



# Release Notes for Cisco ACNS Software, Release 5.0.5, Build 9

---

September 11, 2003



**Note**

---

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

---

## Documentation Survey

Is Cisco documentation helpful? Click [here](#) to give us your feedback.

## Contents

These release notes contain information about ACNS software, Release 5.0.5. These release notes describe the following topics:

- [Introduction, page 2](#)
- [New and Changed Information, page 2](#)
- [Hardware Supported, page 10](#)
- [Important Notes, page 10](#)
- [Caveats, page 11](#)
- [Documentation Updates, page 28](#)
- [Related Documentation, page 28](#)
- [Obtaining Documentation, page 29](#)
- [Obtaining Technical Assistance, page 31](#)
- [Obtaining Additional Publications and Information, page 32](#)



---

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

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

# Introduction

These release notes describe new features, supported hardware, and open and resolved caveats regarding ACNS software, Release 5.0.5.

## New and Changed Information

This section describes existing features that have changed and new features in ACNS software, Release 5.0.5. These features include the following:

- [Configuring User Authentication Fail Over](#)
- [Adding or Removing WMT MMS Allowed Filename Extensions](#)
- [Websense Server Integration with Low-End Content Engine Models](#)
- [Additional Information in show hardware Command Display Output](#)

## Configuring User Authentication Fail Over

Content Engines support three databases: local, TACACS+, and RADIUS, for login and configuration privileges. These databases can be configured as primary, secondary, or tertiary to specify the order in which they should be queried, if a user account is not found in the primary database. However, previous releases of ACNS software did not offer an option to configure user authentication fail-over if an authentication server is unreachable. This allowed Content Engines to query the alternative methods of user authentication by default whenever the primary user authentication method failed. User authentication fail-over is a method by which users will be unable to gain access to the Content Engine using the local database unless the non-local authentication servers (TACACS+ or RADIUS) are unreachable.

In ACNS software, Release 5.0.5, you can configure the user authentication fail-over feature using the **authentication fail-over server-unreachable** global configuration command. This command allows you to specify that a fail-over to the secondary authentication method should occur only if the primary authentication server is unreachable. For example, when a TACACS+ server is enabled for authentication, and the user tries to log in to the Content Engine using an account defined in the local database, login succeeds. With user authentication fail-over configured, users cannot use the local database unless TACACS+ servers are unreachable. Use the **no** version of this command, **no authentication fail-over server-unreachable**, to disable the user authentication fail-over feature.



### Note

---

To use the authentication fail-over feature, you must set TACACS+, or RADIUS as the primary authentication method, and local as the secondary authentication method.

---

The following example sets user authentication fail-over to occur if the authentication server is unreachable:

```
ContentEngine(config)# authentication fail-over server-unreachable
ContentEngine(config)#
```

The following message is displayed when the primary authentication method has been set as local and you attempt to configure user authentication fail-over feature:

```
Either authentication or authorization scheme was set incorrectly.
Please, note the Authentication scheme fail-over due to server unreachable
feature doesn't have any effect if the primary, the secondary authentication
scheme, and the sequence of authentication schemes are configured incorrectly.
```

Use the **show authentication user EXEC** command to find out whether user authentication fail-over is configured on the Content Engine, as shown in the following example:

```
ContentEngine# show authentication user
Authentication scheme fail-over reason: server unreachable

Login Authentication:      Console/Telnet Session
-----
local                      enabled (primary)
radius                     disabled
tacacs                     disabled

Configuration Authentication: Console/Telnet Session
-----
local                      enabled (primary)
radius                     disabled
tacacs                     disabled

ContentEngine#
```

## Adding or Removing WMT MMS Allowed Filename Extensions

Content Engines use a list of filename extensions to decide whether a type of media file should be served by a Windows Media Technologies (WMT). Typically, Content Engines are shipped with a default list of filename extensions to be served by WMT. In previous releases of ACNS software, users were unable to add or delete filename extensions from this list. ACNS software, Release 5.0.5 adds the **wmt mms allow extension** global configuration command to let users add filename extensions to this list. The **no** version of this command, **no wmt mms allow extension**, removes a filename extension from the list.

The default list in the Content Engine contains the following filename extensions:

- asf
- none
- nsc
- wma
- wmv



### Note

The default list of filename extensions includes “none” to enable Content Engines to serve media files without file extensions, such as broadcast aliases or URLs of live encoders. The filename extension nsc is included in the list to enable Content Engines to multicast media files.

The following example adds the file extension mp3 to the list of filename extensions to be served by WMT:

```
ContentEngine(config)# wmt mms allow extension mp3
ContentEngine(config)#
```

The **show wmt mms allow extension EXEC** command shows the filename extensions included in the list after you have added or deleted filename extensions. The **show wmt mms allow extension** command does not display anything if you have not modified the default list.

In the following example of **show wmt mms allow extension** command, the default list of filename extensions has not been modified:

```
ContentEngine(config)# show wmt mms allow extension
ContentEngine(config)#
```

In this example of the **show wmt mms allow extension** command, the filename extension mp3 has been added to the list of file extensions:

```
ContentEngine(config)# show wmt mms allow extension
WMT mms extensions allowed :
asf mp3 none nsc wma wmv
ContentEngine(config)#
```

The following restrictions apply to adding new filename extensions to the list:

- You cannot have more than 20 extensions in the list of allowed filename extensions.
- Filename extensions must be alphanumeric, and the first character of every extension should be a letter.
- You cannot have more than ten characters in a filename extension.

## Websense Server Integration with Low-End Content Engine Models

In ACNS software, Release 5.0.3, Websense server Version 4.4.1 was integrated with higher-end Content Engine models (CE-7305 and CE-7325), running as a separate process instead of running on a separate device. In ACNS software, Release 5.0.5, Websense server integration is extended to the lower-end Content Engine models as well. Websense server Version 4.4.1 can be integrated with ACNS software in the following Content Engine models:

- CE-507AV
- CE-507
- CE-590
- CE-565
- CE-560
- CE-560AV
- CE-510
- CE-7320
- CE-7325
- CE-7305

There are no changes in the way that the Cache application communicates with the Websense server, except that the server now runs on the same device as the Cache application.

The amount of RAM needed for Websense server integration with the Content Engine is about 60 MB to 140 MB. When the Websense server is enabled and the Websense URL database is downloaded for the first time, CPU usage will be high. Therefore, we recommend enabling the Websense server during off-peak times or at times of low network traffic. Otherwise, other processes running on the Content Engine might be affected. When the Websense server stalls, it is automatically restarted.

An image of the Websense server resides in the /local/local1/WebsenseEnterprise directory. All the executables as well as the configuration and logging files are stored in this directory and requires about 150 MB of disk space. An additional 140 MB of disk space is required when the Websense URL database is downloaded, increasing the total disk space requirement to 290 MB. Because of this increased disk space requirement, we recommend increasing the size of the system file system (sysfs) disk partition to be larger than the default value on the Content Engines.

## Configuration of Ports for the Websense Server

The Websense process requires that these four ports be opened for connections either from processes internal to the Content Engine or from external processes such as the PIX firewall:

- Websense server port

This is the TCP port that receives requests for content filtering according to the Websense protocol.

- Block message server port

If the Websense process blocks a URL, it sends a redirect URL to the user. The redirect URL is configured to print out the blocked page and policy for the user. The Websense process listens on this port to receive the pages blocked, serviced by a thread in the Websense server. This thread sends the blocked page in response to the redirected request.

- Configuration server port

This port is required by the Websense GUI to configure the Websense server.

- Diagnostics server port

The Websense server has an exhaustive set of diagnostics that the users can run remotely to diagnose problems in the Websense process. This port is the one that these diagnostics utilities connect to.

Users can configure these ports by modifying the websense.ini file that resides in the /local/local1/WebsenseEnterprise directory. The Websense server must be restarted so that it can pick up the newly configured ports. Default port numbers for these four ports are:

- 15868 (Websense server port)
- 15871 (Websense block message server port)
- 15870 (Websense configuration server port)
- 15869 (Websense diagnostics server port)

Users can modify the ports by exporting a copy of the websense.ini file using FTP from the /local/local1/WebsenseEnterprise directory on the Content Engine, modifying the file, deleting the websense.ini file on the Content Engine, and then sending back the modified file to the Content Engine using FTP.



**Note**

The Websense server needs to be disabled and then reenabled to pick up newly configured ports.

## Changes in CLI Commands for the Websense Server

CLI commands for the Websense server have been changed as follows:

- **url-filter http websense server** *hostname*

The caching software uses this global configuration command to set up communication with the Websense server. This command has been modified to include another variable to signify that the Websense server is local. The revised syntax is as follows:

**url-filter http websense server** {*local* | *hostname*}

If the *local* variable is specified during the configuration, then the caching software sends URL filtering requests to the Websense server running on the Content Engine. On the other hand, if the *hostname* variable is chosen, then the Websense server running on the Content Engine is not used.

- **websense-server enable**

This new global configuration command enables the local Content Engine to act as the Websense server. When this command is used, a back-end script starts the Websense server process through the node manager.

If the default ports are changed, the Websense server must be disabled and reenabled before the changes can be implemented.

- **show url-filter http**

This command has been modified to show the IP address of the local host in the Websense sever IP field when the local host is configured as the Websense server for Websense URL filtering.

- **show websense-server**

This new command shows the configuration for the Websense server configured on the Content Engine. The output of the command includes the configured port numbers for the Websense server port, block message server port, configuration server port, and diagnostics server port; the Websense server version number; and the maximum number of connections.

- **write memory**

This existing EXEC command has been enhanced to save modified Websense configuration files (websense.init and ws.cfg) across disk reconfiguration and ACNS software release upgrades.

User must execute this command in order to retain the most recent configuration modifications, including websense.ini file modifications and the Websense URL filtering configuration changes. The **write memory** command enables the changes made from the external Websense Manager GUI to be saved across disk reconfiguration and upgrade (which might erase disk content).

If the **write memory** command was not used before reboot but after a disk reconfiguration or an ACNS software upgrade that erases disk content, the Websense configurations that were saved when the **write memory** command was last used will be retained. However, if the **write memory** command was never used before, then default configurations will be applied when the content on /local/local1/WebsenseEnterprise directory is erased.

To configure the Websense server to run on the Content Engine, follow these steps:

- 
- Step 1** From the Content Engine GUI, choose **Caching > URL Filtering**. The URL Filtering window appears.
- Step 2** Check the **Websense Server (Local)** check box to configure the Websense server to run on the Content Engine.




---

**Note** The hostname or IP address of the local Websense server is displayed in the Websense Server field. (configurable by the user, in case of Websense Server Remote). The Websense server IP address cannot be configured for this. It is fixed to be 127.0.0.1.

---

- Step 3** Enter information in the following fields:
- **Port**—Enter the port number on which the Websense server is accepting requests. The default value is 15868.
  - **Timeout**—Enter the value in seconds. The range is between 1 and 240 seconds. The default value is 20.
  - **AllowMode**—Check this check box to specify whether the request must be allowed or blocked if no response is received after the value specified in the Timeout field.
- Step 4** Click **Update** to submit the changes.

---

To enable the Websense server using the Content Engine GUI, follow these steps:

- 
- Step 1** From the Content Engine GUI, choose **System > Websense Server**. The Websense Server window appears.
- Step 2** Click **Start** to enable the Websense server. The **Start** button appears only if the Websense server is currently disabled.




---

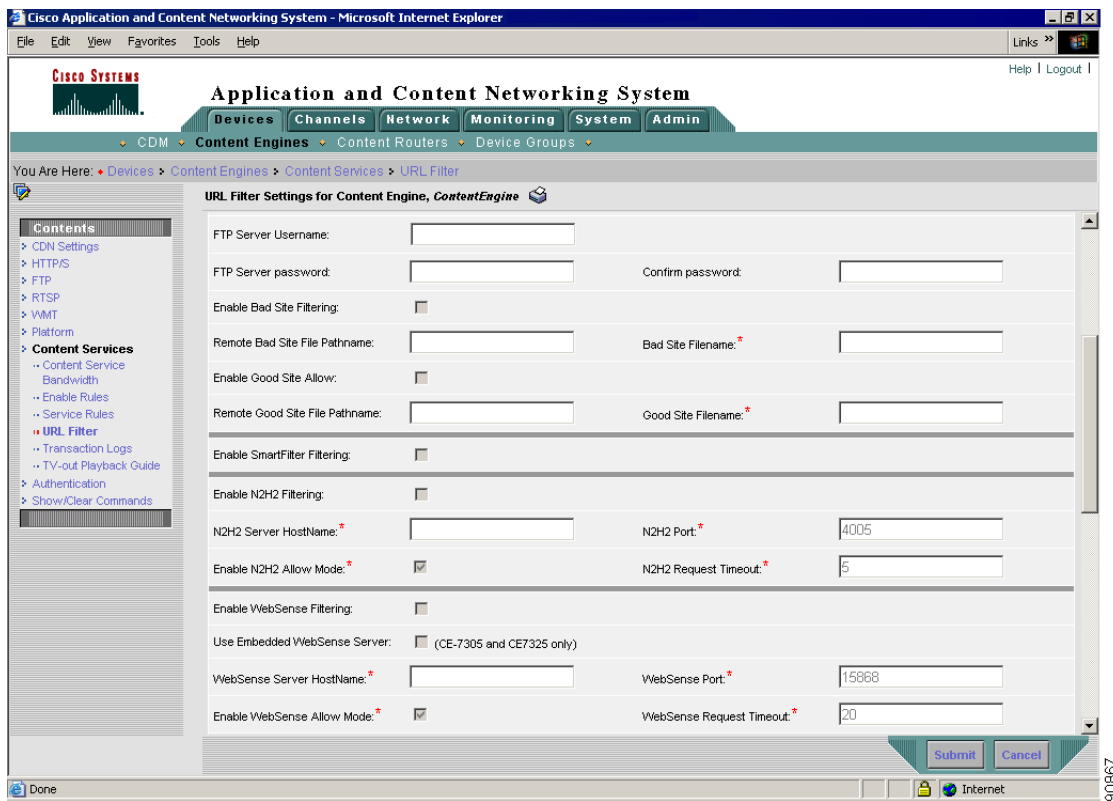
**Note** To stop the Websense server, click **Stop**. The **Stop** button appears only if the Websense server is currently enabled.

---

You can also enable the Websense server using the Content Distribution Manager GUI. To enable the Websense server on the Content Engine, follow these steps:

- 
- Step 1** From the Content Distribution Manager GUI, choose **Devices > Content Engines**.
- Step 2** Click the **Edit** icon next to the Content Engine that you want to view. The Modifying Content Engine window appears.
- Step 3** In the Contents pane, choose **Content Services > URL Filter**. The URL Filter Settings for Content Engine window appears. (See [Figure 1](#).)

Figure 1 URL Filter Settings for Content Engine Window



- Step 4** Click the **Add Settings** button to configure and enable the Websense server to run on the Content Engine. The URL Filter Settings for Content Engine window refreshes itself, with the HTTP URL Filter Settings options activated.
- Step 5** Check the **Enable WebSense Filtering** check box to enable URL filtering using the Websense server.
- Step 6** Check the **Use Embedded WebSense Server** check box to configure the Websense server on the Content Engine. This ensures that the URL filtering software uses the local Websense server and not a remote host as the Websense server.
- Step 7** Enter the host name of the Websense server, the port for receiving requests for URL filtering, and the timeout period for Websense requests.
- Step 8** Check the **Enable WebSense Allow Mode** check box to enable HTTP access to a website if the Websense server does not respond.
- Step 9** Click **Submit** to confirm your settings.

To download the Websense components, such as Explorer, Manager, and Reporter, or to obtain an evaluation key for using the Websense server that runs on the Content Engine, access the following URL and follow the sequence of steps:

<http://www.websense.com/downloads>

To access Websense product setup and implementation documents, access the following URL:

<http://www.websense.com/support/documentation/index.cfm>

## Additional Information in show hardware Command Display Output

The **show hardware EXEC** command has been enhanced in ACNS software, Release 5.0.5 to display additional hardware information for the CE-510 and CE-565 Content Engine models. The **show hardware EXEC** command output for CE-510 and CE-565 displays the exact hardware variant details. These details are displayed against the Manufactured As heading in the output of the command.

The following **show hardware** output displays the hardware details, including the hardware variant details, for a CE-510:

```
ContentEngine# show hardware
Application and Content Networking System Software (ACNS)
Copyright (c) 1999-2003 by Cisco Systems, Inc.
Application and Content Networking System Software Release 5.0.5 (build b8 Aug 1 2003)
Version: ce510-5.0.5

Compiled 21:24:59 Aug 1 2003 by ceuser
Compile Time Options: PP SS

System was restarted on Sat May 10 02:13:04 2003.
The system has been up for 14 minutes, 2 seconds.

Core CPU is GenuineIntel Intel(R) Celeron(R) CPU 1.70GHz (rev 1) running at 1699 MHz.
512 Mbytes of Physical memory.
1 CD ROM drive
2 GigabitEthernet interfaces
1 Console interface
2 USB interfaces [Not supported in this version of software]

Manufactured As: CE-510-K9 [-[8673C1X]-]

BIOS Information:
Vendor                : IBM
Version               : -[PLEC38AUS-C.38]-
Rel. Date             :

Cookie info:
SerialNumber: 78GB030
SerialNumber (raw): 55 56 71 66 48 51 48 0 0 0 0
TestDate: 5-0-2003
ExtModel: CE510
ModelNum (raw): 55 0 0 0 1
HWVersion: 1
PartNumber: 53 54 55 56 57
BoardRevision: 1
ChipRev: 1
VendID: 0
CookieVer: 2
Chksum: 0xfd27

There is no storage-array attached to this box.

List of disk all drives:
disk00: Normal (IDE disk) 38160MB( 37.3GB)
        disk00/04: SYSFS 1023MB( 1.0GB) mounted at /local1
        System use: 6129MB( 6.0GB)
        FREE: 31006MB( 30.3GB)
disk01: Normal (IDE disk) 38162MB( 37.3GB)
        FREE: 38162MB( 37.3GB)
ContentEngine#
```

# Hardware Supported

ACNS software, Release 5.0.5 supports the following hardware platforms:

- NM-CE-BP-SCSI
- NM-CE-BP-20G
- NM-CE-BP-40G
- CDM-4630
- CDM-4650
- CE-7320
- CR-4430
- CE-590
- CE-590-DC
- CE-560
- CE-560AV
- CE-507
- CE-507AV
- CE-510-K9
- CE-565-K9
- CE-7325-K9
- CE-7305-K9

## Important Notes

This section emphasizes important information regarding ACNS 5.0.x software.

## Upgrade Issues

Upgrading a Content Engine running ACNS software, Release 5.0.3 to Release 5.0.5 may fail if the Content Engine had been running for more than three weeks. Cisco recommends that you reload the Content Engine before upgrading from ACNS software, Release 5.0.3 to Release 5.0.5.

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

If you have configured the media file system (mediafs) with ACNS 5.1 software or later, and then downgrade to ACNS 5.0 software, the mediafs disk space assignment is lost and it reverts to 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 ACNS 5.1 software. Because 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 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 (that is, 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.

## Websense Issues When Downgrading to 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 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. Note that the ACNS 5.2.x software does not generate an error message indicating that the WebsenseEnterprise directory has been removed.

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

1. Disable the local (internal) Websense server on the Content Engine.
2. Deactivate the Websense services on the Content Engine.
3. Install the ACNS 5.1 software or ACNS 5.0 software downgrade image on the Content Engine.

## Caveats

This section lists and describes caveats that are open in ACNS software, Release 5.0.5. Caveats describe unexpected behavior in ACNS software. Severity 1 caveats are the most serious; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats.

## Open Caveats - ACNS Software, Release 5.0.5

- CSCdy02581

Symptom: WCCP bypass does not function properly when bypassing large packets from the client. Therefore, the client never receives an acknowledgment from the server for the data sent.

Condition: This problem occurs when the Content Engine bypasses the connection and the server advertises a maximum segment size (MSS) of 1460 bytes.

Workaround: If the client's path is configured to discover the maximum transmission unit (MTU), users can configure a lower value of MTU on the router interface connected to the Content Engine. Thus if a client sends a large packet, the router would drop it and would send an Internet Control Message Protocol (ICMP) message with the reduced MTU value. Clients would then adjust to the lower value.

- 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 will contain 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 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 there are any errors during certificate verification by the ACNS acquirer, then content from that site will not be acquired. With weak authentication, certain errors (for example, errors such as certificate has expired, certificate is not yet valid, and subject issuer mismatch) 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 they should install on their origin servers. Note that the certificate list differs based on the version of the ACNS software. For the ACNS 5.0.5 software release, refer to the following certificate list:

```
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=VeriSign, Inc., OU=Class 1 Public Primary
Certification Authority
    Validity
        Not Before: Jan 29 00:00:00 1996 GMT
        Not After : Jan  7 23:59:59 2020 GMT
    Subject: C=US, O=VeriSign, Inc., OU=Class 1 Public Primary
Certification Authority
-----END CERTIFICATE-----
```

```

-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=VeriSign, Inc., OU=Class 2 Public Primary
Certification Authority
    Validity
        Not Before: Jan 29 00:00:00 1996 GMT
        Not After  : Jan  7 23:59:59 2004 GMT
    Subject: C=US, O=VeriSign, Inc., OU=Class 2 Public Primary
Certification Authority
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=VeriSign, Inc., OU=Class 3 Public Primary
Certification Authority
    Validity
        Not Before: Jan 29 00:00:00 1996 GMT
        Not After  : Jan  7 23:59:59 2004 GMT
    Subject: C=US, O=VeriSign, Inc., OU=Class 3 Public Primary
Certification Authority
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=RSA Data Security, Inc., OU=Secure Server
Certification Authority
    Validity
        Not Before: Nov  9 00:00:00 1994 GMT
        Not After  : Jan  7 23:59:59 2010 GMT
    Subject: C=US, O=RSA Data Security, Inc., OU=Secure Server
Certification Authority
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: O=VeriSign, Inc, OU=www.verisign.com/repository/TestCPS Incorp. By
Ref. Liab.LTD., OU=For VeriSign authorized testing only. No assurances (C)VS1997
    Validity
        Not Before: Mar  4 00:00:00 1997 GMT
        Not After  : Mar  4 23:59:59 2025 GMT
    Subject: O=VeriSign, Inc, OU=www.verisign.com/repository/TestCPS Incorp.
By Ref. Liab. LTD., OU=For VeriSign authorized testing only. No assurances
(C)VS1997
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=AU, ST=Queensland, O=CryptSoft Pty Ltd, CN=Test PCA (1024 bit)
    Validity
        Not Before: Dec  2 21:38:51 1999 GMT
        Not After  : Jul 10 21:38:51 2005 GMT
    Subject: C=AU, ST=Queensland, O=CryptSoft Pty Ltd, CN=Test CA (1024 bit)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd, CN=PCA
    Validity
        Not Before: Jun 15 02:14:29 1997 GMT
        Not After  : Jul 15 02:14:29 1997 GMT
    Subject: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd, CN=CA
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd, CN=PCA
    Validity
        Not Before: Jun 14 22:54:45 1997 GMT
        Not After  : Jul 14 22:54:45 1997 GMT
    Subject: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd, CN=PCA
-----END CERTIFICATE-----

```

```

-----BEGIN CERTIFICATE-----
    Issuer: C=GB, O=UCL, OU=ICE-TEL Project, CN=TrustFactory
    Validity
        Not Before: Apr 22 14:39:14 1997 GMT
        Not After : Apr 22 14:39:14 1998 GMT
    Subject: C=GB, O=UCL, OU=ICE-TEL Project, CN=TrustFactory
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: O=European ICE-TEL project, OU=V3-Certification Authority
    Validity
        Not Before: Apr  2 17:35:53 1997 GMT
        Not After : Apr  2 17:35:53 1998 GMT
    Subject: O=European ICE-TEL project, OU=V3-Certification Authority,
L=Darmstadt
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: O=European ICE-TEL project, OU=V3-Certification Authority
    Validity
        Not Before: Apr  2 17:33:36 1997 GMT
        Not After : Apr  2 17:33:36 1998 GMT
    Subject: O=European ICE-TEL project, OU=V3-Certification Authority
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: O=European ICE-TEL project, OU=V3-Certification Authority,
L=Darmstadt
    Validity
        Not Before: Apr  2 17:35:59 1997 GMT
        Not After : Apr  2 17:35:59 1998 GMT
    Subject: O=European ICE-TEL project, OU=V3-Certification Authority,
L=Darmstadt, CN=U
SER
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=Ca, L=Nepean, OU=No Liability Accepted, O=For Demo Purposes
Only, CN=Entrust Demo Web CA
    Validity
        Not Before: Apr 26 13:35:01 1996 GMT
        Not After : Apr 26 13:35:01 2006 GMT
    Subject: C=Ca, L=Nepean, OU=No Liability Accepted, O=For Demo Purposes
Only, CN=Entrust Demo Web CA
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=AU, ST=Queensland, O=CryptSoft Pty Ltd, CN=Test PCA (1024 bit)
    Validity
        Not Before: Dec  2 21:35:48 1999 GMT
        Not After : Jul 11 21:35:48 2005 GMT
    Subject: C=AU, ST=Queensland, O=CryptSoft Pty Ltd, CN=Test PCA (1024 bit)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=RSA Data Security, Inc., OU=Commercial Certification
Authority
    Validity
        Not Before: Nov  4 18:58:34 1994 GMT
        Not After : Nov  3 18:58:34 1999 GMT
    Subject: C=US, O=RSA Data Security, Inc., OU=Commercial Certification
Authority
-----END CERTIFICATE-----

```

```

-----BEGIN CERTIFICATE-----
    Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
OU=Certification
Services Division, CN=Thawte Server CA/Email=server-certs@thawte.com
    Validity
        Not Before: Aug  1 00:00:00 1996 GMT
        Not After  : Dec 31 23:59:59 2020 GMT
    Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
OU=Certification Services Division, CN=Thawte Server
CA/Email=server-certs@thawte.com
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
OU=Certification
Services Division, CN=Thawte Premium Server CA/Email=premium-server@thawte.com
    Validity
        Not Before: Aug  1 00:00:00 1996 GMT
        Not After  : Dec 31 23:59:59 2020 GMT
    Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
OU=Certification Services Division, CN=Thawte Premium Server
CA/Email=premium-server@thawte.com
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=AU, ST=Queensland, L=Brisbane, O=CryptSoft Pty Ltd,
OU=development, CN=CryptSoft Dev CA
    Validity
        Not Before: Mar 22 13:34:04 1997 GMT
        Not After  : Mar 22 13:34:04 1998 GMT
    Subject: C=AU, ST=Queensland, L=Brisbane, O=CryptSoft Pty Ltd,
OU=development, CN=CryptSoft Dev CA
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=AU, ST=Queensland, L=Brisbane, O=CryptSoft Pty Ltd,
OU=WORTHLESS CERTIFICAT
ION AUTHORITIES, CN=ZERO VALUE CA - DEMONSTRATION PURPOSES ONLY
    Validity
        Not Before: Apr  3 13:22:54 1997 GMT
        Not After  : Apr  3 13:22:54 1998 GMT
    Subject: C=AU, ST=Queensland, L=Brisbane, O=CryptSoft Pty Ltd,
OU=WORTHLESS CERTIFICA
TION AUTHORITIES, CN=ZERO VALUE CA - DEMONSTRATION PURPOSES ONLY
-----END CERTIFICATE-----

```

- CSCdy89507

Symptom: When ACNS network users use an external authentication server such as TACACS+, RADIUS, Windows NT LAN Manager (NTLM), or Lightweight Directory Access Protocol (LDAP) for authentication, authorization, and accounting of user accounts, the authentication server settings cannot be changed.

Condition: This occurs in ACNS software, Release 5.0 and later.

Workaround: Users need to remove the authentication server from service when they want to change the settings for any of the external authentication servers, such as TACACS+, RADIUS, NTLM, or LDAP. This can be done using the Local Authentication Settings window or the Authentication Scheme Settings window in the Content Distribution Manager GUI.

- CSCdz32182

Symptom: When the user tries to add port 8443 for incoming HTTPS proxy requests on a Content Engine using the **https proxy incoming 8443** command, the following message appears:

```
Port 8443 is reserved for application the Cdm_UI_http
```

**Condition:** This occurs when port 8443 is reserved for the HTTPS incoming proxy by the Content Distribution Manager GUI and port 8443 therefore cannot be used on a Content Engine where no Content Distribution Manager GUI is running. However, on a Content Distribution Manager, it is appropriate to reserve port 8443, because this port is used as the Content Distribution Manager GUI port.

**Workaround:** Use a different port that is not reserved. You can check reserved ports using the commands **show services port** *port-number* for a specific port or **show services summary** for a collective summary of all used ports.

- CSCdz35191

**Symptom:** For pre-positioned Windows Media content, if the content is defined in the manifest file to be WMT over HTTP play and if NTLM authentication is enabled from the Content Distribution Manager, the Content Engine fails to handle the authentication with the origin server properly. You are repeatedly prompted for a username and password even though you have already entered the proper username and password.

**Condition:** This occurs in ACNS software, Release 5.0 and later.

**Workaround:** Choose one of the following options to avoid this problem.

- Use MMS play rather than HTTP play in the manifest file definition.
- Use HTTP play, but disable authentication.
- Use HTTP play with basic authentication.

- CSCdz41188

**Symptom:** The cache service unexpectedly restarts after running for 3 months.

**Condition:** The cache service automatically restarts when it runs for a relatively long time under production traffic.

**Workaround:** The cache service is automatically restarted by a node manager. Therefore, no special workaround action is necessary.

- CSCdz44596

**Symptom:** A multicast receiver Content Engine obtains content through unicast before the multicast sender has delivered the content through multicast.

**Condition:** This problem occurs when the Content Engine has a parent forwarder that is not the multicast sender but which has already received the content. The Content Engine contacts the parent and downloads the content through unicast.

**Workaround:** Take one of the following actions:

- Configure the channel to be multicast only using the Creating New Channel window in the Content Distribution Manager GUI.
- Place the receiver Content Engine directly under the multicast sender, so that the multicast sender is the forwarder for the Content Engine.

- CSCdz67216

**Symptom:** The CLI does not allow you to assign a device group and reports only the first Content Engine with insufficient space. You might have to try a few times to assign a device group.

**Condition:** You are using the CLI to assign a device group to a channel, and multiple Content Engines have insufficient space for the channel quota.

**Workaround:** Either verify which Content Engines have space before you use a CLI command, or make sure that device groups contain similar Content Engines and that Content Engines are assigned consistently to device groups.

- CSCdz68730
 

Symptom: Users experience a brief outage of HTTP services, and the following message is logged in the syslog.txt file:

```
Service 'cache' died due to signal 15: Terminated.
```

Condition: This occurs when multiple services are enabled on lower-end Content Engine models, especially the CE-507. The system might be running low on memory.

Workaround: Cache service is resumed automatically. Users need to reduce the number of services on low-end Content Engine models such as the CE-507.
- CSCdz74319
 

Symptom: Users receive a DNS failure message when the cache process is unable to resolve the host names presented in the URL.

Condition: DNS failure occurs when users attempt to access a website. However, this symptom is transient and rare.

Workaround: Use the reload function of the browser, although the problem disappears on its own after a short while.
- CSCdz75101
 

Symptom: An error alert on the system log page indicates a failure to configure an IP address.

Condition: The Content Distribution Manager accepts invalid IP addresses that you enter as the NTLM server for authentication.

Workaround: Make sure that you enter a valid IP address.
- CSCdz76591
 

Symptom: When the user tries to copy a file from the FTP server and install the software release file on the Content Engine, using the **copy ftp install {hostname | ip-address} remotefiledir remotefilename** command, the following error message appears:

```
ruby_upgrade: cannot create lock file 'ruby_upgrade.lock' : Permission denied
```

Condition: This error occurs when the user uses TACACS+ as the login authentication method for device management.

Workaround: There is no known workaround.
- CSCdz82188
 

Symptom: The number of MPEG-1 concurrent streams that is streamed over HTTP is low on a CE-7325. The download of MPEG-1 files is found to be slower than the rate at which the files need to be played on a Windows Media Player. In addition, monitoring of the SNMP event MIB is interrupted.

Condition: This symptom is observed when ten MPEG-1 streams are pre-positioned across four Content Engines, each having an internal disk, and the HTTP bit rate is set to 1.1 Mbps.

Workaround: The files need to be encoded in other formats, or the MPEG-1 files must be streamed using Windows Media Technologies (WMT) or RTSP instead of HTTP.
- CSCdz86310
 

Symptom: When a user configures certain settings for RealProxy, RealServer, or WMT using CLI commands, the following message appears:

```
The evaluation has already expired
```

However, when the same settings are configured using the GUI, no error message is displayed, but an error is recorded in the System Message Log window in the Content Distribution Manager GUI.

Condition: This occurs when an evaluation license is used and the evaluation period has expired.

Workaround: Purchase and install a permanent license. Do not use the evaluation license anymore.

- CSCea14491

Symptom: If the server responds with a “100 Continue” message for a POST request from the user, the Content Engine stops parsing all requests on the connection, and subsequent requests are not handled properly.

Condition: This symptom occurs in ACNS software, Release 4.2.5 or earlier, and all 5.0.x releases.

Workaround: To partially address the problem with proxy connection, users can upgrade to ACNS software, Release 4.2.7 and later in which ACNS closes the connection after serving the request. This results in slightly higher latency because of a break in the persistent connection. Known servers respond with the “100 Continue” message to the POST request method only.

- CSCea25617

Symptom: Login and configuration authentication servers can be enabled without having to configure an IP address or host name. For example, even if no TACACS+ servers are configured, you can still enable login authentication using TACACS+. This can be verified by using the **show authentication user** and **authentication login tacacs enable** commands.

Condition: When the **disable local login authentication** command is used to disable local authentication, the CLI believes that TACACS+ authentication has been already enabled and allows users to disable local authentication for login. In this scenario, the user can never log in to the Content Engine, because there are no configured TACACS+ servers and local authentication is also disabled.

Workaround: There is no known workaround.

- CSCea27285

Symptom: Users cannot play live streaming content from a Windows Media Server that is trying to obtain a stream from a Content Engine broadcast station alias.

Condition: This problem occurs when a Microsoft Windows Media Server is configured to obtain a WMT live stream from the Content Engine. The user’s media player receives a “corrupted data” error or “invalid state” error. This problem does not occur if the stream that has been obtained from the Content Engine is not a live stream. The Windows Media Server is failing to retrieve the stream from the Content Engine, which in turn is obtaining the stream from the origin server.

Workaround: There is no known workaround. If possible, users should use a Content Engine to obtain the stream from a Windows Media Server.

- CSCea27565

Symptom: The F1 key might not work with certain terminal settings to access the BIOS menu.

Condition: This symptom occurs on either the CE-7305 or the CE-7325 only. With certain terminals, the F1 key might not work well because the terminal emulation program might use the F1 key for its own purposes, or send an incorrect F1 key sequence to the Content Engine. Without the F1 key, the user cannot press F1 to access the BIOS menu at system boot time.

Workaround: Tune the terminal emulation program settings, or connect a keyboard and monitor to the Content Engine to access the BIOS.

- CSCea36192
 

Symptom: When a user enables streaming (RTSP, WMT, and Cisco Streaming Engine) on the Content Engine Network Module from the Content Distribution Manager GUI, some of the streaming configuration settings are lost. These include WMT license key installed, RTSP server real-subscriber accept-license-agreement, rtsp server real-subscriber enable, rtsp proxy media-real enable, rtsp proxy media-real license-key installed, rtsp ip-address rtsp server, and cisco-streaming-engine enable.

Condition: This symptom occurs when the user performs an upgrade or downgrade after applying the settings.

Workaround: The user must choose the RTSP and WMT settings from the Contents pane on the Content Distribution Manager GUI and resubmit the configurations.
- CSCea43509
 

Symptom: The Content Distribution Manager GUI shows that an upgrade on a Content Engine has failed when the upgrade has in fact been successful. However, the CLI on the Content Engine shows the correct upgrade information.

Condition: This symptom occurs because the upgrade meta file has the wrong software version. In other words, the version in the meta file does not match the version of the upgrade file.

Workaround: Currently, there is no known workaround.
- CSCea46917
 

Symptom: The Windows Media Player will continue to wait forever to play a media file if the source is a media file that is configured to play in a loop from the Windows Media Server, and if the Content Engine is configured for unicast-in multicast-out multicast delivery of streaming media.

Condition: This occurs only when the source is a Windows Media Server and the media file is configured to loop and when the Content Engine is configured for unicast-in multicast-out.

Workaround: Avoid using a loop file from the Windows Media Server. Users can pre-position the media file to the Content Engine and multicast the file from the local disk before configuring it to play in a loop.
- CSCea60143
 

Symptom: Performing a software upgrade or downgrade using the Content Distribution Manager GUI shows the status as updateFailed in the device listing windows, such as the Content Engines window. This failure occurs when the software upgrade or downgrade encounters an error on the target device. Once a request for upgrade or downgrade is received by the target device, attempts to upgrade or downgrade software occur only once.

Condition: This occurs in ACNS software, Release 5.0 and later.

Workaround: Users need to avoid some of the following common error conditions:

  - Do not manually reload the target device if the software upgrade or downgrade status is shown as Pending or in an intermediate state (such as Downloading or Writing Flash).
  - Check whether there is no pending update that has already been written to flash memory using the **show flash** command. If any pending update is found, reload the device.
  - In the case of a pre-positioned update file URL, ensure that it is fully replicated on that Content Engine before triggering a software upgrade or downgrade.
  - In the case of a direct update file URL, ensure that the device can successfully connect to the target host for an FTP or HTTP download and that the specified update file is present.

If any of the above errors occur, clear that error and request another software upgrade or downgrade using the Content Distribution Manager GUI.

- CSCea73660
 

Symptom: The RealProxy player stops playing live split streams after a few hours. The video frame stops and the media cache statistics of the RTSP proxy show that no packets have been received.

Condition: This occurs on Content Engines running ACNS software, Release 5.0.3 and later.

Workaround: Close the RealProxy player and restart it. The audio and video will be available again.
- CSCea75877
 

Symptom: With WCCP Version 2 enabled, Windows XP clients might experience problems in accessing remote systems with shared files and folders that are running Windows 2000 Server and Internet Information Services (IIS) server.

Condition: This problem occurs when an attempt is made to connect to a remote system by specifying the Universal Naming Convention (UNC) name of a resource or mapping a network drive. Although connection is established with the remote system, it takes approximately 10 minutes for the shared resource to connect. This is because the Content Engine affects the Server Message Blocks (SMB) protocol.

Workaround: Take one of these actions:

  - Include the Windows XP client as a deny entry in the WCCP redirect access list on the router. Determine whether access to the shared file or folder is possible.
  - If access is possible, remove the Windows XP client from the WCCP redirect access list on the router and add the Windows XP client as a static bypass entry on the Content Engine. Determine whether access to the shared file or folder is possible.
  - Turn off the WebDAV request method on the Windows XP client or Windows 2000 Server. This might work in certain situations. This can be done by changing the value of the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\MRxDAV\Start to 0. Alternatively, WebDAV can also be turned off by adding a new DWORD value entry called DisableWebDAV in the Windows 2000 Server Registry under HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters and restarting the IIS server.
- CSCea81020
 

Symptom: When the Content Engine is used in transparent or proxy mode in conjunction with an Internet Security and Acceleration (ISA) proxy as a downstream proxy that does NTLM authentication, contents take a long time to download.

Condition: This symptom occurs when a Content Engine is used in conjunction with an ISA proxy that does NTLM authentication.

Workaround: There is no known workaround.
- CSCea85009
 

Symptom: The **ip name-server serial-lookup** global configuration command fails to query each of the configured name servers iteratively in case the primary name server responds in the negative.

Workaround: There is no known workaround.
- CSCea88122
 

Symptom: After thousands of playlist position changes for a playlist that is scheduled to loop playback continuously or for an extended period, the TV-out service might run out of memory. Interruption in playback occurs and core files are generated.

Under some error conditions, such as loss or unavailability of media files on the cdnfs, a playlist might change its position rapidly, thereby exhibiting this behavior after several hours of continuously failed playback.

Condition: This occurs on the CE-507-AV, CE-560-AV, and CE-510 or CE-560 with optional AV decoder card installed, running ACNS software, Release 5.0 or later.

Workaround: Perform any of the following workarounds:

- Disable and reenable TV-out service on the Content Engine using the **no tvout enable** and **tvout enable** global configuration commands.
  - Correct any error conditions that cause rapid playlist position changes.
  - Schedule TV-out playback so that playlists are periodically stopped and restarted according to various repeat intervals.
- CSCea89557

Symptom: The **acquirer check-time-for-old-content [channel-id *channel\_num* | channel-name *channel\_name*]** EXEC command does not work. The following messages are displayed when the command is used with valid root Content Engine channel ID and names:

```
ContentEngine# acquirer check-time-for-old-content channel-id 291
Unable to get the channel information record for channel= 291
This CE is not the root CE for this channel = 291
Failed to check the last modified time in DB
```

```
ContentEngine# acquirer check-time-for-old-content channel-name channeltest
Unable to get the channel information record for channel= 291
This CE is not the root CE for this channel = 291
Failed to check the last modified time in DB
```

Workaround: Use the **acquirer check-time-for-old-content** EXEC command without the channel ID and channel name parameters. This command will display the incorrect last modified time for all channels of the root Content Engine.

- CSCea91755

Symptom: When the ACNS software is upgraded, the database upgrade fails because a table is found to exist already. This appears as an upgrade error in the `syslog.txt` log file. The Centralized Management System (CMS) does not start on the device, and the device appears as offline in the device listing windows in the Content Distribution Manager GUI.

Condition: If a device is downgraded from ACNS software, Release 5.0.5 to ACNS software, Release 5.0.1, and subsequently deregistered from the Content Distribution Manager and reregistered with the Content Distribution Manager, the local database tables that were created as part of ACNS software, Release 5.0.5 remain in the database. The existence of these tables causes a later ACNS software upgrade to fail.

Workaround: This problem occurs only if the downgraded device is deregistered from the Content Distribution Manager. However, it is also possible to downgrade a device, keep it registered with the Content Distribution Manager, and later upgrade the device. In situations that require the downgraded device to be deregistered from the Content Distribution Manager, the database needs to be cleared of all tables before you reregister the device.

The sequence of CLI commands to deregister and reregister a device is as follows.

1. **cms deregister**
2. **cms database delete**
3. **cms enable**

The **cms deregister** command removes the registration information from the Content Distribution Manager and removes known database tables. The **cms database delete** command removes all tables, including any table that might have been created as part of another ACNS software release. The **cms enable** command registers the device with the Content Distribution Manager, creates the local database, and starts the CMS processes.

- CSCea93249

Symptom: Installing an upgraded version of ACNS software, Release 5.0.x deletes all content in the existing SmartFilter directory. Therefore, if SmartFilter software was previously installed for URL filtering, installation of a newer version of ACNS software, Release 5.0.x causes filtering to be disabled.

Condition: This symptom occurs if the user installs an upgraded version of ACNS software, Release 5.0.x on a Content Engine running SmartFilter software.

Workaround: SmartFilter, Version 3.1.2 is shipped with ACNS software, Release 5.0.x and contains SmartFilter software policy information stored on remote SmartFilter Administration Servers. Use the SmartFilter Administration Console to reapply the configuration settings on the Content Engine, and manually download the SmartFilter Control List. Once the Control List has been downloaded to the Content Engine, URL filtering will recommence.

- CSCeb02494

Symptom: A multi-bit rate (MBR) media file, after being preloaded, returns partial cache-hit upon proxy style request.

Condition: This problem was observed with only one MBR media file.

Workaround: There is no known workaround. The media file will be fully cached after proxy style request is served.

- CSCeb07223

Symptom: When the network experiences significant packet loss, the multicast sender may send fewer bytes than the actual file size. This causes multicast reception to fail on all receivers.

Condition: The network suffers a lot of multicast packet loss when the multicast session is about to end.

Workaround: In /local1/multicast-expert-config/, set a pgmfx configuration file on the multicast sender to turn off Pragmatic General Multicast (PGM) congestion control, turn up the proactive forward error correction (FEC), and on the Content Distribution Manager GUI, set the FEC to 16.

- CSCeb30020

Symptom: When Microsoft Internet Information Services (IIS) server 4.0 is used as the FTP server and DOS format is used as the directory listing format, acquisition of content fails and error 712 (file size mismatch) occurs. This problem occurs because the IIS server calculates the file size incorrectly. When you compare the calculated file size with the downloaded file size, a mismatch is found and the downloaded file is ignored.

Condition: This problem occurs in ACNS software, Releases 5.0.1 and 5.0.3. Also, it is observed only with IIS server 4.0. IIS server 5.0 functions properly.

Workaround: There is no known workaround.

- CSCeb34946

Symptom: The Content Engine is unable to play audio only files over playback with Content Engine AV units.

Condition: This occurs as the Content Engine is looking to synchronize audio and video tracks, but there is no video track.

Workaround: Record the audio-only files with blank video tracks.
- CSCeb43206

Symptom: The Content Engine CLI allows users to enter proxy-protocol exclusion lists that use wildcards. When users try to do the same in the Content Distribution Manager GUI, the Content Distribution Manager displays an error.

Workaround: Use the CLI to make these configuration settings until the GUI is brought to parity with the CLI.
- CSCeb46306

Symptom: Users cannot submit a GUI page where \ (the backslash character) is used as file separator in input fields.

Condition: The ACNS GUI does not allow directories with a \ as a file separator, but only / (a forward slash). The ACNS CLI accepts \ as a file separator.

Workaround: Use the corresponding CLI command instead of the GUI.
- CSCeb48853

Symptom: Services do not start in the ACNS network, and no message is displayed.

Condition: When a default gateway is not configured, services do not start.

Workaround: Configure a default gateway in the ACNS GUI.
- CSCeb49962

Symptom: The default behavior of the GUI does not match that of the CLI for the command **http object url-validation enable**. In the CLI, the default is to enable the command, but in the GUI the default is to disable the command.

Workaround: Enable the command in the GUI.
- CSCeb76891

Symptom: The Content Engine is unable to authenticate users using LDAP.

Condition: The authentication mode process in the Content Engine does not release the sockets, and after some time (1 or 2 weeks) there are no sockets left for new requests.

Workaround: Restart the Content Engine.
- CSCeb80646

Symptom: The administrator cannot access the Content Engine from the ACNS GUI if the fail-over feature is configured and the primary authentication scheme is not working.

Condition: This problem occurs with the web server if fail-over is configured and the primary authentication scheme is not working. When the primary authentication scheme is not working, the administrator can access the Content Engine using Content Distribution Manager, Telnet, SSH, or FTP.

Workaround: The administrator should use Telnet or the Content Distribution Manager to access the Content Engine.

- CSCeb08849

Symptom: In ACNS software, Release 5.0.3, when the number of characters for the Group Names parameter exceeds 256, LDAP authentication does not work for those users.

Workaround: Limit the number of characters for the Group Names parameter to be less than 256.
- CSCin14344

Symptom: No CLI command is available in ACNS software, Release 5.0 and later releases to clear WCCP generic routing encapsulation (GRE) packet-related information. Although a CLI command (**show wccp gre**) is available to display the WCCP GRE counters, there is no CLI command currently available to clear them.

Condition: This symptom is observed regardless of whether WCCP is enabled or disabled on the Content Engine.

Workaround: There is no known workaround.
- CSCin19219

Symptom: Any changes in the Content Engine's DNS cache configuration do not take effect immediately.

Condition: This situation occurs when the **dns listen** and **dns pin** commands are used to configure an IP address and port number to listen for requests and map the IP addresses to their corresponding host names.

Workaround: Use the **no dns enable** and **dns enable** commands to disable and enable the Content Engine's DNS caching server, which will result in the DNS caching server picking up the changed configurations.
- CSCin28274

Symptom: Under certain conditions, if the user configures one valid and one invalid FTP server for exporting transaction logs, the **show statistics transaction-logs** command displays the entry for the valid FTP server twice. As a result of the duplicate entry, the counters are not correspondingly incremented with the number of files that are exported through FTP.

Condition: This symptom is observed on Content Engines running ACNS software, Release 5.0.

Workaround: The **clear statistics transaction-logs** command can be used to clear the transaction log export statistics and the duplicate entry for the valid FTP server.
- CSCin30153

Symptom: The client does not receive a requested object if the Websense server is not reachable or if the Websense server timeout value is greater than the configured default timeout value.

Condition: This symptom is observed only under the following conditions:

  - The request from clients is a transparent request.
  - URL filtering through Websense is enabled in the Content Engine.
  - The Websense server is not reachable.
  - The Websense server timeout value is greater than 60 seconds.

Workaround: The Websense server timeout value must be configured to be less than 60 seconds.
- CSCin30480

Symptom: The Content Router returns an error instead of proxying the request from the origin server when a playback request for WMT content on the Content Router fully qualified domain name is redirected to a Content Engine. This happens if you use the Content Router for routing WMT content and the content is not yet replicated to a Content Engine.

Condition: This occurs in ACNS 5.0 software when the following circumstances have occurred:

- The administrator publishes an incorrect URL.
- The administrator publishes a URL without first pre-positioning the content.

Workaround: Publish the Content router fully qualified domain name URL only after content has been fully replicated on the Content Engines.

- CSCin35914

Symptom: The Software Update File Registration window in the Content Distribution Manager GUI displays the following error message for a valid meta file URL:

```
Transaction not completed
sun.net.ftp.FtpProtocolException:port
```

Condition: This occurs when the Content Distribution Manager host name contains numeric values. For example, if the software update file URL is 7305.cisco.com, Linux systems encounter problems when Java attempts to resolve the URL to an IP address. This is because only 7305 is considered instead of 7305.cisco.com. As a result, the URL is resolved to a strange IP address, 0.0.28.137 for 7305, causing the Content Distribution Manager GUI to display an error message even though the meta file URL might be valid. Also, this problem occurs if the update meta file is hosted on an FTP server.

Workaround: Perform one of the following workarounds:

- Make sure that the Content Distribution Manager host name contains at least one nonnumeric value.
- Host the update meta file on an HTTP server and use the HTTP URL instead of an FTP URL for performing software updates.

- CSCin37628

Symptom: A user other than an administrator with privilege level 15 does not possess super user privileges.

Condition: This occurs when a user other than an administrator is configured to be a super user with privilege level 15.

Workaround: Users need to log in as administrators to perform tasks that require super user privileges.

- CSCin39180

Symptom: Authentication of users who want to access the Content Engine fails if more than one TACACS+ server is configured incorrectly.

Condition: This occurs when three TACACS+ servers are configured, with the first and the second servers being unreachable and therefore invalid. The Content Engine fails to authenticate the user using the third TACACS+ server, which is valid.

Workaround: There is no known workaround. Users need to configure the TACACS+ servers properly for authentication of users who access the Content Engine.

- CSCin41994

Symptom: If the **cdnfs browse EXEC** command is used and the filename or the directory name of pre-positioned content contains a space, the command does not display the information contained in the file, nor does it browse through the **cdnfs** files and directories.

Condition: This occurs in Content Engines running ACNS software, Release 5.0.5.

Workaround: There is no known workaround.

- CSCin52843  
Symptom: Unexpected rule patterns are configured if an asterisk (\*) is used as a regular expression pattern in the Rules window in the Content Engine GUI.  
Condition: This problem occurs in all ACNS 5.x releases when the Content Engine GUI is used to configure rule patterns that accept regular expressions.  
Workaround: Use double quotes to configure regular expression patterns in the Content Engine GUI.

## Resolved Caveats - ACNS Software, Release 5.0.5

- CSCdz16529  
ACNS 5.x software uses certain CLI commands that are important for ACNS network functionality and need to be managed using device groups. If any of these commands are configured using the device CLI or GUI, these settings are not stored as part of the ACNS network-wide configuration data of the Content Distribution Manager and are overwritten by the Content Distribution Manager. In addition, if these settings are configured on the Content Engine or Content Router before it is registered with the Content Distribution Manager, they are not displayed in the running configuration.
- CSCea21899  
When the URL for playback of a media file is specified with two question marks and RealProxy is configured on the Content Engine, RealServer is unable to resolve the request for playback.
- CSCea82736  
The Centralized Management System (CMS) on the Content Engine cannot start and the Content Engine is shown as offline or pending in the Content Distribution Manager (CDM) GUI.
- CSCea84338  
Acquisition stops when a manifest file contains URLs in multiple-byte languages, such as Korean.
- CSCea84995  
The SmartFilter application does not perform URL filtering when all of the following conditions are present:
  - The **http avoid-multiple-auth-prompt** global configuration command is used to avoid multiple authentication windows.
  - **No-auth** rules are configured and the **rule** command is enabled.
  - SmartFilter URL filtering is enabled.
  - The authentication scheme enabled is something other than NTLM.
  - Requests are proxy-style (either proxy caching or transparent caching, when requests are intercepted by WCCP routers).
- CSCea93794  
Windows Media Player Version 9 returns an error while trying to retrieve pre-positioned MPEG files from the Content Engine.
- CSCeb08304  
In ACNS software, Releases 5.0.1 and 5.0.3, NTLM authentication stops working after a few hours.

- CSCeb09185  
ACNS software, Release 5.0.3 or earlier running on Content Engine models CE-560, CE-590, or CE-7320 with the Storage Array SA-7 or SA-14 displays the following message on bootup or when **disk** commands are executed:  
`You are using unsupported hardware.`
- CSCeb09940  
On reboot, the Content Engine resets the interface to half duplex from full duplex.
- CSCeb12698  
In ACNS software, Release 5.0.3, the Content Engine becomes unresponsive to all input under heavy HTTP load.
- CSCeb29136  
The video in a video on-demand program streaming over MMSU, when accessed through a Virtual Private Network (VPN) connection, stops playing when you seek a new location in the video. This problem occurs when you play the video-on-demand (VOD) program using Windows Media Player 9.0.
- CSCeb44480  
When you use the `acns5_cdm_ip.meta` file to automatically register to a Content Distribution Manager while upgrading from ACNS software, Release 4.x to 5.0, the upgrade succeeds, but the Content Engine does not register with the Content Distribution Manager.
- CSCeb60677  
The Content Engine loads HTTP pages very slowly for some websites, for example, `http://www.yahoo.com`. This symptom occurs when Internet Explorer accesses any web site that requires a Windows Media Player upgrade.
- CSCin46853  
Functions that use swap space, such as upgrades and rule statistics, fail because of a full RAM disk partition.

**The following caveats have been resolved in ACNS software, Release 5.0.5, build 9:**

- CSCec13338  
The status of the Content Engine appears as Offline in the Content Distribution Manager GUI after the Content Engine has been running for a while. The startup configuration information on the Content Engine might be lost after a reload operation.
- CSCec13816  
The following error message is displayed in the syslog file of a routing Content Engine:  

```
%CE-CMS-4-1: ds_getStruct got error : 1 for key /stat/routing/summary connection 44
%CE-CMS-4-1: ds_getStruct: unable to get `/stat/routing/summary' from dataserver",
java: %CE-CMS-4-1: got error rc trying to retrieve global" routing statistics
```

  
This problem occurs with the Centralized Management System (CMS) while collecting statistics or setting system configuration properties.
- CSCec14884  
Too many connections by the Centralized Management System (CMS) might cause the Content Engine to be reloaded automatically, and the startup configuration on the device might be lost.

# Documentation Updates

This section describes some documentation updates.

## SmartFilter and the No-Auth Rule Interaction

The **no-auth** rule permits specific login and content requests to bypass authentication and authorization features such as LDAP, RADIUS, SSH, or TACACS+. For example, any requests from the source IP address (src-ip) of 172.16.53.88 are not authenticated.

```
ContentEngine(config)# rule enable
ContentEngine(config)# rule action no-auth pattern-list 1 protocol all
ContentEngine(config)# rule pattern-list 1 src-ip 172.16.53.88 255.255.255.255
```

If ACNS software is configured for authentication and SmartFilter URL filtering, requests that are allowed to bypass authentication will also bypass the URL filter.

## Related Documentation

Your product shipped with a minimal set of printed documentation, as well as a Documentation CD. The printed documentation provides enough information for you to install and initially configure your product. The CD contains additional product documentation (user guides, configuration manuals, and so forth), which you can access and print out.

### Product Documentation Set

In addition to these release notes, the product documentation set includes:

- *Documentation Guide*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*

Refer to the *Documentation Guide* for a complete documentation roadmap and URL documentation links for this product.

### Hardware Documentation

- *Cisco Content Engine 7305 and 7325 Hardware Installation Guide*
- *Installing the Cisco Content Engine 7305 and 7325*
- *Installing Field-Replaceable Units in the Cisco Content Engine 7305 and 7325*
- *Cisco Content Engine 7320 Product Description Note*
- *Cisco Content Engine 510 and 565 Hardware Installation Guide*
- *Installing the Cisco Content Engine 510 and 565*
- *Installing Field-Replaceable Units in the Cisco Content Engine 510 and 565*
- *Cisco Storage Array Installation and Configuration Guide*
- *Release Notes for Cisco Content Delivery Manager 4630*
- *Cisco Content Distribution Manager 4650 Product Description Note*
- *Cisco Content Distribution Manger 4630 Hardware Installation Guide*
- *Cisco Content Router 4430 Hardware Installation Guide*

- *Cisco Content Engine 500 Series Hardware Installation Guide*
- *Release Notes for the Cisco Content Engine 500 Series*
- *Cisco Content Networking Hardware Installation Guide for the Seven-Rack Unit Chassis*

#### Software Documentation

- *Cisco ACNS Software Deployment and Configuration Guide, Release 5.0*
- *Cisco ACNS Software Caching Configuration Guide, Release 5.0*
- *Cisco ACNS Software Command Reference, Release 5.0*
- *Cisco ACNS Software Maintenance and Troubleshooting Guide*
- *Cisco ACNS Software Migration Guide, Release 5.0*
- *Cisco ACNS Software API Guide, Release 5.0*
- *SmartFilter for Cisco Content Engine User's Guide, Release 3.1*

#### Online Help

Content Distribution Manager GUI online help system

## Release-Specific Documents

For ACNS software, Release 5.0.5, the document “Creating Manifest Files for Cisco ACNS Software, Release 5.0.5” replaces Chapter 6, “Creating Manifest Files” in the *Cisco ACNS Software Deployment and Configuration Guide, Release 5.0*. You can access the updated manifest file chapter for ACNS software, Release 5.0.5 from the following URL:

[http://www.cisco.com/en/US/products/sw/comntsw/ps491/prod\\_configuration\\_guide09186a008017a530.html](http://www.cisco.com/en/US/products/sw/comntsw/ps491/prod_configuration_guide09186a008017a530.html)

To download the Websense components, such as Explorer, Manager, and Reporter, or to obtain an evaluation key for using with the Websense server that runs on the Content Engine, access the following URL and follow the sequence of steps:

<http://www.websense.com/downloads>

To access the set of documents on Websense product setup and implementation, access the following URL:

<http://www.websense.com/support/documentation/index.cfm>

## Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

## Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

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

## Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

[http://www.cisco.com/en/US/partner/ordering/ordering\\_place\\_order\\_ordering\\_tool\\_launch.html](http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html)

All users can order annual or quarterly subscriptions through the online Subscription Store:

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

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:  
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can send your comments in e-mail to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

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

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

We appreciate your comments.

## Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.

### Cisco TAC Website

The Cisco TAC website (<http://www.cisco.com/tac>) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

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

### Opening a TAC Case

The online TAC Case Open Tool (<http://www.cisco.com/tac/caseopen>) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

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

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

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

## TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## Obtaining Additional Publications and Information

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

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:  
[http://www.cisco.com/en/US/products/products\\_catalog\\_links\\_launch.html](http://www.cisco.com/en/US/products/products_catalog_links_launch.html)
- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:  
<http://www.ciscopress.com>
- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:  
<http://www.cisco.com/go/packet>
- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:  
<http://www.cisco.com/go/iqmagazine>
- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:  
[http://www.cisco.com/en/US/about/ac123/ac147/about\\_cisco\\_the\\_internet\\_protocol\\_journal.html](http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html)
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:  
<http://www.cisco.com/en/US/learning/index.html>

---

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

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered Network* mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

