Release Notes for AsyncOS 11.0.0 for Cisco Web Security Appliances

Published: April 30, 2017

Revised: June 5, 2018

Contents

Cisco Systems, Inc.
www.cisco.com

What's New

Feature	Description
Cisco Defense Orchestrator Integration	You can connect your appliances with Cisco Defense Orchestrator and analyze security policy configuration of your appliances to identify and resolve policy inconsistencies, model policy changes to validate their impact, and orchestrate policy changes to achieve consistency and maintain clarity in security posture. The Cisco Defense Orchestrator is a cloud-based platform that helps network operations staff establish and maintain an end-to-end security posture by managing security policies across Cisco security devices. See the "Connect the Appliance to Cisco Defense Orchestrator" chapter in the user guide or online help.
Simplified appliance registration on CTA	You can use the CTA Template option to automatically select fields and criteria required to send W3C logs to the Cisco Cognitive Threat Analytics (CTA) system. See the "Monitor System Activity Through Logs" chapter in the user guide or online help.
Secondary DNS servers	You can now specify secondary DNS servers to resolve host name queries not resolved by the primary name servers. You can also set priority levels for the servers. The secondary DNS servers receive host name queries when the primary DNS servers return the following errors: • No Error, no answer section received. • Server failed to complete request, no answer section. • Name Error, no answer section received. • Function not implemented. • Server Refused to Answer Query. See the "Connect, Install, and Configure" chapter in the user guide or online help.
`supportrequest` command enhancement	You can send a set of system and configuration information to be attached to the service request automatically, if you specify the service request number in the optional step while using the `supportrequest` command. See the "Command Line Interface" appendix in the user guide or online help.
Virtual Appliance Enhancement	Virtual appliances can now be deployed on Microsoft Hyper-V version 5.0. 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.

Configuration Changes and Constraints in Cisco Defense Orchestrator Mode

This section specifies the changes and constraints in your appliance and Cisco Defense Orchestrator after on-boarding your device to Cisco Defense Orchestrator.

There are no limitations in the appliance's web interface other than what is specified below. Authentication is not supported from the Cisco Defense Orchestrator.

For release 11.0, Cisco Defense Orchestrator supports policy management for the Web Security Appliance's global and non-global access policies, only. Use the appliance's web interface for all other configuration settings (including Authentication).

Note Constraints apply only to Access Policies and Reporting.

Constraints in the Web Security Appliance after on-boarding:

In the appliance, you will not be able to configure the features that are administered through the Cisco Defense Orchestrator. Configurations for these features are migrated to the Cisco Defense Orchestrator when the appliance is on-boarded. All other configuration settings in the appliance are set to default settings.

Except the features that are administered through the Cisco Defense Orchestrator, all other features will be available in your appliance.

After on-boarding, Access Policies are controlled through Cisco Defense Orchestrator. Exceptions are specified below. You can configure the following Access Policies features only in the Web Security Appliance:

- Access Policies - Policy Definitions
  - Protocols and User Agents
  - Anti-Malware and Reputation
- Custom URL Categories (External Live Feed Category)

You can configure the following features only in the Cisco Defense Orchestrator:

- Custom URL Categories (Local Custom Category) - This feature will become available shortly.
- URL Filtering, Applications, and Objects (except size and custom MIME type)
- Global and non global access policies
- Access Policies support:
  - Adding multiple access policies is supported.
  - Adding, reordering, deleting access policies is supported.
  - URL filtering (Predefined URL Category Filtering), applications, and objects (object types), with the following limitations:
  - Bandwidth limits for applications and application-types is not supported.
  - Object sizes, custom MIME types is not supported.
  - For archived objects, inspect is not supported.
  - Advanced membership definitions for access policies and identities are not supported.

- Range Request Forwarding is not supported.
- Time and volume quota management is not supported.
- Safe Search, Referred Exceptions, Site Content Rating are not supported for URLs.

If reporting through Cisco Defense Orchestrator is enabled:

- Summarized reports in the Cisco Defense Orchestrator will be available.
- Reporting will also be available in the Web Security Appliance.
- Reporting will not be available in the Security Management Appliance.

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 for This Release

The following models:

- S000V
- S100V
- S300V
- S600V
- x90
- x80
- x70 (Cisco Web Security Appliance S170 is not supported.)

Some 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

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 Before you start the upgrade process, see Pre-upgrade Requirements, page 5 and Installation and Upgrade Notes, page 5.

You can upgrade to release 11.0.0-641 of AsyncOS for Cisco Web Security appliances from the following versions:

- 8.0.8-118
- 8.5.3-069
- 8.5.4-038
- 9.0.1-162
- 9.1.0-157
- 9.1.1-074
- 9.1.2-022
- 9.1.2-029
- 10.0.0-233
- 10.1.0-204
- 10.1.1-230
- 10.5.0-358
- 11.0.0-613

Pre-upgrade Requirements

Update RAID Controller Firmware

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

Compatibility Details

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.

Note This release is not compatible with, and cannot be used with, the currently available Security Management releases. A compatible Security Management release will be available shortly.

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 and later)
- IE (Version 7 and later) and latest releases of Firefox and Chrome browsers on Windows 7 and later.

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

Step 1 Set up your virtual appliance with this AsyncOS release using the documentation described in Deploying a Virtual Appliance, page 7.

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.

Demo Security Certificate Encryption Strength

The encryption strength of the demo security certificate is 1024 bits both before and after upgrade to AsyncOS 8.5. With upgrade to AsyncOS 9.1.1, it is 2048 bits. With AsyncOS 10.5 and later, when FIPS mode is enabled, the demo security certificate strength is changed to 4096 bits.

Post-upgrade Reboot

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

Upgrading AsyncOS for Web

Before You Begin

Perform preupgrade requirements, including updating the RAID controller firmware. See Pre-upgrade Requirements, page 5.

Step 1 Log in as Administrator.

Step 2 On the System Administration > Configuration File page, save the XML configuration file off the Web Security appliance.

Step 3 On the System Administration > System Upgrade page, click **Available Upgrades**.

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

Step 4 Click **Begin Upgrade** to start the upgrade process. Answer the questions as they appear.

Step 5 When the upgrade is complete, click **Reboot Now** to reboot the Web Security appliance.

Note To verify the browser loads the new online help content in the upgraded version of AsyncOS, you must exit the browser and then open it before viewing the online help. This clears the browser cache of any outdated content.

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

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 from AsyncOS 9.x.x and later releases, 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.

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

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 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 12.

Known and Fixed Issues

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

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

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.0.0-641&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.0.0&sb=afr&sts=open&svr=3nH&bt=custV

Finding Information about Known and Resolved Issues

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

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, 11.0.

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.

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.

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

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

Support Site for legacy IronPort: Visit http://www.cisco.com/web/services/acquisitions/ironport.html.

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