



# Release Notes for Cisco ACNS Software, Release 4.2.13

---

January 14, 2004

ACNS 4.2.13b1



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 4.2.13. These release notes describe the following topics:

- [Contents, page 1](#)
- [Introduction, page 2](#)
- [Additional Hardware Supported, page 2](#)
- [Caveats, page 2](#)
- [Documentation Updates, page 7](#)
- [Related Documentation, page 7](#)
- [Obtaining Documentation, page 8](#)
- [Documentation Feedback, 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 © 2004 Cisco Systems, Inc. All rights reserved.

# Introduction

ACNS software, Release 4.2.13 is a maintenance release. These release notes describe supported hardware, and open and resolved caveats regarding ACNS software, Release 4.2.13.

## Additional Hardware Supported

ACNS software, Release 4.2.13 supports the same hardware that was supported by ACNS software, Release 4.2.11. The Content Engine Network Module for the 2600, 3600, and 3700 series branch office routers is supported. 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, Release 4.2 recovery image, 3 DES (Data Encryption Standard)

## Caveats

This section lists and describes caveats that are still open in ACNS software, Release 4.2.13, and caveats that were resolved in this release. Caveats describe unexpected behavior in ACNS software, Release 4.2.13. Severity 1 caveats are the most serious; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats.

### Open Caveats - ACNS Software, Release 4.2.13

- 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 when 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: 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.

- CSCdy03638

Symptom: A banner message cannot be set in Content Engines running ACNS software, Release 4.x.

Workaround: There is no known workaround.

- CSCdy68833

Symptom: A core dump is seen under /local1/core\_dir for Real-Time Streaming Protocol (RTSP) and the video server.

Condition: This core dump is generated by the video server when the E-CDN software is enabled in a CE-507.

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.

- CSCdz74319

Symptom: Users receive a DNS failure message when the Cache application 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.

- 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.

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

- CSCea27277

Symptom: iMac systems running OS X and Windows Media Player 7.1 cannot stream E-CDN video-on-demand (VOD) content from ACNS software, Release 4.2.5.

Condition: This symptom affects iMac systems only. Windows systems work correctly.

Workaround: There is no known workaround.

- CSCea27285

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

Condition: This problem occurs when a 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 an "invalid state" error. This problem does not occur if the stream that has been obtained from the Content Engine is not a live stream. However, playing a stream from the Windows Media Server fails. 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.

- CSCea63021

Symptom: Web servers that interoperate with Content Engines in reverse proxy caching mode seem to fail. The Content Engine's syslog.txt and error log files display this message:

```
HTTP Proxy may be down! Keepalives halted
```

Condition: This problem occurs when WCCP support is enabled on Content Engines. The WCCP keepalive messages are not being sent to the Content Engine by the WCCP-enabled router at the prescribed interval. Therefore, the Content Engine assumes that the connection is down because it does not receive a response from the WCCP-enabled router.

Workaround: Reboot the Content Engine.

- CSCea64579

Symptom: Clients rebuffer streaming media content repeatedly when Content Engines are connected in a chained manner. This typically occurs twice a week.

Condition: Each Content Engine is configured with a broadcasting alias to deliver an incoming stream from the upstream Content Engines using multicasting. The root Content Engine at the top of the chain obtains streaming content from the Windows Media Server using the broadcasting alias. Windows Media Technologies clients that are connected to the downstream Content Engines rebuffer the live stream repeatedly and begin to fail.

Workaround: Restart the Content Engine at the top of the chain.

- CSCea87884

Symptom: Requests for content intercepted and redirected by a WCCP-enabled router to a CE-507 cause the Content Engine to pause indefinitely.

Condition: This occurs on a Content Engine running ACNS software, Release 4.2.x with HTTP persistent connection configuration options set and when the content distributed from the origin server to the Content Engine exceeds the values specified in the Content-length header of a response.

Workaround: Disable persistent connections on the Content Engine using the **no http persistent-connections all** global configuration command.

- CSCeb37717

Symptom: When Windows NT LAN Manager (NTLM) authentication is configured on a Content Engine, the Content Engine fails to query each of the configured name servers iteratively if the primary name server fails.

Condition: The Content Engine sends the fully qualified domain name (FQDN) only to the first name server in the list of name servers specified for name and address resolution (using the **ip name-server** {*ip-addresses* | **serial-lookup**} global configuration command). The Content Engine sends only the host name and not the FQDN to the remaining configured name servers. As a result, if the first name server fails, the name does not get resolved.

Workaround: Disable NTLM authentication using the **no ntlm server enable** global configuration command.

- CSCeb44480

Symptom: When you perform an upgrade from ACNS software, Release 4.x to ACNS software, Release 5.x and use the `acns5_cdm_ip.meta` file to automatically configure the Content Engine to use the ACNS software 5.x Content Distribution Manager and enable the Centralized Management System (CMS) at the end of the upgrade, the entire process is not completed as desired. At the end of the upgrade, the Content Engine is not configured to use the ACNS software 5.x Content Distribution Manager and the CMS is not enabled.

Condition: This problem occurs when the `acns5_cdm_ip.meta` file is imported through the `MANUAL_UPGRADE` channel on the Content Engine during the upgrade from ACNS software, Release 4.x to ACNS software, Release 5.x. When the file is imported through the `MANUAL_UPGRADE` channel, the filename changes. However, the upgrade process still searches for the original filename instead of the filename of the imported `acns5_cm_ip.meta` file.

Workaround: Place the `acns5_cdm_ip.meta` file in the `/local/local1` directory on the Content Engine.

- CSCeb46128

Symptom: When SmartFilter software is configured for URL filtering on Content Engines, it is possible to bypass the SmartFilter software policy by making a request for a partial download of the blocked category of sites.

Condition: This problem occurs when the Content Engine serves as a proxy and a partial download is performed of the category for which you have chosen to deny access. When the partial download option is used, the SmartFilter software policy is not verified and access is therefore allowed.

Workaround: There is no known workaround.

- CSCeb46370

Symptom: A restart of the Content Engine causes certain error messages to be displayed in the `syslog`. However, the Content Engine continues to function normally. An example of the error message is:

```
Jun 20 15:00:02 CNNYFLUAR01 Nodemgr: Start service 'mingetty' using: '/sbin/mingetty --noclear ttyS0 vt100' with pid: 14281
```

Workaround: There is no known workaround.

- CSCeb48523
 

Symptom: Newly constructed websites which are still under construction and which have broken hyperlinks fail to download. The following error message appears on any web browser:

The page cannot be displayed

Condition: This problem occurs when a CE-590 running ACNS software, Release 4.2.9 is used for proxy-style or reverse proxy style caching.

Workaround: There is no known workaround.
- CSCin42046
 

Symptom: Establishing a connection to the Content Distribution Manager using FTP from the CLI is very slow. It takes about 10 minutes before the CLI prompts you for the username and password.

Condition: This problem occurs when you attempt to connect to a CDM-4630 running ACNS software, Release 4.2.9.

Workaround: There is no known workaround.
- CSCin49402
 

Symptom: The **clear cache real-proxy** EXEC command does not clear the RealProxy cache content.

Condition: This problem occurs when RealProxy is enabled on a Content Engine. When you clear the RealProxy cache content, configure the RealPlayer proxy settings to enable the Content Engine as the RealProxy, and request a media file, the RealProxy statistics are incorrectly displayed. This situation occurs on a Content Engine running ACNS software, Release 4.2.11 or Release 4.2.13.

Workaround: There is no known workaround.
- 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 day, month, or year.

Condition: This problem occurs in E-CDN software, Release 2.1 or later (including ACNS software, Release 4.x).

Workaround: There is no known workaround.

## Resolved Caveats - ACNS Software, Release 4.2.13

- CSCed43563
 

After January 10, 2004 at 1:30 p.m. UTC, all Content Engines begin appearing offline intermittently in the Content Distribution Manager GUI. Content import and replication are not affected. Device configuration management is not affected. However, content requests will not be redirected to a Content Engine if the content routing device believes that the Content Engine is offline.



**Note**

---

This problem was never experienced with Content Engines that are running ACNS 5.x software.

---

# 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. The printed documentation provides enough information for you to install and initially configure your product.

### Product Documentation Set

In addition to these release notes, the 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 4.2.13* (The release notes you are reading now.)
- *SmartFilter for Cisco Content Engine User's Guide, Release 3.0.2*

# Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

## Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

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

## 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 Ordering tool:  
<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](mailto:bug-doc@cisco.com).

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

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

We appreciate your comments.

# Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-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 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. The Cisco TAC website is located at this URL:

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

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 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. The online TAC Case Open Tool is located at this URL:

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

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.


- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Go to this URL to visit the company store:  
<http://www.cisco.com/go/marketplace/>
- 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://cisco.com/univercd/cc/td/doc/pcat/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users 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/ipj>
- 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>

---

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 © 2004 Cisco Systems, Inc. All rights reserved.

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

