Release Notes for AsyncOS 8.6 for Cisco Web Security Appliances

Published: March 3, 2015

Contents

Cisco Systems, Inc.
www.cisco.com

What's New

What's New in Cisco AsyncOS 8.6

Feature	Description
Virtual Appliance enhancements	• Virtual appliances can now be deployed on a KVM hypervisor running on the following Linux platforms: – Red Hat Enterprise Linux Server 7.0 – Ubuntu Server 14.04.1 LTS Thin provisioning is supported for disk storage. • You can configure the Cisco appliance license and configuration files to load automatically upon initial startup. For details, see the *Cisco Content Security Virtual Appliance Installation Guide*, available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html **Important!** See Virtual Appliance Running on KVM Hangs on Reboot, page 6.

What's New in Cisco AsyncOS 8.5

Feature	Description
High Availability	This release provides a built-in high availability option suitable for deployments in which the appliance runs in explicit mode with a proxy. For more information, see the "Connect, Install, and Configure" chapterin the User Guide.
2048-bit certificates	The key length for SSL certificates generated or processed by the appliance is now 2048 bits.
LDAP authentication	LDAP protocol is now supported for authenticating administrative users of the appliance.
Volume and Time Quotas	You can apply time and volume quotas to access policies and decryption policies. Quotas allow individual users to continue accessing an Internet resource (or a class of Internet resources) until they exhaust the data volume or time limit imposed.

Feature	Description
Web Security Virtual Appliance enhancements	• Support for VMWare ESXi 5.5 • Support for thin provisioning in ESXi • Now, after the virtual appliance license expires, there is a six-month grace period during which the appliance continues to process web transactions, but without security services You can configure the appliance to send you alerts when the license expiration date approaches. • Evaluation feature keys can now be deployed on virtual appliances
Authentication by machine ID	For deployments in Connector mode with Active Directory, this release introduces the option to authorize access based on device ID.
Advanced Malware Protection enhancements	• Advanced Malware Protection can now detect malware in archived or compressed files. • You can now select the interface used to communicate with an AMP server. • File analysis now supports analysis of additional file types. Supported file types are determined by the cloud service and can change at any time. When you configure the File Analysis feature, you can choose which file types to send for analysis, and you can choose to receive alerts when the options change. For more information, see "Which Files Can Have their Reputation Evaluated and Be Sent for Analysis?" in the Release Notes, and the chapter "File Reputation and File Analysis" in the on-line help or User Guide for information about supported file types and alerts.
AAA Audit logging	AsyncOS is enhanced to standardize AAA-related logging across multiple logs, and to centralize them into a central log subscription. This new log subscription will be exportable via syslog.
Password security enhancements	The following password enhancements have been introduced for locally-defined administrative users: • Show a password strength indicator to a user entering a new password. Password strength is enforced by the password requirements that you specify. • Disallow certain words in passwords. (You upload a list of forbidden words to the appliance.) • The option to generate a password by clicking a button. For more information, see the "Setting Password Requirements for Administrative Users" and "Adding Local User Accounts" sections in the User Guide.
Web Tracking enhancement	There is a new "All Malware" option when you filter web tracking results by Malware Threat.
Cisco Content Security Management Virtual Appliance	You can now manage multiple Web Security appliances with a virtual content security management appliance that has the same functionality as a physical hardware appliance.

Feature	Description
Trusted Root Certificate management	Trusted Root Certificate management was moved from Security Services > HTTPS Proxy to Network > Certificate Management.
DNS server failover	If the primary DNS server is non-responsive for a user-specified number of queries, it is considered to have failed and queries are automatically directed to the secondary server.

Release Classification

Each release is identified by the release type (ED - Early Deployment, GD - General Deployment, etc.) For an explanation of these terms, see http://www.cisco.com/c/dam/en/us/products/collateral/security/web-security-appliance/content-security-release-terminology.pdf.

Upgrade Paths

There are no upgrade paths to this release.

Installation Notes

- Compatibility Details
- Deploying a Virtual Appliance
- Configuration Files

Compatibility Details

- Compatibility with Cisco AsyncOS for Security Management
- IPv6 and Kerberos Not Available in Cloud Connector Mode
- Functional Support for IPv6 Addresses
- Availability of Kerberos Authentication for Operating Systems and Browsers

Compatibility with Cisco AsyncOS for Security Management

For compatibility between this release and AsyncOS for Cisco Content Security Management releases, see the compatibility matrix at: http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html.

IPv6 and Kerberos Not Available in Cloud Connector Mode

When the appliance is configured in Cloud Connector mode, unavailable options for IPv6 addresses and Kerberos authentication appear on pages of the web interface. Although the options appear to be available, they are not supported in Cloud Connector mode. Do not attempt to configure the appliance to use IPv6 addresses or Kerberos authentication when in Cloud Connector mode.

Functional Support for IPv6 Addresses

Features and functionality that support IPv6 addresses:

- Command line and web interfaces. You can access WSA using http://[2001:2:2::8]:8080 or https://[2001:2:2::8]:8443
- Performing Proxy actions on IPv6 data traffic (HTTP/HTTPS/SOCKS/FTP)
- IPv6 DNS Servers
- WCCP 2.01 (Cat6K Switch) and Layer 4 transparent redirection
- Upstream Proxies
- Authentication Services
  - Active Directory (NTLMSSP, Basic, and Kerberos)
  - LDAP
  - SaaS SSO
  - Transparent User Identification through CDA (communication with CDA is IPv4 only)
  - Credential Encryption
- Web Reporting and Web Tracking
- External DLP Servers (communication between WSA and DLP Server is IPv4 only)
- PAC File Hosting

Features and functionality that require IPv4 addresses:

- Internal SMTP relay
- External Authentication
- Log subscriptions push method: FTP, SCP, and syslog
- NTP servers
- Local update servers, including Proxy Servers for updates
- Authentication services
- AnyConnect Security Mobility
- Novell eDirectory authentication servers
- Custom logo for end-user notification pages
- Communication between the Web Security appliance and the Security Management appliance
- WCCP versions prior to 2.01
- SNMP

Availability of Kerberos Authentication for Operating Systems and Browsers

You can use Kerberos authentication with these operating systems and browsers:

- Windows servers 2003, 2008, 2008R2 and 2012
- Latest releases of Safari and Firefox browsers on Mac (OSX Version 10.5+)
- IE (Version 7+) and latest releases of Firefox and Chrome browsers on Windows 7 and XP.

Kerberos authentication is not available with these operating systems and browsers:

- Windows operating systems not mentioned above
- Browsers not mentioned above
- iOS and Android

Deploying a Virtual Appliance

To deploy a virtual appliance, see the *Cisco Content Security Virtual Appliance Installation Guide*, available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html.

Migrating from a Hardware Appliance to a Virtual Appliance

There is no migration path from hardware appliances to this release.

Configuration Files

Generally, configuration files from earlier AsyncOS releases are incompatible with later AsyncOS releases and vice-versa.

Documentation Updates

The following information supplements information in the Online Help and/or User Guide for this release

Virtual Appliance Running on KVM Hangs on Reboot

This is a KVM issue. For more information, see https://www.mail-archive.com/kvm@vger.kernel.org/msg103854.html and https://bugs.launchpad.net/qemu/+bug/1329956.

Step 1 Check the following:

```
cat /sys/module/kvm_intel/parameters/enable_apicv
```

Step 2 If the above value is set to Y:

a. Stop your virtual appliances and reinstall the KVM kernel module:

```
rmmod kvm_intel
```

```
modprobe kvm_intel enable_apicv=N
```

b. Restart your virtual appliance.

The Force Reset Option is Not Supported (KVM Deployments)

The Force Reset option in KVM is not supported, especially during startup.

This is the equivalent of pulling the plug on a hardware appliance.

Network Connectivity Works Initially on KVM Deployments, Then Fails

Problem Network connectivity is lost after previously working.

Solution This is a KVM issue. See the section on "KVM: Network connectivity works initially, then fails" in the OpenStack documentation at http://docs.openstack.org/admin-guide-cloud/content/section_network-troubleshoot.html.

Slow Performance, Watchdog Issues, and High CPU Usage on KVM Deployments

Problem Appliance performance is slow, watchdog issues occur, and the appliance shows unusually high CPU usage when running on an Ubuntu virtual machine.

Solution Install the latest Host OS updates from Ubuntu.

General Troubleshooting for Virtual Appliances Running on Linux Hosts

Problem Issues with virtual appliances running on KVM deployments may be related to host OS configuration issues.

Solution See the troubleshooting section and other information in the *Virtualization Deployment and Administration Guide*, available from https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/pdf/Virtualization_Deployment_and_Administration_Guide/Red_Hat_Enterprise_Linux-7-Virtualization_Deployment_and_Administration_Guide-en-US.pdf.

A Proxy is Not Supported for Communications with the File Analysis Server

Using a proxy is not supported for communications between the Web Security appliance and the file analysis service in the cloud, even if an upstream proxy is transparent to the Web Security appliance and communications with the File Reputation service use a proxy.

Which Files Can Have their Reputation Evaluated and Be Sent for Analysis?

The criteria for evaluating a file's reputation and for sending files for analysis may change at any time. Criteria are available only to registered Cisco customers. See *File Criteria for Advanced Malware Protection Services for Cisco Content Security Products*, available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html.

In order to access this document, you must have a Cisco customer account with a support contract. To register, visit https://tools.cisco.com/RPF/register/register.do.

Known and Resolved Issues

Use the Cisco Bug Search Tool to find information about known and fixed defects.

Bug Search Tool Requirements

Register for a Cisco account if you do not have one. Go to https://tools.cisco.com/RPF/register/register.do.

Lists of Known and Fixed Issues

Known issues	There are no known issues in this release.
Fixed issues	This release does not include fixes to issues in previous releases.

Finding Other Bugs

Step 1 Go to https://tools.cisco.com/bugsearch/.

Step 2 Log in with your Cisco account credentials.

Step 3 Enter search criteria.

Step 4 If you have questions or problems, click the **Help** or **Feedback** links at the top right side of the tool.

Related Documentation

Documentation for this product is available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html.

Documentation for Cisco Content Security Management Appliances is available from http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html.

Support

Knowledge Base

You can access the Cisco Knowledge Base on the Cisco Customer Support site at the following URL:

http://www.cisco.com/web/ironport/knowledgebase.html

Note You need a Cisco.com User ID to access the site. If you do not have a Cisco.com User ID, you can register for one here: `https://tools.cisco.com/RPF/register/register.do`

Cisco Support Community

Cisco Support Community is an online forum for Cisco customers, partners, and employees. It provides a place to discuss general web security issues as well as technical information about specific Cisco products. You can post topics to the forum to ask questions and share information with other Cisco users.

Access the Cisco Support Community for web security and associated management:

https://supportforums.cisco.com/community/5786/web-security

Customer Support

International: Visit http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Support Site: Visit http://www.cisco.com/en/US/products/ps11169/serv_group_home.html

For non-critical issues, you can also access customer support from the appliance. For instructions, see the User Guide or online help.