



Release Notes for AsyncOS 12.0 for Cisco Content Security Management Appliances

Published: November 26, 2018

Revised: December 06, 2018

Contents

- [What's New In This Release, page 2](#)
- [Changes in Behaviour, page 7](#)
- [Comparison of Web Interfaces, AsyncOS 12.0 vs. Previous Releases, page 8](#)
- [Upgrade Paths, page 12](#)
- [Compatibility with Email and Web Security Releases, page 12](#)
- [Installation and Upgrade Notes, page 12](#)
- [Known and Fixed Issues, page 15](#)
- [Related Documentation, page 15](#)
- [Service and Support, page 16](#)



What's New In This Release

Feature	Description
New Web Interface for Reporting, Quarantine and Tracking	<p>The appliance now has a new web interface to search and view:</p> <ul style="list-style-type: none"> • Email Reports <p>You can now view email reports from the Reports drop-down based on the following categories:</p> <ul style="list-style-type: none"> - Email Threat Reports - File and Malware Reports - Connection and Flow Reports - User Reports - Filter Reports <p>For more information, see the "Using Centralized Email Security Reporting on the New Web Interface" chapter in the user guide.</p> <ul style="list-style-type: none"> • Spam Quarantine <ul style="list-style-type: none"> - You can now view and search for spam and suspected spam messages in Quarantine > Spam Quarantine > Search page in the web interface. - You can view, add, and search for domains added in the safelist and blocklist in Quarantine > Spam Quarantine > Safelist or Blocklist page in the web interface. <p>For more information, see the "Spam Quarantine" chapter in the user guide.</p> <ul style="list-style-type: none"> • Policy, Virus and Outbreak Quarantines <p>You can view and search for policy, virus and outbreak quarantines in Quarantine > Other Quarantine > Search page in the web interface.</p> <p>For more information, see the "Centralized Policy, Virus, and Outbreak Quarantines" chapter in the user guide.</p> <ul style="list-style-type: none"> • Message Tracking <p>You can search for messages or a group of messages depending on your search criteria in Tracking > Search page in the web interface..</p> <p>For more information, see the "Tracking Messages" chapter in the user guide.</p> <p>For more information, see Accessing the New Web Interface, page 11.</p> <p>Important!</p> <ul style="list-style-type: none"> • Make sure that the AsyncOS API ports configured in Management Appliance > Network > IP Interfaces, are opened on the firewall. The default AsyncOS API HTTP/HTTPS port is 6080/6443. • Also ensure that if <code>trailblazerconfig</code> is enabled, the HTTP/HTTPS port must be opened on the firewall. The default HTTP/HTTPS port is 801/4431.

The <code>trailblazerconfig</code> CLI Command	<p>You can use the <code>trailblazerconfig</code> command to route your incoming and outgoing connections through HTTP and HTTPS ports on the new web interface.</p> <p>Please note that this feature is still in beta.</p> <p>For more information, see "The trailblazerconfig CLI Command" section of the user guide.</p>
Support for new features in AsyncOS 12.0 for Cisco Email Security Appliances	<p>You can now view the following reports on the Reporting page of the Security Management appliance:</p> <ul style="list-style-type: none"> • External Threat Feeds • Sender Domain Reputation <p>For more information, see the "Using Centralized Email Security Reporting" chapter in the user guide.</p> <p>You can now view outgoing TLS connections summary for DANE Success and DANE Failure scenarios. For more information, see "SMTP DNS-based Authentication of Named Entities" section of the user guide or online help for <i>AsyncOS 12.0 for Cisco Email Security Appliances</i>.</p> <p>You can now use the following message events to search for messages on the Message Tracking page of the Security Management appliance:</p> <ul style="list-style-type: none"> • External Threat Feeds • Sender Domain Reputation • DANE Failure
Metrics Bar Widget	<p>The Metrics Bar widget enables you to view the real time data of the file analysis done by the Cisco Threat Grid appliance on the Advanced Malware Protection report page.</p> <p>For more information, see "Advanced Malware Protection Page" section of the user guide.</p>

<p>Advanced Malware Protection Report Enhancement</p>	<p>The Advanced Malware Protection Report page has the following enhancements:</p> <ul style="list-style-type: none"> • A new section - Incoming Malware Files by Category to view the percentage of blacklisted file SHAs received from the AMP for Endpoints console that are categorized as Custom Detection. The threat name of a blacklisted file SHA obtained from AMP for Endpoints console is displayed as Simple Custom Detection in the Incoming Malware Threat Files section of the report. • A new section - Incoming Malware Files by Category to view the percentage of blacklisted file SHAs based on the threshold settings that are categorised as Custom Threshold. • You can click on the link in the More Details section of the report to view the file trajectory details of a blacklisted file SHA in the AMP for Endpoints console. • A new verdict - Low Risk is introduced when no dynamic content is found in a file after file analysis. You can view the verdict details in the Incoming Files Handed by AMP section of the report. <p>For more information, see the "Using Centralized Email Security Reporting on the New Web Interface" chapter in the user guide.</p>
<p>New Web Interface for Web Reporting and Tracking</p>	<p>The appliance now has a new web interface to search and view:</p> <ul style="list-style-type: none"> • Web Reports You can now view web based reports from the Reports drop-down based on the following categories: <ul style="list-style-type: none"> - General Reports - Threats Reports • Web Tracking You can search for web transactions depending on your search criteria. On your Security Management appliance , click on the Web dropdown and choose Tracking > Web Tracking Search page. <p>For more information on web reports and web tracking, see "Using Centralized Web Reporting and Tracking" chapter of the user guide.</p> <p>Important!</p> <ul style="list-style-type: none"> • Make sure that the AsyncOS API ports configured in Management Appliance > Network > IP Interfaces, are opened on the firewall. The default HTTP/HTTPS port is 6080/6443. • Also ensure that if <code>trailblazerconfig</code> is enabled, the HTTP/HTTPS port must be opened on the firewall. The default HTTP/HTTPS port is 801/4431. <p>For more information, see Accessing the New Web Interface, page 11.</p>
<p>HTTPS Reports Page</p>	<p>You can now view the overall aggregation of the HTTP/HTTPS traffic and the summary of the ciphers based on the client and server side connection for each HTTP/HTTPS traffic, on the HTTPS Reports report page.</p> <p>For more information, see "Using Centralized Web Reporting and Tracking" chapter of the user guide.</p>

Support for Smart Software Licensing	<p>Smart Software Licensing enables you to manage and monitor Cisco Email Security appliance licenses seamlessly. To activate Smart Software licensing, you must register your appliance with Cisco Smart Software Manager (CSSM) which is the centralized database that maintains the licensing details about all the Cisco products that you purchase and use.</p> <p> Caution After you enable the Smart Licensing mode on your appliance, you may not be able to rollback to the Classic Licensing mode.</p> <p>For more information, see the "Common Administrative Tasks" chapter in the user guide.</p>
Integrating the Appliance with Cisco Threat Response Portal	<p>You can integrate your appliance with Cisco Threat Response portal, and perform the following actions in Cisco Threat Response portal:</p> <ul style="list-style-type: none"> • View the email reporting, message tracking, and web tracking data from multiple appliances in your organization. • Identify, investigate and remediate threats observed in the email reports, message tracking and web tracking. • Resolve the identified threats rapidly and provide recommended actions to take against the identified threats. • Document the threats in the portal to save the investigation, and enable collaboration of information among other devices on the portal. <p> Note You can perform the above actions only when the Cisco Threat Response portal supports integration of your Content Security Management appliance. The Cisco Threat Response portal does not support the AsyncOS 12.0 for Cisco Content Security Management Appliances - Limited Deployment Release.</p> <p>For more information, see the "Assigning Network and IP Addresses" chapter in the user guide.</p>

<p>Support for the Office 365 Web Service External URL Categories feature in AsyncOS 11.5.1-124 for Cisco Web Security Appliances</p>	<p>This release supports the Office 365 Web Service External URL Categories feature in AsyncOS 11.5.1-124 for Cisco Web Security Appliances.</p> <p>For more information, see the “Using Centralized Web Reporting and Tracking” chapter in the user guide.</p>
<p>Web Traffic Tap Policies for web</p>	<p>Cisco Content Security Management appliance now allows you to set Web Traffic Tap Policies. You can define the Web Traffic Tap Policies based on which web traffic that passes through the Web Security appliance will be tapped.</p> <p>You must enable the Web Traffic Tap feature in Web Security appliance to set the Web Traffic policies in the Security Management appliance.</p> <p>Four new sections are included in the Overview report page. The sections are:</p> <ul style="list-style-type: none"> • Web Traffic Tap Status • Web Traffic Tap Summary • Tapped HTTP/HTTPS Traffic • Tapped Traffic Summary <p>For more information about the report, see the “Using Centralized Web Reporting and Tracking” chapter in the user guide.</p>

Changes in Behaviour

Change in Report Pages	<p>The following reports are changed on the new web interface, in this release:</p> <ul style="list-style-type: none"> • Overview report page is renamed to Mail Flow Summary. • Outbreak Filters report page is renamed to Outbreak Filtering. • Virus Types report page is renamed to Virus Filtering. • Advanced Malware Protection, AMP File Analysis, AMP Verdict Updates and Mailbox Auto Remediation report pages are merged as Advanced Malware Protection. • Incoming Mail and Outgoing Senders report pages are merged as Mail Flow Details. • TLS Connections report page is renamed to TLS Encryption. • Geo-Distribution report page is renamed to Connection by Country. • Internal Users report page is renamed to User Mail Summary. • Web Interaction Tracking report page is renamed to Web Interaction. <p>For more information, see "Understanding the Email Reporting Pages" section in the user guide</p>
Changes in Accessing the Spam Quarantine	<p>The administrative users can now access the Spam Quarantine page on the new web interface of the appliance.</p> <p>You can navigate to Quarantine > Spam Quarantine > Search page to access the Spam Quarantine page.</p> <p>The end-users can now access the Spam Quarantine portal using the following URL format -</p> <p><code>https://example.com:<https-api-port>/eug-login</code></p> <p>where <code>example.com</code> is the appliance host name and <code><https-api-port></code> is the AsyncOS API HTTPS port opened on the firewall.</p> <p> Note Local and externally-authenticated users cannot log into the end-user spam quarantine portal.</p>

Changing the User's Password After Expiry	Users are prompted to change the password after the user account is expired. For more information, see "Changing the User's Password After Expiry" section in the user guide.
Changes in Demo Certificates	<p>Prior to this release, the appliance was pre-configured with a demonstration certificate to enable the TLS connections. After you upgrade to this release, the appliance generates a unique certificate to enable TLS connection. The existing demonstration certificate that is used in the following configurations are replaced with the new certificate:</p> <ul style="list-style-type: none"> • Mail Delivery • LDAP • Networking • URL Filtering • SMTP Services

Comparison of Web Interfaces, AsyncOS 12.0 vs. Previous Releases

Web Interface Page or Element	AsyncOS 12.0	Previous Releases
Landing Page	After you log in to the Security Management appliance, the Mail Flow Summary page is displayed.	After you log in to the appliance, the System Status page is displayed.
Product Drop-down	You can switch between the Email Security Appliance and the Web Security Appliance from the Product drop-down.	You can use the Email or Web tab to switch between the Email Security Appliance and the Web Security Appliance.
Reports Drop-down	You can view reports for your Email and Web Security Appliances from the Reports drop-down.	You can view reports for your Email and Web Security Appliances from the Reporting drop-down menu.
Management Appliance Tab	Click  on the Security Management appliance to access the Management Appliance tab.	You can enable and configure reporting, message tracking and quarantines, as well as configure network access, and monitor system status.
My Reports Page	Click  on the Security Management appliance and choose Email > Reporting > My Reports to access the My Reports page.	You can customize your reports dashboard by assembling charts (graphs) and tables from existing report pages.

Web Interface Page or Element	AsyncOS 12.0	Previous Releases
Reporting Data Availability Page	Click  on the Security Management appliance and choose Email > Reporting > Reporting Data Availability to access the Reporting Data Availability page.	You can view, update and sort data to provide real-time visibility into resource utilization and email traffic trouble spots.
Scheduling & Archiving Reports	Click  on the Security Management appliance and choose Email > Reporting > Scheduled Reports to schedule your reports. Click  on the Security Management appliance and choose Email > Reporting > Archive Reports to archive your reports.	You can schedule reports using the Email > Reporting > Scheduled Reports page, and archive your reports using the Email > Reporting > Archived Report page of the Security Management appliance.
Reporting Overview Page	The Email Reporting Overview page on the Security Management appliance has been redesigned as Mail Flow Summary page in the new web interface. The Mail Flow Summary page includes trend graphs and summary tables for incoming and outgoing messages.	The Email Reporting Overview page on the Security Management appliance provides a synopsis of the email message activity from your Email Security appliances. The Overview page includes graphs and summary tables for the incoming and outgoing messages.
Advanced Malware Protection Report Pages	The following sections are available on the Advanced Malware Protection report page of the Reports menu: <ul style="list-style-type: none"> • Summary • AMP File Reputation • File Analysis • File Retrospection • Mailbox Auto Remediation 	The Email > Reporting drop-down menu of the Security Management appliance has the following Advanced Malware Protection report pages: <ul style="list-style-type: none"> • Advanced Malware Protection • AMP File Analysis • AMP Verdict Updates • Mailbox Auto Remediation
Outbreak Filters Page	The Past Year Virus Outbreaks and Past Year Virus Outbreak Summary are not available in the Outbreak Filtering report page of the new web interface.	The Email > Reporting Outbreak Filters page displays the Past Year Virus Outbreaks and Past Year Virus Outbreak Summary.

Web Interface Page or Element	AsyncOS 12.0	Previous Releases
Spam Quarantine (Admin and End-User)	<p>Click Quarantine > Spam Quarantine > Search in the web interface to access the Spam Quarantine page.</p> <p>The end users can now access the Spam Quarantine portal using the following URL - <code>https://example.com:<https-api-port>/euq-login</code> where <code>example.com</code> is the appliance host name and <code><https-api-port></code> is the AsyncOS API HTTPS port opened on the firewall.</p>	-
Policy, Virus and Outbreak Quarantines	<p>Click Quarantine > Other Quarantine on the new web interface.</p> <p>You can only view Policy, Virus and Outbreak Quarantines on the Security Management appliance.</p>	You can view, configure and modify the Policy, Virus and Outbreak Quarantines on the appliance.
Select All action for Messages in Quarantine	You can select multiple (or all) messages in a quarantine and perform a message action, such as, delete, delay, release, move, etc.	You cannot select multiple messages in a quarantine and perform a message action.
Maximum Download Limit for Attachments	The maximum limit for downloading attachments of a quarantined message is restricted to 25 MB.	-
Rejected Connections	To search for rejected connections, click Tracking > Search > Rejected Connection tab on the Security Management appliance.	-
Query Settings	The Query Settings field of the Message Tracking feature is not available on the Security Management appliance.	You can set the query timeout in the Query Settings field of the Message Tracking feature.
Message Tracking Data Availability	Click  on the on the Security Management appliance and choose Email > Message Tracking > Message Tracking Data Availability to access Message Tracking Data Availability page.	You can view the missing-data intervals for your appliance.

Web Interface Page or Element	AsyncOS 12.0	Previous Releases
Verdict Charts and Last State Verdicts	Verdict Chart displays information of the various possible verdicts triggered by each engine in your appliance. Last State of the message determines the final verdict triggered after all the possible verdicts of the engine.	Verdict Charts and Last State Verdicts of the messages are not available.
Message Attachments and Host Names in Message Details	Message attachments and host names are not displayed in the Message Details section of the message on the Security Management appliance.	Message attachments and host names are displayed in the Message Details section of the message.
Sender Groups, Sender IP, SBRS Score and Policy Match in Message Details	Sender Groups, Sender IP, SBRS Score, and Policy Match details of the message is displayed in the Message Details section of the message on the Security Management appliance.	Sender Groups, Sender IP, SBRS Score, and Policy Match details of the message is not available in the Message Details section of the message.
Direction of the Message (Incoming or Outgoing)	Direction of the messages (incoming or outgoing) is displayed in the message tracking results page on the Security Management appliance.	Direction of the messages (incoming or outgoing) is not displayed in the message tracking results page.

Accessing the New Web Interface

The new web interface provides a new look for monitoring reports, quarantines and searching for messages.

You can access the new web interface in any one of the following ways:

- Use the following URL - `https://example.com:<https-api-port>/ng-login`
where `example.com` is the appliance host name and `<https-api-port>` is the AsyncOS API HTTPS port opened on the firewall.
- Log into the appliance and click **Security Management Appliance is getting a new look. Try it !** to navigate to the new web interface.

The new web interface opens in a new browser window and you must log in again to access it. If you want to log out of the appliance completely, you need to log out of both the new and legacy web interfaces of your appliance.

The end-users can now access the Spam Quarantine on the new web interface using the following URL:

`https://example.com:<https-api-port>/euq-login`

where `example.com` is the appliance host name and `<https-api-port>` is the AsyncOS API HTTPS port opened on the firewall.

Upgrade Paths

You can upgrade to release 12.0.0-322 from the following version:

- 11.0.0-136
- 11.4.0-812
- 11.5.0-110
- 11.5.1-115
- 12.0.0-225
- 12.0.0-305

**Note**

This release is compatible with AsyncOS 12.0.0 for Cisco Email Security Appliances and AsyncOS 11.7.0 for Cisco Web Security Appliances.

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>.

Installation and Upgrade Notes

- [Important Additional Reading, page 12](#)
- [Virtual Appliance, page 12](#)
- [Pre-Upgrade Requirements, page 13](#)
- [IPMI Messages During Upgrade, page 13](#)
- [Upgrading to This Release, page 14](#)
- [Post-Upgrade Notes, page 15](#)

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 12](#).
 - 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.

Pre-Upgrade Requirements

Perform the following important preupgrade tasks:

- [Verify Associated Email and Web Security Appliance Versions, page 13](#)
- [Back Up Your Existing Configuration, page 13](#)

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 12](#).

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 [Pre-Upgrade Requirements, page 13](#).
- 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 13](#).
-

Important! After you upgrade to this release, you can try any one of the following steps to make the navigation in your browser seamless:

- Accept the certificate used by the web interface and use the following URL syntax:
`https://hostname:<https_api_port>` (for example, `https://some.example.com:6443`) in a new browser window and accept the certificate. Here `<https_api_port>` is the AsyncOS API HTTPS port configured in **Network > IP Interfaces**. Also, ensure that the API ports (HTTP/HTTPS) are opened on the firewall.
- Enable the Trailblazer Configuration using CLI (`trailblazerconfig enable <https_port> <http_port>`). Also, ensure that these ports (HTTP/HTTPS) are opened on the firewall. Keep in mind that this feature is still in beta. If the problem persists, contact Cisco Customer Support.

You can run the `trailblazerconfig > enable` command using the CLI to avoid the following issues:

- Requiring to add multiple certificates for API ports in certain browsers.
- Redirecting to the legacy web interface when you refresh the Spam quarantine, Safelist or Blocklist page.
- Metrics bar on the Advanced Malware Protection report page does not contain any data.

For more information, see section “The trailblazerconfig Command” of the user guide.



Note Reboot your appliance or clear your browser cache if you are unable to access the web interface. If the problem persists, contact Cisco Customer Support.

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

Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509131&rls=12.0.0&sb=anfr&sts=open&bt=custV
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509131&rls=12.0.0&sb=anfr&sts=fd&bt=custV

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

Documentation For Cisco Content Security Products:	Is Located At:
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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.

© 2018 Cisco Systems, Inc. All rights reserved.