



# Release Notes for Cisco ACNS Software, Release 4.2.3

---

January 6, 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 4.2.3. These release notes describe the following topics:

- [Introduction, page 2](#)
- [New and Changed Information, page 2](#)
- [Additional Hardware Supported, page 2](#)
- [Caveats, page 3](#)
- [Documentation Updates, page 6](#)
- [Related Documentation, page 7](#)
- [Obtaining Documentation, page 8](#)
- [Obtaining Technical Assistance, page 9](#)
- [Obtaining Additional Publications and Information, page 10](#)



---

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

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

# Introduction

These release notes describe new features, supported hardware and open and resolved caveats regarding ACNS software, Release 4.2.3.

## New and Changed Information

This section describes existing features that have changed and new features in ACNS software, Release 4.2.3. The enabling HTTP TCP keepalive feature is new.

### Enabling HTTP TCP Keepalive

Content Engines by default do not send TCP keepalive messages to the clients or server when the connection is idle (that is, when no data is transmitted between the Content Engine and its clients or the server). In ACNS software, Release 4.2.3, you can force the Content Engine to send keepalive probes using the **http tcp-keepalive** global configuration command. HTTP TCP keepalives are disabled by default. The **http tcp-keepalive enable** global configuration command enables this feature. Use the **no** version of this command, **no http tcp-keepalive**, to disable this feature.

When HTTP TCP keepalive feature is enabled, the Content Engine sends TCP-keepalives on idle TCP connections using the keepalive configuration parameters (such as TCP keepalive timeout, TCP keepalive probe count, and TCP keepalive probe interval).



#### Note

You must set the TCP keepalive parameters using the **tcp** global configuration command and the **keepalive-probe-cnt**, **keepalive-probe-interval**, and **keepalive-timeout** keywords.

When the HTTP TCP keepalive feature is enabled, the output of the **show running-config** command shows this. When this feature is disabled, the command output does not show anything for **http tcp-keepalive**.

You can run the **show http tcp-keepalive** command to determine the status of the HTTP TCP keepalive feature (whether enabled or disabled).

## Additional Hardware Supported

ACNS software, Release 4.2.3 now 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

Part Number	Description
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 were resolved in ACNS software, Release 4.2.3, and caveats that are still open in this release.

Caveats describe unexpected behavior in ACNS software, Release 4.2.3. Severity 1 caveats are the most serious; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats.

### Resolved Caveats - Release 4.2.3

- CSCdw68467  
When the **copy startup-config running-config** command is used, the shell prompt is not returned.
- CSCdw82157  
The **disk configure** command does not use the remaining (unused) space on disk00 for mediaafs storage.
- CSCdx04092  
The embedded Windows Media Player in an HTML page fails to display the ASF file, if you use an ASX file containing the WMT Play URL from the CDM Previewer page to invoke an imported ASF file.
- CSCdx28999  
“Permission denied” messages are received when you import a folder using FTP drag and drop with Netscape 4.7. Subsequent attempts to import files using FTP drag and drop fail, and “unable to find the file or directory” messages are displayed.
- CSCdx93083  
RADIUS authentication fails when the primary RADIUS server is not responding or is slow to respond even though the secondary RADIUS server is available.
- CSCin06235  
The SNMP client cannot authenticate itself using Secure Hash Algorithm (SHA)-based authentication.

### Open Caveats - ACNS Software Release 4.2.3

- 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 channels and then clicks the Upgrade button at the top of the Software Upgrade page.

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

Create a MANUAL\_UPGRADE channel and subscribe all appropriate Content Engines to it

1. Import the upgrade files to the MANUAL\_UPGRADE channel.
2. 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 and 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.

- CSCdv66971

Symptom: The system can pause indefinitely when the user downgrades from ACNS software, Release 4.x to E-CDN Release 3.x.

Condition: This problem occurs when the Content Engine, Content Router, or Content Distribution Manager console port is connected to a console server (for example, Cisco 2500 series) and if there is no active Telnet session on the console server port to which the Content Engine, Content Router, or Content Distribution Manager is connected.

The problem occurs in this situation because the console server, with no active session on the port in question, sends serial line flow control commands to the Content Engine, Content Router, or Content Distribution Manager to have it stop sending characters. This blocks the downgrade from continuing.

Workaround: Use one of the following workarounds:

- Start a Telnet session on console server during the upgrade and downgrade process so that the console output from the Content Engine, Content Router, or Content Distribution Manager can be displayed to the Telnet session.
- Remove the console cable from the device.
- Connect the serial cable to a PC running communications software.

- 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.

- CSCdx04177

Symptom: You cannot use sami (Synchronized Accessible Media Interchange) files with Windows Media Technologies (WMT) playing from the Content Distribution Manager or Content Engine.

Workaround: There is no known workaround.

- CSCdx18600

Symptom: The output from the **show clock** CLI command may not display the correct time zone name.

Conditions: This symptom occurs when the **show clock** CLI command is used on systems running ACNS software.

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 length is longer than 14 characters, the authentication fails.

Condition: When you use 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.

- CSCdy48345

Symptom: An intermittent popup may appear on the Internet Explorer (IE) browser when NTLM request authentication is enabled on a Content Engine.

Condition: This problem has occurred when the authentication cache timeout value is set to a very small value (for example, 3 minutes) and the authentication cache entry times out frequently. The root cause for this is still under investigation.

Workaround: If popups appear for some specific sites, the **rule no-auth** command can be configured to help alleviate the problem.

For example, for the site <http://windowsupdate.microsoft.com>, the **no-auth rule** command be configured as:

**rule no-auth url-regex http://windowsupdate\.microsoft\.com\***

- CSCdy57463

Symptom: Entries cannot be deleted from the Media Editors Media Properties page in the Content Distribution Manager GUI.

Workaround: Remove the URL and then enter spaces in the text box and click the Save button. This permanently removes the URL.

- CSCdy74268

Symptom: The CE-5xxAV stops playing after the user clicks the Next button on the Content Engine home page several times in a short period (about 2 seconds.) If the Content Engine stops playing, TV output cannot be controlled.

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 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.

- CSCdy80099

Symptom: Users cannot see the free space “not assigned to channel” section on the Content Engine System page.

Workaround: Click the Update Storage Capacity button on the Content Engine System page. If the Content Engine (single disk) is Version 2.1, then the free space must be at least 7 GB. If the Content Engine is Version 3.x, then add an additional 1.2 GB.

- CSCdy80647

Symptom: It is possible to start the upgrade from ACNS software, Release 4.1.1 to Release 4.2.1 before the release is completely replicated. This causes the Content Engine appear to be upgraded as listed in the Content Distribution Manager GUI. However, the CLI **show version** command reports the upgrade as Version 4.1.1.

Workarounds: Allow ample time for the release to replicate to the Content Engine. A CLI upgrade may be necessary.

- CSCdy84704

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

Workaround: There is no known workaround.

- CSCdz00782

Symptom: TCP connections for HTTP traffic appear to be broken.

Conditions: This occurs when IP spoofing is being used and bypass entries show up in the output of the CLI **show bypass list** command.

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.

Conditions: This occurs in ACNS software, Release 4.2.1.

Workarounds: There is no known workaround.

- CSCin10011

Symptom: If a user is in more than one group (with the same user ID) and if one of the groups has been configured in an access list, then the user will always be denied access even if the group is allowed.

Workaround: You need to set the access list to “permit any.”

## 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.

