



Release Notes for Cisco ACNS Software, Release 5.5.9

March 21, 2008



Note

The most current Cisco documentation for released products is available at Cisco.com at <http://www.cisco.com>.

Contents

This release note contains information about the Cisco Application and Content Networking System (ACNS) 5.5.9 software. This release note contains the following topics:

- [Introduction, page 1](#)
- [System Requirements, page 2](#)
- [New and Changed Information, page 4](#)
- [Open Caveats in the ACNS 5.5.9 Release, page 5](#)
- [Resolved Caveats in the ACNS 5.5.9 Release, page 5](#)
- [Product Documentation Set, page 12](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 14](#)

Introduction

The ACNS software combines the technologies of demand-pull caching and pre-positioning for accelerated delivery of web applications, objects, files, and streaming media; the ACNS software runs on Cisco Content Engines, Content Distribution Manager, and Content Router hardware platforms, as well as Cisco Wide Area Application Engine appliances.

This release note is intended for administrators who will be configuring, monitoring, and managing devices that are running the ACNS 5.5.9 software. This release note describes the new product features, the supported hardware, and the open and resolved caveats regarding the ACNS 5.5.9 software release.



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

© 2008 Cisco Systems, Inc. All rights reserved.

System Requirements

This section describes which hardware and software products are compatible with the ACNS 5.5.9 software. This section includes the following topics:

- [Hardware Platforms Supported in the ACNS Software, page 2](#)
- [Software Component Versions Supported in the ACNS Software, page 3](#)

Hardware Platforms Supported in the ACNS Software

Table 1 shows the hardware platforms supported in each ACNS software release. An “X” indicates that the software supports the hardware models listed in that row.

Table 1 Hardware and ACNS Software Compatibility Matrix

Hardware Model	ACNS Support Software								
	5.3.1	5.3.3	5.3.7	5.4.1	5.4.3	5.5.1	5.5.5	5.5.7	5.5.9
CE-507 CE-560 CE-590 CR-4430 CDM-4630	X	X	X	X	X	X	X	X	X
CE-7320 CDM-4650	X	X	X	X	X	X	X	X	X
NM-CE-BP-SCSI NM-CE-BP-40G NM-CE-BP-80G	X	X	X	X	X	X	X	X	X
CE-510 CE-510A CE-565 CE-565A	X	X	X	X	X	X	X	X	X
CE-7305 CE-7305A CE-7325 CE-7325A	X	X	X	X	X	X	X	X	X
CE-511 CE-566	X	X	X	X	X	X	X	X	X
WAE-511 WAE-611		X	X	X	X	X	X	X	X
WAE-7326		X	X	X	X	X	X	X	X
WAE-512 WAE-612					X	X	X	X	X
WAE-674									X
WAE-7341									X

REVIEW DRAFT – CISCO CONFIDENTIAL**Table 1** Hardware and ACNS Software Compatibility Matrix (continued)

Hardware Model	ACNS Support Software								
	5.3.1	5.3.3	5.3.7	5.4.1	5.4.3	5.5.1	5.5.5	5.5.7	5.5.9
NME-WAE-502-K								X	X
NM-WAE-522									X

**Note**

The ACNS 5.4.3 release is the required minimum software release for the WAE-512 and WAE-612 appliances. The ACNS 5.3.3 release is the required minimum software release for the WAE-511, WAE-611, and WAE-7326 appliances.

Software Component Versions Supported in the ACNS Software

Table 2 describes which integrated SmartFilter and Websense versions are supported in the ACNS software releases.

Table 2 Component Versions Supported in the ACNS Software

ACNS Software Release	SmartFilter Version Supported	Websense Version Supported
ACNS 5.2.1	Version 4.0.1	Version 5.2
ACNS 5.3.x	Version 4.0.1	Version 5.2
ACNS 5.4.1	Version 4.0.1	Version 5.5.2 ¹
ACNS 5.4.3	Version 4.1.1	Version 5.5.2
ACNS 5.5.1	Version 4.0.1	Version 5.5.2
ACNS 5.5.5	Version 4.1.1	Version 5.5.2
ACNS 5.5.7	Version 4.1.1	Version 5.5.2
ACNS 5.5.9	Version 4.1.1	Version 5.5.2

1. The integrated Websense Enterprise software Version 5.5 in the ACNS software requires a minimum of 512 MB of RAM. We recommend that you upgrade the RAM on your device to 512 MB or greater, or move your integrated Websense server to another device that has at least 512 MB of RAM. When additional Websense components are enabled (such as the Network Agent), the ACNS software requires a minimum of 1 GB of RAM.

**Note**

Performance is optimal when Websense Enterprise Manager, the Websense Policy Server, and all other Websense components are situated in the same LAN. If all components are not in the same LAN, you may experience communication latency between Websense Enterprise Manager and other components. A significant increase in latency may lead to a communication failure.

New and Changed Information

This section describes the following new and changed features in the ACNS 5.5.9 software release:

- [2-GB Download Support, page 4](#)
- [Increased CFS Partition Sizing, page 4](#)
- [New SmartFilter tarball, page 4](#)
- [Enhanced coredump Storage, page 4](#)
- [Support for WAE-674, WAE-7341, and NM-WAE-522 Hardware, page 5](#)

2-GB Download Support

The ACNS 5.5.9 release supports downloads that are greater than 2 GB only if the request has content-length and **icap respmond** is not enabled. This support applies only to the HTTP protocol.

The ACNS 5.5.9 release does not support the HTTPS or the FTP-over-HTTP protocol.

Increased CFS Partition Sizing

The ACNS 5.5.9 release increases the CFS size in a single disk from 64 GB to 256 GB.

New SmartFilter tarball

The ACNS 5.5.9 release introduces a feature in the new smartfilter tarball, which supports the sf control list download. The maximum size of the sf control list is 200 MB. The earlier versions of the ACNS software did not support the filtering if the sf control list download was greater than 200 MB. In the ACNS 5.5.9 release, the filtering succeeds when the sf control list size increases beyond 200 MB.

Enhanced coredump Storage

The ACNS 5.5.9 release introduces an option of storing the tar file in the core directory. If any process terminates, the software stores the information in the corresponding log file and the log file is saved in a tar file. This tar file gets stored in the core directory, and you can use the FTP protocol to access this tar file.

The option of storing the tar file in the core directory is applicable for the following processes:

- cache
- wmt related processes
- icap_daemon
- http_authmod
- ftp_ctlpxy
- dns
- streamBwcontrol
- stream_schedule

REVIEW DRAFT – CISCO CONFIDENTIAL

Support for WAE-674, WAE-7341, and NM-WAE-522 Hardware

The ACNS 5.5.9 release operates on the WAE-674, WAE-7341, and NM-WAE-522 hardware.

Open Caveats in the ACNS 5.5.9 Release

This section lists the open caveats in the ACNS 5.5.9 release.

- **CSCsm39100**

Symptom: When using TACACS to provide authentication services, authentication fails even though the correct credentials were presented.

Conditions: This problem occurs if the TACACS query response contains additional information, such as "Your password will expire in 4 days" .

Workaround:None.

- **CSCsm43571**

Symptom: The wmt_be cores are generated in the NM-522 module during the SSPL stress.

Condition: This problem occurs when there is an SSPL vod stress and the device is an NM-522 module.

Work around: None.

Resolved Caveats in the ACNS 5.5.9 Release

This section lists the resolved caveats in the ACNS 5.5.9 release.

- **CSCec09045**

Symptom: The requested page is either not received or is loaded slowly.

Condition: This problem occurs when the origin server sends back a response with "Connection: close" but does not close the connection. The CE keeps waiting for the server to close the connection, until it times out. The request is not processed until the previous request is completed, which causes a delay.

Workaround: Configure a static bypass entry for the server.

- **CSCsd99636**

Symptom: The use of outgoing bandwidth is greater than expected.

Condition: This problem occurs because the Fast Cache (FC) is calculated for every missed case. Usually, the outgoing bandwidth is calculated with the FC because data is sent at a higher rate if you enable the FC on the client and the WAE.

Because the FC only supports cache hit cases, you should calculate outgoing bandwidth on the FC only for cache hit cases. This allocation is reset when the playback ends for that stream.

Workaround: None.

- **CSCse04951**

Symptom: The application fails intermittently in the CE. The client station receives frames with incorrect TCP checksums.

REVIEW DRAFT – CISCO CONFIDENTIAL

Condition: This problem occurs when the application makes an HTTP or FTP-over-HTTP request for data and that data is noncacheable and arrives from the server in IP fragments.

Workaround: Use the **tcp server-mss** command to prevent fragmentation.

- **CSCse21542**

Symptom: The CLI written to the CE is different from what was entered in the GUI.

Condition: This problem occur when there are multiple outgoing proxies listed in the GUI for a CE.

Workaround: None.

- **CSCsi10052**

Symptom: A core occurs in the ftp_ctlpxy process in the ACNS module.

Condition: This problem occurs in the ftp proxy process.

Workaround: None. Restart the process.

- **CSCsi16813**

Symptom: You receive block pages for FTP-over-HTTP requests.

Condition: This problem occurs when the ICAP and urlfilter are enabled at the same time and the urlfilter is blocking requests from 127.0.0.1.

Workaround: Change the IP address 127.0.0.1 in the URL filtering configuration.

REVIEW DRAFT – CISCO CONFIDENTIAL

- **CSCsi47286**

Symptom: The cache core file is in the /local1/core_dir and the core file is in the sf_lookup_ldap_groups.

Condition: This problem occurs when SmartFilter is enabled.

Workaround: None. The cache process is restarted automatically.
- **CSCsj07986**

Symptom: A core dump occurs in the ACNS software.

Condition: This problem occurs when you query the cceWmtTotalClientErrors variable.

Workaround: None. The SNMP process is restarted automatically.
- **CSCsj08016**

Symptom: A crash occurred on the ACNS software due to the webserver module.

Condition: None.

Workaround: None.
- **CSCsj21531**

Symptom: Delays from 3 to 15 or more seconds occur while the ACNS software is receiving HTML pages and objects.

Condition: This problem occurs on ACNS 5.5.5.4 when the first configured name-server is down and the ICMP is unreachable for the DNS queries.

Workaround: Either remove the first name-server from the ACNS configuration or fix the server problem.
- **CSCsj26798**

Symptom: An SNMP core occurs in the CE.

Condition: This problem occurs when you query for the ACTONA-ACTASTOR-MIB (which is not supported in the ACNS software) for the first time.

Workaround: None. The SNMP process is restarted automatically.
- **CSCsj36452**

Symptom: The SmartFilter does not function on certain web sites.

Condition: This problem occurs when the module has been running for two weeks or longer.

Workaround: Restart the cache process.
- **CSCsj49720**

Symptom: While deleting a reference to a pac file template, the previously configured pac template reference stops working.

Condition: This problem occurs when you create two pac file references to two different pac file templates that share the same CZ file.

Workaround: Use a different CZ file for the deleted reference.
- **CSCsj80235**

Symptom: Clients fail to browse into an empty directory or upload file into an empty directory.

Condition: This problem occurs when the client is set to use the CE as an FTP-over-HTTP proxy and attempts to access an empty directory on an FTP server.

Workaround: None.

REVIEW DRAFT – CISCO CONFIDENTIAL**• CSCsj82298**

Symptom: When you make a change to an item in a device group, the complete configuration configured in that device group is pushed to all devices in the group, including the WCCP redirection/return selections and the I2-return line. When the CE receives the I2-return line, it pushes this line to the router.

The router sees this I2-return line and notifies the cache that it does not support a I2-return line. At the same time, it renegotiates the WCCP parameters, which causes the Catalyst 6500 series switch to drop the current WCCP session.

Condition: This problem occurs each time a change is made to an item in a device group because the complete configuration in that device group is pushed to all the devices in the group.

Workaround: If the problem occurs when you are modifying the bypass list, create a new device group called BypassListEntriesDeviceGroup, and add all the required content engines to this group. Because only the bypass entries are configured in this device group, these bypass entries are pushed.

• CSCsj93406

Symptom: Critical messages that are related to SNMP are logged in the syslog.

Condition: This problem occurs when you query the tcpConnState MIB.

Workaround: None.

• CSCsj98779

Symptom: An McastSender or McastReceiver Core occurs frequently in the CE and no multicast distribution progress occurs.

Condition: This problem occurs under the following two conditions:

- The port channel is configured on the CE.
- The CE is multicast enabled and assigned to a multicast channel and cloud.

Workaround: Remove the port channel configuration.

• CSCsk00788

Symptom: Cisco WMS returns a 500 server error.

Conditions: This problem occurs when the CE receives a URL for an asx file that is missing an asx extension.

Workaround: Perform one of the following actions:

- Add an asx extension to the asx file so that it is sent to the client through the apache www server.
- Disable WMT on the CE.
- Downgrade to 5.4.x or 5.3.x.

• CSCsk02645

Symptom: A request for the broadcast alias has been redirected to an invalid proxy instead of to the origin server.

Condition: This problem occurs when DNS is configured as round-robin.

Workaround: Enter the **dns pin** command to obtain the IP address of the DNS server as requested by the CE.

REVIEW DRAFT – CISCO CONFIDENTIAL**• CSCsk06669**

Symptom: The icap_daemon crashes and prevents the CE from serving HTTP requests for approximately 30 seconds until the icap_daemon restarts.

Condition: This problem occurs when the CE is configured with Websense and the icap modes are enabled.

Workaround: None.

• CSCsk08291

Symptom: Some follow-redirect requests have failed.

Condition: This problem occurs when the client requests are pipelined to the CE, and the 302 response from the origin server that matches the follow-redirect configuration has a content-length greater than 1024 bytes.

Workaround: None.

• CSCsk50003

Symptom: A core is generated in the CE when you enter the **show programs program name** command.

Condition: This problem occurs when the multicast station is configured and you enter the **show programs program name** command in the CE.

Workaround: None.

• CSCsk51843

Symptom: Incoming or outgoing streams for multicasts are not available.

Condition: This problem occurs after an ACNS video program has been created for multicasting.

Workaround: Remove the old wmt_wget files in the tmp directory.

• CSCsk55302

Symptom: The SNMP process crashed.

Condition: This problem occurs when the software comes up.

Workaround: None.

• CSCsk70926

Symptoms: The Protocol field of the source URL shows FAILED instead of HTTP or RTSP.

Condition: This problem occurs in a managed live program when you enter the **show program program-name** command.

Workaround: None.

• CSCsk92804

Symptom: LDAP group searches may result in improperly populated group membership lists for users whose primary group is Domain Users.

Users may be able to access resources, even if the access lists specifically deny access to those resources based on improperly cached credentials.

Condition: This problem occurs when the Active Directory is used for NTLM authentication and LDAP group searches and interdomain trusts are established to allow users from different domains to authenticate with the CE HTTP proxy.

REVIEW DRAFT – CISCO CONFIDENTIAL

Access lists are used to authorize users based on their membership to the Domain Users group of an FQDN domain, such as domain1.cisco.com\Domain Users. Does not affect NTLM-based access-lists, such as DOMAIN1\Domain Users.

Workaround: Do not use fqdn.domain.com\Domain Users for any access-list based authentication, where fqdn.domain.com is any AD domain.

- **CSCsk93119**

Symptom: The server receives multiple authentication prompts while using NTLM as the authentication mechanism.

Condition: This problem occurs in the following conditions:

- When the ACNS WAE has been configured to have the ISA server as the outgoing proxy.
- When NTLM authentication is enabled in the ISA server.

Workaround: None.

- **CSCsl04335**

Symptom: There is a conflict between the ACNS 5.5.7.7 release and WMT version 9 when a CE is connected to the Internet router directly only for streaming and not for the web cache. The traffic flow is **User PC ...> Core router ...> PIX FW ...> CE**

Condition: This problem occurs when two users (for example, user A and user B) use the same setup of Windows IE, are on the same VLAN, and access the same CE. In this example, user A can open the video file, but user B cannot open the video file.

Workaround: Use the **bypass** command to bypass the CE for packets that are destined to another network.

- **CSCsl11205**

Symptom: Statistics for the Cisco Streaming Engine are appearing incorrectly in the CLI and the GUI.

Condition: This problem occurs when the Cisco Streaming Engine is configured.

Workaround: None.

- **CSCsl13042**

Symptom: The CE maintains separate incoming connections for each sspl live-split client.

Condition: This problem occurs during the live split of the server-side playlist content.

Workaround: None.

- **CSCsl35087**

Symptom: The CE goes into an overload bypass and there are many connections in the CLOSE_WAIT state.

Conditions: This problem occurs when WCCP with IP spoofing is configured and a server-side persistent connection is enabled.

Workaround: Disable the server-side persistence.

- **CSCsl44067**

Symptom: ACNS 5.5.7 is considered as an unknown ACNS module when you configure it through the GUIs.

Condition: This problem occurs when the CDM is running ACNS 5.5.7.

Workaround: Upgrade the CDM ACNS 5.5.9.

REVIEW DRAFT – CISCO CONFIDENTIAL

- **CSCsI52931**

Symptom: The channel fails to parse the manifest.

Condition: This problem occurs when you do all of the following:

 - Select the channel content.
 - Select a line within the channel content.
 - Expand the "x rules defined" section using the triangle.
 - Highlight an existing rule.

Workaround: Readd a simple match rule that requires a minimal one byte file.
- **CSCsI54600**

Symptom: The DNS servers stop responding to DNS requests for domains serviced by the content route.

Condition: This problem occurs when a user sends an NS lookup for an NS record to the CR, and the CR responds to the DNS server with a record response. The response should have been negative and the server should have replied that it did not know the name of the NS record.

Workaround: Set the DNS server negative cache to 0.
- **CSCsI92148**

Symptom: A kernel crash has occurred in the ACNS 5.5.5 release.

Condition: This problem occurs when the TCP-related traffic runs on the ACNS module.

Workaround: None.
- **CSCsm15825**

Symptom: The proxy responds with an error code for the incorrect header when a redirected URL is sent for a SmartFilter blocked page.

Condition: This problem occurs when the SmartFilter is configured in the ACNS software and the upstream proxy is used.

Workaround: None.
- **CSCsm20191**

Symptom: A DNS request for an AAAA record returns a "Name Error" even if the record is available.

Condition: This problem occurs when the Content Router sends an AAAA record request before it sends the A record (disable IPv6).
- **CSCsm36270**

Symptom: Crash alarms have been found on the device.

Condition: This problem occurs when the SNMP core (core.smmgcd.) is found on the core directory.

Workaround: None. The SNMP process should restart automatically.
- **CSCsm42427**

Symptom: The CE is configured with ACNS 5.4.5.7.

Condition: This problem occurs when you log into the CE through SSH and there is no record of your IP address.

Workaround: None.

REVIEW DRAFT – CISCO CONFIDENTIAL

- **CSCsm45518**
Symptom: The client receives an error when the RTSP streaming fails for a few video files.
Condition: This problem occurs when the header size of the video file is greater than 32 KB.
Workaround: None.
- **CSCsm46689**
Symptom: WMT has generated a core.
Condition: This problem occurs when the log line is parsed. In this case, WMT does not have the number of fields as expected.
Workaround: None.
- **CSCsm73461**
Symptom: A Wmt_be core file has been generated.
Condition: This problem occurs when the Getparameter is interpreted as a Setparameter.
Workaround: None.
- **CSCsm87858**
Symptom: SNMP fails during the SHA authentication.
Condition: This problem occurs when you attempt to walk the MIBS using the SHA authentication.
Workaround: None.

Product Documentation Set

In addition to this release note, the following document types are included in the product documentation set. An online help system is included in the product software.

- [Regulatory Compliance, Safety Information, and Licensing](#)
- [Hardware Documents](#)
- [Software Documents](#)
- [Online Help](#)

REVIEW DRAFT – CISCO CONFIDENTIAL**Regulatory Compliance, Safety Information, and Licensing**

- *Documentation Guide and License and Warranty for Cisco ACNS Software, Release 5.5.x*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*

Hardware Documents

- *Cisco Wide Area Application Engine 512 and 612 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 511 and 611 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 7326 Hardware Installation Guide*
- *Cisco Content Engine 7305 and 7325 Hardware Installation Guide*
- *Cisco Content Engine 511 and 566 Hardware Installation Guide*
- *Cisco Content Engine 510 and 565 Hardware Installation Guide*
- *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 Documents

- *Cisco ACNS Software Upgrade and Maintenance Guide, Release 5.x*
- *Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.5*
- *Cisco ACNS Software Command Reference, Release 5.5*
- *Cisco ACNS Software API Guide, Release 5.5*
- *Cisco ACNS software Program Manager for IP/TV User Guide, Release 5.4*
- *Release Notes for Cisco ACNS Software Program Manager for IP/TV, Release 5.4*

Online Help

The Content Distribution Manager GUI and the Content Engine GUI both have context-sensitive online help that can be accessed by clicking the **HELP** button. ACNS software includes the following online help systems:

- Content Distribution Manager GUI online help system for centrally managed ACNS networks
- Content Engine GUI online help system for locally deployed Content Engines

REVIEW DRAFT – CISCO CONFIDENTIAL

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0801R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.