



# Release Notes for Cisco ACNS Software, Release 4.2.5

---

January 21, 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 4.2.5. These release notes describe the following topics:

- [Introduction, page 2](#)
- [Additional Hardware Supported, page 2](#)
- [Caveats, page 2](#)
- [Documentation Updates, page 9](#)
- [Related Documentation, page 9](#)
- [Obtaining Documentation, page 10](#)
- [Obtaining Technical Assistance, page 11](#)
- [Obtaining Additional Publications and Information, page 13](#)



---

**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 the open and resolved caveats regarding ACNS software, Release 4.2.5.

## Additional Hardware Supported

ACNS software, Release 4.2.5 supports the Content Engine Network Module for the 2600, 3600, and 3700 series branch office routers. The following table lists the supported branch office router part numbers and descriptions.

Part Number	Description
NM-CE-BP-20G	Content Engine NM-Basic Perf-20 GB
NM-CE-BP-40G	Content Engine NM-Basic Perf-40 GB
NM-CE-BP-SCSI	Content Engine NM-Basic Perf-SCSI adapter
EM-CE-20G=	Expansion Module, 20-GB IDE, field upgrade
EM-CE-40G=	Expansion Module, 40-GB IDE, field upgrade
EM-CE-SCSI=	Expansion Module, SCSI controller, field upgrade
MEM-CE-256U512D	512-MB DRAM factory upgrade for NM-CE-BP
MEM-CE-256D=	256-MB DRAM field upgrade
MEM-256CF-4.2.K9=	256-MB Compact Flash with ACNS software, 4.2 recovery image, 3 DES (Data Encryption Standard)

## Caveats

This section lists and describes caveats that are still open in the ACNS software, Release 4.2.5, and caveats that were resolved in this release. Caveats describe unexpected behavior in ACNS software, Release 4.2.5. Severity 1 caveats are the most serious; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats.

### Open Caveats - ACNS Software Release 4.2.5

- CSCdt62678

**Symptom:** The software upgrade fails if the user clicks the Upgrade button before the upgrade files are replicated to the Content Engines.

**Condition:** The user has imported the software upgrade files to the MANUAL\_UPGRADE channel and then clicks the Upgrade button at the top of the Software Upgrade page before the upgrade files are fully replicated.

**Workaround:** The user needs to follow these steps for a successful software upgrade:

1. Create a MANUAL\_UPGRADE channel and subscribe all appropriate Content Engines to it.
2. Import the upgrade files to the MANUAL\_UPGRADE channel. Go to the Import Progress page and wait for the import to be 100 percent completed.

3. Wait 20 minutes.

4. Click the Channel Console button and wait for the replication status of the MANUAL\_UPGRADE channel to be 100 percent completed.
  5. Go to the Software Upgrade page, choose the appropriate Content Engines, and then click the Upgrade button.
  6. Wait 20 minutes for the upgrade to be completed and then go to the Software Upgrade page to verify the software version number for each selected device.
- CSCdw84848  
Symptom: The contents of a file whose name exceeds 215 characters cannot be imported.  
Condition: This occurs on a Content Distribution Manager 4630 or 4650 running ACNS software, Release 4.2.  
Workaround: Rename filenames so that they are shorter than 215 characters.
  - CSCdy02581  
Symptom: WCCP bypass does not function properly while bypassing packets of large size 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: There is no known workaround.
  - CSCdy03638  
Symptom: A banner message cannot be set in Content Engines running ACNS software, Release 4.x.  
Workaround: There is no known workaround.
  - CSCdy16548  
Symptom: When you use ACNS software to verify Windows NT LAN Manager (NTLM)-supplied passwords on a Windows server, if the password is longer than 14 characters, the authentication fails.  
Condition: When you enter a password that is longer than 14 characters on a Windows 2000 or Windows XP system, authentication fails.  
Workaround: Do not use an NTLM user password that is longer than 14 characters.
  - CSCdy68833  
Symptom: Core dump is seen under /local1/core\_dir for Real-Time Streaming Protocol (RSTP) and video server.  
Condition: This core is generated by video server when the E-CDN software is enabled in a CE-507.  
Workaround: There is no known workaround.
  - CSCdy74268  
Symptom: The CE-5xxAV stops playing, and TV output cannot be controlled.  
Condition: This symptom occurs after the user clicks the Next button on the Content Engine home page several times in a short period (about 2 seconds).  
Workaround: There is no known workaround.

- CSCdy76795

Symptom: The CE-5xxAV runs 9 hours ahead of Japan Standard Time (JST) in the playlist review when the time zone is set to JST (Asia/Tokyo, GMT + 9 hours). In other words, the time is an additional 9 hours ahead of GMT.

Condition: This symptom appears when you change time zones for the Content Engine.

Workaround: There is no known workaround.
- CSCdy80020

Symptom: Occasionally, when a CE-507 is being upgraded from E-CDN software, Release 3.0.3 to ACNS software, Release 4.2.1, it requires the rescue image after an upgrade is attempted.

Workaround: Click the Update Storage Capacity button on the Content Engine System page in the Content Distribution Manager GUI to be sure that you have at least 1.2 GB of space not assigned to channels. You can also reboot the Content Engine from the Content Engine System page in the Content Distribution Manager GUI and wait 15 minutes. This ensures that the Content Engine is stable and ready for upgrade.
- CSCdy84704

Symptom: After the time zone is changed to another region, the system time (which is shown in the Identification window on the Content Distribution Manager GUI) does not change.

Workaround: There is no known workaround.
- CSCdz01265

Symptom: The Content Engine is not deleting orphaned contents if a subscribed channel is removed when that Content Engine is shut down.

Condition: This occurs in ACNS software, Release 4.2.1.

Workaround: There is no known workaround.
- CSCdz03816

Symptom: The WMT statistics display conflicting information in certain situations. In this case, the **show statistics wmt streamstat** command displays connections that are unaccounted for. This symptom might be observed when the Content Engine is fully loaded and the WMT traffic is high.

Condition: The generic cause of this problem has not been determined so far, although it is closely associated with the internal structure-wise synchronization between unicast and multicast sessions.

Workaround: The user needs to use the **clear statistics wmt** command to clear the conflicting results. This ensures that the number of connections is displayed correctly once again.
- CSCdz10104

Symptom: Importing a large number of files using FTP is not successful if the filenames do not have extensions. The import process proceeds normally until a few hundred files have been successfully imported. However, the import process stops after that.

Condition: This problem is observed when the content items or files do not have filename extensions (for example, specifying the filename as “123” instead of “123.gif”).

Workaround: There is no reliable workaround, although restarting the E-CDN application will restart the import process, but some files might be lost during the process.

- CSCdz56234  
Symptom: The **ip domain-name** CLI command cannot be used to specify more than one domain.  
Condition: This symptom is observed in a Content Engine using the E-CDN application in which the IP domain name configuration is overwritten with that specified in the E-CDN configuration.  
Workaround: If the user needs multiple domain names to be set on the Content Engine, all related DNS settings must be made from the individual Content Engine and not from the Content Distribution Manager GUI.
- CSCsp01389  
Symptom: The default start and stop times are those of the user's system device and not of the TV-out device. This is observed when the TV-out device is in a different time zone with a different date, month, or year.  
Condition: This occurs in E-CDN software, Release 2.1 or later (including ACNS software, Release 4.x).  
Workaround: There is no known workaround.

## Resolved Caveats - Release 4.2.5

- CSCdv03845  
When **rule** commands are specified from the command line interface (CLI), rules follow case-sensitive comparison with the namespaces that have been previously created. This method of case-sensitive comparison allows multiple entries with the same value, but different cases.
- CSCdw04645  
When a request is sent with nonmatching headers and the requested object is not in the cache, the server reply is not cached.
- CSCdx04177  
You cannot use SAMI (Synchronized Accessible Media Interchange) files with Windows Media Technologies (WMT) playing from the Content Distribution Manager or Content Engine.
- CSCdx12654  
The message that appears when the user configures Web Cache Communication Protocol (WCCP) for the media cache needs to be modified and made consistent with the message displayed for the WCCP WMT configuration.
- CSCdx53108  
An inconsistent time stamp is recorded in the syslog. The syslog.txt file displays some messages in local time and other messages in Universal Coordinated Time (UTC) or Greenwich Mean Time (GMT).
- CSCdy29190  
The Microsoft Media Server UDP (MMSU) service is not started or stopped when WCCP or WMT caching is enabled or disabled through the graphical user interface (GUI). However, the MMSU is updated when WCCP or WMT caching is enabled through the CLI.
- CSCdy35907  
The reply code field in the HTTP transaction log does not accurately reflect the actual error condition. For many of the error conditions, the reply code field in the HTTP transaction log is not mapped to the corresponding error message.

- CSCdy57463  
Entries cannot be deleted from the Media Editors Media Properties page in the Content Distribution Manager GUI.
- CSCdy80099  
Users cannot see the free space “not assigned to channel” section on the Content Engine System page.
- CSCdz00639  
Content Engines in transparent (WCCP) mode will append :80 to URLs while sending requests to an upstream proxy. If the upstream proxy is configured to do URL filtering, filtering might not work as expected. Some URL filtering devices might not function as expected when port numbers are added to the URLs.
- CSCdz00782  
TCP connections for HTTP traffic are broken if the Generic Routing Encapsulation (GRE) packets are fragmented when IP spoofing is used. The bypass entries appear in the output of the **show bypass list** command.
- CSCdz01735  
A live broadcast is interrupted on a WAN with network congestion when the Content Engine sends a broadcast or multicast to other Content Engines to play WMT files and uses a WMT encoder situated far away from the broadcast Content Engine.
- CSCdz04071  
The expiration date available under the Media Editor cannot be removed once it has been set in ACNS software, Release 4.2.1. The date value can be modified, but it cannot be removed. The Media Editor page continues to display the expiration date.
- CSCdz06906  
The **show wmt proxy** command does not show the Microsoft Media Server (MMS) outgoing proxy configuration even if it is configured, although the **show running-config** command displays the outgoing proxy configuration.
- CSCdz10973  
The **show wmt** CLI command does not show the WMT cache unique-stream-key configuration.
- CSCdz11148  
The cache GUI does not display active or live streams, although the CLI displays them. This is observed after the WMT streams have been active and running for 2 hours.
- CSCdz13833  
The WMT outgoing proxy server does not function when the DNS lookup fails.
- CSCdz26582  
When the Content Engine is enabled in proxy mode with a third-party plug-in (such as SmartFilter) and the response from the original server does not include an HTTP header, then the Content Engine is unable to send the requested page to the client.
- CSCdz32826  
The SNMP agent code does not handle an unsupported storage array (HP), causing the SNMP GET routine to read incorrect information. Therefore, the information is unable to reach the SCSI adapter card.

- CSCdz34244  
When a hierarchical WMT stream that splits Content Engine deployment is used, it is noticed that the maximum value in current usage displayed with the **show statistics wmt multicast** command displays a large value in gigabits. This causes WMT to stop working, forcing a reboot of the cache.
- CSCdz34954  
This problem is observed in a live broadcast infrastructure with 1 encoder, 1 head Content Engine as a live split broadcaster, and 22 downstream Content Engines. After a couple of hours of live broadcasting, all the downstream Content Engines become disconnected, and the connection between the head Content Engine and the encoder is also cut off, causing the live streaming to fail.
- CSCdz34971  
The WMT multicast station cannot be stopped in certain cases. The station is found to be present even after the **wmt multicast-station stop name** command is issued.
- CSCdz36916  
A video on demand (VOD) freezes and buffers every 4 to 5 seconds. In other words, the VOD stops playing after 5 minutes when WMT caching is enabled.
- CSCdz37891  
The Microsoft SharePoint application fails to run on a Content Engine running ACNS software, Release 4.2.3.
- CSCdz38595  
A core file is generated because of the crash of the MMS server. The core file occurs when the bandwidth drops to a very low bit rate or when the encoder stops.
- CSCdz39476  
The Content Engine is configured for client spoofing and Layer 2 (L2) redirect. When the client makes a request for the proxy.pac file, the Content Engine immediately replies with an HTTP REFRESH response and creates a bypass. If client spoofing is disabled on the Content Engine, bypass will not occur.
- CSCdz40786  
With the WMT outgoing proxy configured, a downstream Content Engine does not send a proxy-style request to the upstream proxy server.
- CSCdz46196  
With authentication bypass enabled on a Content Engine in transparent mode and both the **ip cef** and **ip route-cache** commands disabled on a Cisco 7200 router, it is found that authentication bypass fails.
- CSCdz47536  
The WMT HTTP code is unable to handle an outgoing proxy server's 407 responses. This is observed when a Content Engine is configured as an outgoing proxy with WMT disabled and authentication enabled.
- CSCdz48692  
The tools that are used to report the HTTP transaction log are unable to process the Content Engine HTTP transaction log when the Content Engine is configured for the Apache transaction log format using the **transaction-logs format apache** command. This is because the date and time field in the Content Engine HTTP transaction log does not conform to the standard Apache Common Log Format.

- CSCdz49175  
The date and time stamp in the HTTP transaction log is incorrect occasionally for a few entries. This condition is more likely to occur on Content Engine models with multiple processors, such as the CE-7320.
- CSCin22279  
The configuration of HTTP headers appended by the Content Engine is shown when either of two commands, namely, the **show http all** CLI command or the **show http append** CLI command, is used but not with both the commands.

## 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 500 Series Hardware Installation Guide*
- *Cisco Content Distribution Manager 4630 Hardware Installation Guide*
- *Cisco Content Router 4430 Hardware Installation Guide*
- *Cisco Content Networking Hardware Installation Guide for the Seven-Rack Unit Chassis*

### Software Documentation

- *Cisco ACNS Software Caching Configuration Guide, Release 4.2*
- *Cisco ACNS Software Command Reference, Release 4.2*
- *Cisco ACNS Software E-CDN Administrator's Guide, Release 4.2*
- *Cisco ACNS Software Maintenance and Troubleshooting Guide*
- *Release Notes for Cisco ACNS Software, Release 4.2*
- *SmartFilter for Cisco Content Engine User's Guide, Release 3.0.2*

## 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 web sites 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 monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Registered Cisco.com users can order the Documentation CD-ROM (product number DOC-CONDOCCD=) 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>

- Registered Cisco.com users can order the Documentation CD-ROM (Customer Order Number DOC-CONDOCCD=) through the online Subscription Store:  
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) 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 e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit your comments by mail by using the response card 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

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) Website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

## Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

<http://www.cisco.com>

## Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The avenue of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

### Cisco TAC Website

You can use the Cisco TAC website to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC website, go to this URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

<http://www.cisco.com/en/US/support/index.html>

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC website so that you can describe the situation in your own words and attach any necessary files.

### Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

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

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

# 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 monthly periodical that provides industry professionals with the latest information about the field of networking. You can access *Packet* magazine at this URL:  
[http://www.cisco.com/en/US/about/ac123/ac114/about\\_cisco\\_packet\\_magazine.html](http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_packet_magazine.html)
- *iQ Magazine* is the Cisco monthly periodical that provides business leaders and decision makers with the latest information about the networking industry. You can access *iQ Magazine* at this URL:  
[http://business.cisco.com/prod/tree.taf%3fasset\\_id=44699&public\\_view=true&kbns=1.html](http://business.cisco.com/prod/tree.taf%3fasset_id=44699&public_view=true&kbns=1.html)
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in the design, development, and operation of 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, with current offerings in network training listed at this URL:  
[http://www.cisco.com/en/US/learning/le31/learning\\_recommended\\_training\\_list.html](http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html)

---

This document is to be used in conjunction with the documents listed in the “Related Documentation” section.



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

