Release Notes for AsyncOS 9.1.x for Cisco Web Security Appliances

Published: January 11, 2016

Revised: April 20, 2018

Contents

Cisco Systems, Inc.
www.cisco.com

What's New

Note **For AsyncOS 9.1.3 versions**: After an upgrade, if the appliance is configured with Kerberos, the authentication processes will exhibit high CPU usage. We recommend reducing the number of concurrent Kerberos authentications, or using IP surrogates with surrogate timeouts above 15 minutes. This will prevent latency for end user web requests. For the traffic that cannot use IP surrogates, use an identification profile and session cookies-based authentication surrogates. Be aware that when you commit changes to Identification Profiles, end-users must re-authenticate.

New in Release 9.1.3-021 (MD - Maintenance Deployment - Refresh)

This release contains the following upgrades and enhancements:

- Samba version has been upgraded to version 4.5.8.
- SMB v2 and v3 protocols are supported.
- Web proxy custom headers character limit is increased to 998.

This release contains a number of bug fixes; see the "Fixed issues" search in Lists of Known and Fixed Issues, page 18 for additional information.

New in Release 9.1.3-016 (MD - Maintenance Deployment)

- Samba version has been upgraded to version 4.5.8.
- SMB v2 and v3 protocols are supported.
- Web proxy custom headers character limit is increased to 998.
- This release contains a number of bug fixes; see the "Fixed issues" search in Lists of Known and Fixed Issues, page 18 for additional information.

New in Release 9.1.2-029 (GD - General Deployment)

- This release contains a number of bug fixes; see the "Fixed issues" search in Lists of Known and Fixed Issues, page 18 for additional information.

New in Release 9.1.2-022 (MD - Maintenance Deployment)

- This release contains a number of bug fixes; see the "Fixed issues" search in Lists of Known and Fixed Issues, page 18 for additional information.

New in Release 9.1.2-010 (GD - General Deployment)

- New subcommands added to `advancedproxyconfig` > `miscellaneous` CLI command:
  - `Do you want to enable URL lower case conversion for velocity regex?` – Let's you enable or disable default regex conversion to lower case for case-insensitive matching. Use if you are experiencing issues with case sensitivity.
  - `Do you want to forward TCP RST sent by server to client?` – Let's you enable and disable TCP RST (reset) forwarding. Enable only if TCP RST flags are not being forwarded properly.

New in Release 9.1.1-074 (GD - General Deployment)

- We added a new CLI command, `networktuning`, which can be used to change send and receive buffer sizes. Use carefully; see the section "Upload/Download Speed Issues" in the Troubleshooting chapter of the user guide for more information.
- New subcommands for listing and deleting unprocessed report data added to `diagnostic` > `reporting` CLI command:
  - `DBSTATS` – List DB and Export Files
    (Displays the list of unprocessed files and folders under export_files and always_onbox folders.)
  - `DELETEEXPORTDB` – Delete Export Files
    (Deletes all unprocessed files and folders under export_files and always_onbox folders.)
  - `DELETEJOURNAL` – Delete Journal Files
    (Deletes all aclog_journal_files.)

Release 9.1.1-073 - Deprovisioned

This release was deprovisioned on July 20, 2016.

New in Release 9.1.1-041 (LD - Limited Deployment)

This release supports:

- Virtual appliances and 70-series (except S170) and 80-series hardware.
- Migration of configuration files from the above appliances to the new 90-series hardware.

New in Release 9.1.0-157

- Support for 90-series hardware appliance models with extended hard drive, fiber-optic NIC, dual AC power supply, and DC power supply. For details, see http://www.cisco.com/c/en/us/products/collateral/security/content-security-management-appliance/data_sheet_c78-729630.html.
- Bug fixes. See Lists of Known and Fixed Issues, page 18.

New in Release 9.1.0-070

This release supports the new 90-series hardware models:

- S190
- S390
- S690

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.

Supported Hardware

Release 9.1.2-022

- All virtual appliance models.
- The following hardware models:
  - S170
  - S370
  - S670
  - S380
  - S680
  - S190
  - S390
  - S690

Release 9.1.2-010

- All virtual appliance models.
- The following hardware models:
  - S170
  - S370
  - S670
  - S380
  - S680
  - S190
  - S390
  - S690

Release 9.1.1-074

- All virtual appliance models.
- The following hardware models:
  - S170
  - S370
  - S670
  - S380
  - S680
  - S190
  - S390
  - S690

Some pre-90-series hardware models require a memory upgrade before you can install or upgrade to this AsyncOS release. For more information, see http://www.cisco.com/c/en/us/support/docs/field-notices/638/fn63931.html

Release 9.1.1-041

- All virtual appliance models.
- The following hardware models:
  - S370
  - S670
  - S380
  - S680
  - S190
  - S390
  - S690

Note This release does not support S170 hardware.

Some pre-90-series hardware models require a memory upgrade before you can install or upgrade to this AsyncOS release. For more information, see http://www.cisco.com/c/en/us/support/docs/field-notices/638/fn63931.html

Release 9.1.0 (Builds -070 and -157)

This release supports only the new 90-series hardware models. Virtual appliances are not supported.

Upgrade Paths

Important! After an upgrade, on S190, S390, and S690 appliances which have read-only root partitions, the output of the `ipcheck` command may display the usage of the root partition as more than 100%. Please be advised that this normal, and will not have any functional impact.

Note For important information about hardware upgrades, see Migrating from Older Hardware to x90 Hardware Appliances, page 10.

- Upgrades to Release 9.1.3-021 (MD - Maintenance Deployment - Refresh), page 6
- Upgrades to Release 9.1.3-016 (MD - Maintenance Deployment), page 6
- Upgrades to Release 9.1.2-022 (MD - Maintenance Deployment), page 7
- Upgrades to Release 9.1.2-010 (GD - General Deployment), page 7
- Upgrades to Release 9.1.1-074 (GD - General Deployment), page 8

- Upgrades to Release 9.1.1-041 (LD - Limited Deployment), page 8
- Upgrades to Release 9.1.0-157 (LD - Limited Deployment), page 9

Upgrades to Release 9.1.3-021 (MD - Maintenance Deployment - Refresh)

Note Before you start the upgrade process, see Pre-upgrade Requirements, page 9 and Installation and Upgrade Notes, page 9.

You can upgrade to release 9.1.3-021 of AsyncOS for Cisco Web Security appliances from the following versions:

- 8-5-3-069
- 8.5.4-038
- 9.0.1-162
- 9.1.0-157
- 9.1.1-074
- 9.1.2-010
- 9.1.2-022
- 9.1.2-033
- 9.1.2-039
- 9.1.3-016

Upgrades to Release 9.1.3-016 (MD - Maintenance Deployment)

Note Before you start the upgrade process, see Pre-upgrade Requirements, page 9 and Installation and Upgrade Notes, page 9.

You can upgrade to release 9.1.3-016 of AsyncOS for Cisco Web Security appliances from the following versions:

- 8-5-3-069
- 8.5.4-038
- 9.0.1-162
- 9.1.0-157
- 9.1.1-074
- 9.1.2-010
- 9.1.2-022
- 9.1.2-033
- 9.1.2-039

Upgrades to Release 9.1.2-022 (MD - Maintenance Deployment)

Note Before you start the upgrade process, see Pre-upgrade Requirements, page 9 and Installation and Upgrade Notes, page 9.

You can upgrade to release 9.1.2-022 of AsyncOS for Cisco Web Security appliances from the following versions:

- 8-5-3-069
- 8.5.4-038
- 9.0.1-162
- 9.0.1-204
- 9.1.1-074
- 9.1.2-010

Upgrades to Release 9.1.2-010 (GD - General Deployment)

Note Before you start the upgrade process, see Pre-upgrade Requirements, page 9 and Installation and Upgrade Notes, page 9.

You can upgrade to release 9.1.2-010 of AsyncOS for Cisco Web Security appliances from the following versions:

- 8-5-3-069
- 9.0.1-162
- 9.0.1-204
- 9.1.1-074
- 9.1.1-507
- 9.1.1-508
- 9.1.1-510

Upgrades to Release 9.1.1-074 (GD - General Deployment)

Note Before you start the upgrade process, see Pre-upgrade Requirements, page 9 and Installation and Upgrade Notes, page 9.

You can upgrade to release 9.1.1-074 of AsyncOS for Cisco Web Security appliances from the following versions:

- 7.7.0-761
- 7.7.0-809
- 8.0.6-119
- 8.0.7-142
- 8.0.7-149
- 8.0.8-113
- 8.0.8-118
- 8.5.1-021
- 8.5.2-024
- 8.5.2-027
- 8.5.3-051
- 8.5.3-064
- 8.5.3-069
- 8.5.4-038
- 8.8.0-085
- 9.0.1-162
- 9.0.1-204
- 9.1.0-070
- 9.1.0-157
- 9.1.0-158
- 9.1.1-028
- 9.1.1-041
- 9.1.1-062
- 9.1.1-073

Release 9.1.1-073 Deprovisioned

This release was deprovisioned on July 20, 2016.

Upgrades to Release 9.1.1-041 (LD - Limited Deployment)

Note Before you start the upgrade process, see Pre-upgrade Requirements, page 9 and Installation and Upgrade Notes, page 9.

You can upgrade to release 9.1.1-041 of AsyncOS for Cisco Web Security appliances from the following versions:

- 7.7.0-761
- 7.7.0-809
- 8.0.6-119
- 8.0.7-142
- 8.0.7-149
- 8.0.8-113
- 8.0.8-118
- 8-5-1-021
- 8-5-2-024
- 8-5-2-027
- 8-5-3-051
- 8-5-3-064
- 8-5-3-069
- 8.8.0-085
- 9.0.1-162
- 9.1.0-070
- 9.1.0-157
- 9.1.0-158

Upgrades to Release 9.1.0-157 (LD - Limited Deployment)

Note Before you start the upgrade process, see Installation and Upgrade Notes, page 9.

You can upgrade to release 9.1.0-157 of AsyncOS for Cisco Web Security appliances from the following version:

- 9.1.0-070

Upgrades to Release 9.1.0-070

Upgrades to this AsyncOS release are not supported.

Pre-upgrade Requirements

Update RAID Controller Firmware (Older Hardware Only)

The following does NOT apply to 90-series hardware.

Before upgrading the AsyncOS software, update the RAID controller firmware as described in *Cisco Update for RAID Controller Firmware (For S360/S370/S660/S670 only, reboot required) Release Notes*.

Check Post-upgrade Requirements Before Upgrading

Some existing functionality will not work after upgrade until you make changes. To minimize downtime, familiarize yourself with and prepare for those requirements before upgrading. See Important! Actions Required After Upgrading.

Installation and Upgrade Notes

- Migrating from Older Hardware to x90 Hardware Appliances
- Compatibility Details
- Deploying a Virtual Appliance
- Configuration Files
- Demo Security Certificate Encryption Strength
- Post-upgrade Reboot
- Changes in Behavior

Migrating from Older Hardware to x90 Hardware Appliances

Release 9.1.1-041

Migration of configurations from x60 hardware is not supported.

Instructions in this topic apply only to configuration migration from x70 or x80 hardware or from virtual appliances.

Note In order to migrate your configuration, both the old hardware and the new hardware must be running the identical AsyncOS version, including build number. The AsyncOS version you choose must be supported on both hardware models.

Step 1 Upgrade your new 90-series hardware to the latest supported version of AsyncOS (build number is important.)

Step 2 Upgrade your old appliance to the same AsyncOS release, including build number.

Step 3 Save the configuration file from your upgraded hardware appliance.

Step 4 Load the configuration file from the old appliance onto the new appliance.

If your old and new appliances have different IP addresses, deselect Load Network Settings before loading the configuration file.

Step 5 Commit your changes.

Step 6 Go to Network > Authentication and join the domain again. Otherwise identities won't work.

Release 9.1.0 (Builds -070 and -157)

Release 9.1.0 does not support x60, x70, or x80 hardware and thus configuration files cannot be migrated from those appliances. You must manually configure new appliances running this release.

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

Note In order to migrate your configuration, both the old and the new appliances must be running the identical AsyncOS version, including build number. The AsyncOS version you choose must be supported on both appliances.

Step 1 Set up your virtual appliance with a supported AsyncOS release using the documentation described in Deploying a Virtual Appliance, page 12.

Step 2 Upgrade your hardware appliance to this AsyncOS release.

Step 3 Save the configuration file from your upgraded hardware appliance.

Step 4 Load the configuration file from the hardware appliance onto the virtual appliance.

If your hardware and virtual appliances have different IP addresses, deselect Load Network Settings before loading the configuration file.

Step 5 Commit your changes.

Step 6 Go to Network > Authentication and join the domain again. Otherwise identities won’t work.

Configuration Files

When you upgrade AsyncOS for Web from the web interface or Command Line Interface (CLI), the configuration is saved to file in the /configuration/upgrade directory. You can access the upgrade directory using an FTP client. Each configuration file name is appended with the version number, and passwords in the configuration file are masked so they are not human readable. (bug 47966)

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

Demo Security Certificate Encryption Strength

This section applies only to upgrades from releases earlier than AsyncOS 8.5.

The encryption strength of the demo security certificate is 1024 bits both before and after upgrade to AsyncOS 8.5 and later.

Post-upgrade Reboot

You must reboot the Web Security appliance after you upgrade AsyncOS for Web.

Changes in Behavior

This section describes changes in behavior from previous versions of AsyncOS for Web that may affect the appliance configuration after you upgrade to the latest version.

- Default Cipher Suites for Proxy Services, page 13
- Special Characters No Longer Allowed in Regular Expressions, page 13
- Special Characters Allowed in Active Directory User Names, page 14
- Limit on Number of Concurrent Sessions, page 14
- List of Available Upgrades, page 14
- Support Requests Require CCO ID and Support Contract, page 14
- New Certificate Management Page, page 14
- Exporting Web Tracking Data, page 14
- SNMP Monitoring, page 14
- X-Authenticated-Groups Header Format, page 14

Default Cipher Suites for Proxy Services

From AsyncOS 9.1.1 onwards, the default cipher suites available for Proxy Services are modified to include only secure cipher suites. If you are upgrading to AsyncOS 9.1.x, see Change the Default Proxy Services Cipher Suites to Cisco Recommended Cipher Suites, page 16.

Special Characters No Longer Allowed in Regular Expressions

You can no longer use “`.*`” to begin or end a regular expression. You also cannot use “./” in a regular expression intended to match a URL, nor can you end such an expression with a dot.

Special Characters Allowed in Active Directory User Names

Prior to AsyncOS 9.0, attempts to join an Active Directory domain with a user name that included special characters would produce an error. Now the following special characters can be used in domain user names: ` ~ ( ) { } ! # ^ _ $ & (however, note that % is not yet supported).

Limit on Number of Concurrent Sessions

Beginning in AsyncOS 8.5, individual users are limited to a maximum of 10 concurrent sessions; this total includes both CLI and Web interface sessions.

List of Available Upgrades

Beginning in AsyncOS 8.5, all available releases appear in the list of available upgrades, including releases that would previously have been provisioned only to a limited number of customers as a limited release.

Each release in the list is identified by the release type (ED - Early Deployment, GD - General Deployment, MD - Maintenance 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.

Support Requests Require CCO ID and Support Contract

Beginning in AsyncOS 8.5, in order to open a support request from the appliance, you must enter a CCO ID and a support contract ID.

New Certificate Management Page

Beginning in AsyncOS 8.5, certificate management functionality has been moved from the Security Services > HTTPS Proxy page to a new, stand-alone page: Network > Certificate Management.

Exporting Web Tracking Data

Previously, when exporting web tracking data as CSV, the data was sorted by timestamp. Beginning in AsyncOS 8.5, this data is not sorted.

SNMP Monitoring

Beginning in AsyncOS 8.5, the following functionality is different from previous implementations:

Message authentication and encryption are mandatory when enabling SNMPv3. Passwords for authentication and encryption should be different. The encryption algorithm can be AES (recommended) or DES. The authentication algorithm can be SHA-1 (recommended) or MD5.

X-Authenticated-Groups Header Format

Beginning in AsyncOS 8.5, if LDAP authentication and External Data Loss Prevention are configured on the appliance, AsyncOS sends the X-Authenticated-Groups header in this format:

LDAP://(*LDAP server name*)/(*groupname*).

Previously, the format was LDAP://(*groupname*). This software change may require changes to policies or other automation relying on the X-Authenticated-Groups header. [Defect: CSCum91801]

Removed "Unknown" and "Unnamed" Malware Reporting Options

Beginning in AsyncOS 7.5.1, all malware transactions are categorized, and the Malware Category "Unknown" and the Malware Threat "Unnamed" no longer exist. Thus, you cannot filter the Web Tracking report by "Unknown" or "Unnamed."

However, some older malware data may still appear as "Unnamed Malware Threat" and "Unknown Malware Category"; links to Web Tracking reports and filtering within Web Tracking will not be available for this now-incorrectly categorized information.

Upgrading AsyncOS for Web

Before You Begin

- Perform pre-upgrade requirements, including updating the RAID controller firmware. See Pre-upgrade Requirements, page 9.
- Log in as Administrator.

Step 1 On the System Administration > Configuration File page, save the XML configuration file off the Web Security appliance.

Step 2 On the System Administration > System Upgrade page, click **Available Upgrades**.

The page refreshes with a list of available AsyncOS for Web upgrade versions.

Step 3 Click **Begin Upgrade** to start the upgrade process. Answer the questions as they appear.

Step 4 When the upgrade is complete, click **Reboot Now** to reboot the Web Security appliance.

Note **Important!** Do not interrupt power to the appliance for any reason (even to troubleshoot an upgrade issue) until at least 20 minutes have passed since you rebooted. If you have an x80 or x90 hardware appliance, do not push the power button until all LEDs are lit. If you have a virtual appliance, do not use the hypervisor or host OS tools to reset, cycle, or power off the virtual machine.

Step 5 Verify that the browser loads the new online help content in the upgraded version of AsyncOS:

Exit the browser and then open it before viewing the online help. This clears the browser cache of any outdated content.

Step 6 Configure new functionality as desired. New features are typically not enabled by default.

Important! Actions Required After Upgrading

In order to ensure that your appliance continues to function properly after upgrade, you must address the following items:

- Change the Default Proxy Services Cipher Suites to Cisco Recommended Cipher Suites, page 16
- Upgrading from non-ISE Releases and AsyncOS 8.5 with ISE Preview, page 16
- Virtual Appliances: Required Changes for SSH Security Vulnerability Fix, page 17
- File Analysis: Required Changes to View Analysis Result Details in the Cloud, page 17
- File Analysis: Verify File Types To Be Analyzed, page 17
- Unescaped Dots in Regular Expressions, page 17

Change the Default Proxy Services Cipher Suites to Cisco Recommended Cipher Suites

From AsyncOS 9.1.1 onwards, the default cipher suites available for Proxy Services are modified to include only secure cipher suites.

However, if you are upgrading to AsyncOS 9.1.x, the default Proxy Services cipher suites are not modified. For enhanced security, Cisco recommends that you change the default Proxy Services cipher suites to the Cisco recommended cipher suites after the upgrade. Do the following:

Procedure

Step 1 Log in to your appliance using the web interface.

Step 2 Click **System Administration** > **SSL Configuration.**

Step 3 Click **Edit Settings**.

Step 4 Under **Proxy Services**, set the **Cipher(s) to Use** field to the following field:

```
EECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA:!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA
```

Caution Make sure that you paste the above string as a single string with no carriage returns or spaces.

Step 5 Submit and commit your changes.

You can also use the `sslconfig` command in CLI to perform the above steps.

Upgrading from non-ISE Releases and AsyncOS 8.5 with ISE Preview

All AsyncOS versions that did not include ISE support (that is, all versions prior to 8.5.0-497), and the limited-availability AsyncOS 8.5 “ISE Preview” release, did not require the Admin and pxGrid certificates, which are necessary in all subsequent Cisco AsyncOS releases in order to enable ISE support. Therefore, when you upgrade from a non-ISE release, or from an ISE Preview installation with

ISE enabled, the ISE feature will not operate correctly until the two additional certificates are provided (go to **Network** > **Identity Services Engine**).

Virtual Appliances: Required Changes for SSH Security Vulnerability Fix

Requirements in this section were introduced in AsyncOS 8.8.

The following security vulnerability will be fixed during upgrade if it exists on your appliance: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150625-ironport.

If you did not patch this issue before upgrading, you will see a message during upgrade stating that it has been fixed. If you see this message, the following actions are required to return your appliance to full working order after upgrade:

- Remove the existing entry for your appliance from the known hosts list in your ssh utility. Then ssh to the appliance and accept the connection with the new key.
- If you use SCP push to transfer logs to a remote server (including Splunk): Clear the old SSH host key for the appliance from the remote server.
- If your deployment includes a Cisco Content Security Management Appliance, see important instructions in the Release Notes for that appliance.

File Analysis: Required Changes to View Analysis Result Details in the Cloud

The requirement in this section was introduced in AsyncOS 8.8.

If you have deployed multiple content security appliances (web, email, and/or management) and you want to view detailed file analysis results in the cloud for all files uploaded from any appliance in your organization, you must configure an appliance group on each appliance after upgrading. To configure appliance groups, see the “File Reputation Filtering and File Analysis” chapter in the user guide PDF. (This PDF is more current than the online help in AsyncOS 8.8.)

File Analysis: Verify File Types To Be Analyzed

The File Analysis cloud server URL changed in AsyncOS 8.8, and as a result, the file types that can be analyzed may have changed after upgrade. You should receive an alert if there are changes. To verify the file types selected for analysis, select **Security Services > Anti-Malware and Reputation** and look at the Advanced Malware Protection settings.

Unescaped Dots in Regular Expressions

Following upgrades to the regular-expression pattern-matching engine, you may receive an alert regarding unescaped dots in existing pattern definitions after updating your system. Any unescaped dot in a pattern that will return more than 63 characters after the dot will be disabled by the Velocity pattern-matching engine, and an alert to that effect will be sent to you, and you continue to receive an alert following each update until you correct or replace the pattern. Generally, unescaped dots in a larger regular expression can be problematic and should be avoided.

Documentation Updates

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

Sophos No Longer Scans Archive Files

As of AsyncOS 9.0, scanning of archive (.zip) files has been disabled in the Sophos scanner.

Additional Information

The User Guide PDF may be more current than the online help. To obtain the User Guide PDF and other documentation for this product, click the **View PDF** button in the online help or visit the URL shown in Related Documentation, page 20.

Known and Fixed Issues

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

- Requirements for Access to Bug Information, page 18
- Lists of Known and Fixed Issues, page 18
- Finding Information about Known and Resolved Issues, page 20

Requirements for Access to Bug Information

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 and Fixed Issues in Release 9.1.3-021

Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=9.1.3&sb=afr&sts=open&svr=3nH&bt=custV
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=9.1.3-021&sb=fr&svr=3nH&bt=custV

Known and Fixed Issues in Release 9.1.3-016

Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=9.1.3&sb=afr&sts=open&svr=3nH&bt=custV
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=9.1.3-016&sb=fr&svr=3nH&bt=custV

Known and Fixed Issues in Release 9.1.2-022

Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=9.1.2&sb=afr&sts=open&svr=3nH&bt=custV
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=9.1.2-022&sb=fr&svr=3nH&bt=custV

Known and Fixed Issues in Release 9.1.2-010

Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=9.1.2&sb=afr&sts=open&svr=3nH&bt=custV
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=9.1.2-010&sb=fr&svr=3nH&bt=custV

Known and Fixed Issues in Release 9.1.1-074

Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=9.1.1&sb=afr&sts=open&svr=3nH&bt=custV
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=9.1.1-074&sb=fr&svr=3nH&bt=custV

Known and Fixed Issues in Release 9.1.1-041

Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=9.1.1&sb=afr&sts=open&svr=3nH&bt=custV
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=9.1.1-041&sb=fr&svr=3nH&bt=custV

Known and Fixed Issues in Release 9.1.0-157

Known Issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=9.1.0&sb=anfr&sts=open&bt=custV
Fixed Issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=9.1.0-157&sb=fr&svr=3nH&bt=custV

Known and Fixed Issues in Release 9.1.0-070

Known Issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=9.1.0&sb=anfr&sts=open&srtBy=byRel&bt=custV
Fixed Issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=9.1.0-070&sb=fr&svr=3nH&srtBy=byRel&bt=custV

Finding Information about Known and Resolved Issues

Use the Cisco Bug Search Tool to find the most current information about known and resolved defects in shipping releases.

Note If you have questions or problems, click the **Help** or **Feedback** links at the top right side of the tool. There is also an interactive tour; to view it, click the link in the orange bar above the search fields.

Before You Begin

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

Procedure

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

Step 2 Log in with your Cisco account credentials.

Step 3 Click **Select from list** > **Security** > **Web Security** > **Cisco Web Security Appliance**, and click **OK**.

Step 4 In Releases field, enter the version of the release, for example, 9.1.

Step 5 Depending on your requirements, do one of the following:

- To view the list of resolved issues, select **Fixed in these Releases** from the Show Bugs drop down.
- To view the list of known issues, select **Affecting these Releases** from the Show Bugs drop down and select **Open** from the Status drop down.

Related Documentation

Hardware installation and maintenance information is available from: http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html

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

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

Note To get support for virtual appliances, call Cisco TAC and have your Virtual License Number (VLN) number ready.

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

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

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