



Release Notes for Cisco ACNS Software, Release 5.5.27

September 3, 2012



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 5.5.27.

This release note contains the following topics:

- [Support for 7371](#)
- [Additional Disk Space on ACNS-VB](#)
- [Hardware Platforms Supported in the ACNS Software](#)
- [Software Component Versions Supported in the ACNS Software](#)
- [Software Version 5.5.27 Resolved and Open Caveats](#)
- [Product Documentation Set](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines](#)



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

Support for 7371

ACNS 5.5.27 release supports WAE -7371 hardware. The device modes supported are CE and CDM.

Additional Disk Space on ACNS-VB

ACNS-VB 5.5.21 and later versions reserve less disk space for system use, leaving more disk space for other purposes. This change is not applied during a regular upgrade process. To procure additional disk space, a complete installation needs to be performed.

For steps to procure additional free disk space on an ACNS-VB, please refer to ACNS 5.5.21 release notes.

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, 5.5.17, 5.5.19, 5.5.21, 5.5.23, 5.5.25	5.5.27
CE-507 CE-560 CE-590 CR-4430 CDM-4630	X	X	X	X	X
CE-7320 CDM-4650	X	X	X	X	X
NM-CE-BP-SCSI NM-CE-BP-40G NM-CE-BP-80G	X	X	X	X	X
CE-510 CE-510A CE-565 CE-565A	X	X	X	X	X
CE-7305 CE-7305A CE-7325 CE-7325A	X	X	X	X	X
CE-511 CE-566	X	X	X	X	X
WAE-511 WAE-611	X	X	X	X	X
WAE-7326	X	X	X	X	X
WAE-512 WAE-612		X	X	X	X
WAE-674				X	X
WAE-7341				X	X
NME-WAE-502-K			X	X	X
NM-WAE-522				X	X
WAE-7371					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. ACNS 5.5.27 is the required minimum software release for WAE-7371.

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
ACNS 5.5.19	Version 4.1.1	Version 5.5.2
ACNS 5.5.21	Version 4.1.1	Version 5.5.2
ACNS 5.5.23	Version 4.1.1	Version 5.5.2
ACNS 5.5.25	Version 4.1.1	Version 5.5.2
ACNS 5.5.27	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 5.5.27 Resolved and Open Caveats

The following sections list the resolved and open caveats in the ACNS 5.5.27 release.

- [Software Version 5.5.27 Resolved Caveats](#)
- [Software Version 5.5.27 Open Caveats](#)

Software Version 5.5.27 Resolved Caveats

This section lists the resolved caveats in the ACNS 5.5.27 release:

- **CSCtx32411**—Server response with status 301 redirect containing Cache-Control directives that dictate not to store, is cached by CE and delivered for subsequent client request.
Workaround: Disable caching of a problematic URL using a rule.
- **CSCtx86471**— Sysreport CLI accepts and generates report for future dates.
- **CSCtz88848**—Current open SSL version in ACNS is vulnerable for CVE-2012-2110 and CVE-2012-2131, which allows remote attackers to conduct buffer overflow attacks, and cause a denial of service.
- **CSCua16982**—Response for prepositioned content with range request is missing Content-Type header.
- **CSCua22817**—Current version of Linux kernel in ACNS is vulnerable to CVE-2005-3181, which may lead to a memory leak that allows attackers to cause a denial of service.
- **CSCua48057**—ACNS Listing API **getObjectById** is not returning the ContentIP address in a standard format. Sometimes the address is shown with just the IP_Address and sometimes the address is shown as HOSTNAME#IP_Address.
- **CSCua52525**—Playing a corrupt WMV file with huge packet length results in high CPU and memory usage, while trying to allot memory to hold this packet.
- **CSCub15270**—SNMP error messages are seen in syslog while booting the CE.
- **CSCub28618**—When Multicast is disabled in the Sender or Receiver in the multicast A&D process, the CE shows a minor alarm and the CDM GUI shows a major alarm. Need to increase the severity of **svcnomcastenable** alarm in CE.

Software Version 5.5.27 Open Caveats

This section lists the open caveats in the ACNS 5.5.27 release.

- **CSCtz72352**—Under certain unknown scenarios, icap sockets get into CONNECTING state but are unable to complete. After timeout, cache process follows error handling.
Workaround: A script can be provided to monitor and restart the icap process automatically to handle such situations.
- **CSCua78707**—During NTLM negotiation, sometimes the HTTP connection is closed by the CE and the client browser displays the unexpected password prompt.
Workaround: None
- **CSCub65561**—ACNS is vulnerable to Java's Floating-Point issue (CVE-2010-4476).
Workaround: None

- **CSCtc05567**—Rescue CD may not reconfigure controller, on platforms with hardware RAID and at least one logical drive setup.
Workaround: Use the RAID setup utility during POST to delete all logical drive.
- **CSCtz76320**—When more than one router and CE are in the farm and when one particular interface is going down, the CE with lower ip address gets 100% bucket allotment instead of sharing the load among the CEs.
Workaround: Restart wccp service in any one of the interface(s).
- **CSCub25431**—Priority 0 not recognised by Gigabit 2/0 interface in standby group.
Workaround: Use priority number other than zero for Gigabit 2/0 interface.
- **CSCub31326**—Enabling DNS while standby is configured as primary interface fails and throws error.
Workaround: Configure gigabit interface as primary interface and enable dns service.

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](#)
- [Software Documents](#)
- [Online Help](#)

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*
- *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>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1005R)

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.

© 2009-2012 Cisco Systems, Inc. All rights reserved.