



Release Notes for Cisco ACNS Software, Release 5.0.7, Build 10

October 13, 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 5.0.7. These release notes describe the following topics:

- [Introduction, page 2](#)
- [New and Changed Information, page 2](#)
- [Hardware Supported, page 4](#)
- [Important Notes, page 6](#)
- [Caveats, page 7](#)
- [Documentation Updates, page 24](#)
- [Related Documentation, page 25](#)
- [Obtaining Documentation, page 26](#)
- [Documentation Feedback, page 27](#)



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

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

- [Obtaining Technical Assistance, page 27](#)
- [Obtaining Additional Publications and Information, page 28](#)

Introduction

These release notes describe supported hardware and open and resolved caveats regarding ACNS software, Release 5.0.7.

New and Changed Information

This section describes existing features that have changed and new features in ACNS software, Release 5.0.7. These features include the following:

- [IP Address Spoofing for Transparent Proxy-style Requests](#)
- [Enabling or Disabling Persistent Connections](#)
- [Global Site Selector \(GSS\) Based Routing](#)

IP Address Spoofing for Transparent Proxy-style Requests

ACNS software, Release 5.0.x does not perform IP address spoofing for transparently intercepted proxy-style requests. In ACNS software, Release 5.0.7, IP address spoofing is performed for transparently intercepted proxy-style requests also when the Content Engine is configured to use the proxy server from the original request to fetch the content.

To configure the Content Engine to use the proxy server from the original request, users can use the **proxy-protocols transparent original-proxy** global configuration command.

About Proxy-style and Server-style HTTP Requests

The client sends a proxy-style HTTP request if the client has been configured to use a proxy server or an automatic proxy configuration file (PAC file) to make client requests to go through a forward proxy server. The client sends the request to the IP address of the proxy server, with the complete destination URL including the name of the origin server in the HTTP method. In the case of a server-style HTTP request, the client sends the request directly to the destination server with the HTTP Host: header containing the domain name of the origin server, and the HTTP method (for example, GET) containing the path to the file or script that the client is requesting.

The proxy-style request for myfile.html located in mydirectory in the domain myserver.com, when transparently intercepted, will have the following initial HTTP line:

```
GET http://myserver.com/mydirectory/myfile.html HTTP/1.1
```

The server-style request for myfile.html located in mydirectory in the domain myserver.com, when transparently intercepted, will have the following initial HTTP line:

```
GET /mydirectory/myfile.html HTTP/1.1
```

Enabling or Disabling Persistent Connections

Content Engines by default use persistent connections to the server for improving performance. Previous releases of ACNS software provided users with limited options to enable or disable persistent connections in Content Engines. These options allowed users to enable or disable persistent connections to all requests, requests for persistent connection to all clients, or requests for persistent connection to all servers. There were no options to disable requests for persistent connections to specific domains, IP addresses, or ports.

ACNS software, Release 5.0.7 introduces the **rule action no-persistent-connection** global configuration command, which allows users to disable or enable persistent connections for specific domains, source and destination IP addresses or ports. This is useful when a server does not support persistent connections.

The **rule action no-persistent-connection** global configuration command has the following options:

- **all**—Do not use persistent connection for all connections
- **client-only**—Do not use persistent connection for client connections alone
- **server-only**—Do not use persistent connection for server connections alone

Users can specify the criteria for disabling persistent connections by creating a pattern list using one or more of the following supported patterns:

src-ip
dst-ip
dst-port
url-regex
domain
header-field user-agent
header-field referer
header-field request-line

The usage of rule command for disabling persistent connections is:

```
rule action no-persistent-connection pattern-list list_num [protocol (http|https|ftp)]
```

The following table describes the syntax for this command.

action	Describes the action that the rule is to take.
no-persistent-connection	Sets persistent connections configuration options.
pattern-list	Configures the pattern list.
<i>list_num</i>	Pattern list number (1-512)
protocol	Protocol for which this rule is to be matched.
http	Matches this rule with the HTTP protocol.
https	Matches this rule with the HTTPS protocol.
ftp	Matches this rule with the MMS protocol.

The following example disables persistent connection for the domain mywebsite.com, based on a pattern (pattern number 10) in the pattern list.

```
ContentEngine(config)# rule action no-persistent-connection server-only pattern-list 10
```

```
WARNING: rule action no-persistent-connection will affect end-to-end NTLM authentication
to these servers
```

```
ContentEngine(config)#
```

```
ContentEngin590#show rule all
```

```
Rules Template Configuration
```

```
-----
```

```
Rule Processing Enabled
```

```
Actions :
```

```
rule action no-persistent-connection server-only pattern-list 100 protocol all
```

```
Pattern-Lists :
```

```
rule pattern-list 100 domain mywebsite.com
```

```
ContentEngine#
```

Global Site Selector (GSS) Based Routing

ACNS software, Release 5.0.7 introduces GSS-based routing as an additional method of content routing. This is in addition to the routing methods using Content Routers and WCCP, and proxy-based routing currently used in ACNS software, and is a pure DNS based routing method.

To use GSS-based routing in ACNS software, users must do the following:

1. Add appropriate rules in GSS to redirect the given routed domain to different Content Engines.
2. While creating or modifying Web Sites in Content Distribution Manager, enter the given routed-domain name in the Requested-routed FQDN field and check the Pure DNS Routing check box. This facilitates pure DNS routing provided by GSS.

Once this is completed, users can publish the URLs using the routed-domain name as the hostname.

Hardware Supported

ACNS software, Release 5.0.7 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.

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 5.0.7. Caveats describe unexpected behavior in ACNS 5.0 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 5.0.7

- 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 sent 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 5.0.7 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 CDN 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 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 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 user name and password even though you have already entered the proper user name 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 needs to be performed.

- 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, has already received the content. The Content Engine contacts the parent and download the content through unicast.

Workaround: You can do one of the following to avoid this problem:

- Configure the channel to mcast-only on channel 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.

- 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 vanishes 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.lck' : 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.
- 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 on 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 Darwin Streaming Server) 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.

- CSCea51815

Symptom: Content Engine model CE-565 shows lower http performance when attached to the Storage Array device SA-7 compared to a CE-565 not attached to SA-7 device.

Condition: This problem occurs when the CE-565 has WMT enabled and attached to the SA-7 device.



Note The storage array device is used for CFS.

Workaround: Use less CFS if a storage array device is attached to the Content Engine.

- CSCea59264

Symptom: When user submits WMT Multicast Stations page in Content Distribution Manager, ACNS software displays an error message.

Condition: This problem occurs when there is a leading space entered in the Address field.

Workaround: Return to the WMT Multicast Stations page and submit after entering the address without a leading space.

- 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.

- 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.

- CSCea88838

Symptom: Content Engine does not accept the DHCP address and CMS is not enabled. This results in Content Distribution Manager indicating the device to be inactive.

Condition: When auto registration is disabled and reenabled on a Content Engine, the DHCP offer is not accepted because the Content Distribution Manager hostname cannot be resolved. This occurs if there is no interface that does not have an IP address through which the Content Distribution Manager hostname can be resolved.

Workaround: Do not disable and reenable auto registration. If you re-enable auto registration, reboot the device to accept DHCP offer, and to restart CMS to register the device with the Content Distribution Manager.

- 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.

- CSCea90203

Symptom: Socket write error occurs when a port channel on a non-existent port channel is disabled using the **no interface portChannel** global configuration command.

Condition: This error occurs on the Content Engine models CE-7325, CE-7305, CE-7320, and CE-510, since there is no port channel configuration on these Content Engines.

Workaround: Do not use the **no interface portChannel** global configuration command for non-existent port channels.

- 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 5.0.7 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 5.0.7 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: An 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 has a lot of loss, the multicast sender may send a few bytes less than the actual file size. This causes the 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 pgm congestion control, turn up the proactive FEC, and on CDM GUI, set FEC to 16.
- CSCeb34946

Symptom: 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.
- CSCeb35954

Symptom: The **show websense-server** EXEC command shows the licensed users as zero.

Condition: Websense Manager contacts the Websense server when the user enters the license key and expiry date, and tries to download the Websense database from the Websense website. If the Content Engine running Websense server fails to download the Websense database because of network filtering errors, the **show websense-server** EXEC command shows the licensed users as zero.

Workaround: Configure a Content Engine which can download the Websense database as proxy in the Websense Manager.
- CSCeb37567

Symptom: Unicast distribution is temporarily interrupted.

Condition: This occurs when there is no multicast sender configured at the beginning of distribution.

Workaround: There is no known workaround.
- CSCeb48853

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

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

Workaround: Configure a default gateway in the ACNS GUI.

- CSCeb49014

Symptom: All contents are deleted when a new root Content Engine is selected or the old root Content Engine goes offline and a temporary root Content Engine is elected, and if the channel is using crawl job to acquire contents.

Condition: This problem occurs in ACNS software, Release 5.0.3.

Workaround: Pressing the **Refetch** button in the Channels page in the Content Distribution Manager GUI causes the new root Content Engine to acquire and distribute the content again.

Workaround: Enable the command in the GUI.

- CSCeb56333

Symptoms: An SNMP query to ccmHistoryEventTable on a Cisco Content Engine returns Management Information Base (MIB) instances with fixed index. According to CISCO-CONTENT-ENGINE-MIB definition, each new event stored in this table should be assigned a progressive unique index.

Condition: This problem occurs on Cisco Content Engines running ACNS release 5.0.3 or below.

Workaround: There is no known workaround.

- CSCeb77349

Symptom: When configuring a Content Engine for RADIUS authorization, the Content Engine sends two distinct Access-Requests to the AAA server.



Note The second Access-Request is identical to the first, except for the RADIUS ID. This causes problems with One-Time-Password (OTP) servers, which do not accept the second request (carrying an identical password as the first one), and send back an Access-Reject, causing the Content Engine to deny access to the user.

Condition: The problem is observed when users try to log on to the Content Engine using Telnet.

Workaround: There is no known workaround.

- CSCeb83282

Symptom: When IP address changes are made on the Content Engine with WCCP enabled, existing connections break, and for 30 seconds new connections are not accepted.

Condition: This problem occurs when users change IP addresses on the Content Engine with WCCP enabled.

Workaround: Disable WCCP before changing IP addresses on the Content Engine.

- CSCeb85057

Symptom: Content Engine displays the following error message:

```
KERNEL: assertion (atomic_read(&sk->wmem_alloc) == 0) failed
```

Condition: Content Engines display this error message during normal operation.

Workaround: Ignore the error message.

- CSCec21671

Symptom: The Content Engine GUI loads slowly and some images on the GUI does not load.

Condition: This problem occurs when TACACS is enabled as primary authentication for login and configuration access to the Content Engine.

Workaround: Use local user ID with local authentication as primary authentication.

- CSCec31432

Symptom: Transaction log shows cache miss for range requests to pre-positioned content.

Condition: This problem occurs when request for pre-positioned content contains HTTP range headers.

Workaround: There is no known workaround.
- CSCec36290

Symptom: Using Windows XP with Windows Media Player 9.0.0.3008 installed, embedded Microsoft media files (for example .asf files) cannot be retrieved over HTTP from a Content Engine that has the media files prepositioned.

Condition: When the Content Engine has the media file prepositioned, and is not configured for either WMT or proxy, media files must be retrieved over HTTP from prepositioned store on the Content Engine.

Workaround: Users can do the following to avoid this problem:

 - Use a Windows 2000 device or a different version of Windows Media Player
 - Enable WMT on the Content Engine
- 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.

- 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 CDM 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.

- 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 5.0.7.

Workaround: Currently, there is no known workaround.

- CSCin42531

Symptom: In the Bandwidth Setting for the Device Groups window, when the user tries to navigate to any page (when there are more than 10 bandwidth records) using the pagination counter at the bottom of the page, an error message is displayed.

Workaround: Select All or a number higher than the default value (10) in the Rows field to display the record you want to edit in the first page.

- CSCin55484

Symptom: A prepositioned content object is lost after performing disk configuration and reloading the Content Engine.

Condition: If the amount of CDNFS content present is close to the amount of disk space allocated to CDNFS, then CDNFS content is removed to ensure that CDNFS filesystem can be resized properly to hold the saved content. In ACNS software, Release 5.0.x, the content is moved out of the filesystem (if other filesystems that can hold the content are detected), or deleted (if other filesystems that can hold the content are not detected) on performing a disk configuration, if 90% or more of the CDNFS filesystem is used.

Workaround: Users can do one of the following to avoid this problem:

- Do not perform disk configuration.
- Ensure that the amount of content present is less than 90% of the disk space allocated to the newly specified CDNFS filesystem.
- Upgrade to ACNS 5.1, which always preserves content when you perform a disk configuration, disregarding the amount of disk space specified for CDNFS.

Resolved Caveats - ACNS Software, Release 5.0.7

- CSCea82736

The Centralized Management System (CMS) on the Content Engine does not start and the Content Engine appears offline or pending in the Content Distribution Manager GUI.

- CSCea88615

Content Engine plays back at a bandwidth higher than the upper bandwidth limit set for RealProxy sprayer if the second stream is started concurrently with the first stream, or if the second stream is started with the first stream playing at a lower bandwidth because of buffering frames

- CSCeb09850

In Content Engine models CE-510, CE-565, CE-7305, and CE-7325, the **show interface** command shows the mode as autoselect even when the interface settings such as speed and duplex mode are configured with some values.

- CSCeb27589

The **show cdp neighbors** command in Content Engine does not display any output, and generate core files when there is a Cisco device with empty spaces in the product name is in layer 2 vicinity of the Content Engine.

- CSCeb36762

When user accesses the interactive session of **cdnfs browse** CLI command, and then terminates the terminal (Telnet or SSH session) without exiting the **cdnfs-browse** shell, the CPU utilization of the Content Engine goes up to very high levels. Several features of the Content Engine may not work at their full performance potential because of low CPU availability.

- CSCeb37945

Content Engine proxy authentication fails when Content Engine is used as an outgoing proxy for ISA server and has proxy authentication enabled.

- CSCeb43206

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

- CSCeb43323

When a Content Engine running ACNS software is used as an FTP proxy, the MIME type of objects delivered with extension .jpg are reported as image/jpeg instead of image/jpg and default type is application/octet-stream instead of application/octet-stream.

- CSCeb43328

Content Engines running ACNS software when configured as FTP proxy on receiving HEAD request issues STOR command for the object and hence the object in the FTP server is truncated to 0 bytes.

- CSCeb46128
SmartFilter does not filter http requests with Range headers.
- CSCeb46306
ACNS GUI reports error when you enter "\" as separator for remote FTP directory name in transaction logging GUI page.
- CSCeb49962
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.
- CSCeb53236
Content Engines running transparent caching using WCCP and with NTLM authentication on does not strip NTLM authentication headers when sending request to origin server.
- CSCeb53685
Content Distribution Manager log files for Content Engines and Content Routers show the following error:

`Unexpected critical error on the node, %CE-CLI-2-170016: /ruby/bin/get_config: failed to pick up startup-configuration: /diamond/bin/config -f /tmp/startup.conf ig = (1,11)`
,
- CSCeb60085
In Content Distribution Manager, if hostname is used in **cdm ip** global configuration command to configure the device, the hostname disappears after users reboot the device. The **show running configuration EXEC** command output does not show the hostname after users reboot the device.

If the host name entry is configured for **cdm ip** global configuration command in the Content Engine cannot be resolved, this configuration is lost after reload.
- CSCeb70636
In WCCP mode, FTP proxy request fails if the outgoing proxy of the Content Engine is an ISA proxy and has NTLM authentication enabled.
- CSCeb73697
The Maximum TCP window size of 128KB supported by ACNS software severely limits the FTP transfer capabilities of servers that normally run much larger window sizes.
- CSCeb76891
Content Engine is unable to authenticate users using LDAP. after authenticating a few hundred thousand requests.
- CSCeb80646
Administrator cannot access the Content Engine using ACNS Content Engine GUI if fail-over feature is configured and primary authentication scheme is down.
- CSCeb82728
DNS lookup fails sometimes without any reason, and configured domain names disappear.

- CSCeb83185
When using DHCP to configure the network settings on a Content Engine, domain names do not get configured on the system, if the Content Engine receives more than one domain name in the DHCP server response.
- CSCeb85062
Some specialized clients cannot access some web sites, when server side persistent connection breaks.
- CSCec04207
Websense on-box server is not installed, and /sw/websense directory is missing, after ACNS software, Release 4.x is upgraded to ACNS software, Release 5.0.3, and Websense CLIs fail.
- CSCec09350
Content engine fails to act as proxy to serve WMT type content (files with extensions .wma, .wmv, .asf, and .asx.)
- CSCec13338
Content Engine is shown offline on Content Distribution Manager after running for some time. Sometimes Content Engine also loses start up and running configurations.
- CSCec14884
CMS uses too many data server connections and causes the data server to stop.
- CSCec19689
Content Distribution Manager GUI does not recognize large CDNFS partitions on a Fibre Channel storage array.
- CSCec22074
RealSystem Server 7, 8, RealServer G2, and Helix server 9.x are vulnerable to a root exploit when certain types of character strings appear in large numbers in URLs intended for the server's protocol parsers.
- CSCec28564
In ACNS software, Release 5.0.x, **copy running-config startup-config** command and **write memory** command fail in diskless mode.
- CSCec32387
A network device running SSH server based on the OpenSSH implementation may be vulnerable to a Denial of Service (DoS) attack when an exploit script is repeatedly run against the same device.
- CSCec41202
The OpenSSH team has announced a bug which affects the OpenSSH buffer handling code. This bug has the potential of being remotely exploitable.
- CSCec41413
A network device running SSL server based on the OpenSSL implementation may be vulnerable to a Denial of Service (DoS) attack when a client presents a malformed certificate. The network device is exposed to this vulnerability even if it is configured not to authenticate certificates from the client.
- CSCec49804
The % (percentage) sign is missing in syslog messages generated by kernel while adding meta data. When these messages are forwarded for central storage to CiscoWorks 2000, the syslog daemon in CiscoWorks 2000 rejects the messages, as they do not conform to expected syntax.

- CSCin30480
When content routing (CR FQDN) is used for fetching WMT content and if the content is not yet replicated to the Content Engine for which the request is redirected to, the Content Engine returns an error instead of proxying the request to the origin server.
- CSCin37628
Any user except admin with privilege level 15 cannot perform super-user tasks.
- CSCin52300
When the Content Engine receives a request for a cached object with range headers and if SmartFilter is enabled and configured to allow that request, cache process in the Content Engine stops.
- CSCin52441
Cache process restarts if rule hit is seen for set-dscp action for client cache-hit case with mime-type as pattern.
- CSCin52843
Unexpected rule patterns are configured if asterisk (*) is used as regular expression pattern in the Rules window on Content Engine GUI.
- CSCin53335
Content Engine stops responding and reboots automatically when proxy is restarted.
- CSCin54497
cms_ce process restarts frequently after the network configuration parameters such as name server, and domain name are changed for the Content Engine using the Content Distribution Manager GUI.

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
- Cisco Content Delivery Networking Products Getting Started Guide

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 Manager 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*
- *Release Notes for Cisco ACNS Software, Release 5.0*
- *SmartFilter for Cisco Content Engine User's Guide, Release 3.1*

- Creating Manifest Files for Cisco ACNS Software, Release 5.0.3
- Release Notes for Cisco ACNS Software, Release 5.0.3
- Release Notes for Cisco ACNS Software, Release 5.0.5

Online Help

Content Distribution Manager GUI online help system.

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

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

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

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

Click Subscriptions & Promotional Materials in the left navigation bar.

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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 e-mail comments about technical documentation to 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-a-day, 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. If you do not hold a valid Cisco service contract, please contact your reseller.

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

Using the online TAC Case Open Tool (<http://www.cisco.com/tac/caseopen>) is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which 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 the recommended resources, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (P1 and P2 cases are those in which 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

- Cisco Press publishes a wide range of general networking, training and certification titles. Both new and experienced user will benefit from these publications. 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/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

- 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.

 Printed in the USA on recycled paper containing 10% postconsumer waste.

