Release Notes for AsyncOS 11.5.x for Cisco Web Security Appliances

Published: July 31, 2019

Contents

Cisco Systems, Inc.
www.cisco.com

What's New

What's New in AsyncOS 11.5.3-016 - MD (Maintenance Deployment)

This release contains a number of bug fixes; see the Known and Fixed Issues, page 21 for additional information.

What's New in AsyncOS 11.5.2-020 - MD (Maintenance Deployment)

Feature	Description
Enable or Disable Incremental Updates	You can use the CLI command `updateconfig` > `setup` to enable or disable incremental updates from the Web Reputation service. If you disable incremental updates, the appliance will continue to download the full updates from the Cisco server. **Note** Disabling incremental updates will result in delays in receiving updated web reputation information on the appliance. For more information, see the "Web Security Appliance CLI Commands" chapter in the user guide.
Support for Outbound ACL on the management port	A new subcommand OUTBOUNDACL is added to the CLI command `fipsconfig` to restrict IP addresses on the management port. Using this subcommand, you can configure IP addresses to which you want to restrict the appliance from making any outbound connections. This subcommand is available only in FIPS mode. You can perform the following actions using the subcommand OUTBOUNDACL: • Add New • Edit • Delete • Clear

Feature	Description
Support to configure login history	A new subcommand LOGINHISTORY is added to the CLI command `adminaccessconfig` to configure the number of days for which the login history is retained. Default value is 1 day. This is available in both FIPS and non-FIPS mode.
Support to configure maximum concurrent login sessions	A new subcommand `maxsessions` is added to the CLI command `adminaccessconfig` to configure the maximum number of concurrent sessions of the appliance through the Command Line Interface and web interface. Default value in FIPS mode is 3 and non-FIPS mode is 10. This is available in both FIPS and non-FIPS mode.
WBRS enhancement	Currently when the WBRS update fails, it will revert to factory default settings. The new WBRS enhancement ensures that if the WBRS update fails, or download of the files fail during the update process, the WBRS reverts to the previous version. It will not revert to factory default settings.

This release contains a number of bug fixes; see the Known and Fixed Issues, page 21 for additional information for additional information.

What's New in AsyncOS 11.5.1-125 - GD (General Deployment) Refresh

This release contains a number of bug fixes; see the Known and Fixed Issues, page 21 for additional information.

What's New in AsyncOS 11.5.1-124 - GD (General Deployment) Refresh

Feature	Description
Office 365 Web Service External URL Categories	You can configure your appliance with Microsoft Office 365 web service's external live feed which serves URLs and IPs. The web service URL must not contain a *ClientRequestId*, and must have JSON as the format. See the "Classify URLs for Policy Application" chapter in the user guide.

What's New in AsyncOS 11.5.1-115 - GD (General Deployment)

Feature	Description
Web Traffic Tap	You can configure your appliance to tap the HTTP and HTTPS web traffic that passes through the appliance and copy it to a Web Security appliance interface in-line with the real time data traffic.You can tap the traffic based on the policy filters that you define. The selected tap interface must be connected to an external security device for analysis, forensics, and archiving. See "Perform System Administration Tasks" chapter in the user guide. Four new sections are included in the Overview report page. The sections are: • Web Traffic Tap Status • Web Traffic Tap Summary • Tapped HTTP/HTTPS Traffic • Tapped Traffic Summary See "Web Security Appliance Reports" chapter in the user guide.
AMP Clear Cache	You can now clear the cache of AMP file reputation dispositions for clean, malicious, and unknown files. See "Configuring Security Services" chapter in the user guide.
AMP Upstream Proxy Settings for File Analysis	You can now configure an upstream proxy for file analysis. See "File Reputation Filtering and File Analysis" chapter in the user guide.
Support for Submitting Compressed Files for Cisco Threat Grid Analysis	You can now submit compressed files to Cisco Threat Grid for analysis without extracting them. This improves efficacy by reducing the number of file submissions. See "File Reputation Filtering and File Analysis" chapter in the user guide.
Kerberos support for high availability clusters	You can use the **Use keytab authentication** option in the Kerberos High Availability section, while creating or editing an Active Directory realm, to enable Kerberos authentication for all appliances in high availability clusters. See "Acquire End-User Credentials" chapter in the user guide.
Support for HTTP PATCH requests	Cisco Web Security appliance now includes a new CLI command `httppatchconfig`. You can use this command to enable or disable outgoing HTTP PATCH requests. See "Command Line Interface" chapter in the user guide.

Feature	Description
Virtual Appliance Enhancement	Cisco Web Security virtual appliances can now be deployed on VMware vSphere Hypervisor (ESXi) 6.5. For more information, see the *Cisco Content Security Virtual Appliance Installation Guide*, available from: https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html
Enhancements	
Authentication for Kerberos	A new CLI command `modifyauthhelpers` is added to configure the number of Kerberos authentication helpers within a range of 5 to 21 for BASIC, NTLMSSP, and NEGO.

What's New in AsyncOS 11.5.0-614 - LD (Limited Deployment)

Feature	Description
Cisco Cloudlock-specific W3C Logs	You can configure your appliance to send W3C access logs to the Cisco Cloudlock portal for analysis and reporting. These custom W3C logs provide better visibility into the SaaS usage of the customers. Cisco Cloudlock is a cloud-native CASB and cloud cybersecurity platform that protects users, data, and applications across Software-as-a-Service, Platform-as-a-Service, and Infrastructure-as-a-Service. See the "Monitor System Activity Through Logs" chapter in the user guide or online help.
Cisco CTA-specific W3C Logs Enhancements	You can now configure and send the CTA-specific custom W3C logs to the CTA portal for analysis using the new Cisco Cognitive Threat Analytics page on the appliance's web interface. A new log field (*r-ip*) is added as a default field in CTA log that enables you to include website IP address in case of upstream deployment. You can also choose to anonymize the username, IP address, and user group field values of the log so that the client related information will not be disclosed to external systems like CTA to which the logs are pushed to. See the "Monitor System Activity Through Logs" chapter in the user guide or online help.
Scheduled Policy Expiration	You can now set the expiry time for Access and Decryption policies. The policies are automatically disabled once they exceed the set expiry time. You will receive alerts three days prior to expiry and also on expiry. See the "Create Policies to Control Internet Requests" and "Perform System Administration Tasks (for alerts)" chapters in the user guide or online help.
User Count Report	The User Count page displays information about the total number of authenticated and unauthenticated users of the appliance. See the "Web Security Appliance Reports" chapter in the user guide or online help.
Anonymization and Deanonymization of W3C Log Fields	You can now choose to anonymize the username, IP address, and user group field values of the W3C logs so that the client related information will not be disclosed to external servers to which the logs are pushed to. To view the actual values of the anonymized log field values, you must deanonymize the field values using the Deanonymization feature. See the "Monitor System Activity Through Logs" chapter in the user guide or online help.

Feature	Description
IPv6 Address Enhancement	Cisco Web Security appliances support IPv6 addresses for the following protocols: • NTP • RADIUS • Syslog • SNMP
AMP for Endpoints Console Integration	You can now integrate your appliance with AMP for Endpoints console, and add your own blacklisted or whitelisted file SHAs. After the integration, when a file SHA is sent to the File Reputation server, the verdict obtained for the file SHA from the File Reputation Server is overridden by the verdict already available for the same file SHA in the AMP for Endpoints console. To integrate your appliance with AMP for Endpoints console, see the "Configuring Security Services" chapter in the user guide. The Advanced Malware Protection Report page now includes a new section - **Malware Files by Category** to view the percentage of blacklisted file SHAs received from the AMP for Endpoints console. The threat name of a blacklisted file SHA is displayed as **Simple Custom Detection** in the Malware Threat Files section of the report. See the "File Reputation Filtering and File Analysis" chapter in the user guide or online help.
Advanced SSL Debugging	Cisco Web Security appliance now includes an OPENSSL command tool: `ssltool`. This command executes different OPENSSL commands from appliance's CLI to troubleshoot SSL connections. The administrators can use this command to debug HTTPS/SSL/TLS issues. See the "Command Line Interface" chapter in the user guide or online help.
Support for Network Interface Card (NIC) Pairing	A new subcommand `pairing` is added to the main CLI command `etherconfig` to view and configure NIC pairing. Support for NIC pairing is available only for hardware devices.
Cache Expiry Period for File Reputation disposition values	You can configure the cache expiry period for File Reputation disposition values through the *Security Services* > *Anti-Malware and Reputation* > *Advanced Malware Protection Services* > *Advanced* > *Advanced Settings for Cache* page in the web interface.

Feature	Description
Virtual Appliance support for Amazon Web Services (AWS)	You can deploy Cisco Web Security and Security Management Virtual Appliances on Amazon Elastic Compute Cloud (EC2) on Amazon Web Services (AWS). **Note** The L4 Traffic Monitor functionality is not supported. The AMI IDs for Cisco Web Security virtual appliances (AsyncOS 11.5.0-614) are as shown below: S100V - coeus-11-5-0-614-S100V-AMI-110518 S300V - coeus-11-5-0-614-S300V-AMI-120518 S600V - coeus-11-5-0-614-S600V-AMI-120518 See the "Deploying Cisco Web Security and Security Management Virtual Appliances on Amazon Elastic Compute Cloud on Amazon Web Services" guide. See Related Documentation, page 24 for the location of the guide.
List of Ciphers for AsyncOS 11.5. for Cisco Web Security Appliances	A new document that lists the supported and unsupported ciphers (SSL and SSH) for AsyncOS 11.5. for Cisco Web Security Appliances is available now. See https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html
Enhancements	
DNS configuration updates	A new CLI command `advancedproxyconfig->miscellaneous->Do you want to disable IP address in Host Header?` is added to block IP address in the host header.
URL size configuration for proxy requests	The CLI command *`maxhttpheadersize`* can be used to set the maximum URL size for proxy requests.
SSH configuration	The following subcommands are added to the CLI command `sshconfig`: • `Incomplete SSH session timeout (in secs)` Default value is 60. • `Unsuccessful SSH login attempts allowed` Default value is 3.
FIPS mode update	• The maximum number of concurrent sessions allowed for FIPS mode is 3. • The maximum number of concurrent sessions allowed for non-FIPS mode is 10.

Changes in Behavior

Changes in Behavior in AsyncOS 11.5.1

External URL category for the Microsoft Office 365 feed format	The external URL category for the Microsoft Office 365 feed format, which provides Office 365 exemptions, might fail to update after 2018-10-02 due to Microsoft migration from an XML feed to a Web Representational State Transfer (REST) API-based format. AsyncOS 11.7.0-330 for Web Security appliances supports the Microsoft Office 365 Web Service.
Web Traffic Tap Range Requests	All transactions with requests containing range headers will be tapped until the response header is complete. The response body will not be tapped. Access log will contain the TAP_UNSUP_RREQ error-code to indicate this.
Log Subscription Names	Non ACII characters in log subscription names is not supported.

Changes in Behavior in AsyncOS 11.5.0

Verification of secure authentication certificate	While performing an upgrade, if the secure authentication certificate is not FIPs-complaint, it will be replaced with the default certificate of the latest path to which the appliance is upgraded to. This happens only when the customer has used the default certificate before the upgrade.
Removal of unsupported ciphers during upgrade	The ciphers and host keys which are not supported are removed when you perform upgrade from releases prior to10.5. See https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html
Loading the appliance configuration	Loading of configuration fails, if the following parameters are not compliant with adopted standards: • `https_cert` • `authorized_keys` • `hostkey` • `ssh ciphers`
DNS configuration updates	Default value is changed from 1 to 0 for *`advancedproxyconfig->dns->Find web server by`* subcommand in CLI.
SSH configuration	Default value of the number of unsuccessful SSH login attempts is changed from 6 to 3. You can use the following subcommand of the CLI command `sshconfig` to change the default value. • `Unsuccessful SSH login attempts allowed`

User network access	The IP address of the appliance is automatically added to the access list, when you try to add IPs through *System Administration>Network Access* on the appliance's web interface.

`tail` command	Displays the end of a log file. Command accepts log file name as parameter. The command has been modified and now you must 'Press Ctrl-C' to stop scrolling, then `q` to quit.
	Example 1
	`example.com> tail`
	`Currently configured logs:`
	`1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll`
	`2. "amp_logs" Type: "AMP Engine Logs" Retrieval: FTP Poll`
	`…`
	`…`
	`Enter the number of the log you wish to tail.`
	`[]> 9`
	`Press Ctrl-C to stop scrolling, then `q` to quit.`
	`~`
	`~`
	`Thu Dec 14 10:03:07 2017 Info: Begin Logfile`
	`~`
	`…`
	`"CTRL-C" + "q"`
	Example 2
	`example.com> tail system_logs`
	`Press Ctrl-C to stop scrolling, then `q` to quit.`
	`~`
	`~`
	`Thu Dec 14 09:59:10 2017 Info: Begin Logfile`
	`…`
	`…`
	`"CTRL-C" + "q"`

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 11.5, 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

Note Before you start the upgrade process, see Pre-upgrade Requirements, page 15 and Installation and Upgrade Notes, page 16.

Upgrade Paths for 11.5.3-016 - MD (Maintenance Deployment)

You can upgrade to release 11.5.3-016 of AsyncOS for Cisco Web Security appliances from the following versions:

- 10.1.3-039
- 10.1.4-007
- 10.1.4-017
- 10.5.1-296
- 10.5.2-072
- 10.5.3-025
- 10.5.4-018
- 11.5.0-614
- 11.5.1-125
- 11.5.2-020
- 11.5.3-007

Upgrade Paths for 11.5.2-020 - MD (Maintenance Deployment)

You can upgrade to release 11.5.2-020 of AsyncOS for Cisco Web Security appliances from the following versions:

- 10.1.1-235
- 10.1.3-039
- 10.1.3-054
- 10.1.4-007
- 10.1.4-017
- 10.5.1-296
- 10.5.2-072
- 10.5.3-025
- 10.5.4-018
- 11.5.0-614
- 11.5.1-125

Upgrade Paths for 11.5.1-125 - GD (General Deployment) Refresh

You can upgrade to release 11.5.1-125 of AsyncOS for Cisco Web Security appliances from the following versions:

- 9.1.1-074
- 9.1.2-022
- 9.1.3-024
- 10.1.1-235
- 10.1.3-039
- 10.1.3-054
- 10.5.1-296
- 10.5.2-072
- 11.0.0-641
- 11.5.0-476
- 11.5.0-614
- 11.5.1-115
- 11.5.1-124

Upgrade Paths for 11.5.1-124 - GD (General Deployment) Refresh

You can upgrade to release 11.5.1-124 of AsyncOS for Cisco Web Security appliances from the following versions:

- 9.1.1-074
- 9.1.2-022
- 9.1.3-024
- 10.1.1-235
- 10.1.3-039
- 10.1.3-054
- 10.5.1-296
- 10.5.2-042
- 10.5.2-061
- 10.5.2-072
- 11.0.0-641
- 11.5.0-476
- 11.5.0-614
- 11.5.1-115

Upgrade Paths for 11.5.1-115 - GD (General Deployment)

You can upgrade to release 11.5.1-115 of AsyncOS for Cisco Web Security appliances from the following versions:

- 9.1.1-074
- 9.1.2-022
- 9.1.3-024
- 10.1.1-235
- 10.1.3-039
- 10.1.3-054
- 10.5.1-296
- 10.5.2-042
- 10.5.2-061
- 10.5.2-072
- 11.0.0-641
- 11.5.0-476
- 11.5.0-614
- 11.5.1-102
- 11.5.1-105

Upgrade Paths for 11.5.0-614 - LD (Limited Deployment)

You can upgrade to release 11.5.0-614 of AsyncOS for Cisco Web Security appliances from the following versions:

- 9.1.2-022
- 9.1.3-024
- 10.1.1-235
- 10.1.2-050
- 10.5.1-296
- 10.5.2-042
- 11.0.0-641
- 11.5.0-476

Pre-upgrade Requirements

Upgrade from Earlier Versions of AsyncOS with CTA Log Subscription, to AsyncOS 11.5

Upgrade from AsyncOS 11.0 to 11.5

The following conditions should be met, if you have already configured a CTA log in AsyncOS 11.0 version and want to upgrade to AsyncOS 11.5 version:

- The log name must be ‘cta_log’.
- Retrieval method for the log must be ‘scp_push’.
- The ‘CTA Enable’ checkbox must be checked. Only then it will be considered as a CTA log after upgrading to 11.5 version.
- In case, any of the above mentioned conditions is not met, the log will be considered as a standard log after upgrade.

Upgrade from AsyncOS Pre-11.0 Releases to 11.5

The following conditions must be met, if you have already configured a CTA log in AsyncOS pre-11.0 releases and want to upgrade to AsyncOS 11.5 version:

- The log name must be ‘cta_log’.
- Retrieval method for the log must be ‘scp_push’. Only then it will be considered as a CTA log after upgrading to 11.5 version.

- In case, any of the above mentioned conditions is not met, the log will be considered as a standard log after upgrade.

Upgrade from AsyncOS Earlier Versions with Cloudlock Log Subscription to AsyncOS 11.5

The following conditions must be met, if you have already configured a Cloudlock log in AsyncOS earlier releases and want to upgrade to AsyncOS 11.5 version:

- The log name must be 'cloudlock_log'.
- Retrieval method for the log must be 'scp_push'. Only then it will be considered as a Cloudlock log after upgrading to 11.5 version.
- In case, any of the above mentioned condition is not met, the log will be considered as a standard W3C log after upgrade

.

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 the appliance 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 the appliance and DLP Server is IPv4 only)
- PAC File Hosting
- Protocols: NTP, RADIUS, SNMP, and syslog over management server

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 18.

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.

Upgrading AsyncOS for Web

Before You Begin

Perform preupgrade requirements. See Pre-upgrade Requirements, page 15.

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 **Upgrade Options**

Step 4 Select **Download** or **Download and Install** as required.

Choose from the list of available upgrades.

Step 5 Click **Proceed** to start the upgrade or download. Answer the questions as they appear.

If you chose **Download only**, the upgrade will be downloaded to the appliance.

Step 6 (If you chose **Download and install**) 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, page 20
- Virtual Appliances: Required Changes for SSH Security Vulnerability Fix, page 20
- File Analysis: Required Changes to View Analysis Result Details in the Cloud, page 21
- File Analysis: Verify File Types To Be Analyzed, page 21
- Unescaped Dots in Regular Expressions, page 21

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.

Note This patch is required only for virtual appliance releases that were downloaded or upgraded before June 25, 2015.

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 24.

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

Lists of Known and Fixed Issues in Release 11.5.3-016

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.5.3-016&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.5.3&sb=afr&sts=open&svr=3nH&bt=custV

Lists of Known and Fixed Issues in Release 11.5.2-020

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.5.2-020&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/searchkw=*&pf=prdNm&pfVal=282521310&rls=11.5.2&sb=afr&sts=open&svr=3nH&bt=custV

Lists of Known and Fixed Issues in Release 11.5.1-125

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.5.1-125&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.5.1&sb=afr&sts=open&svr=3nH&bt=custV

Lists of Known and Fixed Issues in Release 11.5.1-124

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.5.1-124&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.5.1&sb=afr&sts=open&svr=3nH&bt=custV

Lists of Known and Fixed Issues in Release 11.5.1-115

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.5.1-115&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.5.1&sb=afr&sts=open&svr=3nH&bt=custV

Lists of Known and Fixed Issues in Release 11.5.0-614

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.5.0-614&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.5.0&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, 11.5.1

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.

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 virtual appliances is available from

https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.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.

List of Ciphers for AsyncOS 11.5. for Cisco Web Security Appliances is available from

https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.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://community.cisco.com/t5/web-security/bd-p/5786-discussions-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.