse dnslookup in SmartFilter.

- CSCsd58836

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

  Condition: This problem occurs when the Content Engine runs on ACNS 5.3 or 5.4 and the HTTPS request is at least set at 20 TPS (Transactions Per Second).

  Workaround: Downgrade the Content Engine to ACNS 5.2.

- CSCsd63119

  Symptom: The 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 clearing the browser cache first.

  Workaround: The browser cache should be cleared after every request.

- 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: There is no known workaround.

- CSCsd78318

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

  Condition: This problem occurs when the origin server responds to the preceding request with the HTTP status 207 that stops the Content Engine from processing further TCP stream requests.

  Workaround: Disable persistent connections by configuring the no-persistent-connection server-only rule action.

- CSCsd82649

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

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

  Workaround: Downgrade to the ACNS 5.1.9.5 software.

- CSCsd87378

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

  ```
  Network name cannot be found
  ```

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

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

- CSCsd89303

  Symptom: The Content Engine stops serving live streams abruptly.

  Condition: This problem occurs when the Content Engine has been running for a while.

Workaround: Reload the Content Engine.

- CSCsd90763

  Symptom: The Content Engine stops functioning.

  Condition: This problem can occur under no special conditions.

  Workaround: There is no known workaround. However, a power cycle may be required to reload the Content Engine.

- CSCsd91249

  Symptom: The following issues are observed when URL filtering is enabled in Websense:

  a. The user/group filtering policies are not applied.

  b. Clients are constantly prompted for authentication.

  Condition: This problem occurs when an active directory holds a large customer database containing names of the customers formatted as Last, First with a comma included.

  Workaround: There is no known workaround.

- CSCsd94410

  Symptom: When you enter the **show alarms history detail** command on the Content Engine, this alarm message displays:

  ```
  The cache service died
  ```

  Condition: This problem occurs within 2 minutes of reloading the Content Engine with the ACNS 5.4.1 SPECIAL4 B5 image on a WAE-CE73xx and WAE-CE5xx.

  Workaround: There is no known workaround.

- CSCsd95049

  Symptom: A core file for the exec_show_running-config process also exists in the /local1/core_dir directory, and the following major alarm is seen in the Content Distribution Manager GUI or in the Content Engine CLI when you enter the **show alarm** command:

  ```
  Major Alarms:
  -------------
  Alarm ID Module/Submodule Instance
  -------- ---------------- --------
  1 core_dump sysmon core
  ```

  Condition: This problem may be related to a multiprocessor platform, such as a CD-7325 that has been upgraded from ACNS 5.3.x to ACNS 5.4.1 and then downgraded to ACNS 5.3.x.

  Workaround: There is no known workaround.

- CSCse04951

  Symptom: The ACNS 5.3.1 software fails intermittently through the Content Engine.

  Condition: This problem occurs when the ACNS software makes an ftp-over-http request for data from an external website.

  Workaround: Restart the customer application.

- 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: There is no known workaround.

- CSCse08263

  Symptom: The Content Engine that runs the ACNS software version 5.3.5.6 is taken out of the cache farm, becomes idle, and creates a core every 4 minutes.

  Condition: This problem occurs if Websense is enabled.

  Workaround: There is no known workaround.

- CSCse22425

  Symptom: The Content Engine enters the kernal debugger mode.

  Condition: This condition occurred with a Content Engine 7305 that was running traffic with SmartFilter enabled.

  Workaround: There is no known workaround.

# Resolved Caveats—ACNS 5.5.1 Software

This section lists the caveats that have been resolved in the ACNS 5.5.1 software release. The resolved caveats are grouped into the following categories:



## AAA Accounting Resolved Caveats

- CSCei04025

  The Content Engine does not allow you to log in. The Content Engine generates messages about mingetty being killed by signal 25. This problem occurs if the debug authentication feature (you have entered the **debug authentication** user EXEC command) has been enabled and is not disabled.

- CSCsc06687

  The Content Engine does not allow FTP access when a user uses root as a username for FTP.

- CSCsd57339

  All users are able to access the entire file system of the ACNS software when the **sshd allow-non-admin-users** command is enabled. Only admin users should have access to the entire file system.

## Acquisition and Distribution Resolved Caveats

- CSCsc22469

  Altris RapiDeploy fails to download pre-positioned content from the Content Engine and contacts the origin web server for software downloads.

- CSCsc83707

  All pre-positioned content is lost throughout the content distribution network. This problem occurs when the root Content Engine fails and the temporary root takes over. However, the temporary root either cannot access the manifest file or cannot access the origin server (or both). The temporary root deletes all of the content that it previously had pre-positioned from the root Content Engine. All of the other Content Engines also delete all of their content.

- CSCsd76836

  The files are that retransmitted to the Content Engines result in duplicated files during a multicast distribution. This problem occurs when a new Content Engine is assigned as the primary sender of the multicast cloud for the channel, when a root Content Engine of the channel is changed, or a root Content Engine failover occurs.

- CSCsd84482

  The memory leak in the Acquisition and Distribution module can cause the Content Engine to run out of memory over several months of system uptime.

## DNS Resolved Caveats

- CSCsd28066

  When you enter the **domain name server ip** command, you cannot use the number 255 in the IP address when you boot up the Content Engine.

## ICAP Resolved Caveats

- CSCeh34004 and CSCsc29267

  Downloading large files over ICAP-enabled ACNS networks fails before the download is completed because of compatibility issues with the data trickling feature of the WebWasher ICAP server.

- CSCei61774

  The ICAP process does a core dump if you delete the ICAP service from the Content Engine. This problem occurs if the Content Engine is running the ACNS 5.3.1 software or a later release.

- CSCsd14159

  The ICAP daemon on the Content Engine crashes and generates a core file. However, the ICAP daemon restarts on its own. This problem occurs when the ICAP service is enabled on the Content Engine.

- CSCsd59596

  The cache process stops communicating with the ICAP daemon. The ICAP daemon does not receive any request for content when the ICAP reqmod service is enabled on the Content Engine.

- CSCsd65189

  The browser stops responding when you refresh a URL or repeat a URL request. This problem occurs when the ICAP respmod service for virus scanning is enabled on the Content Engine.

## Management Resolved Caveats

- CSCei91572

  The order of the access control lists (ACLs) can appear out of order in the Content Distribution Manager GUI even though the configuration on the device is correct.

- CSCsc64327

  The Content Distribution Manager GUI does not respond. On rare circumstances, the internal system log processes will operate concurrently. This situation causes a deadlock, which causes the Content Distribution Manager GUI to become unresponsive.

- CSCsd02269

  The Content Distribution Manager that runs on a WAE-611 device fails to retrieve a manifest file that is fairly large (13 MB).

- CSCsd30034

  The Content Distribution Manager GUI does not restrict the number of static bypass entries. The number of static bypass entries are restricted to 50 when you are using the **bypass static** command to create the static bypass list. If you have created more than 50 static bypass entries using the Content Distribution Manager GUI, the system experiences problems because of the number mismatch.

- CSCsd58837

  The primary Content Distribution Manager of an ACNS network that has more than 1000 Content Engines shows many Content Engines offline after you add or replace a standby Content Distribution Manager in that ACNS network.

- CSCsd73961

  The statistics for the HTTP hit ratio in the Content Distribution Manager GUI is not shown as a percentage as shown in the CLI.

- CSCsd86169

  The hostname configuration of the Content Engine is lost and the Content Engine shows that it is offline in the Content Distribution Manager GUI. The device responds to the console access.

## Proxy and Caching Resolved Caveats

- CSCei13929

  Websense configurations (for example, the downloaded database and license information) are lost. This problem occurs only if you use the Content Distribution Manager GUI to perform the Websense configuration.

- CSCsb81144

  The cache process does a core dump and then gets restarted. This problem is caused by certain pass-through NTLM requests.

- CSCsb81163

  HTTPS requests fail when the **https proxy outgoing monitor** command is configured.

- CSCsc56266

  The cache process on the Content Engine crashes when the Content Engine makes a mem_hash_lookup() call.

- CSCsc66435

  When the Content Engine is overloaded, the Content Engine sends the HTTP 505 error a "temporarily out of resource" message.

- CSCsd38167

  A network router reports an error saying that the Content Engine is not responding to WCCP. The cache process on the Content Engine appears to have stopped. This problem occurs on Content Engines that run one of the following releases of the ACNS software: 5.2.7, 5.3.5, or 5.4.1.

- CSCsd47637

  A Cisco Streaming Engine RTSP on-demand program that is created by using the **cisco-streaming-engine broadcast id test source source-rtsp** command fails if you have used a hostname in the RTSP URL instead of the IP address.

- CSCsd70190

  When user authentication and rules are enabled on the Content Engine, the address space and memory consumption of the HTTP cache process increases. Based on the amount of traffic, the HTTP cache process may fail and restart from time to time.

- CSCsd78727

  The ACNS software accepts and forwards proxy requests on TCP ports 553 (RTSP gateway port) and 554 (RTSP proxy port). These proxy ports are enabled in the ACNS software by default and the CLI command cannot disable the ports.

## Rules Resolved Caveats

- CSCsd11891

  When you copy and paste rules to the Content Distribution Manager GUI, Content Distribution Manager returns either of the following error messages:

  ```
  CLI call failed, with "?" character where user expected a space
  CLI call succeeds, but an unexpected "?" character appears
  ```

  This problem occurs if the rule copied from another application was using a nonbreaking space instead of a normal space.

## Software Upgrade and Downgrade Resolved Caveats

- CSCsd20115

  Entering the **http proxy incoming 80** CLI command in the Content Engine causes the HTTP proxy to fail.

- CSCsd40679

  A change in the error log syntax affects the monitoring functions because network management systems that parse the error log for monitoring fail to interpret the message. This problem is caused by upgrading the Apache server from version 1.3.27 to 1.3.33, which uses a different location for the thread ID in the error log.

- CSCsd42056

  If you enable SmartFilter, the CPU usage shows 100 percent.

- CSCsd78914

  There is a delay in the availability of all services provided by the Centralized Management System (CMS) service after the Content Engine boots up.

## Windows Media Resolved Caveats

- CSCeg60760

  If many live streaming requests are being served by the Content Engine, the CPU usage increases up to 99 percent.

## Other Resolved Caveats

- CSCsc24879

  If the Content Engine model CE-7325 or CE-7320 is running the ACNS 5.3.3.8 software or a later release, it can hang or go into the kernel debugger (kdb) mode.

- CSCsc58252

  A mask is not assigned to a WCCP farm of Content Engines, and the WCCP view continuously changes. This problem can occur if the WCCP farm changes before a mask is assigned to any of the Content Engines in the farm.

- CSCsc65654

  The Content Engine stops serving HTTP requests for content, and persistent connections fail to time out. This problem can occur if you are using a Content Router to redirect HTTP requests for content, and persistent connections are enabled on the Content Engine. This problem occurs only for byte-range requests when the bit-rate control is configured.

- CSCsc75322

  The Content Engine neither raises an alarm nor creates an error log when it stops sending a negative acknowledgement (NACK) because of a disk full status or failure.

- CSCsc81507

  The Content Engine loses manually entered routes. This problem occurs when you have a large number of routes configured both manually and through device group settings on Content Distribution Manager on the Content Engine.

- CSCsc83680

  New files cannot be pre-positioned and older files cannot be deleted because UNS is full. This problem occurs when the file system is full and UNS cannot rewrite the required journal files.

- CSCsc83687

  Under the ext2 file system, the cdnfs corruption causes a UNS directory to be assigned a regular filename, which takes up disk space that is not cleaned up by a cdnf cleanup. This problem can occur if the Content Engine is running the ACNS 5.2.x or an earlier release.

- CSCsc84977

  The Content Engine shows 100 percent CPU usage and logs “RAM disk full” error messages in the syslog. Users are not able to access the Content Engine during this state. This problem occurs on edge Content Engines that have Cisco Streaming Engine live programs (IP/TV programs or managed live programs created on Content Distribution Manager) configured on them.

- CSCsd04224

  The manifest validator is unable to process a manifest file larger than 10 MB.

- CSCsd06577

  The export of transaction logs fails if there is any log file that does not follow the naming convention of using an underscore ( _ ) in the filename.

- CSCsd21268

  The interface duplex hardcode fails under the following conditions:

  - The interface is hardcoded to full-duplex.
  - The interface is disconnected while it is hardcoded.
  - The interface is disconnected during bootup.

- CSCsd47975

  The upload of binary files to the Content Engine fails. The Content Engine closes the connection before completing the file transfer if the ICAP service is enabled on the Content Engine.

- CSCsd57898

  The Content Engines at the root and edge locations do not show any media files associated with IP/TV program channels after the IP/TV Program Manager has been taken offline and restored. This problem occurs if the manifest file for the ACNS Channel with which the IP/TV programs are associated checks for programs before the IP/TV Program Manager database is restored.

- CSCsd66292

  The log entry created on completion of a multicast transmission of a file carries a wrong time stamp. Instead of the end time of the multicast transmission, the log entry shows the start time of the multicast.

- CSCsd66384

  The client browser receives an HTTP 400 bad request error. This problem occurs when the Content Engine receives an HTTP 200 OK response with the TCP FIN flag set.

- CSCsd82687

  The Content Engine reboots with the following error in the syslog:

  ```
  %CE-NODEMGR-0-330045: Rebooting the device because service 'dataserver' is dead
  ```

# 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 5.5.x*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*

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

### Hardware Documentation

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

### Software Documentation

- *Cisco ACNS Software Upgrade and Maintenance Guide, Release 5.x*
- *Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.5*
- *Cisco ACNS Software Command Reference, Release 5.5*
- *Cisco ACNS Software API Guide, Release 5.5*
- *Cisco ACNS software Program Manager for IP/TV User Guide, Release 5.4*
- *Release Notes for Cisco ACNS Software Program Manager for IP/TV, Release 5.4*

## Online Help

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

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

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

# Obtaining Documentation, Obtaining Support, and Security Guidelines

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

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