Release Notes for Cisco ACNS Software, Release 5.5.25

February 13, 2012

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 5.5.25.

This release note contains the following topics:

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

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.

To procure additional free disk space on an ACNS-VB, follow these steps:

Note This procedure to procure additional disk space will result in a loss of all previous data, including configuration and cached data.

Step 1 Download the 5.5.25 rescue-cdrom.iso image.

Step 2 Stop the ACNS-VB in WAAS by using the following command:

WAE# virtual blade vb_number stop 0

Step 3 After the session stops, change the boot cd-image disk image location to the 5.5.25 ISO image by using the following commands:

WAE(config)# virtual-blade vb_number

WAE(config-vb)# boot cd-image disk /local1/vbs/rescue-cdrom.iso

Step 4 Change the boot option of the virtual blade to cd-rom by using the following commands:

WAE(config)# virtual-blade vb_number

WAE(config-vb)# boot from cd-rom

Step 5 Start the virtual blade by using the following command:

WAE# virtual-blade vb_number start

Step 6 Install ACNS 5.5.25. Follow the installation procedure described in the Cisco ACNS Software Upgrade and Maintenance Guide. This guide is available at the following location:

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/acns/maintenance/v5x/upgrade/guide/6695bkup.html#wpxref65415

Step 7 After the ACNS installation is complete, stop the virtual blade session by using the following command:

WAE# virtual-blade vb_number stop 0

Step 8 After the session stops, change the boot option of the virtual blade to disk by using the following commands:

WAE(config)# virtual-blade vb_number

WAE(config-vb)# boot from disk

Step 9 Start the virtual blade and check the new disk space when ACNS-VB starts. Additional disk space will now be available.

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
CE-507 CE-560 CE-590 CR-4430 CDM-4630	X	X	X	X
CE-7320 CDM-4650	X	X	X	X
NM-CE-BP-SCSI NM-CE-BP-40G NM-CE-BP-80G	X	X	X	X
CE-510 CE-510A CE-565 CE-565A	X	X	X	X
CE-7305 CE-7305A CE-7325 CE-7325A	X	X	X	X
CE-511 CE-566	X	X	X	X
WAE-511 WAE-611	X	X	X	X
WAE-7326	X	X	X	X
WAE-512 WAE-612		X	X	X
WAE-674				X
WAE-7341				X
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. 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
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

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 5.5.25 Resolved and Open Caveats

The following sections list the resolved and open caveats in the ACNS 5.5.25 release.

Software Version 5.5.25 Resolved Caveats

This section lists the resolved caveats in the ACNS 5.5.25 release:

- **CSCtw71706**—ACNS supports the use of weak SSL ciphers. This may enable an attacker to launch man-in-the-middle attacks and monitor or tamper with sensitive data.

  Workaround: None.

- **CSCto48167**—Cached authenticated content is delivered to unauthorized clients. The issue impacts only basic http authenticated objects. NTLM authenticated objects or objects delivered from pre-positioned channels are not impacted.

  Workaround: Disable http cache-authenticated basic.

- **CSCtl76221**—Errorlog-cache reports the number of CPUs as two for the NM-522 device that has a single CPU.

  Workaround: None.

- **CSCtn52938**—Misleading error messages are displayed while deleting a Content Engine (CE) from a CDM. This occurs when the root content engine of a channel to which the content engine is linked is inactive.

  Workaround: Activate the root CE.

- **CSCtn67421**—Priority value not recognized by the standby group when maximum priority value is configured for standby group.

  Workaround: None.

- **CSCto76186**—Application server is FIN'ing a connection due to an application level timeout. The content engine is not forwarding this FIN back to the client.

  Workaround: Increase the application server timeout to equal to or greater than the client application idle time.

- **CSCtq50864**—The CE modifies the WMT server response while sending a response to the client. When non-existent media content is requested by the client, the media server responds with a "404 Not Found" response. But the CE sends a "500 Server Error" to the client.

  Workaround: Disable interception in the CE such that the client contacts the server directly.

- **CSCtu21723**—ACNS is susceptible to NTP Daemon Denial-of-Service.

  Workaround:

  - Filter NTP mode 7 packets coming into and/or going out of your network.
  - Filter NTP mode 7 packets where both the source and destination ports are 123, the privileged NTP port.
  - Employ anti-spoofing IP address filters at your borders to prevent UDP traffic claiming to be from a local address that originate outside your network.

- **CSCtg27425**—wmt_be process aborts and creates core file due to invalid data received while playing a file.

  Workaround: None.

Software Version 5.5.25 Open Caveats

This section lists the open caveats in the ACNS 5.5.25 release.

- **CSCto52286**—The MTU value is not retained after assigning and removing the interface from the port channel and MTU value in running configuration differs from that in show interface CLI.

  Workaround: Re-apply the MTU CLI in the interface.

- **CSCto57980**—Two interfaces of different MTU values can be assigned to a port-channel/standby group.

  Workaround: Set a default MTU value for both the GIG interfaces.

- **CSCts22565**—Member interfaces show as up and running after the standby/port-channel group interface is administratively shut.

  Workaround: None.

- **CSCts33279**—A denial of service vulnerability has been found in the way the multiple overlapping ranges are handled by the Apache HTTPD server. Ref: CVE-2011-3192

  Workaround: None.

- **CSCtt00287**—Apache Tomcat server contains a vulnerability that allows remote attackers to execute an arbitrary web script that pulls the cookie data. Ref: CVE-2002-1567.

  Workaround: None.

- **CSCtx32411**—Server response with status 301 redirect containing Cache-Control:max-age=0 is stored in cache and delivered for subsequent client request.

  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
- 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*
- *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