Release Notes for AsyncOS 11.0 for Cisco Content Security Management

Published: June 14, 2017
Revised: June 12, 2018

Contents

Cisco Systems, Inc.
www.cisco.com

What's New

What's New In Cisco AsyncOS 11.0.0-136 - MD (Maintenance Deployment)

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

What's New In Cisco AsyncOS 11.0.0-133 - MD (Maintenance Deployment)

Feature	Description
Kerberos support for high availability clusters	Cisco Web Security appliance now supports Kerberos for high availability clusters. While creating or editing an Active Directory realm, you can use the **Use keytab authentication** option in the Kerberos High Availability section, to enable Kerberos authentication for all appliances in high availability clusters. For details, see the following topics in the user guide: • Creating an Active Directory Realm for Kerberos Authentication Scheme, • Creating a Service Account in Windows Active Directory for Kerberos Authentication in High Availability Deployments

What's New In Cisco AsyncOS 11.0.0-132 - MD (Maintenance Deployment)

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

What's New In Cisco AsyncOS 11.0.0-128 - MD (Maintenance Deployment)

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

What's New In Cisco AsyncOS 11.0.0-115 - GD (General Deployment)

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

What's New In Cisco AsyncOS 11.0.0-112 - LD (Limited Deployment) Refresh

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

What's New In Cisco AsyncOS 11.0.0-060 - LD (Limited Deployment)

Feature	Description
Support for TLS v1.2	Cisco Email Security appliance now supports an additional SSL method: TLS v1.2. If you were not using TLS v1 prior to the upgrade, the SSL methods are not automatically set to TLS v1.2 after the upgrade. You can use the `sslconfig` command in CLI to view or modify the existing SSL configuration. **Note** The highest supported TLS or SSL method in the client advertisement is always selected during the negotiation.

Support for new features in AsyncOS 11.0 for Cisco Email Security Appliances	Reporting support for the following new feature in AsyncOS 11.0 for Cisco Email Security Appliances: • Geo Distribution. Use this report page to view details such as: – Top incoming mail connections based on country of origin in graphical format. – Total incoming mail connections based on country of origin in tabular format. For details, search for the relevant terms in the email reporting chapter of the user guide. The following reports have been enhanced to show details of outgoing messages scanned by the AMP engine: Advanced Malware Protection • AMP File Analysis • AMP Verdict Updates • Overview Page • Outgoing Destinations • Outgoing Senders • Internal Users For details, search for the relevant terms in the email reporting chapter of the user guide.
Support for Two-Factor Authentication	Cisco Content Security Management appliance now supports two-factor authentication that ensures secure access when you log into your appliance. You can configure two-factor authentication for your appliance through any standard RADIUS server that complies with a standard RFC. You can enable two-factor authentication in one of the following ways: • **System Administration** > **Users** page in web interface. See the "Distributing Administrative Tasks" chapter in the user guide or online help. • `userconfig` > `twofactorauth` command in CLI. If you have enabled two-factor authentication on your Email Security appliance, you can add it to a Security Management appliance using pre-shared keys. Use the `smaconfig` > `add` command in the CLI to configure this setting.

Upgrade Paths

Upgrading to Release 11.0.0-136 - MD (Maintenance Deployment)

You can upgrade to release 11.0.0-136 from the following versions:

- 8-3-6-039
- 9-1-1-005
- 9-1-1-702
- 9-5-2-023
- 9-5-2-033
- 9-6-0-051
- 9-6-0-066
- 9-6-1-019
- 9-6-1-027
- 10-0-0-013
- 10-0-0-055
- 10-0-0-088
- 10-0-0-096
- 10-0-0-865
- 10-1-0-037
- 10-1-0-052
- 11-0-0-033
- 11-0-0-042
- 11-0-0-054
- 11-0-0-059
- 11-0-0-060
- 11-0-0-112
- 11-0-0-115
- 11-0-0-116
- 11-0-0-128
- 11-0-0-132
- 11-0-0-133

Upgrading to Release 11.0.0-133 - MD (Maintenance Deployment)

You can upgrade to release 11.0.0-133 from the following versions:

- 8-3-6-039

- 9-1-1-005
- 9-1-1-702
- 9-5-2-023
- 9-5-2-033
- 9-6-0-051
- 9-6-0-066
- 9-6-1-019
- 9-6-1-027
- 10-0-0-013
- 10-0-0-055
- 10-0-0-088
- 10-0-0-096
- 10-0-0-865
- 10-1-0-037
- 10-1-0-052
- 11-0-0-033
- 11-0-0-042
- 11-0-0-054
- 11-0-0-059
- 11-0-0-060
- 11-0-0-112
- 11-0-0-115
- 11-0-0-116
- 11-0-0-128
- 11-0-0-132

Upgrading to Release 11.0.0-132 - MD (Maintenance Deployment)

You can upgrade to release 11.0.0-132 of AsyncOS for Cisco Content Security Management from the following versions:

- 8.3.6-039
- 9.1.1-005
- 9.1.1-702
- 9.5.2-023
- 9.5.2-033
- 9.6.0-051
- 9.6.0-066
- 9.6.1-019

- 9.6.1-027
- 10.0.0-013
- 10.0.0-055
- 10.0.0-088
- 10.0.0-096
- 10.1.0-037
- 10.1.0-052
- 11.0.0-033
- 11.0.0-042
- 11.0.0-054
- 11.0.0-059
- 11.0.0-060
- 11.0.0-112
- 11.0.0-115
- 11.0.0-116
- 11.0.0-128

Upgrading to Release 11.0.0-128 - MD (Maintenance Deployment)

You can upgrade to release 11.0.0-128 of AsyncOS for Cisco Content Security Management from the following versions:

- 8.3.6-039
- 9.1.1-005
- 9.1.1-702
- 9.5.2-023
- 9.5.2-033
- 9.6.0-051
- 9.6.0-066
- 9.6.1-019
- 9.6.1-027
- 10.0.0-013
- 10.0.0-055
- 10.0.0-088
- 10.0.0-096
- 10.1.0-037
- 10.1.0-052
- 11.0.0-033
- 11.0.0-042

- 11.0.0-054
- 11.0.0-059
- 11.0.0-060
- 11.0.0-112
- 11.0.0-115
- 11.0.0-116

Upgrading to Release 11.0.0-115 - GD (General Deployment)

You can upgrade to release 11.0.0-115 of AsyncOS for Cisco Content Security Management from the following versions:

- 8.3.6-039
- 9.1.1-005
- 9.1.1-702
- 9.5.2-023
- 9.5.2-033
- 9.6.0-051
- 9.6.0-066
- 9.6.1-019
- 9.6.1-027
- 10.0.0-013
- 10.0.0-055
- 10.0.0-088
- 10.0.0-096
- 10.1.0-037
- 10.1.0-052
- 11.0.0-033
- 11.0.0-042
- 11.0.0-054
- 11.0.0-059
- 11.0.0-060
- 11.0.0-112

Upgrading to Release 11.0.0-112 - LD (Limited Deployment) Refresh

You can upgrade to release 11.0.0-112 of AsyncOS for Cisco Content Security Management from the following versions:

- 8.3.6-039
- 9.1.1-005

- 9.1.1-702
- 9.5.2-023
- 9.5.2-033
- 9.6.0-051
- 9.6.0-066
- 9.6.1-019
- 9.6.1-027
- 10.0.0-013
- 10.0.0-055
- 10.0.0-088
- 10.0.0-096
- 10.1.0-037
- 10.1.0-052
- 11.0.0-033
- 11.0.0-042
- 11.0.0-054
- 11.0.0-059
- 11.0.0-060

Upgrading to Release 11.0.0-060 - LD (Limited Deployment)

You can upgrade to release 11.0.0-060 of AsyncOS for Cisco Content Security Management from the following versions:

- 8.3.6-039
- 9.1.1-005
- 9.1.1-702
- 9.5.2-023
- 9.5.2-033
- 9.6.0-051
- 9.6.0-066
- 9.6.1-019
- 9.6.1-027
- 10.0.0-013
- 10.0.0-055
- 10.0.0-088
- 10.0.0-096
- 10.1.0-037
- 10.1.0-052

- 11.0.0-033
- 11.0.0-042
- 11.0.0-054
- 11.0.0-059

Content Security Release Terminology

For an explanation of terms like LD, ED, GD, and MD that are used in labeling content security product releases, see https://supportforums.cisco.com/blog/12309231/content-security-release-terminology.

Compatibility with Email and Web Security Releases

Compatibility with AsyncOS for Email Security and AsyncOS for Web Security releases is detailed in the Compatibility Matrix available from http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html.

Changed Information

In addition to the changes described in the New Features table above, the following functionality on your appliance has changed from previous releases and may require your attention.

Change in Timeout value for End-user Quarantine storage subsystem	From AyncOS 11.0 onwards, the End-User Quarantine storage subsystem timeout value has been set to 10 minutes.
Changes in Launch Migration Wizard functionality	From AsyncOS 11.0 onwards, you can launch the Migration Wizard to configure the migration process of Policy, Virus and Outbreak Quarantines, even if you have not configured any policy quarantines in your email security appliance.
Changes in Username Length	Prior to this release, the username length was limited to 16 characters. After you upgrade to this release, the username length is limited to 32 characters.

Installation and Upgrade Notes

Important Additional Reading

You should also review the release notes for your associated Email and Web security releases.

For links to this information, see Related Documentation, page 15.

Virtual Appliance

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

Upgrading a Virtual Appliance

If your current Virtual Appliance release does not support more than 2TB of disk space, and you want to use more than 2 TB of disk space with this release, you cannot simply upgrade your virtual appliance.

Instead, you must deploy a new virtual machine instance for this release.

When you upgrade a virtual appliance, the existing licenses remain unchanged.

Migrating From a Hardware Appliance to a Virtual Appliance

Step 1 Set up your virtual appliance using the documentation described in Virtual Appliance, page 11.

Step 2 Upgrade your physical appliance to this AsyncOS release.

Step 3 Save the configuration file from your upgraded physical appliance

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

Be sure to select appropriate options related to disk space and network settings.

What To Do Next

If you will use your hardware appliance as a backup appliance, see information about backups in the user guide or online help. For example, you should ensure that the backup appliance does not pull data directly from managed email and web security appliances, or publish configurations to web security appliances.

Preupgrade Requirements

Perform the following important preupgrade tasks:

- Verify Associated Email and Web Security Appliance Versions, page 11
- Back Up Your Existing Configuration, page 12

Verify Associated Email and Web Security Appliance Versions

Before upgrading, verify that the Email Security appliances and Web Security appliances that you want to manage will run releases that are compatible. See the Compatibility with Email and Web Security Releases, page 10.

Back Up Your Existing Configuration

Before upgrading your Cisco Content Security Management appliance, save the XML configuration file from your existing Security Management appliance. Save this file to a location off the appliance. For important caveats and instructions, see the "Saving and Exporting the Current Configuration File" section in the user guide or online help.

IPMI Messages During Upgrade

If you are upgrading your appliance using the CLI, you may observe messages related to IPMI. You can ignore these messages. This is a known issue.

Defect ID: CSCuz33125

Upgrading to This Release

Step 1 Address all topics described in Preupgrade Requirements, page 11.

Step 2 Follow all instructions in the "Before You Upgrade: Important Steps" section in the user guide PDF for THIS release.

Step 3 Perform the upgrade:

Follow instructions in the "Upgrading AsyncOS" section of the "Common Administrative Tasks" chapter of the user guide PDF for your EXISTING release.

Note 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 a virtual appliance, do not use the hypervisor or host OS tools to reset, cycle, or power off the virtual machine.

Step 4 After about 10 minutes, access the appliance again and log in.

Step 5 Follow instructions in the "After Upgrading" section of the user guide PDF for THIS release.

Step 6 If applicable, see Migrating From a Hardware Appliance to a Virtual Appliance, page 11.

Alert: Battery Relearn Timed Out (RAID Event) on 380 or 680 Hardware

Problem You receive an alert with subject "Battery Relearn Timed Out" for 380 or 680 hardware.

Solution This alert may or may not indicate a problem. The battery relearn timeout, in itself, does not mean there is any problem with the RAID controller. The controller can recover in the subsequent relearn. Please monitor your email for any other RAID alerts for the next 48 hours, to ensure that this is not the side-effect of any other problem. If you do not see any other RAID-related alerts from the system, then you can safely ignore this alert.

Post-Upgrade Notes

Traceback Issue after Upgrading

After upgrading to AsyncOS 11.0.0-115 version from AsyncOS 11.0.0-112 on M190 and M170 models, if you run the `etherconfig > media` command using the CLI, a Traceback error is displayed. Contact TAC to assist you in resolving this issue.

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, page 13
- Lists of Known and Fixed Issues, page 13
- Finding Information about Known and Resolved Issues, page 14

Note Known issues on Cisco Email Security Appliances and Cisco Web Security Appliances may appear in or impact functionality of Cisco Content Security Management Appliances.

Known issues in previous content security management releases may also affect 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

Known Issues	**AsyncOS 11.0.0-136**	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509131&rls=11.0.0-136&sb=afr&sts=open&svr=3nH&bt=custV
	AsyncOS 11.0.0-133	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509131&rls=11.0.0-133&sb=afr&sts=open&svr=3nH&bt=custV
	AsyncOS 11.0.0-132	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509131&rls=11.0.0-132&sb=afr&sts=open&svr=3nH&bt=custV
	AsyncOS 11.0.0-128	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509131&rls=11.0.0-128&sb=afr&sts=open&svr=3nH&bt=custV
	AsyncOS 11.0.0-115	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509131&rls=11.0.0-115&sb=afr&sts=open&svr=3nH&bt=custV

	AsyncOS 11.0.0-112	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509131&rls=11.0.0-112&sb=afr&sts=open&svr=3nH&bt=custV
	AsyncOS 11.0.0-060	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509131&rls=11.0.0-060&sb=afr&sts=open&svr=3nH&bt=custV

Fixed Issues	**AsyncOS 11.0.0-136**	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509131&rls=11.0.0-136&sb=fr&svr=3nH&bt=custV
	AsyncOS 11.0.0-133	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509131&rls=11.0.0-133&sb=fr&svr=3nH&bt=custV
	AsyncOS 11.0.0-132	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509131&rls=11.0.0-132&sb=fr&svr=3nH&bt=custV
	AsyncOS 11.0.0-128	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509131&rls=11.0.0-128&sb=fr&svr=3nH&bt=custV
	AsyncOS 11.0.0-115	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509131&rls=11.0.0-115&sb=fr&svr=3nH&bt=custV
	AsyncOS 11.0.0-112	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509131&rls=11.0.0-112&sb=fr&svr=3nH&bt=custV
	AsyncOS 11.0.0-060	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509131&rls=11.0.0-060&sb=fr&svr=3nH&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.

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 > Security Management > Cisco Content Security Management 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.

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 15.

Information about other resources, including Tech Notes and the Cisco support community, is in the Additional Resources chapter in the online help and User Guide PDF.

Related Documentation

In addition to the main documentation in the following table, information about other resources, including the knowledge base and Cisco support community, is in the More Information chapter in the online help and User Guide PDF.

Documentation For Cisco Content Security Products:	Is Located At:
Security Management appliances	http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Web Security appliances	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html
Email Security appliances	http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html
Command Line Reference guide for content security products	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html
Cisco Email Encryption	http://www.cisco.com/c/en/us/support/security/email-encryption/tsd-products-support-series-home.html

Service and Support

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

Cisco TAC: 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.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.