Release Notes for Cisco ACNS Software, Release 5.5.13 and 5.5.15

July 20, 2009

Note The most current Cisco documentation for released products is available on Cisco.com.

Contents

This release note contains information about the Cisco Application and Content Networking System (ACNS) software version 5.5.13 and 5.5.15.

Note If you are running ACNS version 5.5.13 we recommend that you upgrade to ACNS version 5.5.15 at your earliest convenience.

This release note contains the following topics:

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

ACNS Support on a WAAS Virtual Blade

ACNS 5.5.13 introduces ACNS-VB (ACNS software support on a WAAS virtual blade). The ACNS-VB feature allows ACNS 5.5.13 or later to run on a WAAS virtual blade and be managed from the Central Distribution Manager. ACNS-VB is supported on WAAS version 4.1.3 or later.

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	5.3.3	5.3.7	5.4.1	5.4.3	5.5.1	5.5.5	5.5.7	5.5.9	5.5.11	5.5.13, 5.5.15
CE-507 CE-560 CE-590 CR-4430 CDM-4630	X	X	X	X	X	X	X	X	X	X
CE-7320 CDM-4650	X	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	X
CE-510 CE-510A CE-565 CE-565A	X	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	X
CE-511 CE-566	X	X	X	X	X	X	X	X	X	X
WAE-511 WAE-611	X	X	X	X	X	X	X	X	X	X
WAE-7326	X	X	X	X	X	X	X	X	X	X
WAE-512 WAE-612				X	X	X	X	X	X	X
WAE-674								X	X	X
WAE-7341								X	X	X

Table 1 Hardware and ACNS Software Compatibility Matrix (continued)

Hardware Model	5.3.3	5.3.7	5.4.1	5.4.3	5.5.1	5.5.5	5.5.7	5.5.9	5.5.11	5.5.13, 5.5.15
NME-WAE-502-K							X	X	X	X
NM-WAE-522								X	X	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. The ACNS 5.5.13 release is the required minimum software release for ACNS-VB running on WAAS virtual blade.

Software Component Versions Supported in the ACNS Software

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

Table 2 Component Versions Supported in the ACNS Software

ACNS Software Release	SmartFilter Version Supported	Websense Version Supported
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
ACNS 5.5.11	Version 4.1.1	Version 5.5.2
ACNS 5.5.13	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.

The following software component restrictions apply to the NME-WAE-502:

- On-box SmartFilter is not supported on the NME-WAE-502 running ACNS version 5.5.7 and later. Off-box SmartFilter is supported on the NME-WAE-502 running ACNS version 5.5.7 and later.
- On-box Websense is not supported on the NME-WAE-502 running ACNS version 5.5.7 and later. Off-box Websense is not supported on the NME-WAE-502 running ACNS versions 5.5.7 and 5.5.9. Off-box Websense is supported in ACNS version 5.5.11 and later.

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.

Software Version 5.5.15 Resolved and Open Caveats

The following sections list the resolved and open caveats in the ACNS 5.5.15 release.

Software Version 5.5.15 Resolved Caveats

This section lists the resolved caveats in the ACNS 5.5.15 release.

- **CSCta47218**—SNMP errors are seen in the syslog when SNMP is configured. The following error is shown in the syslog after upgrading to 5.5.13: "CE-SNMP-3-430005: get_ifIndex: Failed open /proc/net/dev. errno: 24,Too many open files." This issue occurs under normal working conditions when the MIB hrProcessorTable is queried multiple times and files are left open. Eventually, the total number of open files supported by the process is exceeded.
- **CSCsy62388**—If kernel kdb is enabled, the CE will drop to the KDB prompt or reboot spontaneously under rare circumstances. This is a rare scenario when HTTP packets get fragmented.

Software Version 5.5.15 Open Caveats

This section lists the open caveats in the ACNS 5.5.15 release.

- **CSCta25754**—Syslog messages are not sent when the unit is reloaded and the syslog configuration has to be reentered to restart. However, syslog entries still show in the configuration after a reboot. This issue occurs every time the unit is rebooted on the CE2636 platform.
- **CSCta76909**—Webserver process becomes unresponsive after rescuing using the "***" option. This issue occurs with a CE running version 5.5.7 or earlier when rescuing the unit remotely. Workaround: None. The webserver process restarts itself and the CE-GUI is reachable.

The additional open caveats for software version 5.5.15 are the same as those open caveats for software version 5.5.13, with the exception of CSCsy62388, which is resolved for 5.5.15. For details, see the "Software Version 5.5.13 Open Caveats" section on page 7.

Software Version 5.5.13 Resolved and Open Caveats

The following sections list the resolved and open caveats in the ACNS 5.5.13 release.

Software Version 5.5.13 Resolved Caveats

This section lists the resolved caveats in the ACNS 5.5.13 release.

- **CSCsb63246**—When entering a rule action no-proxy with failover modifier, the CLI does not accept pattern lists containing groupname, groupname-regex or username as valid rule patterns.

- **CSCsr25336**—User requests without the question mark (?) are not logged in the working.log. User requests to the URL with the question mark that hit the rule are logged in working.log. This occurs when rules have been configured to rewrite a URL containing ?.* (question mark followed by any characters) to a URL without ? (question mark and the following characters).
- **CSCsr62793**—The command **sh ntp status** does not display the status of NTP servers configured. This occurs under normal conditions when more than one valid NTP server is configured on the CE.
- **CSCsu01044**—FTP downloads fail when native FTP WCCP is enabled. Long response line is received from the server after the response code 230-.
- **CSCsu02168**—After enabling debug HTTP cache and logging at level 7, "transfer 2147483647 byte" is shown regardless of the actual size of the content.
- **CSCsu36304**—RTSP does not stream with a layer 4 switch and with WCCP enabled. This occurs on ACNS 5.5.7 running RTSP on a layer 4 switch and with WCCP enabled.
- **CSCsu51480**—Cache core is found on the device when Websense is enabled.
- **CSCsu94861**—HTTP keepalive halted message repeated in syslog. This occurs when the cache app misses sending a keepalive message to the WCCP process.
- **CSCsv03977**—CVE-2006-5794 - Might allow attackers to bypass authentication.
  CVE-2006-5052 - Allows remote attackers to determine the validity of usernames via unknown vectors involving a GSSAPI “authentication abort.”
- **CSCsu76586**—DNS servers stop responding to DNS request for domains serviced by Content Route. This occurs when a user sends a DNS lookup for an MX record to the CR. The CR responds to DNS server with an A record response.
- **CSCsu67156**—RTSPU playback buffers when ACNS on a virtual blade is put as proxy in WM player. This occurs only for the RTSPU protocol. The ACNS on a virtual blade should be the proxy in WM player.
- **CSCsv44893**—Cache Core occurs when there is a NULL in the Header Line and the size of the header is greater than 1024.
- **CSCsv54756**—Internal Exception Error seen in CDM > Services > Video > Programs > Schedule when scheduling programs using the CDM GUI. CMS service restarts when scheduling programs using the CDM GUI.
- **CSCsv79388**—Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default in Cisco products. Only SNMPv3 is impacted by these vulnerabilities. Note: SNMP versions 1, 2 and 2c are not impacted by these vulnerabilities. The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities. Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0960 has also been assigned to these vulnerabilities. This advisory is posted at:
  http://www.cisco.com/warp/public/707/cisco-sa-20080610-snmpv3.shtml.
- **CSCsw36411**—From the menu, the option Devices > <select device> > show all > Prepositioning > Scheduled bandwidth > Aggregate Settings is set to **No** while the intended behavior should be set to **Yes**.
- **CSCsw40196**—Dispatcher core is seen on the device. This occurs when there is an improper close of an SSL connection that uses a previous SSL session.
- **CSCsw79674**—Unable to play a specific type of file when it is prepositioned. This occurs when the file is prepositioned and contains packet/block count as zero in the asf header.

- **CSCsw81097**—Scheduling outgoing BW using GUI shows warning that windows media limit exceeds licensing limit.
- **CSCsx03113**—The transfer of a large object may be gracefully closed prematurely, leading to an incomplete file received without an error message. This occurs when a client downloads an object greater than 512KB. The client connection is much slower compared to server connection and the device is under significant load.
- **CSCsx10437**—Certain multicast distribution log files are not being deleted when the sysfs partition reaches capacity and needs to run cleanup script. The log files that have issues are xxxx_fxdsrc.log and xxxx_feedbk.log.src.
- **CSCsx19118**—The commands **no wccp version 2** and **no wccp router-list** <*number*> <*ip address*> do not appear in the cli-errorlog.
- **CSCsx99875**—The HTTP server in ACNS does not sanitize the Expect header from an HTTP request when it is reflected back in an error message. This may allow cross-site scripting (XSS) using web client components that can send arbitrary headers in requests.
- **CSCsx94394**—The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections. Servers supporting the TRACE method are subject to cross-site scripting attacks, dubbed XST for “Cross-Site Tracing,” when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give their credentials.
- **CSCsy04621**—ACNS is not able to stream a specific type of file with RTSP. WMS9 will still stream with RTSP. This occurs when the encoded media has the following defect: Simple index object is mapping to the wrong packet number for the time 00:00 (33129 in this case, which is almost the end of the file).
- **CSCsy29452**—Unable to specify the RTSPT protocol for the unicast url in a live event after upgrading from ACNS software version 5.4.3 to version 5.5.11.2.
- **CSCsy42841**—Removing a WCCP server from the GUI does not work. Rather than removing the required CLI, the CDM applies it to the CE. This occurs under normal working conditions. The CLI must be used on the CE to remove the WCCP service.
- **CSCsy44585**—NTLM authentication stops working after some time of operation. There is a memory leak at the “http_authmod” process that results in NTLM authentication hang issues. This occurs when the CE is operational for more than a month.
- **CSCsy53080**—The CE that is running a CR service can generate a core due to the cr_backend process crash. This may occur if the coverage zone XML file is not valid according to the XML requirements.
- **CSCsy55853**—BAD_OP message in syslog. This occurs when WMT is enabled and content requested is of very short play duration.
- **CSCsy82839**—The CE sends a request to the secondary Websense server even though the primary Websense server is alive. This occurs when there is a lot of TCP errors between the CE and the Websense server.
- **CSCsy87998**—Scheduled db maint full is conditional. There are times when it does not run but there are database errors reported. When cms database maint full is run from the CLI, the errors clear and the CE operation returns to normal. Running database maintenance unconditional prevents many problems found in large deployments.
- **CSCsy89485**—CE does not send a QUIT command to the FTP server, but in-turn closes the client and server connection. This occurs when the client sends a QUIT command and expects a 221 message from the server.

- **CSCsz11144**—ACNS responds with the entire content, however the response header will have a 206 partial content response. This occurs when **http smart-range enable** command is enabled and a rule not to cache is a hit in a client requesting partial content.
- **CSCsz18750**—ACNS goes to kdb mode after a reload and the syslog consists of the error message:

  KERNEL CRASH DUMP: /local/local1/crash/...
  ....
  <1>kernel BUG at /users1/acns_5.5.9-b9/bfc/linux/kernel-2.6.x/net/core/skbuff.c:91!
  ...

  This occurs rarely when the box is reloaded.
- **CSCsz19188**—ACNS running ICAP causes a crash and a core file. The ICAP server sends header of null-body instead of content.
- **CSCsz33032**—A web site that is left idle for over 2-3 minutes takes a long time to return. This occurs when HTTP persistent connections is enabled on the CE.
- **CSCsz46927**—In rare scenarios, the cache process does not pass any HTTP traffic and none of the HTTP-related stats are shown in the CLI.
- **CSCsz76830**—In rare instances when querying ifEntry, SNMP process cores (snmpced aborts and dumps a core).while querying ifEntry.

Software Version 5.5.13 Open Caveats

This section lists the open caveats in the ACNS 5.5.13 release.

- **CSCsw23921**—ACNS on a virtual blade CPU utilization on average is 75% for WMT- Proxy Live stream test (RTSPT). This occurs when running a performance test for 140 users and file size is 708-kbps on WAE-674-8GB. The CPU utilization is measured by using vmstat output of ACNS on a virtual blade. Workaround: None.
- **CSCsx94151**—Transaction log export fails and transaction logs do not export. Workaround: None.
- **CSCsy62388**—If kernel kdb is enabled, the CE will drop to the KDB prompt or reboot spontaneously under rare circumstances. This is a rare scenario when HTTP packets get fragmented. 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.

Hardware Documents

- *Cisco Wide Area Application Engine 7341, 7371, and 674 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 7326 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 512 and 612 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 511 and 611 Hardware Installation Guide*
- *Installing Hard Disk Drives in the Cisco Wide Area Application Engine 611*
- *Installing the Cisco WAE Inline Network Adapter*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*

Software Documents

- *Cisco WAAS Installation and Configuration Guide for ACNS on a Virtual Blade*
- *Cisco ACNS Software Upgrade and Maintenance Guide, Release 5.5.13*
- *Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.5.13*
- *Cisco ACNS Software Configuration Guide for Locally Managed Deployments, Release 5.5.13*
- *Configuring Cisco Access Routers and the NME-WAE Network Module for ACNS Deployments*
- *Cisco ACNS Command Reference, Release 5.5.13*
- *Cisco ACNS Software API Guide, Release 5.5*

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

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